



Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias de la Computación

EJERCICIOS - REDES DE COMPUTADORAS

Profesor:

José Esteban Torres León

Alumnos:

**Ramírez Martínez Zicury
Rojas Palacios Miguel Ángel
Baleón Aguilar Germán**

**PERIODO
VERANO 2012**

 	Benemérita Universidad Autónoma de Puebla
	Facultad de Ciencias de la Computación

EJERCICIOS

1.- Datos generales.

Materia	Intercomunicación Y Seguridad En Redes
Profesor	José Esteban Torres León
No. Alumnos equipo	3
Nombre Alumnos	Ramírez Martínez Zicury, zicuxoco@hotmail.com Rojas Palacios Miguel Ángel, fcc@drogasoft.com Baleón Aguilar Germán, gba_88@yahoo.com.mx
Cuatrimestre	12
Periodo	VERANO 2012

2.- Competencias genéricas y específicas a desarrollar.

Competencia: capacidad que se adquiere mediante un conjunto de conocimientos, habilidades, actitudes y valores que se han puesto en práctica en diversos contextos.

Genéricas
Competencia de Funcionamiento Competencias de aprender y programar Tratamiento de la información y Programación Autonomía e iniciativa personal
Específicas
Competencia matemática Competencia en el conocimiento y la interacción con el mundo natural

3.- Conocimientos, habilidades, actitudes y valores

Elementos requeridos para el logro de las competencias

Conocimientos	Habilidades	Actitudes y valores
Programación	Acceso y selección de la información	Respeto, Creatividad e Iniciativa
Cálculos Matemáticos	Acceso a formulas y resultados	Tolerancia, Iniciativa Y Respeto

4.- Cuerpo de la Tarea.

Titulo Libro	Redes de Computadoras
Titulo del Capitulo	Capitulo 1 - Introducción
No. Ejercicios	32
Fecha de Realización	VERANO 2012

CAPITULO 1

1. Imagine que ha entrenado a su San Bernardo, Byron, para que transporte una caja con tres cintas de 8 mm en lugar del barrilito de brandy. (Cuando se llene su disco, usted tendrá una emergencia.) Cada una de estas cintas tiene capacidad de 7 gigabytes. El perro puede trasladarse donde quiera que usted vaya, a una velocidad de 18 km/hora. ¿Para cuál rango de distancias tiene Byron una tasa de datos más alta que una línea de transmisión cuya tasa de datos (sin tomar en cuenta la sobrecarga) es de 150 Mbps?

R= El perro puede llevar 21 gigabytes, o 168 gigabytes. Una velocidad de 18 km / hora es igual a 0,005 kilómetros / seg. El tiempo necesario para recorrer una distancia km x es $x / 0,005 = 200 \times \text{seg}$, que arrojó una tasa de datos de $168/200 \times \text{Gbps}$ o 840 Mbps o x. Para $x < 5,6 \text{ km}$, el perro tiene una tasa superior a la línea de comunicación.

2. Una alternativa a una LAN es simplemente un enorme sistema de compartición de tiempo con terminales para todos los usuarios. Mencione dos ventajas de un sistema cliente-servidor que utilice una LAN.

R= El modelo de LAN pueden ser cultivadas de forma incremental. Si la LAN es sólo un cable largo. No puede ser derribado por un solo fallo (si los servidores se replican) Se es probablemente más barato. Se proporciona más potencia de cómputo e interactivo más interfaces.

3. Dos factores de red ejercen influencia en el rendimiento de un sistema cliente-servidor: el ancho de banda de la red (cuántos bits por segundo puede transportar) y la latencia (cuánto tiempo toma al primer bit llegar del cliente al servidor). Mencione un ejemplo de una red que cuente con ancho de banda y latencia altas. A continuación, mencione un ejemplo de una que cuente con ancho de banda y latencia bajas.

R= Un enlace de fibra transcontinental podría tener muchos gigabytes por segundo de ancho de banda, pero la latencia también será alto debido a la velocidad de propagación de la luz sobre miles de kilómetros. En contraste, un módem de 56 Kbps llamar a un ordenador en el mismo edificio que tiene poco ancho de banda y baja latencia.

