Tests

de

Redes de Ordenadores

Test Nº 2

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

1. **¿ Cuál es el tamaño de las direcciones IPv4 ?**

2. **¿ Cuál es el tamaño de las direcciones IPv4 IPn6 ?**

3. **¿ Cómo se denominan las PDU's en TCP ?**

4. **¿ Cómo se denominan las PDU's en UDP ?**

5. **¿ Cómo se denominan las PDU's en IP ?**

6. **¿ Cómo se denominan las PDU's en el nivel de Drivers ?**

7. **¿ Qué significa SNMP ?**

8. **¿ Qué elementos se identifican en la gestión de red ? (SNMP)**

9. **¿ A qué nivel TCP/IP corresponde el protocolo DNS ?**
   a. Nivel 3
   b. Nivel 2
   c. Nivel 4

10. **¿ Cuál de los siguientes niveles TCP/IP implementa un protocolo extremo a extremo ?**
    a. Nivel de Aplicación
    b. Nivel de Transporte
    c. Ambas respuestas son ciertas.

11. **¿ Qué incluye el nivel de red para que el protocolo IP sea salto a salto (Hop by Hop) ?**
    a. Routers
    b. Puentes
    c. Ambas respuestas son ciertas

12. **¿ En qué nivel TCP/IP se añade cabecera y cola durante el proceso de encapsulamiento ?**
    a. Nivel de Red
    b. Nivel de Enlace de Datos
    c. Nivel de Transporte

13. **¿ Qué nivel de la pila TCP/IP es más abstracto ?**

14. **¿ Qué nivel de la pila TCP/IP es menos abstracto ?**

15. **En la pila de protocolos TCP/IP, ¿ en qué nivel y protocolo las PDU's se llaman "segmento" ?**

16. **¿ Dónde se encuentra el usuario ?**
    a. Entre el nivel de Aplicación y el nivel de Transporte
    b. Debajo del nivel físico
    c. Por encima del nivel de aplicación

17. **¿ Qué introduce la capa de Enlace de Datos, como cola, utilizando una red de LAN como infraestructura base ?**
    a. CRC-32, código de redundancia cíclica y detección de errores.
    b. CRC-32, código de redundancia cíclica, detección de errores y delimitador de fin.
    c. CRC-32, código de redundancia cíclica y delimitador de fin.

18. **¿ Dónde está el ARP?**
    a. En el nivel de Red
    b. En el nivel de Drivers
    c. Ninguna de las anteriores es cierta.

19. **¿ En qué puntos se realiza la demultiplexión ?**

20. **¿ Cuáles son los tipos fundamentales de servidores definidos en el modelo cliente-servidor de TCP/IP ?**

21. **Si una máquina de tratamiento de la información tiene múltiples conexiones, ¿ qué apelativo recibe ?**

22. **Si una máquina de tratamiento de la información con múltiples conexiones no está configurada como Router...**

23. **La dirección 130.206.100.2, ¿ qué tipo de dirección es ?**
    a. Dirección IP Primaria Clase B
    b. Dirección IP Secundaria Clase A
    c. Dirección IP Secundaria Tipo C

24. **¿ Cuántas redes pueden existir en una dirección Clase C ?**

25. **¿ Cómo se construye una máscara de red?**
    a. Asignando, según necesidades, un “1” en la posición de los bits que forman parte del identificador de red, y un “0” en los correspondientes al identificador de nodo.
    b. Asignando, según necesidades, un “0” en la posición de los bits que forman parte del identificador de red, y un “1” en los correspondientes al identificador de nodo.
    c. La asignación utiliza 3 caracteres y su especificación ternaria depende del administrador de red. **-> NO, porque se trabaja en binario, y no con señales ternarias.**

26. **¿ Cuál es el número máximo de identificadores de red en la clase A ?**

27. **¿ Cuál es el número máximo de identificadores de red en la clase B ?**

28. **¿ Cuál es el número máximo de identificadores de red en la clase C ?**

29. **¿ Para qué restamos “2” al calcular el nº máximo de identificadores ?**

30. **¿ Cuál de las siguientes opciones no es una subdivisión válida para redes de clase B ?**
    a. 62 subredes – 1082 nodos
    b. 14 subredes – 14 nodos
    c. 30 subredes – 2046 nodos

31. Las máscaras de subred, ¿ qué dígito binario usan para designar el identificador de nodo ?

a. 1
b. 0
c. inoperante o “don’t care”

32. ¿ Cuántos identificadores de nodo diferentes pueden utilizarse en una red Clase C, cuya máscara de subred es M = FF.FF.FF.00 ?

a. 1024
b. 64
c. 128
d. NAEC

33. ¿ A qué clase pertenece la dirección IP 191.206.100.1 ?

a. Dirección IP Primaria clase B
b. Dirección IP Primaria clase C
c. NAEC

34. Dada la dirección IP 191.206.100.1 y la máscara de subred 255.255.255.224, ¿ cuál es la parte que corresponde al ID de red, al ID subred y nodo ?

35. Dada la dirección IP 191.206.100.1 y la máscara de subred 255.255.255.2254, ¿ cuál es la parte que corresponde al ID de subred ?

36. Dada la dirección IP 191.206.100.1 y la máscara de subred 255.255.255.2254, ¿ cuál es la parte que corresponde al ID de nodo ?

37. Calcular el ID-Host (o ID-Nodo), sabiendo que la dirección IP es 132.90.132.5 y la máscara de subred es 255.255.240.0

38. Calcular el ID-Host (o ID-Nodo), sabiendo que la dirección IP es 18.20.16.91 y la máscara de subred es 255.255.255.0

39. La dirección 18.20.16.91 ¿ a qué corresponde ?

40. Si una máquina tiene muchas conexiones

a. Tiene una sola dirección IP
b. Tiene varias direcciones IP
c. NAEC

41. En las SuperRedes, usando 0’s ¿ qué campos se usan ?

42. ¿ Qué implica el término "No Orientado a la Conexión" del protocolo IP ?
   a. Que los sistemas finales no están conectados
   b. Que IP proporciona un servicio de circuito virtual
   c. Que no se mantiene información de estado de los sucesivos datagramas

43. ¿ Cuál de los siguientes campos no está en la cabecera IP ?
   a. Checksum del datagrama
   b. Dirección de red destino
   c. Campo "off-set" del fragmento.

44. Si al valor de partida del campo TTL de la cabecera de un datagrama IP vale 32, y dicho datagrama ha atravesado 13 routers, ¿ cuál puede ser el valor de dicho campo al llegar a su destino ?
   a. Menor o igual a 19
   b. Menor o igual a 32
   c. Igual a 19

45. ¿ Cuál es la función más relevante del protocolo IP ?

46. ¿ Los datagramas IP son de longitud ...?
   a. Variable
   b. Fija

47. ¿ La cabecera de un datagrama-IP es de longitud...?
   a. Variable
   b. Fija

48. ¿ Con qué se relaciona el Tipo de Servicio ?

