Tests

de

Redes de Ordenadores

Test Nº 4

Test de Sistemas de Transmisión de Datos – Curso 99/00 – 4ºA

1. **¿ A qué nivel de la pila TCP/IP pertenece el servicio FTP?**
   a. Al nivel de transporte
   b. *Al nivel de aplicación*
   c. Al nivel de red

2. **¿Qué nombre reciben las PDU's del nivel 2 de la pila TCP/IP?**
   a. Datagramas IP
   b. Tramas
   c. Segmentos TCP

3. **¿En qué nivel de la pila TCP se añade cabecera y cola durante el proceso de encapsulamiento?**
   a. *En el nivel de enlace de datos*
   b. En el nivel de transporte
   c. En el nivel de red

4. **Las funcionalidades que no están presentes en DUP, ¿quién las cubrirá?**
   El nivel de aplicación, el nivel superior

5. **Si elegimos TCP, las aplicaciones que utilicen TCP, ¿tendrán que cubrir todas las funcionalidades que utilice TCP?**
   No

6. **En gestión de red ¿qué aspectos se incluyen?**
   - Configuración
   - Rendimiento
   - Gestión de fallos
   - Seguridad

7. **¿Qué protocolo hace uso directamente del nivel IP?**
   a. *El nivel de enlace de datos*
   b. El nivel de aplicación
   c. Ninguno de los anteriores

8. **¿Cuál de los siguientes niveles TCP/IP implementa un protocolo extremo a extremo?**
   a. *El nivel de aplicación y el nivel de transporte*
   b. El nivel de red
   c. El nivel de transporte

9. **¿Cómo pueden ser los servidores en el modelo cliente-servidor de TCP/IP?**
   a. Iterativos
   b. Concurrentes
   c. Cualquiera de las anteriores
   d. *Iterativos y concurrentes*

10. **¿Cuántos nodos o hosts pueden existir en una dirección CLASE-C?**
    a. *254*
    b. 264
    c. 259

11. **¿Cuántos bits ocupan el identificador de red en una dirección CLASE-B?**
    a. *14 bits*
    b. 21 bits
    c. 7 bits

12. **¿Cuál de las siguientes posibilidades no corresponde a una dirección CLASE-A?**
    a. *su identificador de red es de 14 bits*
    b. su identificador de nodo es de 24 bits
    c. el bit más significativo que identifica la clase de dirección vale 0

13. **¿Cuáles permiten mayor número de computadores?**

CLASE A

14. ¿Cuáles permiten mayor número de redes?

CLASE B

15. ¿Cuántos bits se necesitan para diferenciar los distintos tipos de direcciones IP?

5

16. ¿Cuál es el número máximo de identificadores de red en la clase-A, clase-B y clase-C?

- Clase-A -> $2^7 - 2$
- Clase-B -> $2^{14} - 2$
- Clase-C -> $2^{21} - 2$

17. ¿Cuál de las siguientes afirmaciones no corresponde a una subdivisión válida para redes Clase-B?

a. *14 subredes de 14 nodos*
b. 64 subredes de 1022 nodos
c. 30 subredes de 2046 nodos

18. Dada la dirección IP 130.206.100.1, ¿qué dirección IP representa?

a. dirección primaria
b. dirección Clase-B
c. ninguna de las anteriores es cierta
d. *las afirmaciones 1 y 2 son ciertas*

19. Calcular la máscara de subred para una dirección Clase-D si el identificador de host vale y, el identificador de red y subred vale 128.66.12.0

20. Dada la siguiente máscara de subred y dada la dirección IP, encontrar el identificador de host y el identificador de red + subred

M = 255.255.240.0
DIR IP = 132.90.132.5

DIR_IP = 132.90.1000 0100. 0000 0101
M = 255.255.1111 0000.0000 0000

ID_NODO = 4.5 = (ID_HOST)
ID_RED + SUBRED = 132.90.128.0 (El 0 es el identificador de nodo puesto a cero)

21. ¿Cómo se construye una máscara?

a. *Asignando, según necesidades, un '1' en la posición de los bis que forman parte del identificador de red + subred y un '0' en la parte de identificador de nodo*
b. Asignando un '1' en la posición de los bits que forman parte del identificador de nodo y un '0' en el identificador de red
c. Según el criterio que estime oportuno el administrador de red, utilizando los caracteres de la base de numeración 3

22. ¿A quién identifica la dirección 192.136.74.0?

a. A todas las subredes de una red
b. *A esta red*
c. A la dirección Clase-A LOOPBACK
d. A la dirección del servidor de tiempo residente en Ginebra

23. Obtener el identificador de host y el identificador de red + subred, sabiendo que la máscara M = 255.255.0.0 y la dirección IP es 18.20.16.91

ID_HOST = 16.91
ID_RED + SUBRED = 18.20.0.0

¿Qué clase de dirección es 192.178.16.66?
Clase A

¿Esta máscara 255.255.0.0 es contigua o no contigua?
Contigua

24. Repetir el ejercicio para DIR_IP = 192.178.16.66 y para la máscara M = 255.255.255.192
ID_HOST = 2
ID_RED + SUBRED = 192.178.16.64

¿Qué clase de dirección es 192.178.16.66?
Clase C

Esta máscara 255.255.255.192 ¿es contigua o no contigua?
Contigua

25. Dir_IP = 128.66.12.1
M = FF.FF.FF.0
¿Cuál es el identificador de host? ID_HOST = 1
¿Cuál es el identificador de red + subred? ID_RED + SUBRED = 128.66.12.0
¿A qué clase pertenece? Clase B
La máscara ¿es contigua o no contigua? Contigua

26. ¿Qué tipo de datagramas IP se envían a la dirección LO (Local Host o Loopback)?
a. Los datagramas dirigidos a una dirección unicast
b. *Los datagramas dirigidos a una dirección multicast o de difusión (broadcast)*
c. En IPv4, los datagramas dirigidos a una dirección anycast

27. ¿Qué tipos de dirección destino se definen en IPv4?
a. Direcciones unicast
b. Direcciones multicast y broadcast
c. *Las dos anteriores*
d. El 'c' más las direcciones anycast (Anycast sólo aparecen en la versión 6)

28. ¿Cuál es el identificador de host para la siguiente Dir_IP y para la siguiente máscara?
Dir_IP ¿ 130.97.16.132
M = 255.255.255.192

ID_HOST = 4
ID_RED + SUBRED = 130.97.16.128

29. Dada la dirección 130.206.100.1 y la máscara de subred 255.255.255.192, ¿cuál es la parte de la dirección que corresponde al identificador de red + subred y nodo?
a. El Id_Red son 14 bits, el de subred 3 y el de nodo 5
b. *El Id_Red son 14 bits, el de subred 10 y el de nodo 6*
c. El Id_Red son 21 bits, el de subred 2 y el de nodo 6

30. ¿Qué representa la dirección LOOPBACK?
Permite comunicarse un cliente con un servidor del mismo nodo usando TCP/IP

31. ¿Cuántos identificadores de nodo válidos diferentes pueden emplearse en una red Clase-C cuya máscara de subred es 255.255.255.0?
$2^8 - 2 = 254$

32. Dada la dirección IP 191.64.89.4, señalar a qué clase o categoría de direcciones IP corresponde.
Clase B

33. En el modelo TCP/IP, ¿qué capa alberga los protocolos SNMP y PING?
La capa o nivel de aplicación. La capa 4

34. ¿De qué consta una máscara de subred?
   a. *De '0's para indicar el identificador de nodos y de '1's para indicar el identificador de red+subred*
   b. De '1's para indicar el identificador de nodo y de '0's para indicar el identificador de red+subred
   c. De '1's para especificar el identificador de nodo y de '0's para especificar el identificador de red y valores inoperantes ó don't care para el identificador de subred

35. ¿Qué implica el término no orientado a la conexión en el protocolo IP?
   a. Que las estaciones no están conectadas
   b. *Que no se mantiene información de estado sobre los sucesivos datagramas IP*
   c. Que se utiliza un servicio de red del tipo circuito virtual

36. ¿Cuál es la función de los bits del campo tipo de servicio situado en la cabecera de un datagrama IP?
   a. Especifican si el servicio es orientado o no orientado a la conexión
   b. Sirven para elegir una ruta dentro de las distintas posibles
   c. Sirve para indicar si un datagrama puede o no fragmentarse

37. Función principal del protocolo IP
   Encaminar datagramas IP (enviar paquetes de la forma no orientada a la conexión)

38. ¿Cómo se llaman las UDP del protocolo IP?
   Datagramas IP

39. Tasa BER: Tasa de Bits Erróneos
   Las LAN tienen menor tasa BER que la Red Telefónica Básica

40. ¿Cuál es el formato de un datagrama IP?
   Cabecera + Datos

41. ¿Dónde se encapsula un datagrama IP?
   a. En un mensaje TCP
   b. *En una trama de LLC* (Encapsular es ir hacia abajo)

42. ¿Hay algo por detrás de la parte de datos de una trama de Ethernet (donde se ha encpasulado el datagrama IP)?
   CRC-32

43. ¿La cabecera de un datagrama IP es de longitud fija o variable?
   Variable -> campo longitud de cabecera

44. Campo Tipo de Servicio -> TOS (Type of Service)

45. Encaminar -> Elegir el camino óptimo para un datagrama IP

46. Criterios para elegir el mejor camino para enviar un datagrama IP:
   - El camino que minimice el coste -> Bit C
   - El camino más rápido -> Bit D
   - El camino más fiable (mínima tasa BER) -> Bit R
   - Maximizar el rendimiento –> Bit T

47. Datagramas IP: Longitud Variable

48. Campo IDENTIFICACION: Para que cuando se fragmente un datagrama, el receptor sepa a qué datagrama pertenece cada fragmento que le llega

49. Campos FLAGS y DESPLAZAMIENTOD DEL FRAGMENTO: Para la fragmentación de grandes datagramas

50. ¿Quién es el responsable de restar una unidad al campo TTL (Tiempo de Vida)?

a. El sistema emisor
b. El sistema receptor
c. *Los routers*
d. Los repetidores
e. Los puentes

51. Los routers encargados de disminuir el campo TTL, ¿cuál es su criterio de actuación?

a. Restan una unidad cuando el datagrama lo atraviesa
b. Restan una unidad por cada segundo que el datagrama esté almacenado en el router
c. Restan una unidad por cada conexión establecida precedentemente
d. *Las dos primeras son ciertas*

52. Cuando un router tiene un datagrama durante mucho tiempo, puede llegar a quedárselo, sin llegar a enviarlo a ningún sitio

53. Checksum -> controla los errores sólo en la cabecera

54. Las Dir IP origen y destino, ¿son direcciones MAC?

No, son Dir IP.
Las direcciones MAC son direcciones de 48 bits (de tarjeta de red)

55. ¿Cuándo se produce la fragmentación de un datagrama IP?

