Universidad de Alcalá

Fecha: 13 de mayo de 2014

DEPARTAMENTO DE AUTOMÁTICA
ARQUITECTURA Y TECNOLOGÍA DE COMPUTADORES

Grado en Ingeniería Informática

REDES DE COMPUTADORES

Prueba de conjunto. Test

- **Cada afirmación correctamente contestada vale 0,05 puntos y cada fallo descuenta 0,025.**

Contestar las siguientes cuestiones marcando V (verdadero) o F (falso):

1. En las redes de circuitos virtuales, dos routers pueden establecer una conexión al nivel de la capa de red.
2. Un router realiza la función de *reenvío* y, opcionalmente, la función de *enrutado*.
3. Una máscara de red `255.255.248.0` indica que se reservan 12 bits para la dirección de los *hosts* y 20 bits para la dirección de la subred.
4. Uno de los problemas de tener una red detrás de un router NAT es que no es útil para instalar servicios en ella, pues no es técnicamente posible encaminar el tráfico desde internet hacia dichos servicios.
5. Si un router anuncia la ruta `188.45.18.0/23` y otro distinto anuncia la ruta `188.45.16.0/20` estamos ante un error en el protocolo de enrutamiento.
6. Los paquetes de descubrimiento DHCP lanzados por un cliente llevan `255.255.255.255` como dirección IP fuente y `0.0.0.0` como dirección IP destino.
7. El valor MTU (*maximum transmission unit*) es un parámetro asociado a una ruta determinada e indica el tamaño máximo que pueden tener los datagramas para poder recorrerla.
8. El campo de *longitud del datagrama IP* tiene un tamaño de 16 bits por lo que un datagrama no puede superar $2^{16} - 1$ bytes.
9. Cuando un datagrama llega a su destino, el campo TTL (*tiempo de vida*) de la cabecera IP siempre ha de tener el valor 0.
10. En el anuncio de una ruta mediante el protocolo BGP, el atributo AS-PATH contiene una lista de los sistemas autónomos que esa ruta ha atravesado hasta el momento.
11. Una trama del protocolo de enlace puede encapsular tanto paquetes del protocolo ICMP como paquetes del protocolo ARP.
12. La corrección de errores con *paridad par* permite detectar, como su nombre indica, un número *par* de errores en los bits transmitidos.
13. Si el polinomio generador en un código CRC tiene grado r entonces el código corrector que se añade a los datos tiene $r+1$ bits.

14. Los protocolos de acceso al medio por división en tiempo (TDM) y por división en frecuencia (FDM) tienen iguales ventajas e inconvenientes, excepto que en FDM todos los nodos pueden enviar datos a la vez, mientras que TDM no lo permite.

15. El protocolo ALOHA puro es más eficiente que el ALOHA con particiones porque permite a los nodos emitir en cualquier momento.

16. El diseño de los protocolos de la capa de enlace es dependiente del tipo de enlace considerado.

17. En el protocolo BGP los destinos no son hosts sino prefijos CIDR.

18. Un conmutador puede evitar siempre las colisiones entre cualesquiera de los nodos que tenga conectados a sí.

19. Para que dos vectores-código en CDMA sean ortogonales es condición necesaria y suficiente que, al comparar bit a bit los dos vectores, se encuentre que el número de bits que tienen igual signo es igual al número de bits que tienen signo opuesto.

20. El diseño del protocolo CSMA/CA que se utiliza en IEEE 802.11 establece que para minimizar colisiones, se podrán utilizar opcionalmente tramas de tipo RTS/CTS.

21. El servicio de autenticación mutua entre emisor y receptor significa que ambos pueden estar seguros de la identidad de su interlocutor.

22. Los sistemas de clave pública han de ser resistentes a los ataques al texto claro elegido.

23. En la fase de acuerdo de una conexión SSL, el cliente y el servidor intercambian sus certificados.

24. Sea H una función resumen. Para autenticar al emisor de un mensaje m, basta con que el receptor reciba el par $(m, H(m))$.