4. ¿Además del ancho de banda y la latencia, qué otros parámetros son necesarios para dar un buen ejemplo de la calidad de servicio ofrecida por una red destinada a tráfico de voz digitalizada?

R= Un tiempo de entrega uniforme que se necesita para voz, por lo que la cantidad de fluctuación en la red es importante. Esto podría ser expresado como la desviación estándar del tiempo de entrega. Tener pequeño retraso, pero una gran variabilidad en realidad es peor que una variabilidad algo más de tiempo de retardo y baja.

5. Un factor en el retardo de un sistema de conmutación de paquetes de almacenamiento y reenvío es el tiempo que le toma almacenar y reenviar un paquete a través de un conmutador. Si el tiempo de conmutación es de 10 μseg , ¿esto podría ser un factor determinante en la respuesta de un sistema cliente-servidor en el cual el cliente se encuentre en Nueva York y el servidor en California? Suponga que la velocidad de propagación en cobre y fibra es $2/3$ de la velocidad de la luz en el vacío.

R= No. La velocidad de propagación es de 200.000 km / seg o 200 metros por microsegundos. En 10 microsegundos que la señal viaja a 2 km. Así, cada conmutador añade el equivalente de 2 km de cable extra. Si el cliente y el servidor están separados por 5000 km, que atraviesa hasta 50 conmutadores se suma a sólo 100 km de la ruta total, que es sólo el 2%. Por lo tanto, conmutación retardo no es un factor importante en estas circunstancias.

6. Un sistema cliente-servidor utiliza una red satelital, con el satélite a una altura de 40,000 km. ¿Cuál es el retardo en respuesta a una solicitud, en el mejor de los casos?

R= La solicitud tiene que ir arriba y abajo, y la respuesta tiene que ir arriba y abajo. La longitud total del trayecto recorrido es, pues, 160.000 kilómetros. La velocidad de la luz en el aire y el vacío es de 300.000 km / seg, por lo que el retardo de propagación por sí sola es $160000/300000 \text{ seg}$ o aproximadamente 533 mseg.

7. En el futuro, cuando cada persona tenga una terminal en casa conectada a una red de computadoras, serán posibles las consultas públicas instantáneas sobre asuntos legislativos pendientes. Con el tiempo, las legislaturas

existentes podrían eliminarse, para dejar que la voluntad popular se exprese directamente. Los aspectos positivos de una democracia directa como ésta son bastante obvios; analice algunos de los aspectos negativos.

R= Obviamente no hay una única respuesta correcta aquí, pero los siguientes puntos parecen relevantes. El sistema actual tiene mucho de inercia (controles y equilibrios) construido en él. Esta inercia puede servir para mantener el desarrollo económico, legal y los sistemas sociales sean un vuelco cada vez que un partido diferente llega al poder. Además, muchas personas tienen opiniones fuertes sobre la polémica cuestiones sociales, sin saber muy bien los hechos de la materia. Permitir a pocos dictámenes motivados a ser escrito en la ley puede ser indeseable. El potencial efectos de las campañas de publicidad por parte de grupos de intereses especiales de un tipo u otro también tienen que ser considerados. Otra cuestión importante es la seguridad. Una gran cantidad de la gente podría preocuparse por un chico de 14 años de hackear el sistema y la falsificación de los resultados.

8. Cinco enrutadores se van a conectar en una subred de punto a punto. Los diseñadores podrían poner una línea de alta velocidad, de mediana velocidad, de baja velocidad o ninguna línea, entre cada par de enrutadores. Si toma 100 ms de tiempo de la computadora generar e inspeccionar cada topología, ¿cuánto tiempo tomará inspeccionarlas todas?

R= Llame a los routers A, B, C, D y E. Hay diez líneas posibles: AB, AC, AD, AE, BC, BD, BE, CD, CE y DE. Cada uno de estos tiene cuatro posibilidades (Tres velocidades o la línea no), por lo que el número total de topologías es de $4^{10} = 1.048.576$. A 100 ms cada uno, que se necesita 104,857.6 segundos, o un poco más de 29 horas a inspeccionar a todos.