Cuando un datagrama es grande

¿Qué contiene el campo de longitud en cada uno de los fragmentos?

Contiene la longitud del fragmento

56. ¿Cuál de las siguientes opciones no se especifica en la cabecera IP?

a. El registro de ruta seguida por un datagrama
b. *El tamaño máximo de los datagramas de una conexión*
c. El registro de marca de tiempo

57. ¿Qué opciones se deben copiar en todos los fragmentos de datagrama IP?

a. *Encaminamiento desde el origen flexible* (Da igual que sea flexible o estricto)
b. Registro de ruta
c. Marca de tiempo

58. Un datagrama IP. ¿tiene una longitud mínima?

Sí. Sólo la cabecera sin opciones

59. ¿Cuál es la longitud mínima de una cabecera?

20 bytes

60. ¿Qué campos de la cabecera de un datagrama IP están relacionados con la fragmentación y el reensamblado?

- Identificación
- Flags -> 3 bits
- Desplazamiento del fragmento u offset -> se mide en octetos

61. ¿Por qué en IEEE 802.3 se puede transportar menos información útil de usuario?

Los campos:

- Longitud
- LLC

- SNAP

Reducen la posibilidad de transportar menos información útil de usuario

62. ¿Cuál es la función de los bits de los campos checksum de la cabecera de un datagrama IP?

El control de errores en la cabecera de un datagrama IP

63. Si el valor original del campo TTL, de un datagrama IP es 32, y dicho datagrama ha atravesado 13 router ¿cuál puede ser el valor de dicho campo al llegar a su destino?

a. *Menor o igual que 19* (Puede ser menor si el datagrama está mucho tiempo retenido en el router. Por cada segundo que está retenido en el router, se resta una unidad)
b. Menor o igual que 32
c. Igual a 19

64. ¿Cómo se encapsula un paquete (datagrama IP) en una trama Ethernet?

65. ¿Qué se puede hacer para que un datagrama y su posible contestación sigan la misma ruta?

a. Utilizar la opción de registro de ruta
b. *Utilizar la opción de registro de ruta y encaminamiento desde el origen estricto*
c. Usar la opción de registro de ruta y encaminamiento desde el origen flexible

66. ¿Qué campo o campos de la cabecera del datagrama IP tienen longitud variable?

Uno. el campo de opciones

67. ¿En qué unidad se mide la longitud total de un datagrama?

a. En palabras de 32 bits
b. En palabras de 16 bits
c. *En octetos*

68. Modalidades de encaminamiento desde el origen:

- Estricto -> todas las rutas encadenadas
- Flexible -> obligamos la primera ruta y para las siguientes tenemos opciones

69. ¿Qué campos de la cabecera IP se modifican al fragmentar un datagrama IP?

a. Flags y desplazamiento del fragmento
b. Checksum
c. Longitud total y las dos anteriores

70. ¿Qué función tiene la opción 'timestamp' (marca de tiempo)?

a. Registrar la hora y aumentar el puntero
b. *Registrar la hora y aumentar el puntero y aumentar el campo de overflow*
c. Registrar la hora

71. ¿Qué significado tiene el flag H encontrado en las tablas de encaminamiento?

a. Que la ruta está activa
b. *Que la ruta es específica* (Host)
c. Que la ruta es indirecta

U -> Activa
G -> Router (Gateway)
D -> Dirección creada por ICMP
M -> Dirección modificada

72. ¿Cuál de las siguientes afirmaciones es incorrecta?

a. *El tamaño de las cabeceras de los datagramas IP incluye un campo de número de secuencia para implementar el control de flujo de ventana deslizante* (No orientado a la conexión -> No control de flujo -> _No protocolo de ventana deslizante)

b. *Las longitudes de los datagramas IP dependen del campo de longitud variable denominado tipo de servicio*
c. Las cabeceras de los datagramas IP incluyen información para el proceso de fragmentación que ocurre en función de la MTU del interfaz

73. ¿Cuál es la función principal de la capa de red IP?
El encaminamiento de paquetes (datagrama)

74. ¿Qué dos protocolos complementan la funcionalidad de IP?
- ICMP
- IGMP -> comunicación multicast

75. ¿Qué estructura de información usa el protocolo IP para llevar a cabo las decisiones de encaminamiento?
Tabla de encaminamiento

76. ¿Cuántos tipos de encaminamiento hay?
- Directo
- Indirecto -> incorpora routers o pasarelas entre emisor y receptor

77. ¿Qué campos se consultan en el encaminamiento directo para saber si se trata de un encaminamiento directo o indirecto?
El identificador de red

78. Cuando un router retransmite un datagrama que ha recibido previamente, ¿qué campos modifica en la cabecera si el datagrama no tiene opciones? (No hay fragmentación)
Si hubiera, se modificaría el desplazamiento y los flags correspondientes
a. Ninguno
b. Todos
c. *Algunos* (Tiempo de vida (TTL) y el checksum)

79. Tipos de interfaz:
- LO (por defecto -> dir Clase-A)
- LAN
- Enlaces de tipo serie

80. En una tabla de encaminamiento:
Al menos la dirección LO (Loopback)

81. ¿Cuántas rutas tendrá en su tabla de encaminamiento un host conectado a dos redes que a su vez no tienen ningún router directamente conectado a ellas?
a. Una; la del interfaz Loopback
b. Dos; las de sus dos interfaces
c. *La de loopback y las de sus dos interfaces*

82. Significado del flag 'M':
La dirección fue modificada mediante un mensaje ICMP de redirección

83. Protocolo NAT : tener unas pocas direcciones duplicadas en el interior de una organización, pero son direcciones individuales hacia el exterior

84. Unicast - > enviar a 1
Multicast -> enviar a varios
Difusión o broadcast -> enviar a todos

85. En una tabla de encaminamiento sólo se encuentra la dirección LOOPBACK. Eso significa:
a. *Que la máquina está aislada*
b. Que la máquina conecta con todas las demás de forma directa
c. La conexión de la máquina con el exterior es inalámbrica

86. ¿Cuántas rutas podrán especificarse como máximo en la opción registro de ruta del protocolo IP?

a. Tantas como routers atraviese el datagrama
b. $2^8 = 256$
c. *Ninguna de las anteriores*

87. ¿Cómo se envía una petición ARP?

a. Mediante una difusión IP
b. *Mediante una difusión o broadcast del nivel enlace de datos*
c. Mediante el envía a la dirección IP de destino correspondiente

88. ¿Cuántos caracteres hexadecimales se usan para representar las direcciones físicas?

48 bits / 4 = 12 caracteres hexadecimales

89. En la resolución de direcciones, ¿cuántos protocolos se usan y cuáles son?

Son dos: ARP y RARP

¿Cuál usa servidores para la función de resolución de direcciones?

RARP

Cuando tenemos varios servidores RARP -> tolerancia a fallos

90. ¿Dónde están ubicados ARP y RARP? ¿Son protocolos deslizantes o fijos?

Entre las capas 1 (enlace de datos) y 2 (IP)

91. En la petición ARP, ¿qué dirección IP se coloca en busca de su correspondiente dirección física?

a. La del emisor
b. *La del receptor*
c. La de grupo (clase D)

92. ¿Cómo son las respuestas ARP?

Unicast

93. ¿Cuál es la métrica para indicar la longitud HW (paquete ARP)?

Octetos o bytes

94. ¿Cuántos tipos distintos de mensajes ha definido el protocolo ARP?

Dos:

- Petición (broadcast)
- Respuesta (unicast)

95. En un mensaje ARP, ¿qué campo(s) se encuentran vacíos?

Uno, la dirección Ethernet Destino

96. En una respuesta ARP, ¿qué campo(s) se encuentran vacíos?

Ninguno

97. En el paquete petición, si no sabemos la dirección HW destino, ¿qué metemos ahí?

Una dirección de broadcast (todo '1')

98. ¿Cómo se puede averiguar la dirección IP de todos los routers existentes entre nuestro sistema y otro destino si hay al menos 10 redes entre ambos?

a. No es posible en ningún caso
b. Mandando mensajes sucesivos, incrementando en una unidad cada vez, el campo TTL
(Esto es para obtener el número, no la dirección)
c. Haciendo uso de la funcionalidad TOS de la cabecera IP
d. *Ninguna de las anteriores*

99. ¿Cuál es la finalidad del protocolo RARP?

a. Obtener la dirección IP de una máquina a partir de su dirección HW

b. Permite obtener las direcciones IP de aquellas estaciones que carecen de disco
c. *Ninguna de las anteriores es cierta* (Son a y b)

100. ¿En qué protocolo, ARP o RARP, se utilizan servidores?
a. En ambos protocolos
b. En el protocolo ARP
c. *En ninguno de los protocolos* (RARP)

101. En el protocolo RARP, ¿qué información se obtiene tras ser aplicado?
a. La dirección HW de la estación origen
b. La dirección HW de la estación destino
c. *La dirección del nivel de red*

ARP -> IP -> DIR_MAC
RARP -> DIR_MAC ->IP

102. ¿Dónde está ubicado el protocolo ICMP?