25. Si en una red *Token Ring*, el perímetro es muy grande, mejora sensiblemente la eficiencia de la red.

26. Las tramas de Ethernet 10BASE-T, 100BASE-T y Gigabit no se diferencian en nada.

27. El espacio de direcciones MAC es tiene un tamaño de 2^{46} direcciones.

28. El número máximo de redes VLAN que pueden configurarse en un computador que soporta el protocolo 802.1Q es de 2^{12}.

29. La cuarta dirección MAC que incluye la trama IEEE 802.11 se emplea únicamente para redes *ad hoc*.

30. En el protocolo IEEE 802.11i están separados el servidor de autenticación y el punto de acceso.

Universidad de Alcalá

Nombre:

Fecha: 13 de mayo de 2014

DEPARTAMENTO DE AUTOMÁTICA
ARQUITECTURA Y TECNOLOGÍA DE COMPUTADORES

Grado en Ingeniería Informática
REDES DE COMPUTADORES

Prueba de conjunto. Problemas

- **Cada problema debe resolverse en el espacio reservado para ello y vale 0,5 puntos.**

Problema 1

Sea un medio compartido en el que están presentes solamente dos nodos, A y B, separados una distancia d. La velocidad de propagación de la señal en ese medio es v. Cada nodo emite a una velocidad de transmisión R. La longitud de las tramas es igual a L.

Se utiliza el protocolo puro CSMA/CD donde cada nodo sondea el canal antes de transmitir y, si está libre, empieza la transmisión de manera inmediata. Si durante la transmisión detecta una colisión, interrumpe instantáneamente la transmisión.

En estas condiciones, se pide:

1. Si el nodo A empieza a transmitir en el instante t_0, ¿durante qué periodo de tiempo debiera B estar en silencio para que la transmisión se termine sin colisiones?

2. Si B detecta señal en el canal antes de transmitir, ¿cuánto tiempo debería esperar para tener cierta garantía de encontrar el canal libre?

3. Suponiendo un perfecto acuerdo en las transmisiones de A y de B, de forma que no se produzcan colisiones, ¿cuál sería la eficiencia del canal, es decir, qué porcentaje de tiempo está realizando un trabajo de transmisión útil? Expresarlo en función de d, v, L y R.

Problema 2

La siguiente función iterativa

$$x_{i+1} = a \cdot x_i + b \pmod{m}$$

se puede usar como generadora de bits aleatorios de la siguiente manera:

1. se da un valor inicial x_0, que es la clave;
2. se aplica la función anterior iterativamente cuantas veces se quiera para obtener los valores x_1, $x_2, \ldots$
3. la secuencia de bits aleatorios está constituida por el $\mathsf{LSB}(x_i)$, con $i = 1, 2, \ldots$, es decir, por el bit menos significativo de cada valor x_i.

Se tiene un sistema de cifrado en flujo que usa el generador anterior, usando como parámetros $m = 137$, $a = 5$, $b = 7$. Usando este sistema, Alicia manda a Benito el siguiente mensaje cifrado (expresado en hexadecimal): `FA08`

Para acordar la clave secreta del cifrador en flujo, Alicia cifra dicha clave utilizando para ello la clave pública de Benito, cuyos parámetros son $\{n = 527, e = 37\}$. La clave cifrada que Alicia envía resulta ser (expresada en decimal): `141`

Teniendo en cuenta que los parámetros privados de Benito son: $\{p = 17, q = 31, d = 13\}$, ¿qué mensaje obtendrá Benito al descifrar?

Problema 3

Considerando la red de routers de la figura y utilizando el algoritmo de Dijkstra, se pide:

1. Calcular las rutas de coste mínimo y sus costes desde el nodo w a todos los nodos de la red.
2. Dibujar el árbol de rutas de coste mínimo desde el nodo w.
3. Escribir la tabla de enrutamiento resultante para el nodo w. ¿Qué pasaría si se cortara el enlace $w - s$?