9. Un grupo de $2n-1$ enrutadores están interconectados en un árbol binario centralizado, con un enrutador en cada nodo del árbol. El enrutador i se comunica con el enrutador j enviando un mensaje a la raíz del árbol. A continuación, la raíz manda el mensaje al enrutador j . Obtenga una expresión aproximada de la cantidad media de saltos por mensaje para un valor grande de n , suponiendo que todos los pares de enrutadores son igualmente probables.

R= La media de enrutador router de ruta es el doble de la media de enrutador de ruta de raíz. Número de la niveles del árbol con la raíz como 1 y el nivel más profundo a medida que n . El camino de la raíz hasta el nivel n requiere $n - 1$ y 0,50 lúpulos, uno de los routers están en este nivel. El camino desde la raíz hasta el nivel $n - 1$ tiene 0.25 de los routers y una longitud de $n - 2$ saltos. Por lo tanto, la longitud del camino medio, l , viene dada por:

$$l = 0.5 \times (n - 1) + 0.25 \times (n - 2) + 0.125 \times (n - 3) + \dots$$

or

$$l = \sum_{i=1}^{\infty} n (0.5)^i - \sum_{i=1}^{\infty} i (0.5)^i$$

Esta expresión se reduce a $l = n - 2$. La media de enrutador enrutador camino es por lo tanto $2n - 4$.

10. Una desventaja de una subred de difusión es la capacidad que se desperdicia cuando múltiples hosts intentan acceder el canal al mismo tiempo. Suponga, por ejemplo, que el tiempo se divide en ranuras discretas, y que cada uno de los hosts n intenta utilizar el canal con probabilidad p durante cada parte. ¿Qué fracción de las partes se desperdicia debido a colisiones?

R= Distinguir $n + 2$ eventos. Eventos 1 a n consisten en la correspondiente acoger con éxito de intentar utilizar el canal, es decir, sin una colisión. La probabilidad de cada uno de estos eventos es $p (1 - p)^{n - 1}$. Evento $n + 1$ es ociosa canal, con una probabilidad $(1 - p)^n$. Evento $n + 2$ es una colisión. Dado que estos $n + 2$ eventos son exhaustivos, sus probabilidades deben sumar a la unidad. La probabilidad de una colisión, la cual es igual a la fracción de ranuras desperdiciadas, a continuación, sólo es $1 - np (1 - p)^{n - 1} - (1 - p)^n$.

11. Mencione dos razones para utilizar protocolos en capas.

R= Entre otras razones para el uso de protocolos de capas, utilizando los lleva a la ruptura el problema de diseño en partes más pequeñas y manejables, y capas significa que los protocolos pueden ser cambiados sin afectar a las más altas o más bajas,

12. Al presidente de Specialty Paint Corp. se le ocurre la idea de trabajar con una compañía cervecera local para producir una lata de cerveza invisible (como medida para reducir los desechos). El presidente indica a su departamento legal que analice la situación, y éste a su vez pide ayuda al departamento de ingeniería. De esta forma, el ingeniero en jefe se reúne con su contraparte de la otra compañía para discutir los aspectos técnicos del proyecto. A continuación, los ingenieros informan los resultados a sus respectivos departamentos legales, los cuales a su vez se comunican vía telefónica para ponerse de acuerdo en los aspectos legales. Por último, los dos presidentes corporativos se ponen de acuerdo en la parte financiera del proyecto. ¿Este es un ejemplo de protocolo con múltiples capas semejante al modelo OSI?

R= No. En el modelo de protocolo ISO, la comunicación física se lleva a cabo sólo en la capa más baja, no en cada capa.

13. ¿Cuál es la diferencia principal entre comunicación orientada a la conexión y no orientada a ésta?