Entre el nivel de red y el de transporte

103. ¿Qué es un PROXY ARP?

Un router que oculta al receptor

104. En los mensajes ICMP ¿tienen algún campo de control de errores?
a. No
b. CRC de grado 32
c. *Sí*
d. CRC de grado 16

105. ¿Dónde se encapsulan los mensajes ICMP?

En datagramas IP

106. ¿Qué campos tiene el formato de todo mensaje ICMP?
- Tipo
- Código
- Checksum
- Contenido dependiente del mensaje ICMP

107. Los algoritmos de detección de errores de los campos checksum en ICMP, IP, UDP, TCP ¿cómo son?

Todos los algoritmos son iguales

108. ¿En qué casos no se debe generar un mensaje ICMP? (podrían crear trastorno al sistema)

Mirar apuntes

109. Clase D -> Dirección multicast

110. El formato de un mensaje ICMP consta de una parte fija y una parte variable. La parte fija es:
a. El campo de sincronización y el campo de longitud de mensaje
b. *El campo de detección de errores y los campos de tipo y código*
c. El campo de datos y el campo de checksum

111. El protocolo ICMP se utiliza para determinar:
a. La velocidad de transmisión de un enlace de datos
b. *Para obtener la máscara de subred*
c. Para obtener la MTU de una interfaz

112. Enunciar eventos que no deben provocar el envío de un mensaje ICMP:
- Un mensaje de error ICMP

- Un datagrama destinado a una dirección de difusión IP o una dirección multicast IP
- Un datagrama enviado como difusión del nivel de enlace
- Un fragmento de un datagrama distinto del primero
- Un datagrama cuya dirección fuente no define a un simple nodo

113. El campo de detección de errores de un mensaje ICMP, ¿qué longitud tiene? y ¿qué abarca?

- 16 bits (No es CRC sino checksum)
- Comprueba todo el mensaje ICMP

114. ¿Qué diferencia esencial existe entre los mecanismos PROXY ARP y ARP gratuito?

a. Ninguna
b. Tratan de la obtención de la dirección HW a partir de la dirección IP y viceversa. (RARP -> si quitamos "viceversa", sería la respuesta correcta)
c. Ambos tratan de obtener la dirección HW de la estación que envía la petición ARP (ARP gratuito)
d. *Ambas tratan de obtener la dirección HW a partir de la dirección IP*

115. ¿Qué proporciona la estadística del comando PING?

La tasa de paquetes perdidos, número de paquetes enviados, etc....
PING -> En el nivel de aplicación
Proveedor de servicios de PING -> ICMP

116. El protocolo ICMP utilizado para el redireccionamiento se basa en el envío de tres mensajes. ¿En qué dirección se propaga el tercero de los mensajes?

a. Del nodo emisor al router por defecto
b. Del router por defecto al router correcto
c. *Del router por defecto al nodo de partida*

117. ¿Dónde se encapsulan los mensajes ICMP?

En datagramas IP

118. ¿Qué longitud abarca la máscara de subred en un mensaje ICMP de obtención de máscara de subred?

32 bits -> igual que una dirección IPv4

119. ¿Cuántos tipos de mensajes ICMP se han definido dentro de los mensajes ICMP de máscara de subred y de prueba de la disponibilidad del destino?

- De la prueba de la disponibilidad de un sistema (2 -> petición y respuesta)
- De máscara de subred (2 -> petición y respuesta)

120. ¿Qué tipo de mensaje ICMP se devuelve procedente de un datagrama IP cuya dirección origen no define un único nodo?

No se debe devolver mensajes a este tipo de datagramas

121. Protocolo IGMP -> Se encapsula en datagramas IP

122. ¿Cómo se llaman las UDP usadas por el protocolo IP?

Datagramas IP

123. ¿Cómo se miden las marcas de tiempo?

En tiempo universal coordinado (mseg)

124. ¿Qué campos personalizan los mensajes ICMP?

El anterior al destino no alcanzable

125. ¿Cuál debe ser la MTU del puerto de salida de un router que obligue a generar un mensaje ICMP de error de destino no alcanzable, si la MTU del puerto de entrada ha sido mayor?

La MTUI del puerto de salida será menor

126. ¿Qué dos técnicas se usan a la hora de genera mensajes SQ para el control de congestión en una red TCP/IP?

a. Envío del mensaje SQ cuando las memorias temporales del receptor crecen por encima de un umbral de seguridad
b. Envío de mensajes SQ cuando la cola de recepción no dé cabida a ningún mensaje adicional
c. *Las dos anteriores son ciertas*

127. ¿Los routers pueden devolver mensajes ICMP de cambio de ruta a otro router?

128. ¿Qué procedimiento tienen los routers para modificar sus tablas de encaminamiento?

a. Mensajes ICMP de cambio de ruta
b. Mensajes de petición de ECO
c. Mensajes SQ (de obtención de fuente)
d. *Ninguna de las anteriores es cierta*

129. ¿Qué comprobaciones no realiza un sistema emisor que ejecuta el protocolo ICMP de cambio de ruta?

a. Comprueba que el router elegido está conectado a su misma red
b. Comprueba que el router correcto también está conectado a su propia red (Aberración)
c. *Ninguna de las anteriores es cierta*

130. ¿Para qué se utilizan los mensajes de notificación de otros problemas?

a. *Cuando el problema planteado por el protocolo IP no esté codificado en los mensajes ICMP estándar*
b. Cuando exista la necesidad de detectar rutas circulares
c. Cuando se precise notificar las rutas a los router

131. ¿Qué tipo de direcciones utiliza el protocolo IGMP?

Multicast (Direcciones secundarias -> Clase D)

132. ¿Cuál es la funcionalidad (relacionada con la semántica) de los mensajes ICMP de detección de rutas circulares? ¿Con qué campo de la cabecera IP están relacionados?

- Para detectar las trayectorias indefinidas de los datagramas (Pueden provocar colapso dos datagramas dando vueltas indefinidamente)
- Relacionados con el tiempo de vida. Cuando el tiempo de vida llega a cero, se descarta el datagrama y se manda un mensaje diciendo que el datagrama seguía una ruta circular

133. Los mensajes ICMP de notificación de rutas son enviados por:

a. Los routers directamente conectados a los nodos encuestados
b. *Los nodos a los routers directamente conectados* (Para activar la tabla de encaminamiento (se elige la mejor ruta))
c. De los routers emisores a los routers encuestados (Lo hacen los protocolos de encaminamiento dinámico)

134. Algunos mensajes ICMP terminan con un campo

a. que contiene la cabecera IP y los últimos 8 bytes del datagrama que ha originado el problema
b. la cabecera IP y un número variable de octetos del datagrama que ha causado el problema
c. la cabecera IP y los 16 primeros octetos del datagrama que ha causado el problema (Son los 8 primeros octetos)
d. *Ninguna de las anteriores es cierta*

135. ¿Cómo es la participación como miembro de un grupo multicast?

Variable o dinámica

136. ¿Cuántos octetos ocupa un mensaje IGMP?

a. 2 palabras de 16 bits
b. *2 palabras de 32 bits (8 octetos)*
c. 4 octetos

137. ¿Dónde afecta el campo de checksum de un mensaje IGMP?

a. Afecta sólo a la cabecera
b. Sólo a los datos
c. *Tanto a la cabecera como a los datos* (En IP el checksum afecta sólo a la cabecera -> es la excepción; en los demás protocolos, el checksum afecta a todo)

138. ¿Cuántos tipos diferentes de mensajes se han definido en el protocolo IGMP?

Dos:

- de petición o query
- de report

139. IANA -> Autoridad de Asignación de Números de Internet

140. El protocolo IGMP trabaja con dos tipos de mensajes. ¿Cuál es el emisor y el receptor de un mensaje de petición y de un mensaje de report?

Query:

- Emisor -> Router
- Receptor -> Host

Report:

- Emisor -> _Host
- Receptor -> Router

141. Cuando un proceso se da de alta en un grupo multicast, ¿qué mensaje IGMP se envía? (y cuáles son los extremos de la comunicación)

- Se envía un mensaje de petición o REPORT
- Extremos de la comunicación:
  - Host
  - Router

142. En el formato de un mensaje IGMP, ¿cuántos octetos permiten transportar la dirección Clase-D?

4 octetos, porque es un protocolo IPv4: dir de 32 bits

143. En un mensaje ICMP de cambio de ruta ¿qué dirección se transporta en el formato?

a. La dirección del nodo emisor
b. La dirección del router por defecto
c. *La dirección del router que debería utilizarse*

144. ¿Cuál de los siguientes protocolos de encaminamiento dinámico no se utilizan en la actualidad?

a. *GGP* (Desaparecido)
b. *EGP* (Está desapareciendo)
c. BGP (Protocolo de pasarela fronteriza)

145. ¿Cuál de los siguientes protocolos utiliza mensajes que no dependen del número de redes?

a. RIP (Protocolo que transporta información de encaminamiento entre router y router)
b. Protocolos vector-distancia (Bellman-Ford)
c. *Protocolos del estado del enlace* (Dependen del número de enlaces)

146. ¿Cuál de los siguientes protocolos de encaminamiento dinámico posee la convergencia más lenta?

a. Protocolos de estado del enlace

b. *Protocolos vector-distancia*
c. Protocolos de encaminamiento estático

147. ¿Cuál es el número máximo de saltos, en RIP?
15 saltos

148. Protocolos de encaminamiento dinámico:
Permiten la comunicación o diálogo entre routers (gateway)
(gateway -> pasarela o router)

149. ¿Dónde están situados los protocolos?
Entre la capa de red y la capa de transporte y aplicación. Están repartidos.