49. ¿ Cuántos campos en la cabecera de un datagrama IP son de longitud variable ?

50. ¿ Cuál es el grado de mecanismo de detección de errores de la información transportafa en un datagrama IP?

51. Indicar un servicio que utilice un tipo de servicio que maximice la fiabilidad

52. ¿ En qué se mide la longitud de la cabecera de un datagrama IP ?

53. ¿ Qué aspectos se hacen máximo o mínimo en el campo TOS ?

54. ¿ Cómo se mide el campo longitud de la cabecera de un datagrama IP ?

55. ¿ Por qué se fragmenta un datagrama ?

56. ¿ Cuántos y cuáles son los campos de la cabecera utilizados para la fragmentación ?

57. ¿ Qué significan las siglas MTU ?, ¿qué relación tiene con la fragmentación de datagramas ?

58. ¿ Dónde se encapsulan los datagramas IP ?

a. Segmentos TCP
b. Datagramas UDP
c. Mensajes ICMP
d. Mensajes ARP
e. NAEC

59. ¿ Cuál es el criterio para saber si 2 nodos están conectados de forma directa ?

60. ¿ Qué componentes integran una tabla de encaminamiento ?

61. ¿ Cuál de los siguientes protocolos no contiene en su cabecera ningún campo que lleve a cabo la demultiplexación?

a. ODP
b. ICMP
c. Ambos contienen un campo para demultiplexar

62. ¿ Cuál es la máscara de subred para una dirección Clase B con 8 bits para el identificador de subred ?

63. ¿ Cuántas rutas tendrá en su tabla de encaminamiento un nodo o sistema conectado a 2 redes que a su vez no tienen ninguna pasarela o router directamente conectado a ellas ?

a. 3 : la de LoopBack y las de sus dos interfaces
b. 1 : la de loopback
c. 2 : las de sus dos interfaces

64. ¿ Qué significa el flag H y dónde se encuentra en el mecanismo de encaminamiento?

65. ¿ Qué parte de la dirección IP se consulta para el encaminamiento ?

66. ¿ Cuál es el tamaño mínimo de la cabecera IP ?

67. ¿ Cuál es el tamaño mínimo de la cabecera IP?

68. ¿ Cómo se llaman los mensajes usados por ICMP que modifican la tabla de encaminamiento ?

a. Petición y Eco.
b. Control de congestión.
c. Destino no alcanzable.
d. NAEC

69. ¿ Cómo se denominan las direcciones de la comunicación multicast ?

a. de 48 bits
b. De 20 bytes.
c. De 128 bits.
d. NAEC.

70. ¿ Qué problemas de IPv4 han sido resueltas en IPv6 ?

71. El protocolo ARP, ¿ qué tipo de mensajes utiliza para la petición de la dirección MAC ?

a. Mensaje “unicast” con la dirección hardware de la máquina destino.
b. Mensaje de difusión a nivel de enlace de datos.
c. Mensaje de difusión a nivel IP.

72. ¿ Cuál es el nº y la especificación de una máquina remota ?

73. ¿ Qué información no existe en uno de los mensajes ARP y cuál es esa información dentro de la PDU ARP ?

74. ¿ Cómo se denominan las PDU en ARP ?

75. ¿ Dónde está ubicado el protocolo ARP ?

76. ¿ Cuántos son los aspectos de mejora en IPv4 ?

77. ¿ Cuántos tipos de dirección se definen en IPv6 ?, ¿ cómo se llaman ?

78. En el protocolo IP, las tablas de encaminamiento de máquinas conectadas a 2 subredes que a su vez tienen conexión con otras subredes, ¿ cuántas entradas de dirección destino tendrán ?

79. El protocolo ARP, ¿ qué tipo de mensajes utiliza ?

80. ¿ Cómo se identifica una dirección de difusión en la capa de enlace de datos ?

81. ¿ Dónde se encapsula un mensaje ARP ?

82. En el funcionamiento del protocolo ARP, cuando se recibe una respuesta en la estación peticionaria, ¿ qué información recoge ésta que no estaba presente en el mensaje de petición ?

83. En el protocolo ARP ¿ qué tipo de conversión se lleva a cabo ?

84. En una dirección IP, ¿ cuántos campos se pueden identificar ?

85. ¿ Cuántos niveles tiene la pila de protocolos TCP/IP, y en qué nivel se ubican los protocolos UDP y FTP ?

86. El protocolo ARP :
- a. Utiliza mensajes con el campo de dirección MAC origen puesto a "11..."
- b. Utiliza mensajes cuyo campo de dirección IP destino está puesto a "1..1"
- c. Cualquiera de los 2 anteriores es cierta
- d. NAEC

87. El protocolo ARP :
- a. Permite obtener las direcciones IP de las máquinas informáticas cuya dirección física sea específica.
- b. Permite obtener las direcciones IP de las máquinas informáticas sin unidades de almacenamiento (disco)
- c. Cualquiera de las anteriores es cierta

88. El protocolo RARP, cuando utiliza varios servidores :
- a. Sólo contestarán los nodos configurados como servidores primarios
- b. Contestarán todos los nodos, primarios y secundarios
- c. En RARP, igual que en ARP, no existen servidores para la resolución de direcciones

89. ¿ Qué se entiende por ARP proxi o proxi arp ?

90. ¿ Cuál es la función del encapsulamiento de mensajes RARP ?

91. ¿ Dónde se encapsulan los mensajes RARP ?

92. ¿ Dónde se ubican los protocolos ARP y RARP dentro de la pila TCP/IP ?

93. En los protocolos ARP y RARP, ¿ qué tipos de mensajes se han definido ?

94. ¿ Cómo es la longitud del protocolo ARP y RARP ?

95. ¿ Dónde se ubica el protocolo ICMP ?

96. ¿ Qué representan las siglas ICMP ?

97. ¿ Qué funciones no incluye en sus mensajes ICMP ?

98. Los mensajes ICMP, ¿ incluyen un mecanismo de detección de errores ?. En caso afirmativo, ¿ afectan a la cabecera o a todo el mensaje ¿

99. Los CheckSum? De IP e ICMP y TCP, ¿ utilizan algoritmos iguales o diferentes ?

100. ¿Por qué eventos no debe aparecer un mensaje de error ICMP ?

101. Los mensajes ICMP que se encapsulan en datagramas IP, ¿ dónde se colocan dentro del datagrama IP ?

a. Dentro del campo de opciones de la cabecera IP.
b. Dentro del campo de relleno de la cola de un datagrama IP.
c. Dentro de una trama del nivel de enlace de datos entre el CRC y el extremo de la cabecera IP.
d. NAEC

102. ¿ Qué operaciones matemáticas se llevan a cabo en la obtención del campo de checksum de un mensaje ICMP?

a. Multiplicación
b. Suma módulo $2^{16} - 1$
c. Complemento a 1

103. ¿ Cuántos mensajes de disponibilidad de destino se han definido en ICMP ?