R= Orientado a la conexión de comunicación tiene tres fases. En el establecimiento fase se realiza una solicitud para establecer una conexión. Sólo después de esta fase ha sido completado con éxito puede la fase de transferencia de datos en marcha y se transportan datos. Luego viene la fase de liberación. La comunicación sin conexión hace no tienen estas fases. Simplemente envía los datos.

14. Dos redes proporcionan servicio confiable orientado a la conexión. Una de ellas ofrece un flujo confiable de bytes y la otra un flujo confiable de mensajes. ¿Son idénticas? Si es así, ¿por qué se hace la distinción? Si no son idénticas, mencione un ejemplo de algo en que difieran.

R= Flujos de mensajes y de bytes son diferentes. En una secuencia de mensajes, la red realiza un seguimiento de los límites del mensaje. En una secuencia de bytes, no lo hace. Por ejemplo, Supongo que un proceso escribe 1024 bytes a una conexión y un poco más tarde escribe otro de 1024 bytes. El receptor tiene una lectura de 2048 bytes. Con una secuencia de mensajes, el receptor recibirá dos mensajes de 1024 bytes. Con un flujo de bytes, los límites del mensaje no cuentan y el receptor obtiene el completo 2048 bytes como una sola unidad. El hecho de que había originalmente dos mensajes distintos se pierde.

15. ¿Qué significa "negociación" en el contexto de protocolos de red? Dé un ejemplo.

R= La negociación tiene que ver con conseguir que ambas partes estén de acuerdo en algunos parámetros o valores que se utilizan durante la comunicación. Tamaño máximo de paquete es un ejemplo, pero hay muchos otros.

16. En la figura 1-19 se muestra un servicio. ¿Hay algún otro servicio implícito en la figura? Si es así, ¿dónde? Si no lo hay, ¿por qué no?

R= El servicio que se muestra es el servicio ofrecido por la capa k de la capa $k + 1$. Otro servicio que debe estar presente está por debajo de la capa k , es decir, el servicio ofrecido a capa k por la capa subyacente $k - 1$.

17. En algunas redes, la capa de enlace de datos maneja los errores de transmisión solicitando que se retransmitan las tramas dañadas. Si la probabilidad de que una trama se dañe es p , ¿cuál es la cantidad media de transmisiones requeridas para enviar una trama? Suponga que las confirmaciones de recepción nunca se pierden.

R= La probabilidad, P_k , de un marco que requiere exactamente k es la probabilidad de transmisiones de las primeras $k - 1$ intentos no, p^{k-1} , multiplicado por la probabilidad de que el k -ésimo la transmisión de tener éxito, $(1 - p)$. El número medio de transmisión es entonces sólo:

$$\sum_{k=1}^{\infty} k P_k = \sum_{k=1}^{\infty} k (1-p) p^{k-1} = \frac{1}{1-p}$$

18. ¿Cuál de las capas OSI maneja cada uno de los siguientes aspectos?:

- (a) Dividir en tramas el flujo de bits transmitidos.
- (b) Determinar la ruta que se utilizará a través de la subred.

R= (a) la capa de enlace de datos. (b) la capa de red.

19. Si la unidad que se transmite al nivel de enlace de datos se denomina trama y la que se transmite al nivel de red se llama paquete, ¿las tramas encapsulan paquetes o los paquetes encapsulan tramas? Explique su respuesta?

R= Marcos encapsular paquetes. Cuando un paquete llega a la capa de enlace de datos, la cosa entera, encabezamiento, datos, y todo, se utiliza como el campo de datos de un cuadro. La todo el paquete se coloca en un sobre (el marco), por así decirlo (suponiendo que cabe).

20. Un sistema tiene una jerarquía de protocolos de n capas. Las aplicaciones generan mensajes con una longitud de M bytes. En cada una de las capas se agrega un encabezado de h bytes. ¿Qué fracción del ancho de banda de la red se llena con encabezados?

R= Con capas n y bytes h añadido por capa, el número total de bytes de cabecera por mensaje es $h \cdot n$, por lo que el espacio perdido en las cabeceras es $h \cdot n$. El total de mensajes tamaño es $M + n h$, por lo que la fracción de ancho de banda desperdiciado en cabeceras es $h \cdot n / (M + h \cdot n)$.