150. La longitud de los mensajes dependen del colectivo de redes que están interconectados -> más redes -> más grandes los mensajes

151. Convergencia -> Tiempo necesario para que todos los router adquieran la misma información.
(Cuando se crean rutas circulares, el tiempo de convergencia puede ser muy grande)

152. ¿Cuál de los siguientes aspectos incorpora RIP2 respecto a RIP?
a. La posibilidad de trabajar con difusión de mensajes
b. *La posibilidad de incluir autentificación en los mensajes*
c. *La posibilidad de trabajar con máscaras de subred*
d. La posibilidad de configurarse como protocolo vector-distancia. (RIP es un protocolo vector-distancia intrínsicamente)

153. En el protocolo RIP, ¿qué técnicas se utilizan para la notificación de la información de las tablas de encaminamiento?
SH -> Split Horizon
RP -> Reverse Poison
TU -> Triggered Updates

154. ¿En dónde se encapsulan los mensajes EGP?
En la parte de datos del datagrama IP

155. En los protocolos de encaminamiento dinámico siguientes, existe un protocolo que no es de vector-distancia. ¿Cuál es?
a. RIP
b. EGP
c. *OSPF* (de estado del enlace)

156. ¿Cuál de los siguientes protocolos de encaminamiento dinámico no se utiliza en la actualidad?
a. IGP (Protocolo de pasarela interna)
b. BGP
c. HGP
d. *GGP*

157. ¿Qué representa en RIP el número de saltos igual a 16?
a. Que la red direccionada es de alta prioridad
b. Que la red alcanzada contiene al administrador de red
c. *Ninguna de las anteriores es cierta* (Se utiliza el Max + 1 para indicar que la red no es alcanzable)

158. ¿Cuáles son las tres modalidades de operación de RIP?
a. ABM, SBM, CBM
b. *TU, RP(es el más usado), SH*
c. CBC, ECB, OFB

159. **¿Qué métrica utiliza el protocolo de encaminamiento dinámico HELLO?**
Basada en retardos y retrasos (alternativa a RIP, que usaba saltos o hops)

160. **Notificar la información de las tablas de encaminamiento**
Trasladar la información de las tablas de encaminamiento a los routers

161. **Métrica utilizada en RIP:** el número de saltos

162. **¿Quién usa el protocolo Rip1 y RIP2?**
Los router

163. **Indicar qué afirmación es correcta en el protocolo HELLO**
a. *Se trata de un protocolo de encaminamiento dinámico sucesor de los protocolos de estado del enlace (OSPF)*
b. Está soportado por el SW de encaminamiento GATED
c. *Es un protocolo de encaminamiento dinámico especialmente diseñado para redes modernas*

164. **¿Cuál de los siguientes parámetros necesarios para la definición de OSPF se encuentran relacionados con el tipo de servicio?**
a. Costo de cada interfaz
b. Métrica utilizada
c. Número de enlaces sondeados

165. **¿Dónde se encapsulan los protocolos OSPF y RIP?**
En datagramas IP (Capa 2)

166. **Protocolo escalable (OSFP) ->** puede crecer

167. **¿Qué parámetros permite configurar OSPF?**
a. El nombre del sistema final donde se almacena la información de usuario
b. *El costo de cada interfaz*
c. *La prioridad del router*
d. *La clave de autenticación para validar las actualizaciones del estado del enlace*

168. **¿Qué representan las siglas LSA en OSPF?**
Notificación del estado del enlace

169. **¿Dónde hay más dificultad para obtener adyacencias?**
En las redes de difusión (en las punto a punto hay menor dificultad)

170. **TOS ->** Campo en la cabecera de los datagramas IP que permite modular distintos parámetros

TEMA 8: UDP

171. **¿De qué partes consta una UDP en UDP?**
a. Cabecera, datos y Cola (La cola en las tramas (CRC-32))
b. Pseudocabecera, cabecera, datos y cola
c. Pseudocabecera, cabecera y datos
d. *Cabecera y datos*

172. **¿Dónde se encapsula una PDU-UDP?**
a. Tramas IP
b. Datagramas TCP
c. *Ninguna de las anteriores es cierta (Datagramas IP)*

173. **El campo de checksum de una PDU-UDP**
a. *Es optativo*
b. *Es recomendable*
c. Es obligatorio

174. **¿Qué representa el campo longitud ubicado dentro de la pseudocabecera UDP?**
La longitud del datagrama, es decir, de la cabecera y los datos

175. **¿Qué tipo de protocolo es UDP?**
a. De tipo circuito virtual
b. *De tipo datagrama* (No orientado a la conexión)
c. Algo intermedio entre las dos cosas anteriores

176. **¿Cómo se denominan las PDUs de UDP?**
Datagramas UDP (Datagrama de U)

177. **Métrica del campo de longitud en UDP**
Octetos

178. **El campo de checksum, ¿dónde se aplica?**
a. Sólo a la cabecera
b. *A todo el datagrama*

179. **¿Dónde se coloca la pseudocabecera dentro de un datagrama UDP?**
a. Cerca de la cabecera
b. Entre los datos
c. En la cola
d. *Ninguna de las anteriores* (En ninguna parte porque no se envía (Un datagrama UDP sólo tiene cabecera y datos))

180. **¿Para qué se usa la pseudocabecera?**
Para calcular el checksum

181. **Componentes que integran el cálculo del checksum:**
Cabecera, pseudocabecera y datos

182. **Comparando la cabecera y la pseudocabecera en UDP, ¿qué campo se repite?**
Longitud (y además tiene la misma interpretación en los dos sitios)

183. **El algoritmo del cálculo del checksum en IP, ICMP, IGMP, UDP, ¿es igual o distinto?**
Son algoritmos iguales (Complemento a 1 de la suma de palabras de 32 bits)

184. **¿Cuál es el tamaño máximo de una cabecera UDP?**
16 bits * 4 = 64 bits

185. **¿Qué información se obtiene en los 8 primeros bytes de datos de un datagrama IP que transporta información UDP?**
La cabecera UDP (Longitud fija)
- Checksum
- Puerto origen y destino
- Longitud del datagrama UDP

186. **¿Qué protocolo ayuda en caso de respuesta negativa a un datagrama UDP?**

Protocolo ICMP de puerto no alcanzable (Sólo interviene cuando el puerto no existe)

187. ¿Cómo se clasifican los números de puerto del protocolo UDP?

Reservados y disponibles

188. En el protocolo UDP, ¿Cuál es el proveedor de servicios? ¿Con qué otros protocolos se relaciona?

189. UDP proporciona un sistema de envío:

a. Fiable y orientada a la conexión
b. No fiable y orientado a la conexión
c. *No fiable y no orientado a la conexión*

190. ¿En qué se mide el campo Longitud de un mensaje UDP?

a. *En octetos*
b. En palabras de 32 bits
c. En palabras de 16 bits

191. ¿Cuál es el valor mínimo del campo Longitud de un mensaje UDP?

a. 0 octetos
b. *8 Bytes*
c. 64 Bytes

192. Cuando se transmite el datagrama UDP, ¿se transmite la pseudo-cabecera?

a. Sí
b. *No*

193. El objetivo de la pseudo-cabecera de un mensaje UDP es

a. Verificar que en el datagrama UDP todos los campos están rellenos
b. *Verificar que el datagrama UDP ha llegado a su destino correcto*
c. Ninguna de las anteriores es cierta

194. En la pseudo-cabecera, el campo Longitud UDP contiene:

a. *La longitud del datagrama UDP sin incluir la pseudo-cabecera*
b. La longitud del campo datos del datagrama UDP
c. La longitud del datagrama UDP incluyendo la pseudo-cabecera

195. Cuando UDP recibe un datagrama, y el número de puerto de destino no se ajusta a ningún puerto de los que están en uso en ese momento, envía un mensaje de error ICMP de:

a. Puerto no existe
b. Datagrama perdido
c. *Puerto no alcanzable*

196. En TCP/IP, los valores altos de puertos se asignan de forma:

a. *Dinámica*
b. Estática
c. Mediante la asignación de puertos “bien conocidos”

197. Cuando un datagrama UDP llega a un router y debe reenviarlo a través de una interfaz cuya MTU es inferior a la del tamaño del datagrama, ¿qué operación llevará a cabo?

a. Observar el contenido del bit de no fragmentación
b. Observar el campo de longitud de la cabecera UDP
c. *Preocuparse del protocolo N2 (L2)* Nivel 2(Nivel de Red)
Al router le llegan datagramas IP, no datagramas UDP, ya que los routers operan a nivel de Red (N2)

TEMA 9: TCP

198. **¿Qué tipo de protocolo es TCP?**

- Orientado a la conexión
- Con conexión fiable
- Protocolo de transporte
- Protocolo que utiliza control de flujo

199. **¿Cómo se denominan las unidades de datos de protocolo en TCP?**

Segmentos TCP

200. **¿Cuánto mide la cabecera mínima en TCP?**

20 bytes -> tamaño mínimo de la cabecera IP

201. **¿Cómo se calcula el campo de checksum en TCP?**

Utilizando la pseudocabecera como en UDP. Utilizamos la cabecera y los datos.