104. ¿ Existe algún mensaje ICMP que permita obtener experimentalmente la máscara de subred ?. en caso afirmativo, ¿ qué longitud se usa para guardar la máscara de subred ?

105. En un mensaje ICMP, ¿ qué campos existen en la 1ª palabra de 32 bits ?

106. Una dirección multicast, ¿ de qué tipo es ?

107. ¿ Son obligatorios los datos en la respuesta de eco ?

108. ¿ Qué mecanismo de control de congestión se define en el protocolo ICMP ?

109. En un mensaje ICMP de petición de cambio de ruta, ¿ cuál es la 3ª fase que se identifica en el flujo de intercambio de información ?

110. ¿ Cuándo se produce un mensaje ICMP de destino no alcanzable ?

111. ¿ Qué información alberga los 8 primeros bytes del datagrama que se guardan al final de un mensaje ICMP de destino no alcanzable ?

112. En el protocolo ICMP, ¿ qué mensaje se utiliza para indicar a un sistema de computación que la dirección por defecto utilizada para direccionar el datagrama no es correcta ?

113. ¿ Qué longitud de palabra se utiliza como referencia para el formato de los mensajes ICMP ?

a. 16 bits.
b. 32 bits.
c. 8 bits.

114. ¿ Cuál es la parte final común a muchos mensajes ICMP ?

115. Los mensajes ICMP de redirección o cambio de ruta suponen el envío de información :

a. De host a host.
b. De host a router.
c. De router a host
d. NAEC

116. En el protocolo ICMP, ¿ cuántos mensajes de notificación de ruta se han definido ?, ¿De dónde a dónde se propagan ?

117. En los mensajes ICMP de detección de rutas circulares, ¿ qué campo de la cabecera del datagrama IP se consulta ?

118. En los mensajes ICMP de cambio de ruta, ¿ qué dirección se transporta ?

a. La dirección del router por defecto.
b. La dirección del router que debería emplearse.
c. La dirección del nodo que causó el problema.

119. ¿ Qué información se transporta en los mensajes ICMP tipificados como destino no alcanzable ?

120. El formato de los mensajes IGMP, ¿ es fijo o variable ?

121. ¿Cómo se denominan los 2 tipos de mensajes IGMP ?

122. Un mensaje IGMP, ¿ tiene campo de protección de errores ?. En caso afirmativo, ¿qué protege ?

123. ¿ Cuál es el algoritmo del checksum en el protocolo IGMP ?

a. Algoritmo basado en los operadores NOT y SUMA Módulo $2^{16} - 1$
b. Un algoritmo que coincide con el algoritmo de checksum usado en TCP.
c. Un algoritmo que coincide con el algoritmo utilizado en IP.
d. Todas las respuestas anteriores son ciertas.

124. ¿ Desde qué punto de partida se envían las querys o peticiones y cuál es el punto de llegada de una petición IGMP ?, ¿ Y el punto de partida y de llegada de un report IGMP ?

125. ¿ Entre qué entidades se definen los protocolos EGP ?
a. Entre sistemas autónomos (los routers) o un ISP y un sistema autónomo.
b. Entre los computadores finales de una red local.
c. Entre los proveedores de servicio internet y os sistemas finales.

126. ¿ Para qué se utilizan los protocolos de encaminamiento dinámico ?
a. Para el intercambio de información sensible entre sistemas finales.
b. Para el intercambio de información entre routers.
c. Para el intercambio de información entre sistemas finales y routers.

127. El protocolo RIP, ¿ cómo está catalogado ?
a. Protocolo de vector-distancia.
b. Protocolo de estado del enlace.
c. Protocolo de gestión de red.

128. ¿ Cuál es la diferencia entre la topología de interconexión de redes de Internet en sus comienzos y la configuración actual de Internet ?

129. Inconvenientes de los protocolos vector-distancia :

130. Los protocolos , ¿ a quién sondean?

131. ¿ Qué aspectos o funcionalidades adicionales introduce la versión 2 de RIP?
a. Limitar el nº de saltos por encima de 10.
b. Introducir autenticación en las notificaciones de ruta.
c. Permitir el uso de máscaras de subred.

132. ¿ Qué función principal realizan los protocolos EGP ?
a. Comunicar entre sí los routers BGP.
b. Utilizar direcciones de red para la notificación de las tablas de encaminamiento.
c. El protocolo EGP ha sido sustituido en las instalaciones modernas por el protocolo BGP.

133. ¿ Dónde se encapsula un mensaje EGP ?
a. En un datagrama IP.
b. En una trama del nivel 2.
c. En un datagrama UDP.

134. ¿ Dónde están los protocolos de encaminamiento dinámico ?
a.
b.
c.

135. ¿ Cuál de los siguientes parámetros necesarios para la definición de OSPF se encuentran relacionados con TOS (Tipo de servicio)?

a. Nivel de congestión en el buffer intermedio.
b. Retardo de transferencia.
c. Costo de cada interfaz.

136. ¿ Qué representan las siglas LSA en el protocolo OSPF ?

137. ¿ Cuál de los siguientes protocolos de encaminamiento dinámico no está incluido en el SW de encaminamiento GATED ?

a. EGP
b. BGP
c. RIP y HELLO

138. ¿ Qué métrica se utiliza en el protocolo HELLO ?

139. ¿ Cuántos niveles de encaminamiento se identifican en OSPF ?

140. ¿ Qué tipo de comunicaciones permite el encadenamiento dinámico ?

141. En el repertorio de protocolos de encaminamiento dinámico, existe uno que incorpora la técnica TU. Se caracteriza porque los routers deben enviar las notificaciones indicando que el costo para alcanzar una red no accesible es 16. ¿ Qué protocolo utiliza ?

a. Protocolo IS-IS.
b. Protocolo OSPF.
c. Protocolo RIP.

142. Enumera al menos 2 limitaciones del protocolo RIPv1

143. ¿ Cómo es el sistema de envío que proporciona UDP ?

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

144. ¿ En qué se mide el campo de longitud de un mensaje UDP ?

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

145. ¿ Cuál es el valor mínimo del campo de longitud de UDP ?

a. 0 octeto
b. 8 bytes.
c. 64 bytes.

146. ¿ Qué tipo de mecanismo de Ventana deslizante utiliza UDP ?

147. ¿ Cómo se denominan los mensajes UDP ?

a. Tramas UDP.
b. Paquetes UDP.
c. Bloques UDP.
d. NAEC.

148. El campo checksum de la cabecera UDP...
a. Es recomendable
b. Es opcional
c. Ambas respuestas son ciertas

149. Cuando se transmite un datagrama UDP, ¿ se transmite la psuedocabecera ?
a. Si.
b. No.
c. A veces.

150. El objetivo de la pseudocabecera de un mensaje UDP es :
a. Verificar que en un datagrama UDP todos los campos están rellenos.
b. Verificar que un datagrama UDP ha llegado a su destino correcto.
c. NAEC.

151. ¿ Dónde se encapsula el protocolo UDP ?