21. Mencione dos similitudes entre los modelos de referencia OSI y TCP/IP. A continuación mencione dos diferencias entre ellos.

R= Ambos modelos se basan en protocolos de capas. Ambos tienen una red, el transporte, y la capa de aplicación. En ambos modelos, el servicio de transporte pueda ofrecer un fiable de extremo a extremo flujo de bytes. Por otro lado, difieren en varias maneras. El número de capas es diferente, el TCP / IP no tiene sesión o las capas de presentación, OSI no es compatible con conexiones en red, y de la OSI tiene tanto servicio orientado a conexión y sin conexión en la capa de red.

22. ¿Cuál es la principal diferencia entre TCP y UDP?

R= TCP es orientado a conexión, mientras que UDP es un servicio sin conexión.

23. La subred de la figura 1-25(b) se diseñó para resistir una guerra nuclear. ¿Cuántas bombas serían necesarias para partir los nodos en dos conjuntos inconexos? Suponga que cualquier bomba destruye un nodo y todos los enlaces que se conectan a él.

R= Los dos nodos en la esquina superior derecha puede ser desconectado del resto por tres bombas anulación de los tres nodos a los que están conectados. El sistema puede soportar la pérdida de dos nodos cualesquiera.

24. Internet está duplicando su tamaño aproximadamente cada 18 meses. Aunque no se sabe a ciencia cierta, una estimación indica que en el 2001 había 100 millones de *hosts* en Internet. Utilice estos datos para calcular la cantidad esperada de *hosts* para el año 2010. ¿Cree que esto es real? Explique por qué.

R= Se duplica cada 18 meses significa un factor de cuatro ganancia en 3 años. En 9 años, la ganancia es entonces 43 o 64, que conduce a 6.4 mil millones de *hosts*.

Mi intuición me dice que es demasiado conservador, ya que para entonces probablemente todos los de la televisión en el mundo y posiblemente miles de millones de otros aparatos serán en la casa de LAN conectado a Internet. La persona promedio en el mundo desarrollado puede tener docenas de Servidores de Internet para ese entonces.

25. Cuando un archivo se transfiere entre dos computadoras, pueden seguirse dos estrategias de confirmación de recepción. En la primera, el archivo se divide en paquetes, y el receptor confirma la recepción de cada uno de manera individual, aunque no confirma la recepción del archivo como un todo. En contraste, en la segunda estrategia la recepción de los paquetes no se confirma de manera individual, sino la del archivo completo. Comente las dos estrategias.

R= Si la red tiende a perder paquetes, es mejor reconocer cada uno por separado, por lo que los paquetes perdidos puede ser retransmitido. Por otro lado, si el red es altamente fiable, el envío de un acuse de recibo al final de la transferencia de toda ahorra ancho de banda en el caso normal (pero requiere que el archivo completo ser retransmitido si incluso un solo paquete se pierde).

26. ¿Por qué ATM utiliza celdas pequeñas de longitud fija?

R= Pequeño, celdas de longitud fija se pueden dirigir a través de conmutadores con rapidez, y completamente en el hardware. Pequeños, de tamaño fijo células también hacen que sea más fácil de construir hardware que maneja muchas células en paralelo. Por otra parte, que no bloqueen líneas de transmisión por mucho tiempo, por lo que es más fácil para proporcionar una calidad de servicio garantías.

27. ¿Qué tan grande era un bit, en metros, en el estándar 802.3 original? Utilice una velocidad de transmisión de 10 Mbps y suponga que la velocidad de propagación en cable coaxial es 2/3 la velocidad de la luz en el vacío.

R= La velocidad de la luz en el cable coaxial es de unos 200.000 km / seg, que es de 200 metros por microsegundos. A los 10 Mbps, se tarda 0,1 microsegundos para transmitir un bit. Por lo tanto, el bit dura 0,1 microsegundos en tiempo, durante el cual se propaga a 20 metros. Por lo tanto, un poco es de 20 metros de largo aquí.