202. **¿Cuántas unidades de datos de protocolo se intercambian en el establecimiento de una conexión TCP?**

Tres

203. **¿Qué entidad TCP realiza una apertura activa y una apertura pasiva?**

Receptor -> Apertura activa
Emisor -> Apertura pasiva

204. **TCP, ¿con qué granularidad de datos trabaja?**

Con bytes

205. **En la fase de liberación de una conexión TCP, ¿cuántos segmentos se utilizan?**

a. 3
b. *4*
c. 1

206. **Los segmentos TCP, ¿incorporan opciones?**

Es optativo

En caso afirmativo ¿cuál es su ubicación dentro de un segmento TCP?

a. Después de los datos
b. *Antes de los datos*
c. Al comienzo del segmento

207. **En TCP, el checksum, ¿cómo es?**

a. Optativo
b. *Obligatorio*
c. Recomendable
d. Discrecional
e. Mandatario

208. **En la cabecera de un segmento TCP se definen los flags:**

a. *El flag URG permite transportar información urgente*
b. *El flag FIN permite indicar al receptor la terminación del envío de datos*
c. *El flag PSH indica al receptor que debe pasar los datos a la aplicación lo antes posible*
d. El flag ACK indica la validez del campo checksum (Valida la recepción de un segmento)

209. **¿Cuántas opciones diferentes se han definido en la cabecera TCP?**

a. *5*
b. 3
c. 4

210. **¿Cuántos flags se definen en la cabecera de un segmento TCP?**

Seis: URG, FIN, PSH, ACK, RST, SYN

211. ¿Qué flag debe estar activo para validar el campo de puntero urgente?

a. ACK
b. SYN
c. RST
d. *URG*

212. ¿Qué flag debe estar activo para validar el campo de número de reconocimiento?

El ACK

213. En la cabecera de un segmento TCP, ¿pueden estar activos varios flags simultáneamente? Poner un ejemplo.

Sí.
Ejemplo: SYN y ACK
FIN y ACK

214. ¿Qué campos integran la pseudocabecera?

a. Números de puerto - Tipo de protocolo - Longitud del segmento
b. Tipo de protocolo – Número de puerto – Longitud de la cabecera
c. *Direcciones Internet – Código de protocolo – Longitud del segmento*

215. El formato de los segmentos TCP, ¿incluye algún campo para poder incrementar el tamaño de la ventana?

Sí

216. En caso afirmativo, indicar el campo

El campo de opciones de escalado de ventana

217. ¿Dónde está ubicado ese campo?

En la cabecera. Al final de la cabecera y justo antes de los datos

218. El protocolo TCP, ¿qué tipo de mecanismo de control de flujo utiliza?

Ventana Deslizante -> Ventana>1

219. El protocolo TCP, ¿cuántas fases utiliza a la hora de la transmisión de la información?

Tres:

- Establecimiento
- Transferencia
- Liberación

220. ¿Cuántos segmentos TCP se usan en la fase de establecimientos de una conexión TCP?

Tres

221. ¿Cuál es la diferencia entre los temporizadores de retransmisión y de persistencia en TCP?

1º Espera de ACKs procedentes del otro extremo
2º La ventana del receptor puede estar cerrada y puede transmitir información sobre el tamaño de ventana aunque ésta esté cerrada -> monitoriza el tamaño de ventana

222. ¿Cuántos temporizadores usa el protocolo TCP?

Cuatro:

- de retransmisión
- de persistencia
- de subsistencia
- 2MSL

223. En UDP, ¿cuántos temporizadores se definen?

Ninguno

224. **Cuando un segmento TCP transporta datos urgentes, el puntero urgente ¿a dónde señala?**

(El puntero urgente sólo es válido, sólo si el flag URG está activo)

a. A la raíz
b. Al kernel del S.O.
c. *Al final de los datos urgentes*

225. **En el protocolo TCP, ¿para qué se utiliza la pseudocabecera?**

Para calcular el campo checksum. (También se calcula con el contenido del segmento TCP)

226. **En el protocolo TCP, ¿qué interpretación presenta el campo de puntero urgente?**

Apunta al final de los datos urgentes. (El flag URG ha de estar activo para que tenga validez)

227. **En el protocolo TCP, ¿qué opciones permiten el registro de ruta?**

No hay. Donde sí hay es en la cabecera de un datagrama IP

¿Cuántos routers pueden inscribirse en esa opción?

228. **En el protocolo TCP, ¿qué mecanismo se utiliza para detectar la desconexión de un extremo de la conexión?**

Temporizador de subsistencia

229. **Checksum de TCP abarca ->** cabecera y datos -> Todo el segmento

230. **Apertura simultánea -> ¿Qué es? ¿Qué flags se activan? ¿Cuántos segmentos se usan? ¿Cuáles son los interlocutores?....**

231. **Después de un proceso de apertura simultánea, ¿qué tiene lugar?**

La fase de transferencia de información

232. **TCP proporciona un servicio**

a. No orientado a la conexión y fiable
b. *Orientado a la conexión y fiable*
c. No orientado a la conexión y no fiable

233. **¿Cómo se llaman las unidades de datos de protocolo de TCP?**

a. *Segmentos*
b. Datagramas
c. Paquetes

234. **¿Cuándo se produce un timeout en TCP?**

a. Cuando se acaba el tiempo de espera después de mandar un segmento de FIN
b. *Cuando no llega reconocimiento positivo de un segmento*
c. Cuando se manda un segmento de datos urgente

235. **El protocolo TCP define:**

a. *Procedimientos para verificar que los datos lleguen correctos*
b. *Esquema para distinguir entre distintos destinos en un sistema*
c. *Procedimientos de recuperación de datos perdidos o corrompidos*
d. *Formato de datos y reconocimiento*
e. *Procedimiento de inicio y liberación de la conexión*

236. **Un socket se define por:**

a. *Una dirección IP y un puerto*

b. Un par de direcciones IP más sus dos puertos
c. Un puerto
d. Una dirección IP

237. ¿En qué se mide la cabecera del segmento TCP?
a. En octetos
b. En palabras de 16 bits
c. *En palabras de 32 bits*

238. La recepción de un segmento FIN significa:
a. *Que no habrá más datos circulando en el mismo sentido*
b. Que la conexión entre los extremos ha finalizado
c. Ninguna de las anteriores

239. La utilización del campo PUNTERO URGENTE es válido:
a. Siempre
b. *Sólo cuando el flag URG está activado*
c. No existe dicho campo en la cabecera del segmento TCP

240. El tamaño de la ventana:
a. Es fijo y de 65.535 octetos
b. *Su límite es de 65.535 y se puede extender*
c. Su límite es de 65.535 octetos y no se puede extender

241. Se entiende por DESTINO LOCAL
a. Aquel cuyo identificativo de red coincide con el de nuestro host (A veces)
b. Aquel cuyo identificativo de subred coincide con el nuestro
c. *Debe coincidir el identificativo de red y el de subred*

242. Un proceso puede estar en el estado FIN_WAIT_2
a. Como máximo 4 seg
b. Al menos 4 seg
c. *Indefinidamente*

243. El mecanismo de control de flujo que emplea TCP es:
a. CRC 32
b. *Ventana deslizante*
c. Aloha ranurado

244. La ventana se cierra cuando...
a. *Se reciben reconocimientos*
b. Se envían datos
c. Nunca se mueve

245. La ventana de congestión es un control de flujo impuesto por:
a. *El emisor*
b. El receptor
c. Un router intermedio

246. La ventana notificada es un control de flujo impuesto por:
a. El emisor
b. *El receptor*
c. Un router intermedio

247. Un temporizador de persistencia
a. *Permite transmitir información acerca del tamaño de la ventana aún cuando el otro extremo haya cerrado su ventana de recepción*
b. Se emplea cuando se está esperando un reconocimiento (temporizador de retransmisión)
c. Se emplea para detectar cuando el otro extremo de la conexión se ha desconectado (temporizador de Subsistencia)

248. ¿Cuáles son las técnicas para mejorar el problema de la transmisión en tiempo real?

a. Streaming y buffering
b. *Compresión y buffering*
c. El estándar H.323 y compresión

249. Para enviar un evento cuya inmediata recepción es crítica la cantidad de datos a transmitir es:

a. *Relativamente grande*
b. Relativamente pequeña
c. No influye el tamaño

250. ¿Qué protocolo utiliza típicamente RTP como medio de transporte?

a. *UDP*
b. TCP
c. SMTP

251. Mediante la técnica buffering si se produce una saturación en la red, y no se recibe nada durante 'x' segundos:

a. el flujo se corta
b. *el flujo no se corta*
c. no ocurre nada

252. El protocolo RTP permite el envío:

a. Unicast
b. Multicast
c. *Ambas*

253. El tipo de paquete RR utiliza estadísticas de transmisión y recepción de participantes que no actúan como emisores activos

a. *No* (Sólo de recepción)
b. Sí
c. A veces

254. La cabecera de los paquetes RTP se compone de:

a. *Marca de tiempo, número del paquete, tipo de formato, identificador de la fuente de sincronización e identificador de otras fuentes*
b. Tipo de enlace, identificador de la fuente de sincronización, marca de tiempo, número de reconocimiento e identificador de otras fuentes que aportan datos
c. Identificador de enlace, tipo de formato, marca de tiempo, identificador de otras fuentes, número de paquete

255. ¿Qué significan las siglas RTSP?

a. Protocolo de estado de enlace en tiempo real
b. *Protocolo de flujo en tiempo real*
c. Protocolo de transporte en tiempo real

256. ¿Y las siglas RTP?

a. Protocolo de transferencia en tiempo real
b. Protocolo de transporte en tiempo real
c. *Las 2 anteriores son correctas*

257. El protocolo RTSP utiliza a RTP como protocolo subyacente. ¿Qué tipo de puerto RTP utiliza?

a. Un número impar
b. *Un número par*
c. Un número cualquiera

258. En un cierre simultáneo en el protocolo TCP, ¿qué entidad efectúa un cierre pasivo?

a. Emisor
b. Receptor
c. El cliente
d. El servidor
e. Ninguno (se lleva a cabo un cierre activo)

TEMA 10: TRANSMISIÓN DE FLUJOS DE AUDIO Y VÍDEO EN TIEMPO REAL

259. ¿Cuáles son las tareas para mejorar el problema de la transmisión en tiempo real?
a. Utilización de buffers y mecanismos de STREAMING (Flujo corriente de información multimedia)
b. Utilización del protocolo H.227
c. *Utilización de los mecanismos de compresión y buffer*