152. En los 8 primeros bytes de la parte de datos de un datagrama IP que transporta un datagrama UDP , ¿ qué hay ?

153. ¿ En qué parte de un datagrama UDP se transmite la pseudocabecera ?
a. En la cabecera
b. En la cola
c. En los datos
d. NAEC.

154. En la pseudocabecera el campo de longitud de un datagrama, ¿ qué contiene ?
a. La longitud del datagrama UDP sin incluir la cabecera.
b. La longitud del campo de datos del datagrama UDP.
c. La longitud del datagrama UDP incluyendo la pseudocabecera.

155. Cuando UDP recibe un datagrama y el nº de puerto de destino no se ajusta a ningún puerto de los que está en uso, envía un mensaje de error ICMP de
a. Puerto no existente.
b. Datagrama perdido.
c. Puerto no alcanzanzable.

156. En TCP/IP, los valores altos de los puertos se asignan :
a. Dinámicamente.
b. Estáticamente.
c. Mediante la asignación de puertos bien conocidos.

157. Cuando la cola asociada a un puerto UDP se satura, los datagramas se descartan. ¿ Qué tipo de mensajes se devuelven ?
a. Puerto no alcanzable.
b. Puerto con cola saturada.
c. Indisponibilidad del S.O.
d. NAEC.

158. ¿ Cómo es el servicio que proporciona TCP ?
a. Fiable y no orientado a la conexión.
b. Fiable y orientado a la conexión.
c. No fiable y no orientado a la conexión.

159. ¿ Cómo se llaman las unidades de datos de protocolos de TCP ?
a. Segmentos.
b. Datagramas.
c. Paquetes.

160. ¿ Cuándo se produce un "timeout" en TCP ?
a. Cuando se acaba un tiempo de espera después de mandar un segmento de fin.
b. Cuando no lleva reconocimiento positivo de un segmento.
c. Cuando se manda un mensaje de datos urgente.

161. El protocolo TCP define :
a. Los rendimientos para verificar que los datos lleguen correctos.
b. Esquema para distinguir entre distintos destino en un sistema.
c. Procedimientos de recuperación de datos perdidos o corrompidos.
d. Formato de datos y reconocimientos
e. Procedimientos de inicio y liberación de la conexión.

162. Un socket se define por :
a. Una dirección IP y un puerto.
b. Un par de direcciones IP y esos 2 puertos.
c. Un puerto.
d. Una dirección IP.

163. Enuncia similitudes entre TCP y UDP :

164. Diferencias entre TCP y UDP :

165. ¿ En qué fase se utiliza el flag FIN ?

166. ¿ En qué fase se utiliza el flag SYN ?

167. ¿Cuántos diferentes flags se pueden definir en la cabecera TCP ?

168. ¿ Cuántos tipos de opciones pueden definirse en la cabecera TCP ?

169. ¿ Qué opción es pareceida a una de las de IP ?

170. ¿ Qué tamaño mínimo tienen las cabeceras de una datagrama IP y un segmento TCP ?

171. ¿ Cuánta información de control posee un datagrama IP, que tiene encapsulado un segmento TCP ?

172. ¿ En qué se mide la cabecera de los segmentos TCP ?
a. En bytes.
b. En palabras de 16 bits.
c. En palabras de 32 bits.

173. La recepción de un segmento FIN significa...
a. Que no habrá más datos en ese sentido.
b. Que la conexión entre ambos extremos ha concluido.
c. NAEC.

174. El uso del campo "puntero urgente", ¿ es válido ?
a. Siempre.
b. Sólo cuando el flag URG está activado.
c. No existe dicho campo en la cabecera TCP.

175. El puntero urgente, ¿ a qué señala ?
a. Al comienzo de la zona de los datos urgentes.
b. Al último byte de la zona de los datos urgentes.
c. Al centro de la zona de datos urgentes.

176. El tamaño de la ventana...
a. Es fijo, y es de 65535 bytes.
b. Su límite es de 65535 bytes, y se puede extender.
c. Su límite es de 65535 bytes y no se puede extender.

177. Un proceso puede estar en el estado FIN_WAIT_2 ...
a. como máximo 4 segundos.
b. Al menos 4 segundos.
c. Indefinidamente.

178. ¿ Quién realiza la apertura activa en TCP ?

179. ¿ Quién realiza la apertura pasiva en TCP ?

180. ¿ Qué relación hay entre el nº de segmentos intercambiados en la fase 1 y 3 en una conexión TCP ?

181. El mecanismo de control de flujo que utiliza TCP es :
a. CRC-32 → Control de errores en nivel MAC.
b. Ventana deslizante.
c. Aloha ranurado → Protocolo de nivel MAC

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

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

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

185. Un temporizador de persistencia...
a. Permite transmitir información acerca de 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.
c. Se emplea para detectar que el otro extremo de la conexión se ha desconectado.

186. Un temporizador de retransmisión...
a. Permite transmitir información acerca de 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.
c. Se emplea para detectar que el otro extremo de la conexión se ha desconectado.

187. Un temporizador de subsistencia...
a. Permite transmitir información acerca de 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.
c. Se emplea para detectar que el otro extremo de la conexión se ha desconectado.

188. En la cabecera de un segmento TCP, ¿ existe algún campo para poder incrementar el tamaño máximo de la ventana ?

189. ¿ Cuáles son las técnicas para mejorar el problema de la transmisión en tiempo real ?
a. Streaming y Buffering.
b. Compresión y Buffering.
c. Estándar H323 y Compresión.

190. 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.

191. 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.

192. El protocolo RTP permite el envío...
a. Unicast.
b. Multicast.
c. Ambas respuestas son ciertas.

193. En Internet, ¿ qué es lo que más se ne3cista a la hora de transmitir multimedia ?

194. ¿ Qué protocolo utiliza típicamente TRP como medio de transporte?
a. UDP.
b. TCP.
c. SMTP.

195. "El tipo de paquete RR utiliza estadísticas de transmisión y recepción de participantes que no actúan como emisores activos (Protocolo RTCP)".
a. No
b. Sí.
c. A veces.

196. ¿ De qué se compone la cabecera de los paquetes RTP ?
a. Marca de tiempo, nº paquete, tipo de formato, ID de la fuente de sincronización e ID de otras fuentes.
b. Tipo de enlace, ID de la fuente de sincronización, marca de tiempo, nº de reconocimiento e ID de otras fuertes que aportan datos.
c. ID de enlace, tipo de formato, marca de tiempo, ID de otras fuentes y nº de paquete.

197. ¿ Qué tipo de puertos utiliza el protocolo RTP ?
a. Valores mayores de 7000.
b. Valores enteros impares.
c. NAEC.

198. ¿ Qué formato de los paquetes RTSP está relacionado con una petición ?
a. Setup.
b. Pause.
c. PLAV.
d. Describe.