28. Una imagen tiene 1024 × 768 píxeles con 3 bytes/píxel. Suponga que la imagen no se encuentra comprimida. ¿Cuánto tiempo tomará transmitirla sobre un canal de módem de 56 kbps? ¿Sobre un módem de cable de 1 Mbps? ¿Sobre una red Ethernet a 10 Mbps? ¿Sobre una red Ethernet a 100 Mbps?

R= La imagen es de 1024 × 768 × 3 bytes o 2.359.296. Esto es 18.874.368 bits. En 56.000 bits por segundo, tarda aproximadamente 337,042 seg. En 1.000.000 bits por segundo, lo toma alrededor de 18,874 seg. En 10,000,000 bits por segundo, tarda unos 1,887 seg. En 100.000.000 de bits por segundo, tarda unos 0,189 seg.

29. Ethernet y las redes inalámbricas tienen algunas similitudes y diferencias. Una propiedad de Ethernet es que sólo se puede transmitir una trama a la vez sobre una red de este tipo. ¿El 802.11 comparte esta propiedad con Ethernet? Comente su respuesta.

R= Es una red inalámbrica de cinco estaciones, de A a E, de tal manera que cada uno está en el rango de sólo su inmediato vecino. Entonces A puede hablar con B, al mismo tiempo D está hablando con E. Wireless redes tienen paralelismo potencial, y de esta manera se diferencian de Ethernet.

30. Las redes inalámbricas son fáciles de instalar, y ello las hace muy económicas puesto que los costos de instalación eclipsan por mucho los costos del equipo. No obstante, también tienen algunas desventajas. Mencione dos de ellas.

R= Una desventaja es la seguridad. Cada hombre entrega al azar que resulta ser en el edificio puede escuchar en la red. Otra desventaja es la fiabilidad. Las redes inalámbricas hacer un montón de errores. Un problema potencial es tercero de la batería la vida, ya que la mayoría de dispositivos inalámbricos tienden a ser móviles.

31. Cite dos ventajas y dos desventajas de contar con estándares internacionales para los protocolos de red.

R= Una ventaja es que si todo el mundo utiliza el estándar, cada uno puede hablar con todo el mundo. Otra ventaja es que el uso generalizado de cualquier norma dará sus economías de escala, como ocurre con los chips VLSI. Una desventaja es que la política compromisos necesarios para lograr la normalización con frecuencia conduce a las pobres normas. Otra desventaja es que una vez que un estándar ha sido ampliamente adoptado, es difícil de cambiar, aunque nuevas y mejores técnicas o métodos que se descubren. Además, por el tiempo que ha sido aceptado, puede ser obsoleto.

32. Cuando un sistema tiene una parte fija y una parte removible (como ocurre con una unidad de CD-ROM y el CD-ROM), es importante que exista estandarización en el sistema, con el propósito de que las diferentes compañías puedan fabricar tanto la parte removible como la fija y todo funcione en conjunto. Mencione tres ejemplos ajenos a la industria de la computación en donde existan estándares internacionales. Ahora mencione tres áreas donde no existan.

R= Hay muchos ejemplos, por supuesto. Algunos sistemas para los cuales existe internacional la estandarización incluyen reproductores de discos compactos y sus discos, Walkman reproductores de cintas y casetes de audio, cámaras y película de 35mm, y los cajeros automáticos y tarjetas bancarias. Áreas en las que la normalización internacional, se carece de incluir reproductores de video y cintas de video (VHS NTSC en los EE.UU., PAL VHS en partes de Europa, SECAM VHS en otros países), teléfonos móviles, lámparas y bombillas (tensiones en los distintos países), eléctricos tomas de corriente y enchufes de electrodomésticos (todos los países lo hace de manera diferente), fotocopadoras y papel (8,5 x 11 pulgadas en los EE.UU., A4 en cualquier otro lugar), frutos secos y tornillos (paso Inglés contra métrico), etc.