260. ¿Qué protocolo usa RTP para el transporte de información multimedia?
a. TCP
b. *UDP* (Protocolo no fiable)
c. SMTP

261. ¿Qué tipo de comunicación permite el protocolo RTP?
a. *Unicast*
b. *Multicast*
c. Anycast

262. Para enviar un evento cuya recepción inmediata es crítica, la cantidad de datos a transmitir es:
a. Relativamente pequeña
b. No depende del tamaño
c. *Relativamente grande*

263. ¿Por qué no es muy importante el ancho de banda en el envío de un mensaje de correo electrónico?
a. Porque la cantidad de datos a transmitir será grande
b. Porque el requisito de la inmediatez en la recepción de información es crítico
c. *Ninguna de las anteriores* Porque la cantidad de datos a transmitir es pequeña y el requisito de inmediatez NO es crítico

264. ¿Se pueden utilizar técnicas de compresión para comprimir distintos tipos de información?
a. *Sí, haciéndolo de la forma adecuada*
b. No, no es posible
c. A veces

265. ¿Qué se sacrifica con el Buffering a costa de obtener un flujo continuo de información?
a. La calidad de la información
b. El tamaño de la información
c. *No reproducir inmediatamente los primeros datos que llegan, sonidos o fotogramas de vídeo*

266. ¿Qué efectos positivos tiene el buffering?
Si hay un corte en la transmisión, el receptor no deja de oir la voz que estaba oyendo, porque al estar almacenada la información en un buffer, ésta se saca del mismo para que el streaming (flujo) no se corte.

267. **¿A qué da soporte RTP? (¿A qué protocolos de nivel superior?)**
Al protocolo H323
RTSP amplía sus capacidades utilizando RTP

268. **Diferencia entre RTP y RTSP**
a. RTP es para audio y RTSP para vídeo
b. RTP es para tiempo real y RTSP no
c. *Ninguna de las anteriores.* RTSP es para tiempo real

TEMA 11: DNS

269. **¿Qué función principal realiza el protocolo DNS (Sistemas de Nombres de Dominio?**
a. Establecer la conversión entre dirección MAC (física) y dir IP (ARP y RARP)
b. *Establecer la conversión entre nombres de dominio y dirección IP* (Ej: Traducir rigel a una dirección IP)
c. Establecer la traducción entre nombres de dominio y dirección MAC

270. **¿Qué son preguntas puntero o también llamadas preguntas inversas?** (Metemos la dir IP y sale el nombre del dominio)
a. Preguntas DNS cuya respuesta se exige con elevada urgencia
b. Preguntas DNS relativas a direcciones IPX
c. *Ninguna de las anteriores* Preguntas DNS relativas a dir IP

271. **¿Cuál es la longitud máxima de una etiqueta en la jerarquía DNS?**
Etiqueta: Concatenación separada por puntos . Ej: rigel.deusto.es
a. Máximo: 32 caracteres
b. *Máximo: 63 caracteres*
c. Máximo: 256 caracteres

272. **¿Qué se entiende por zona dentro de la jerarquía DNS?**
a. Las etiquetas que figuran como hojas dentro del árbol DNS
b. *Un subárbol dentro de la jerarquía DNS*
c. Los nodos de la jerarquía DNS próximos a la raíz

273. **¿Dónde se encapsulan los mensajes DNS?**
a. Dentro del protocolo IP
b. Dentro del protocolo UDP
c. *Dentro del protocolo UDP y a veces dentro del protocolo TCP*

274. **¿Qué es una caché DNS?**
a. Un mecanismo de registro de conversiones dir MAC - dir IP
b. Un mecanismo de registro de conversiones dir IP - dir IPX
Las dos anteriores son conversiones de bajo nivel (ARP)
c. *Ninguna de las anteriores es cierta* Hacen la correspondencia entre dir IP y nombres de dominio (conversión de alto nivel)

275. **¿Qué tipo de campo de control de errores usan los mensajes DNS?**
a. CRC
b. Checksum
c. LRC
d. URC
e. *No tiene campo de control de errores*

276. **¿Cuándo se usa el protocolo del TCP por parte de DNS (para convertir)?**

Cuando excede la capacidad de transporte UDP, entra en funcionamiento TCP porque permite más capacidad de transporte de información

277. ¿Cuántos tipos de mensajes DNS se han definido?

a. *Solo uno, válido para preguntas y respuestas*
b. Uno para preguntas y otro para respuestas
c. Varios para preguntas y uno para respuestas

278. ¿Qué transporta el registro de recursos?

a. Los valores de ancho de banda y velocidad de los canales usados
b. *Las direcciones de red solicitadas*
c. Los parámetros de calidad de servicio negociados en la fase de establecimiento de la conexión

279. ¿DNS permite trabajar con direcciones IPX?

Sí

280. Cuando un cliente realiza una pregunta a un servidor DNS, la respuesta siempre procede de éste?

No, se va preguntando a otros sucesivamente hasta encontrar la respuesta correcta.

281. Una caché DNS, ¿reduce el tráfico en una red IP?

Sí, no sólo hace la traducción, sino que mantener hecha esa traducción durante un tiempo favorece la reducción del tráfico

282. Los nombres de dominio de países, ¿están formados por las 3 primeras letras?

No, por 2 letras

283. ¿En qué partes se puede subdividir la jerarquía o árbol DNS en función de los dominios identificados?

284. Los mensajes DNS:

a. *Hay uno solo definido para consultas y respuestas*
b. Hay varios definidos. Unos para consultas y otros para respuestas
c. Ninguna de las anteriores es cierta

285. Cuando el bit TC está a 1

a. *Con UDP indica que el tamaño total de la respuesta excedía de 512 bytes, por lo que se han devuelto los primeros 512 bytes*
b. Con UDP indica que el tamaño total de la respuesta excedía de 512 bytes, por lo que no se ha podido transmitir
c. Con TCP indica que el tamaño total de la respuesta excedía de 512 bytes, por lo que no se ha podido transmitir

286. La petición del estado del servidor se indica en:

a. El campo RD si está a 0
b. El campo AA si está a 1
c. *El campo código opción si está a 2*

287. Una pregunta inversa es equivalente a:

a. Una pregunta de tipo A
b. *Una pregunta de puntero*
c. Una pregunta estándar

288. Si el tipo de pregunta es A:

a. Se busca el nombre correspondiente a una dirección IP
b. *Se busca la dirección IP correspondiente al nombre preguntado*
c. Ninguna de las anteriores es cierta

289. Respuesta, autoridad e información adicional:
a. *Tienen el mismo formato y éste se denomina Registro de Recurso o RR*
b. Tienen el mismo formato y éste se denomina Registro Autorizado a RA
c. Tienen formatos diferentes

290. La caché que emplean todos los servidores de nombres para indicar el tráfico DNS en Internet, ¿dónde se mantiene?
a. En el "resolver"
b. *En el servidor*
c. En el cliente

291. Cuando se recibe una notificación con el bit TC puesto a 1:
a. Se tiene que volver a enviar la siguiente vez en partes de 512 bytes
b. *Se vuelve a efectuar la misma pregunta utilizando TCP*
c. Ninguna de las anteriores es cierta

REPASO

292. En el protocolo IP se establecen en el formato del datagrama varios tipos de servicio. Indicar cuál de las tres siguientes no pertenece a IP
a. *Minimizar el caudal*
b. Minimizar el coste
c. Minimizar el tiempo

293. En el protocolo ICMP se define un mensaje para el control de congestión. Indicar cómo opera:
a. El router devuelve al sistema receptor un mensaje SQ
b. *El router devuelve al emisor un mensaje SQ*
c. El sistema final devuelve al router por defecto un mensaje SQ

294. ¿Cuántos tipos de direcciones IP incluyen en su formato identificador de red e identificador de host?
a. 4
b. *3*
c. 2

295. En el protocolo TCP, ¿cuál es el tamaño del campo de detección de errores ubicado en la cabecera de un segmento TCP?
16 bits

296. ¿Para qué se utiliza la pseudocabecera en el protocolo IP?
a. Para trabajar con redes privadas virtuales
b. Para adaptarse a direcciones de 128 bits
c. *Para calcular el checksum*
d. Para utilizar direcciones anycast

297. En el protocolo DNS, ¿dónde existe la funcionalidad de control de congestión en un mensaje DNS?
a. En la cabecera
b. En la zona de datos
c. En ambas
d. *DNS no contempla congestión*

298. Dada la dirección 130.215.64.26 indicar:
a. ¿En qué capa de la pila de protocolos TCP/IP está definida?

Capa de red (IP,2)

b. ¿Qué tipo de dirección es?

B, unicast

c. ¿Cuál es el identificador de host si se utiliza una máscara FF.FF.FF.00?

26

299. ¿Cuántos bits tiene una dirección Internet IPv6?

128 bits

300. ¿Cuántos octetos se incluyen dentro de una máscara IPv4?

4 octetos

301. Dentro del protocolo ARP, ¿en qué mensaje el campo de dirección HW destino está vacío?

Mensaje de (respuesta) petición

302. En UDP, ¿qué campos se definen en los 8 primeros bytes?

- Puerto origen
- Puerto destino
- Longitud
- Checksum

Cada uno 16 bits

303. ¿Cómo se llaman las PDU's en el protocolo TCP, UDP e IP/ICMP?