199. ¿ De qué se encarga un "resolver" ?
a. De contador con uno o más servidores de nombres para efectuar la conversión de nombre a dirección solamente.
b. De contador con un único servidor de nombres para efectuar la conversión de nombre a dirección, y viceversa.
c. De contador con uno o más servidores de nombres para efectuar la conversión de nombre a dirección, y viceversa.

200. ¿ Cuándo debe convertir la aplicación el nombre en una dirección IP ?
a. Antes de solicitar a TCP que establezca una conexión.
b. Antes de solicitar a UDP que envíe un datagrama.
c. Ambas respuestas son correctas.

201. ¿ De cuántos caracteres consta la etiqueta de un nodo DNS ?
a. > 65
b. 48
c. 63

202. Se denomina un nombre de dominio absoluto o completamente cualificado aquel que...
a. Termina con un punto.
b. No termina con un punto y no se necesita ser completado.
c. Termina con un punto y necesita ser completado.

203. Las áreas en las que se dividen los dominios de más alto nivel en DNS son...
a. Dominios genéricos, organizacionales y de país.
b. ARPA, dominios organizacionales y geográficos.
c. ARPA, dominios genéricos y organizacionales.

204. ¿ Cuál es el proveedor de servicio de DNS ?

205. Si observamos un dirección "UPV.ES", ¿ a qué hace referencia ?

206. ¿ Qué es una zona en DNS ?
a. Un conjunto de dominios genéricos.
b. Un sub-árbol administrado separadamente.
c. Un sub-árbol administrado conjuntamente con el resto de los sub-árboles.

207. ¿ Cuántos servidores puede tener como mínimo una zona ?
a. 1 : Uno primario.
b. 2 : uno primario y otro secundario.

c. 3 : uno primario y otro secundario.

208. En DNS, ¿ Qué tiene que hacer el administrador cada vez que se añade un nodo a una zona ?

a. Agregar el nombre del nodo al disco del sistema primario solamente.
b. Agregar la dirección IP del nodo al disco del sistema secundario.
c. NAEC.

209. Los mensajes DNS...

a. Hay uno sólo definido para consultas y respuestas.
b. Hay varias definidas : unos para respuestas, y otros para consultas.
c. NAEC.

210. Cuando el bit TC, en un mensaje DNS, 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 512 bytes.
b. Con UDP indica que el tamaño total de la respuesta excedía de 512 bytes, por lo que no se han podido transmitir.
c. Con TCP indica que el tamaño total de la respuesta excedía de 512 bytes, por lo que no se han podido transmitir.

211. En DNS, 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 de opción si está a 2.

212. En los mensajes DNS, ¿ qué posición ocupa el campo de checksum ?, ¿ cuál es el procedimiento del cálculo del checksum ?

213. La cabecera de un mensaje DNS, ¿ es de longitud fija o variable ?, ¿ cuál es, en octetos, su longitud ?

214. En DNS, una pregunta inversa es equivalente a ...

a. Una pregunta de tipo “a”.
b. Una pregunta de tipo puntero.
c. Una pregunta de tipo estándard.

215. En DNS, si el tipo de pregunta es de tipo “a”...

a. Se busca el nombre correspondiente a una dirección IP.
b. Se busca la dirección IP correspondiente al nombre preguntado.
c. NAEC.

216. En el protocolo DNS, respuesta, autoridad e información adicional...

a. Tienen el mismo formato, y este se denomina “Registro de Recurso”.
b. Tienen el mismo formato, y este se denomina “Registro de Autorizado”.
c. Tienen diferente formato..

217. La caché que emplean todos los servidores de nombres para reducir el tráfico DNS en Internet, se mantiene en...

a. El resolver.
b. El servidor.
c. El cliente.

218. Una notificación con el bit TC puesto a “1”...

a. Indica que se tiene que volver a enviar la siguiente vez en partes de 512 bytes.
b. Indica que se vuelve a efectuar la misma pregunta empleando TCP.
c. NAEC.

219. ¿ Cuál es la naturaleza interna de una caché ?

220. DNS, ¿ qué proveedor de servicios utiliza ?

221. ¿ Qué son las transferencias de zonas en DNS ?

222. ¿ Cuáles son las ventajas que proporciona el protocolo TELNET ?
a. No proporciona ninguna ventaja.
b. El servidor permite gestionar múltiples conexión concurrentemente.
c. El servidor sólo permite gestionar una conexión para que no se cargue la red.

223. El protocolo TELNET fue diseñado para ...
a. Trabajar entre 2 nodos cualesquiera y con cualquier terminal haciendo uso de una conexión TCP.
b. Trabajar entre 2 nodos específicos y con cualquier terminal haciendo uso de una conexión UDP.
c. Trabajar entre 2 nodos específicos y con un terminal haciendo uso de una conexión UDP.

224. ¿ Soluciona TELNET el problema de la heterogeneidad ?
a. No.
b. Sí, mediante el Terminal Virtual de red NVT.
c. Sí, mediante el Terminal Virtual de red NDT.

225. ¿ El protocolo TELNET, ¿ dónde está ubicado ?, ¿ cuál es su naturaleza : simétrica o asimétrica ?, ¿ dónde se encapsula ?

226. Indicar si la siguiente afirmación es cierta : *"TELNET puede enviar sus comandos de control haciendo uso de la transmisión de datos urgente de UDP"*
a. Sí, sólo si las envía el cliente.
b. Sí, tanto si las envía el cliente como el servidor.
c. No.

227. *" TELNET permite negociar diferentes opciones para configurar por vez primera la conexión entre clientes "*
a. Sí, es cierto.
b. No, TELNET permite negociar diferentes opciones para reconfigurar la conexión entre clientes y servidor.
c. No, TELNET permite negociar diferentes opciones para reconfigurar la conexión entre clientes.

228. La negociación de opciones, ¿ requiere o no intercambio de bits ?
a. No.
b. Sí, requiere 3 bits.
c. No, requiere el intercambio de 3 bytes : el IAC, seguido por una de las siguientes peticiones : WILL, DO, WONT, DONT, y un byte que especifica la opción que debe habilitarse o deshabilitarse.

229. "SE" es el comando de solicitud de :
a. envío del tipo de terminal.
b. No existe este comando en TELNET.
c. envío del cliente.

230. ¿ Cuántos tipos de operaciones tiene TELNET ?
a. Hay 2 tipos : Half-Duplex, y Full-Duplex.
b. Hay 1 tipo : Half-Duplex.
c. Hay 4 tipos : Half-Duplex, un carácter cada vez, una línea cada vez, y modo línea.

231. El modo Half-Duplex :
a. Es el más habitual en la actualidad.
b. No resulta habitual para los terminales Full-Duplex actuales.
c. No se hace echo local de los caracteres.

232. En el modo de operar "un carácter cada vez", los problemas que se producen son :
a. Los retrasos introducidos por el eco.
b. El volumen de tráfico que se genera.
c. Ambas respuestas son correctas.

233. ¿ Quién envía en TELNET "escapes" ?
a. El servidor.
b. El cliente.
c. Ambos.