Título Libro	Redes de Computadoras
Título del Capítulo	Capítulo 2 – La Capa Física
No. Ejercicios	58
Fecha de Realización	VERANO 2012

CAPITULO 2

1. Calcule los coeficientes de Fourier para la función $f(t) = t$ ($0 \leq t \leq 1$).

$$a_n = \frac{-1}{\pi n}, b_n = 0, c = 1.$$

R=

2. Un canal sin ruido de 4 kHz se muestrea cada 1 mseg. ¿Cuál es la tasa de datos máxima?

R= Un canal de ruido puede llevar una cantidad arbitrariamente grande de información, no importa la frecuencia con que se muestrea. Sólo tienes que enviar una gran cantidad de datos por muestra. Para el 4 kHz entre canales, que 8000 muestras por segundo. Si cada muestra es de 16 bits, el canal puede enviar a 128 Kbps Si cada muestra es de 1024 bits, el canal puede enviar 8.2 Mbps La palabra clave aquí es "silenciosa". Con un canal normal de 4 kHz, el Límite de Shannon no lo permitiría.

3. Los canales de televisión tienen un ancho de 6 Mhz. ¿Cuántos bits/seg se pueden enviar si se usan señales digitales de cuatro niveles? Suponga que el canal es sin ruido.

R= Usando el teorema de Nyquist, se puede probar 12 millones de veces por segundo. Cuatro niveles señales de proporcionar 2 bits por muestra, con una tasa de datos total de 24 Mbps.

4. Si se envía una señal binaria por un canal de 3 kHz cuya relación de señal a ruido es de 20 dB, ¿cuál es la tasa de datos máxima que se puede obtener?

R= Una relación señal-ruido de 20 dB significa $S/N = 100$. Dado que se trata de $\log_2 101$ 6,658, el límite de Shannon es de unos 19.975 Kbps El límite de Nyquist es de 6 Kbps El cuello de botella es por lo tanto, el límite de Nyquist, dando un canal máximo capacidad de 6 Kbps

5. ¿Qué relación de señal a ruido se necesita para poner una portadora T1 en una línea de 50 kHz?

R= Para enviar una señal T1 necesitamos $H \log_2 (1 + S/N) = 1.544 \times 10^6$ con $H = 50.000$. Esto produce $S/N = 230 - 1$, que es aproximadamente 93 dB.

6. ¿Qué diferencia hay entre una estrella pasiva y un repetidor activo en una red de fibra óptica?

R= Una estrella de pasivo no tiene la electrónica. La luz de una fibra ilumina una número de los demás. Un repetidor activo convierte la señal óptica a una eléctrica una para su posterior procesamiento.

7. ¿Cuánto ancho de banda existe en 0.1 micras de espectro a una longitud de onda de 1 micra?

R= Utilice $\Delta f = c\Delta\lambda/\lambda^2$ con $\Delta\lambda = 10^{-7}$ metros y $\lambda = 10^{-6}$. Esto da un ancho de banda de 30.000 GHz

8. Se desea enviar una secuencia de imágenes de pantalla de computadora por una fibra óptica. La pantalla es de 480×640 píxeles y cada píxel ocupa 24 bits. Hay 60 imágenes de pantalla por segundo. ¿Cuánto ancho de banda se necesita y cuántas micras de longitud de onda se necesitan para esta banda a 1.30 micras?

R= La velocidad de datos es de $480 \times 640 \times 24 \times 60$ puntos básicos, lo que es de 442 Mbps Por simplicidad, supongamos una bps por Hz. De la ecuación. (2-3) se obtiene $\Delta\lambda = \lambda^2\Delta f / c$. tenemos $Df = 4,42 \times 10^8$, por lo que $\Delta\lambda = 2,5 \times 10^{-6}$ micras. La gama de longitudes de onda utilizadas es muy corta.

9. ¿Se cumple el teorema de Nyquist para la fibra óptica o solamente para el alambre de cobre?

R= El teorema de Nyquist es una propiedad de las matemáticas y no tiene nada que ver con tecnología. Se dice que si usted tiene una función cuyo espectro de Fourier no contiene ningún senos o cosenos por encima de f , entonces mediante el muestreo de la función a una frecuencia de $2f$ a capturar toda la información que hay. Así, la Nyquist teorema es verdadero para todos los medios de comunicación.