- TCP: segmentos
- UDP: datagrama
- IP: datagrama
- ICMP: mensaje

TEMA 12: TELNET

304. ¿Cómo se denomina al servicio que permite establecer una conexión con un sistema remoto, que pase la entrada del teclado local a la máquina remota y recibe sus respuestas? (Válido únicamente para el sistema UNIX o LINUX)

RLOGIN -> de forma asimétrica
TELNET -> de forma simétrica
Login Remoto

305. En el proceso de conexión Telnet:

a. el cliente establece una conexión UDP con el servidor
b. *el cliente establece una conexión TCP con el servidor*
c. el servidor establece una conexión TCP/IP con el cliente

306. ¿Cuáles de estos servicios no es típico de Telnet?

a. Terminal virtual de red
b. Negociación (Handshaking) de opciones entre cliente y servidor
c. *Conexión de forma asimétrica*

307. ¿Se permiten en Telnet conexiones concurrentes?

Sí

308. ¿Cuál es la función del pseudoterminal Telnet?

Permitir a un programa como el pseudoterminal Telnet transmitir caracteres al sistema operativo como si procedieran de un terminal.

309. ¿Qué significan las siglas NVT? ¿Y de qué se encarga el NVT?

Terminal Virtual de Red
Define el modo en que deben enviarse los datos y comandos a través de la red.
Se encarga de convertir los datos del sistema cliente al formato necesario para ser comprendidos por el servidor.

310. ¿Qué formato de datos utiliza el NVT?

a. *ASCII de 7 bits más un bit de control*
b. ASCII de 6 bits más uno de control
c. BCD

311. ¿Qué carácter se utiliza para separar los datos de los caracteres de control?

a. 0x00
b. *0xFF* (hexadecimal) (campo de 8 bits)
c. 0xF0

312. Proveedor de servicio de Telnet

TCP

313. ¿Cómo se determina el final de los datos urgentes en Telnet?

Utilizando una señal: DM

314. ¿Por qué es necesario que Telnet soporte mensajes urgentes?

a. *Para priorizar comando cuando la ventana del receptor está cerrada*
b. Para mandar los datos importantes
c. Ninguna de las anteriores

315. ¿En qué sentido se puede utilizar el comando DM?

a. Desde el cliente al servidor
b. Desde el servidor al cliente
c. *Las 2 anteriores son ciertas*

316. ¿En qué modos puede operar Telnet?

- Half-duplex
- Un carácter cada vez
- Una línea cada vez (Kludge Line Mode)
- Modo línea

317. ¿Cómo se soluciona en Telnet al problema de la heterogeneidad?

NVT -> Terminal Virtual de Red

TEMA 13: FTP

318. Los servidores FTP realizan una:

a. apertura activa sobre el puerto 21
b. *apertura pasiva sobre el puerto 21*
c. *apertura activa sobre el puerto 20*

319. ¿Cuál es el proveedor de servicios de FTP?

320. FTP:

a. soporta todo tipo de estructuras de ficheros y tipos de ficheros
b. *soporta un número determinado de tipos de ficheros y estructuras de ficheros*
c. soporta todo tipo de ficheros pero solo algún tipo de estructura de fichero

321. ¿Cuáles son las facilidades que proporciona FTP además de la propia transferencia de ficheros?

322. ¿Cuáles son las 2 conexiones TCP para la transferencia de datos?

Conexión de control y conexión de datos

323. ¿Dónde está ubicado FTP en TCP/IP?

Aplicación (capa 4)

324. ¿De qué forma se crean las conexiones de transferencia de datos y los procesos de transferencia de datos?

a. Aleatoriamente
b. *Dinámicamente*
c. Están predeterminadas

325. ¿En qué consiste el modo continuo de transmisión?

a. El fichero se transmite en bloques
b. Se emplea un esquema de compresión
c. *El fichero se transmite con una secuencia continua de bytes*

326. ¿Bajo qué formato se envían las preguntas y las respuestas?

ASCII-NVT

327. ¿Dónde se encuentra el campo TOS (tipo de servicio) utilizado por FTP para maximizar el rendimiento en la conexión de datos?

a. Dentro del segmento TCP
b. Dentro del mensaje FTP
c. Dentro de una trama del nivel 2
d. *Ninguna de las anteriores* En el datagrama IP

328. ¿Cómo FTP consigue la heterogeneidad del funcionamiento de los distintos equipos?

NVT (Terminal Virtual de Red)

329. ¿De cuántos dígitos son las respuestas FTP?

a. 2
b. 4
c. *3*

330. ¿Cómo son las respuestas a través de una conexión de control?

a. Una sola línea
b. *Multilínea*
c. Ninguna es correcta

331. ¿Cómo son los números de puerto desde los que se efectúa la apertura activa del cliente?

a. *Aleatoria*
b. Predefinidas
c. La marca el administrador de red

TEMA 14: BOOTP Y DHCP

332. ¿Cómo soluciona BOOTP la deficiencia de RARP por la cual los servidores deben situarse en la misma red que el cliente?

Al utilizar IP para el envío de sus mensajes, éstos podrán ser reencaminados por los routers, posibilitando que los clientes y servidores no se encuentren en la misma red física

333. ¿Dónde se encapsulan los mensajes BOOTP?

a. *En datagramas UDP*
b. *En datagramas IP*
c. En tramas

334. Señala la sentencia verdadera e indica porque el resto no lo son:

a. El campo número de segundos indica el tiempo que lleva el cliente esperando para recibir una respuesta
b. El campo nombre del fichero de arranque puede ser completado por el cliente (servidor de manera opcional) para indicar el nombre completo del directorio en que se encuentra
c. *El protocolo BOOTP es un protocolo que sirve para arrancar a través de la red*

335. ¿Qué diferencia existe en que sea un servidor normal (o no proxy) el que rellene el campo de dirección IP cliente, a que lo haga un servidor Proxy?

Si es Proxy debe incluir la dirección IP de pasarela

336. ¿Cuáles de los campos definidos en un mensaje BOOTP son de carácter opcional?

a. Nombre del servidor, nombre del fichero de arranque y número de segundos
b. Nombre del fichero de arranque, tipo hardware y longitud de la dirección hardware
c. *Nombre del servidor, nombre del fichero de arranque e información específica del servidor*

337. ¿Qué número de puerto está reservado en BOOTP para el servidor? ¿Y para el cliente?

a. *67 para el servidor y 68 cliente*
b. 67 cliente y 68 servidor
c. ninguna de las anteriores

338. ¿Por qué se asigna un número de puerto de cliente y no se deja que se coja uno aleatorio?

Porque la respuesta que le llega al cliente puede ser una difusión

339. ¿Quién realiza el control de errores en BOOTP?

a. El servidor BOOTP
b. *El cliente BOOTP*
c. Ninguno de los anteriores

340. ¿Qué ocurre cuando un router no es capaz de atender peticiones BOOTP?

a. Los routers siempre podrán atender peticiones BOOTP
b. El servidor será el que envíe directamente la respuesta al cliente
c. *Incluye su dirección IP en el campo dirección IP de pasarela y lo envía al servidor BOOTP incrementando en 1 el campo número de saltos*

341. ¿Qué información contiene los 4 primeros bytes del campo información específica del vendedor en caso de que tenga información?

a. Máscara de subred
b. Time
c. *Ninguna de las anteriores* La dirección IP (“Magic Cookie”) o Pasarela

342. ¿Qué protocolos utilizan las estaciones sin disco?

RARP y BOOTP

¿Cuál es el peor?

RARP

343. ¿Qué es el protocolo DHCP?

El protocolo de Configuración Dinámica de host que proporciona mecanismos para enviar información de configuración a máquinas de una red TCP/IP, permitiendo la reutilización de direcciones IP

344. ¿Qué dos partes se distinguen en DHCP?

Un protocolo para enviar información de configuración específica desde un servidor a una máquina (modelo cliente-servidor) y un mecanismo de asignación de direcciones IP

345. ¿Cuál de las distintas formas de asignación de direcciones IP permite la reutilización de direcciones IP?

a. *Asignación dinámica*
b. Asignación manual
c. Asignación automática

346. ¿Cuál es el parámetro de configuración más importante?

a. Identificativo del servidor
b. Tipo y longitud de dirección hardware
c. *Dirección IP*

TEMA 15: SMTP Y POP3

347. Señalar las dos características verdaderas de SMTP:

a. Es fiable y asegura la entrega al usuario correcto en un ordenador
b. No es fiable y no asegura la entrega al usuario correcto en un ordenador
c. *Es fiable pero no asegura la entrega correcta al usuario de un ordenador*

348. El responsable de agregar el sobre al mensaje:

a. El usuario
b. El agente de usuario
c. *MTA*

349. ¿Qué información contiene el sobre de un mensaje electrónico?

a. La dirección electrónica del emisor, la del destinatario, y el subject del mensaje
b. *La dirección del emisor y la del destinatario*
c. La dirección del destinatario y el subject

350. ¿Quién utiliza la cabecera de un mensaje electrónico?

a. *Agentes de usuario*
b. El MTA
c. Las dos anteriores son ciertas

351. ¿A qué se le suele denominar contenido de un mensaje?

a. *Al conjunto cabecera y cuerpo*
b. Al cuerpo
c. Al conjunto sobre y cuerpo

352. ¿Se puede enviar documentos que no estén en formato NVT ASCII? Si es que sí, decir como:

Sí, a través del correo electrónico, el IETF ha definido MIME

353. El protocolo ESMTP es un protocolo al SMTP sólo que realiza algunas extensiones sobre éste ¿Cuáles son?

a. *Un nuevo comando llamado EHLO, introducir nuevos argumentos en los comandos mailfrom y rcptto y un registro de nuevos servicios*
b. Un nuevo formato de envío de los comandos al servidor y una variación en los estados al conectarse
c. En realidad, las extensiones se refieren al modo de realizar la conexión

354. El modo de recibir el correo en POP3 es:

a. Mediante un MTA de conmutación que permite una conexión continua con el servidor, recibiendo el correo en todo momento
b. *Mediante el uso de MTA que accede dinámicamente al servicio maildrop del servidor recogiendo el correo que guarde cada vez que accedamos a este servicio*
c. El protocolo POP3 no recibe correo sino que lo envía