234. ¿ Cuál es el protocolo más antiguo ?
a. R-Login.
b. Login-Remoto.
c. TELNET

235. FTP nos permite ...
a. Mover ficheros.
b. Acceder a ficheros.
c. Ambas son correctas.

236. ¿ Cuál de los siguientes servicios no es proporcionado por FTP ?
a. Interacción con servidores remotos.
b. Validación de la identificación de usuarios.
c. Transferencia del contenido de un fichero.
d. Validación de los datos del fichero.

237. ¿ Dónde está ubicado FTP ?

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

239. Indicar cuál de las siguientes afirmaciones es correcta :
a. " Mediante la conexión de control de TCP se envían comandos y mediante la conexión de datos se envían respuestas."
b. " Mediante la conexión de datos se transfieren ficheros y se creará una conexión de datos cada vez que se transmite un fichero."
c. " Las conexiones de control y de datos se crean cada vez que se vaya a transmitir un fichero. "

240. ¿ Cuándo se da por terminado el proceso de transmisión de ficheros ?
a. Cuando desaparecen las conexiones de datos y control.
b. Cuando desaparecen las conexiones de control.
c. Cuando desaparecen las conexiones de datos.

241. ¿ Quién realiza una apertura activa para establecer la conexión de control ?
a. El cliente.
b. El servidor.
c. El entorno TCP / IP.

242. ¿ Cuál es el nº de puerto utilizando en la apertura pasivo por parte de un servidor FTP?
a. Mal conocido.
b. Definido por el administrador de red.
c. NAEC:

243. Si no se indica la contrario, los datos transmitidos por FTP...
a. Se transmitirán de forma comprimida.
b. Se transmitirán de forma comprimida y con estructura de fichero.
c. Se transmitirán con estructura de fichero.

244. ¿ Es posible transmitir un fichero con estructura de registro en modo continuo ?
a. Sí, si se indica en fin de cada registro con un código.
b. No.
c. Sí, si se numeran los registros.

245. ¿ Cuál es la diferencia entre un comando de FTP y una respuesta FTP ?
a. Un comando se dirige del cliente al servidor y una respuesta en sentido inverso.
b. Un comando se transfiere por la conexión de control y una respuesta por la de datos.
c. NAEC.

246. ¿ Puede el cliente enviar un fichero al servidor ?
a. No.
b. Sí.

247. ¿ Cómo se puede evitar el tener que mandar respuestas multilíneas por la conexión de control ?
a. Enviando ficheros de tipo local mediante la conexión de datos.
b. Enviando listas de ficheros mediante la conexión de datos.
c. Enviando ficheros en modo bloque.

248. ¿ Qué 2 puertos bien conocidos utilizan los servidores FTP para la apertura pasiva y la activa ?

249. ¿ Qué protocolos son utilizados por estaciones sin disco ?
a. RARP.
b. BOOTP.
c. TCP

250. ¿ En qué protocolo se basa BOOTP ?
a. UDP y TCP.
b. ICMP y TCP.
c. UDP e IP.

251. ¿ Qué campo incorpora como innovador el formato de los mensajes del protocolo BOOTP ?
a. Dirección IP del Cliente.
b. Información específica del vendedor.
c. Dirección hardware del cliente.

252. ¿ Cuántos y cuáles son los puertos reservados para BOOTP, y para qué se emplea ?
a. Un puerto, que es el nº 67 para el servidor.
b. Dos puertos, que son el nº 67 para el servidor y el nº 68 para el cliente.
c. Dos puertos, que son el nº 69 para el servidor y el nº 68 para el cliente.

253. ¿ Para qué es utilizado BOOTP ?
a. Para mejorar las diferencias de UDP e IP.
b. Para solucionar los problemas de RARP.
c. Las 2 anteriores son ciertas.

254. ¿ Qué contiene el campo de información específico del vendedor ?
a. La dir. IP 88.130.83.99, PAD, máscara de subred y time-offset.
b. PAD, mascara de subred y time-offset.
c. NAEC.

255. ¿ Para qué se utiliza DHTP ?
a. Para conseguir información adicional además de la propia IP.
b. Para enviar información de configuración a máquinas de una red TCP/IP.
c. Para conseguir un acoplamiento entre BOOTP y ARP.

256. ¿ Cuántos tipos de asignación IP existen en el protocolo de asignación de direcciones IP ?
a. Asignación dinámica y manual.
b. Asignación automática, dinámica y manual.
c. Asignación automática, dinámica, manual e inteligente.

257. ¿ Qué mecanismo de asignación permite la reutilización de direcciones IP ?
a. Asignación automática.
b. Asignación manual.
c. Asignación dinámica.

258. ¿ Cuál es el campo más importante del formato DHCP ?
a. Dirección hardware del cliente.
b. Dirección IP del cliente - servidor.
c. Dirección IP del cliente.

259. ¿Cuál de las siguientes afirmaciones es cierta ?
a. ” Un servidor DHCP intenta asignar siempre una misma dirección IP a una máquina. “
b. “ El cliente debe incluir su dirección hardware para que el servidor pueda buscar la dirección IP.“
c. “ La información sobre el tiempo de alquiler se incluye en el campo nº de segundos.“

260. ¿ Todas las direcciones hardware son iguales ?

261. ¿ Mediante qué tipo de conexión se realiza una conexión SMTP ?
a. POP3
b. IP
c. TCP

262. ¿ Para qué se utiliza SMTP, TCP ?
a. Para establecer una conexión mucho más rápida.
b. Para garantizar la fiabilidad de intercambios.
c. Para garantizar la entrega al usuario correcto.

263. ¿ Qué indica el sobre de un mensaje al MTA ?
a. El contenido y la interpretación para intercambio de correo a través de una conexión TCP.
b. Argumentos a emplear por MAIL y RCPT.
c. Ambas respuestas son correctas.

264. ¿ Qué puertos bien conocidos se utilizan en SMTP ?

265. ¿ Qué tipo de apertura realizan cliente y servidor en SMTP ?

266. ¿ Qué se ha definido para permitir la transmisión de datos no ASCII ?
a. MTU ASCII.
b. MIM
c. ESMTP.

267. ¿ Qué puerto utiliza POP3 ?
a. 110.
b. 25.
c. Ambas respuestas son correctas.

268. ¿ Por qué están formados os comandos POP3 ?
a. Palabras clave y argumento.
b. Palabras clave, argumento y por CRCF (Retorno de Carro Salto de Línea).
c. Palabras clave, argumento, por CRCF y por ERR.

269. ¿ Por qué estados progresa POP3 ?
a. Estado de autorización y transacción.
b. Estado de autorización, transacción y actualización.
c. Estado de autorización y actualización.

270. ¿ Cuáles son las etiquetas más importantes de un documento HTML ?
a. <HTML>, <AHREF> y <APPLET>.
b. <H1>, <BODY> y <ABRRES>.
c. <HEAD>, <UL> y <SCRIPT>.
d. NAEC.

271. ¿ Para qué sirven las hojas de estilo (CSS) ?
a. Para crear formularios.
b. Para añadir efectos dinámicos a la página.
c. Para aumentar el control del diseñador sobre sus páginas.

272. ¿ Para qué sirve HTTP ?
a. Para transferir datos en tiempo real.
b. Para transferir documentos del tipo hypertext.
c. NAEC.

273. ¿ Diferencias entre HTTP v1.0 y HTTP v1.1 ?
a. Por defecto, la v1.1 mantiene la conexión para hacer peticiones adicionales.
b. En la v1.1 se han introducido formularios.
c. La v1.1 introduce formas de cifrar los datos.

274. ¿ Qué se utiliza para guardar estados HTTP ?
a. Applets.
b. Cookies.
c. Cakes.

275. Una petición HTTP se forma tecleando ...
a. Método, URI y versión de HTTP.
b. Método y URI.
c. Método, URI y opcional versión de HTTP.

276. ¿ Cuál es el error más común en HTTP?, ¿qué indica ?
a. 501.
b. 404.
c. 302.

277. ¿ Cuál de las siguientes afirmaciones son correctas ?
a. *"El procesamiento del Applet se visualiza en el cliente"*.
b. *"El código es multiplataforma"*.
c. *"Se pueden hacer animaciones"*.

278. ¿ Cuál es el proveedor de servicios de http ?

279. ¿ Cuál es la diferencia para indicar código JSP o ASP dentro de un fichero HTML?
a. JSP utiliza <%%código%%> y ASP utiliza <&código%>.
b. ASP utiliza <<código>> y JDP utiliza <&código%>.
c. Ambas utilizan <&código%>.

280. ¿ Para qué se puede utilizar el lenguaje PERL ?
a. CGI.
b. Applets.
c. JSP.
d. ASP.

281. ¿ Cuál es la mayor ventaja de JSP ?
a. Para acceder a BBDD a través de ODBC.
b. Es utilizado extensamente.
c. Puede utilizar el API de Java.p

282. El standard de seguridad que proporciona la arquitectura de comunicaciones base para la interconexión de sistemas abiertos es :
a. ISO-7498-1.
b. ISO-7598-1.
c. ISO-7498-2 / X.800

283. La falsificación de objetos con la intención de suplantar a una entidad en un sistema de redes de computadores se llama...
a. Interrupción.
b. Interceptación.
c. Modificación.
d. Fabricación.

284. Cuando un elemento estratégico del sistema se elimina o está inutilizable o indisponible debido a una amenaza, estamos hablando de...
a. Interrupción.
b. Interceptación.
c. Modificación.
d. Fabricación.

285. Cuando alguien obtiene acceso no permitido a un factor restringido bajo normas de seguridad, está materializando una amenaza del tipo...
a. Interrupción.
b. Interceptación.
c. Modificación.
d. Fabricación.

286. La seguridad del mecanismo de cifrado simétrico depende de...
a. La potencia y robustez del algoritmo de cifrado / descifrado y del secreto de la clave.
b. Del secreto de la clave y del secreto del algoritmo utilizado.
c. La potencia y robustez del algoritmo de cifrado / descifrado y del secreto del algoritmo utilizado.

287. El mecanismo de cifrado asimétrico...
a. Precisa distribuir las claves de una forma segura.
b. No precisa distribuir las claves de una forma segura.
c. Es más complejo y menos lento que el cifrado simétrico.

288. ¿ cuál es la diferencia entre cifrado y descifrado simétrico y asimétrico ?
a. * Asimétrico : una llave para cifrado y descifrado.
   * Simétrico : una llave para cifrado (pública) y otra para descifrado (privada).
b. * Asimétrico : una llave para cifrado y descifrado.
   * Simétrico : una llave para cifrado (pública) y otra para descifrado (privada).
c. NAEC.

289. ¿ Cuál es la diferencia entre mecanismos de seguridad específicos y generalizados ?
a. Los específicos se incorporan a un nivel determinado OSI y los generalizados no.
b. Los generalizados se incorporan a un nivel determinado OSI y los específicos no.
c. NAEC.

290. ¿ Cuáles de las siguientes afirmaciones sobre autenticación de mensajes son correctas ?
a. La parte de datos de un mensaje no es cifrado.
b. El emisor y el receptor tienen la misma clave.
c. Protege contra ataques pasivos.

291. ¿ Qué requisitos debe cumplir un sistema seguro multinivel ?
a. No lectura hacia arriba y no escritura hacia abajo.
b. No lectura hacia abajo y no escritura hacia arriba.
c. No lectura hacia arriba y escritura hacia abajo.
d. NAEC.

292. ¿ Cuál de las siguientes acciones de recuperación es temporal ?
a. Deshabilitar el login durante 5 minutos.
b. Desconectar el ordenador de la red.
c. Creación de una lista negra.

293. ¿ Cómo se puede mejorar la seguridad de un esquema de passwords ?
a. Con un registro de intentos inválidos.
b. Utilizando contraseñas alfanuméricas.
c. Con una desconexión automática tras haberse realizado intentos inválidos.
d. Todas son verdaderas.

294. ¿ Cuáles de las siguientes afirmaciones sobre la firma digital directa son correctas ?
a. La parte de datos de un mensaje no es cifrado.
b. El emisor y el receptor tienen la misma clave.
c. Es el mecanismo que utiliza PGP.

295. ¿ Cuáles de las siguientes afirmaciones sobre la firma digital arbitraria son correctas ?
a. Protege las 2 partes de una comunicación (emisor y receptor) una de la otra.
b. Permite la selección de rutas particulares para el mensaje.
c. Los mensajes tienen que pasar por un notario.

296. El origen de SNMP fue...
a. A mediados de los 90.
b. A mediados de los 80.
c. NAEC.

297. SNMP es...
a. Un sistema orientado a la conexión.
b. Un sistema no orientado a la conexión.
c. Ambas respuestas son correctas.

298. La gestión TCP / IP...
a. Tiene 3 elementos : MIB, SMI y SNMP.
b. Tiene 2 elementos : MIB y SMI.
c. Tiene 1 elemento : SNMP.

299. ¿ Qué PDU es de SNMP versión 2 ?
a. Get-bulk-request.
b. Get-request.
c. Response.

300. Si el campo versión de un mensaje SNMP vale 0 ...
a. Corresponde a SNMP versión 1.
b. Corresponde a SNMP versión 2.
c. No puede valer 0.

301. El campo "Enterprise" de una PDU Trap...
a. Identifica el software agente que generó la PDU trap.
b. Indica la dirección IP de la estación remota.
c. Contiene información adicional del evento.

302. Los indicadores de objeto...
a. No están definidos en ANS.1
b. Son únicos y son un entero.
c. Son únicos y son una secuencia de enteros.

303. BER ...
a. Necesita que se entienda el contexto de la información.
b. Es explícito y ambiguo.
c. Codifica los datos precedidos por un campo tipo y longitud.