355. Una sesión de POP3 progresa a través de varios estados. ¿Cuáles son? ¿Y en qué orden?

a. Estado de conexión, estado de comandos y estado de cierre
b. Estado de envío y estado de recepción
c. *Estado de autorización, estado de transacción y estado de actualización*

356. El comando QUIT que cierra la conexión se puede enviar desde:

a. Estado de autorización
b. Estado de transacción
c. *a y b son correctos*

357. Un servidor POP3 está a la escucha:ç

a. En el puerto 25
b. En el puerto 80
c. *Ninguna de las anteriores es cierta* (Puerto 110)

358. En un mensaje de correo electrónico ¿se puede o no incluir cualquier tipo de fichero?

Sí

359. Un agente de usuario para el tratamiento del correo electrónico:

a. *Se encarga de construir e interpretar los campos de cabecera del mensaje de correo*
b. Deposita el correo utilizando SMTP directamente en el buzón del destino
c. Se encarga de ir depositando el mensaje en cada uno de los agentes de transferencia de mensajes que haya en el camino hasta llegar al buzón del destinatario

TEMA 16: APLICACIONES DISTRIBUIDAS (RPC)

360. Al invocarse un RPC se llama a una función del nodo locas que empaqueta los argumentos en un mensaje de red y los envía al servidor. ¿Cómo se denomina?

a. *Cliente stub*
b. Socket
c. Server stub

361. ¿Cuál de las siguientes opciones se considera un beneficio del RPC?

a. La comunicación se realiza directamente desde cliente al servidor.
b. La programación es más compleja pero más eficiente
c. *Maneja la conversión de argumentos y valores devueltos*

362. **¿Quién fija el campo xid (transaction id) del mensaje de RPC?**
a. *Cliente*
b. Servidor
c. Administrador de red

363. **¿Para qué se usa el campo verified de un mensaje RPC?**
a. Para descubrir errores en el mensaje
b. *Para cifrarlo*
c. Para verificar la recepción del mensaje

364. **¿Cuál de las siguientes codificaciones se usa en la transmisión de mensajes RPC?**
a. NVT
b. *XDR*
c. Codificación ASCII

365. **¿Para qué sirve el port-mapper?**
Para saber la correspondencia entre puertos y programas

366. **Al iniciarse el port-mapper:**
a. Se crea un extremo TCP y efectúa una apertura pasiva en el puerto TCP-111
b. Se crea un extremo UDP esperando recibir datagramas UDP por el puerto 111
c. *Todas las anteriores son correctas*

367. **¿Cómo puede un programa cliente obtener el número de puerto de un programa RPC en el servidor?**
a. Pmapproc-set
b. Pmapproc-dump
c. *Ninguna* Pmapproc-getport

368. **¿Cómo traduciriáis el concepto Port mapper?**
Tabla de Correspondencia de Puertos

369. **En el modelo OSI ¿en qué capa colocariáis XDR?**
Capa de Presentación -> OSI
Capa de Aplicación -> TCP/IP porque no hay de presentación

370. **¿Cómo se denomina al lenguaje empleado para definir interfaces en una arquitectura CORBA?**
IDL

371. **EL DSI:** (Pág 197)
a. Permite la invocación de funciones estáticas en el cliente
b. *Permite la invocación de funciones estáticas en el servidor*
c. *Ninguna de las anteriores es cierta* Dinámicas y estáticas en el servidor

372. **El POM:**
a. Significa Portable Object Manager
b. Es un intermediario entre los POS y los PID
c. *Es un intermediario entre los POS y el sistema de almacenamiento*

373. **El servidor de propiedades:**
a. Proporciona operaciones para garantizar el uso legal de los componentes
b. Permite bloquear el acceso a objetos mientras se está llevando a cabo una transacción.
c. *Permite asociar dinámicamente atributos con valores en cualquier componente*

374. **El servicio de ODBMS:**
a. *Utiliza un lenguaje como OML, requiriendo un precompilador que lo traduzca*
b. Utiliza un lenguaje como SQL para realizar las operaciones sobre la BD
c. Es una extensión del lenguaje OQL

375. ¿Cómo se compatibilizan las diferencias de plataformas en cuanto a formato en una arquitectura CORBA? (Pag 202)

Se utiliza CDR

376. ¿Qué es el DCE?

DCE arquitectura clásica de entorno de computación distribuida

377. ¿Qué problema tiene la tecnología COM?

a. *Unas características tecnológicas menos flexibles que CORBA*
b. Unas características tecnológicas más flexibles pero menos variadas que las de CORBA
c. *Una excesiva dependencia de la plataforma WINDOWS*

TEMA 17: SNMP

378. ¿Qué significa SNMP?

a. Simplemente un Nodo Manipulador de Periféricos
b. Single Natural Manufacturer of Protocols
c. *Un protocolo simple de gestión de red*

379. SNMP es:

a. Un comando que se puede ejecutar en cualquier red
b. Un sistema de nodos manipulables físicamente
c. *Un protocolo de la familia TCP/IP del nivel de aplicación*

380. SNMP...

a. Se definió en las GO, pero no se empezó a utilizar hasta después
b. Experimentó (a) un auge impresionante en la década de los 80
c. *Es el mecanismo dominante en la gestión distribuida de redes de los 90*

381. ¿Cuál es la verdadera?

a. SNMP y CMOT son orientados a la conexión
b. *SNMP es de la familia TCP/IP mientras que CMOT utiliza estándares del modelo OSI*
c. Finalmente (OSI) (COMT) CMOT ha triunfado sobre SNMP porque las redes cada vez son más complejas.

382. Hablando de SNMP, ¿cuál de estas frases es la FALSA?

a. Agente: SW que se encuentra en los elementos de red SNMP
b. *Gestor: son las estaciones de gestión de red que monitorizan la comunicación con los elementos de la red*
c. El Gestor no solo lee la información del Agente sino que también puede modificarla

383. Tres elementos importantes en el TCP/IP

- MIB
- SMI
- SNMP

384. ¿Cuáles son los puertos UDP utilizados por SNMP?

161 (agente) y 162 (gestor)

385. Tipos de mensajes generados en SNMP y qué estación los genera

- Get_request ⇒ Gestor SNMP
- Get_next_request ⇒ Gestor SNMP
- Response ⇒ Agente SNMP

- Set_Request ⇒ Gestor SNMP
- Trap ⇒ Agente SNMP

5 tipos para 2 formatos

386. Tipo de dirección a la que le corresponde el campo dirección del agente de la PDU (Trap)

a. *IP*
b. UDP
c. TCP

387. Enumera al menos tres objetivos de la RMON

- Operación off-line
- Monitorización apropiativa
- Detección y notificación de problemas
- Datos de valor añadido
- Gestores múltiples

388. ¿Qué campo de un mensaje SNMP tiene que ver con la autenticación?

Comunidad
Versión 1 -> sin cifrar

TEMA 18: WORLD WIDE WEB

389. HTML:

a. Es un lenguaje que se utiliza para codificar documentos World Wide Web
b. Describe cómo se han de mostrar los contenidos de un documento
c. *Ambas respuestas son correctas*

390. Indicar cuál de las siguientes afirmaciones es falsa:

a. Las etiquetas de fin nunca contienen atributos
b. *Todas las etiquetas constan de una etiqueta de comienzo y una de fin* (Casi todas pero no todas)
c. La etiqueta de fin es igual que la de comienzo pero precedido de (/)

391. ¿En qué se diferencian el método GET y el HEAD?

a. Son funcionalmente distintos
b. En la información de cabecera
c. *En el área de datos de la respuesta*

392. El método GET y POST se diferencian en:

a. Su funcionalidad
b. En la sección de cuerpo de la petición del cliente
c. *Las dos anteriores son correctas*
d. Ninguna de las anteriores es correcta

393. ¿Qué técnicas son de tipo ServerSide, es decir, se ejecutan en el servidor?

a. Las que utilizan el lenguaje JAVA
b. Applets y CGIs
c. *CGIs y Servlets*

394. Cuando un servidor recibe una petición CGI:

a. *Carga el programa correspondiente en memoria creando un nuevo proceso*

b. Comprueba si el programa ya se está ejecutando para otra petición, y asocia esta petición al mismo proceso
c. Envía al cliente una nueva página html, con el código del programa CGI correspondiente.

395. El código ASP:
a. Se procesa en el cliente al ejecutar el código
b. *Se procesa en el servidor antes de servir la página al cliente*
c. Ninguna de las anteriores es cierta

396. ¿Cuál es la principal diferencia entre ASP y JSP?
ASP -> está desarrollado por Microsoft
JSP -> es Java

397. El resultado que devuelve el servidor tras el procesamiento de una página ASP
a. Es íntegramente código HTML
b. *Tiene una parte estática y otra dinámica*
c. Ninguna de las anteriores es cierta

TEMA 19: SEGURIDAD EN REDES

398. Categorías de mecanismos de seguridad OSI
- Específicos
- Generalizados

399. ¿Qué cifrado precisa del algoritmo RSA?
a. Cifrado convencional o de clave secreta o simétrica
b. *Cifrado de clave pública o asimétrica*
c. Ambas respuestas son ciertas

Privada para firmar, autentificar
Pública del receptor para cifrar ⇒ Estas dos son asimétricas

400. El relleno de tráfico:
a. *Es una función que produce texto cifrado (ruido continuamente, incluso en ausencia de texto en claro)*
b. Es una función que produce texto cifrado (ruido continuamente, sólo en ausencia de texto en claro)
c. Ninguna de las anteriores es cierta

401. En el control de acceso de usuario centralizado:
a. *La red es la que determina si el usuario tiene acceso a la misma y con quién puede comunicarse*
b. La red es transparente, controlado el acceso por el computador destino
c. Ninguna de las anteriores

402. ¿Cuál es la funcionalidad de los mecanismos de integridad?
Que los datos no sean modificados durante la transmisión