304. Los objetos definidos por la MIB...
a. Están organizados en grupos obligatorios para todos los componentes.
b. Están organizados en grupos no obligatorios para todos los componentes.
c. No están organizados en grupos y no son obligatorios para todos los componentes.

305. ¿ Cuál es la dirección de los Trap ?

306. Para su identificador de instancia de las entradas de una tabla...
a. Se hace referencia a las variables simples añadiendo "0" al identificador de objeto de la tabla.
b. Se utiliza un índice asociado a cada tabla.
c. Se utiliza un índice para todas las tablas.

307. ¿ De qué elementos consta la gestión de red en TCP / IP ?

308. El monitor remoto debe ser configurado para captar datos especificando...
a. El tipo de datos.
b. El tipo de datos y la forma en que van a ser recogidos.
c. NAEC.

309. ¿ Cómo establece la estación de gestión los parámetros ?
a. Borrando filas en la tabla de control.
b. Mediante adición y modificación de filas en la tabla de control.
c. Mediante adición y modificación de filas en la tabla de datos.

310. ¿ Qué tiene que contener la etiqueta de propiedad ?
a. No necesita nada.
b. Optativamente, tiene que contener las direcciones IP, nombre de la gestión, nombre de la estación de red, localidad o nº de teléfono.
c. Tiene que contener obligatoriamente todas las opciones de (b)

311. En la SNMP versión 1, ¿ el campo de comunidad está cifrado o no ?

312. ¿ De cuántas partes está compuesta una petición del cliente o respuesta del servidor en el protocolo http ?
a. De 3 partes : Cabecera, título y cuerpo.
b. De 3 partes : Línea de petición o respuesta, cabecera y cuerpo.
c. De 2 partes : Cabecera y cuerpo.

313. Si la petición del cliente no ha tenido éxito...
a. El servidor se desconecta automáticamente.
b. Los datos pedidos no se envían.
c. Se envía una explicación de la causa del fallo.

314. ¿ Qué categorías de cabecera existen ?
a. 2 → petición y respuesta.
b. 3 → GET, HEAD y POST.
c. 4 → Petición, respuesta, general y entidad.

315. Los tipos y subtipos se utilizan para indicar...
a. El tipo de cliente y servidor.
b. El formato del contenido.
c. El formato de la cabecera.

316. ¿ Cuál es el nº de estados del protocolo HTTP ?
a. 5.
b. 9.
c. NAEC.

317. ¿ En qué se diferencian los métodos GET y HEAD ?
a. Son totalmente diferentes.
b. Con el método HEAD, el servidor no envía nada en el área de datos de la respuesta.
c. La información de cabecera de una petición HEAD será diferente que la de una petición GET.

318. La primera línea de respuesta de un servidor HTTP indica...
a. Información de cabecera acerca de él mismo.
b. Estado del servidor.
c. Petición con éxito o no.

319. La desventaja del método GET en CGI es que...
a. No es tan rápido ni tampoco sencillo de implementar.
b. El tamaño de lo que enviamos debe ser limitado.
c. NAEC.

320. La sobrecarga es tratada mediante...
a. Applets.
b. CGI's

c. La sobrecarga no puede ser tratada.

321. En el caso de los applets de JAVA...
a. Se reciben los programas, el cliente los instala, y se ejecutan.
b. El cliente recibe los programas, se instalan automáticamente, y se ejecutan.
c. NAEC.

322. En el caso de ASP, el cliente recibe...
a. Código HTML y código ASP.
b. Se puede dar el caso de que sólo reciba código ASP.
c. Sólo código HTML.

323. ¿ Dónde se situarían las técnicas de backup ?

324. ¿ Qué dos direcciones tiene asociadas un dispositivo de red ?
a. IP (por cada interfaz 48 bits) y Dirección Física.
b. IP (por cada interfaz 32 bits) y Dirección Física.
c. Son 3 → IP (por cada interfaz 48 bits), Dirección Física y MAC.

325. La caché ARP tiene de vida, como máximo...
a. 10 minutos.
b. 15 minutos.
c. 20 minutos.

326. Al proxy ARP se le conoce también como...
a. ARP promiscuo.
b. ARP Hacker.
c. ARP Hack.

327. ¿ Quién puede hacer uso de los mensajes ?
a. IP y sus niveles superiores.
b. IP y sus niveles inferiores.
c. Todos lo9s niveles de TCP / IP.

328. El campo "checksum" perteneciente a todos los mensajes ICMP...
a. No es necesario, pero es muy útil para comprobar los mensajes.
b. Comprueba la parte más importante del mensaje ICMP que lo contiene.
c. Se codifica según el algoritmo utilizado en la cabecera IP.

329. ¿ Qué información contiene el campo "datos opcionales" de la ICMP de los mensajes de petición y respuesta de eco ?
a. Los campos identificador, nº de secuencia y los datos opcionales enviados por el cliente.
b. El campo de datos y nº de secuencia del cliente con datos nuevos.
c. El campo identificador y checksum para comprobar el mensaje completo.

330. ¿ Cuál de los siguientes mensajes ICMP no contiene en su formato un campo con la cabecera IP + los primeros 8 octetos del datagrama ?
a. Mensaje de petición de router.
b. Mensaje de congestión y flujo.
c. Mensaje de destino no alcanzable.

331. ¿ Qué longitud tienen los mensajes ICMP ?
a. 16 bits.
b. 4 octetos.
c. 32 bytes.

332. ¿ Para qué se emplea el campo puntero en un mensaje de problema parametrizable ?
a. Para reconocer qué datagrama originó el error.
b. Para reconocer qué octeto del datagrama originó el error.
c. Para reconocer qué nodo originó el error.

333. ¿ Quién completa el "timestamp" de origen en un mensaje de sincronización de reloj en ICMP ?

a. El receptor.
b. El router.
c. El emisor.

334. ¿ Cuál es el fin del "número de secuencia" del mensaje para la obtención de la máscara de subred ?

a. Se envía como pregunta.
b. Se envía como respuesta.
c. Se envía como orden de los datagramas de respuesta.

335. ¿ Cuál de estos no es un servicio proporcionado por IP multicasting a una aplicación ?

a. Envío de datagramas a destinos múltiples.
b. Envío de múltiples datagramas a un destino.
c. Solicitud de servidores por parte de los clientes.

336. ¿ Cuál de estas no es una característica de un grupo multicast ?

a. La pertenencia a un grupo es dinámica y además los nodos pueden encontrarse en redes distintas.
b. El nº de miembros de un grupo multicast es muy reducido.
c. Pueden tener asignada una dirección permanente.

337. ¿ En qué casos se manda un mensaje de notificación IGMP ?

a. Al agregarse o abandonar un grupo.
b. Al abandonar un grupo.
c. Al agregar un grupo.

338. ¿ Para qué sirve el campo "código" de un protocolo IGMP ?

a. Redireccionar datagramas hacia un nodo de destino.
b. Redireccionar datagramas hacia una red de destino.
c. NAEC.