10. En la figura 2-6 la banda de la izquierda es más angosta que las otras. ¿Por qué?

R= En el texto se afirma que los anchos de banda (es decir, los rangos de frecuencia) de la tres bandas eran aproximadamente iguales. De la fórmula $\Delta f = c\Delta\lambda/\lambda^2$, es claro que para obtener una Df constante, cuanto mayor sea la frecuencia, $\Delta\lambda$ mayor tiene que ser. El eje x en la figura es λ , por lo que la mayor es la frecuencia, la más $\Delta\lambda$ que usted necesita. De hecho, $\Delta\lambda$ es de segundo grado en λ . El hecho de que las bandas son de aproximadamente igual es una característica accidental del tipo de silicio utilizado.

11. A menudo las antenas de radio funcionan mejor cuando el diámetro de la antena es igual a la longitud de la onda de radio. Las antenas prácticas tienen diámetros desde 1 cm hasta 5 m de diámetro. ¿Qué rango de frecuencias cubre esto?

R= Comience con $\lambda f = c$. Sabemos que c es 3×10^8 m / s. Para $\lambda = 1$ cm, se obtiene 30 GHz Para $\lambda = 5$ m, se obtiene 60 MHz Así, la banda es cubierto 60 MHz a 30 GHz

12. El desvanecimiento por múltiples trayectorias alcanza un máximo cuando los dos haces llegan desfasados 180 grados. ¿Qué tan diferentes deben ser las trayectorias para que el desvanecimiento sea máximo para un enlace de microondas de 1 GHz de 50 km de largo?

R= A 1 GHz, las olas son de 30 cm de largo. Si una onda se desplaza 15 cm más del otro, llegarán fuera de fase. El hecho de que el enlace es de 50 km de longitud es irrelevante.

13. Un rayo láser de 1 mm de diámetro se apunta a un detector de 1 mm de diámetro a 100 m en el techo de un edificio. ¿Cuánta desviación angular deberá tener el láser antes de que pierda al detector?

R= Si el haz está desactivada de 1 mm en el extremo, se pierde el detector. Esto equivale a un triángulo con la base de 100 metros y la altura de 0,001 m. El ángulo es una cuyo tangente es así 0,00001. Este ángulo es de aproximadamente 0,00057 grados.

14. Los 66 satélites de órbita baja en el proyecto Iridium se dividen en seis collares alrededor de la Tierra. A la altitud que están utilizando, el periodo es de 90 minutos. ¿Cuál es el intervalo promedio de transferencias de celdas para un transmisor fijo?

R= Con 66/6 y 11 satélites por collar, cada 90 minutos 11 satélites pasan sobrecarga. Esto significa que hay un tránsito cada 491 segundos. Por lo tanto, habrá ser un handoff aproximadamente cada 8 minutos y 11 segundos.

15. Considere un satélite a una altitud de satélites geoestacionarios pero cuyo plan de órbitas se inclina hacia el plano ecuatorial a un ángulo ϕ . Para un usuario fijo en la superficie de la Tierra a una altitud norte ϕ , ¿este satélite da la impresión en el cielo de que no tiene movimiento? De lo contrario, describa su movimiento.

R= El satélite se mueve de ser directamente sobre la cabeza hacia el horizonte sur, con una excursión máxima de la vertical de 2ϕ . Se tarda 24 horas para ir directamente desde arriba a la excursión máximo y luego vuelve.

16. Cuántos códigos de oficina central local había antes de 1984, cuando cada oficina central tenía el nombre de los tres dígitos de su código de área y los primeros tres dígitos del número local? Los códigos de área iniciaban con un

dígito en el rango de 2–9, tenían un 0 o un 1 como su segundo dígito, y terminaban con cualquier dígito. Los primeros dos dígitos de un número local siempre estaban en el rango de 2–9. El tercer dígito podía ser cualquiera.

R= El número de códigos de área fue de $8 \times 2 \times 10$, que es 160. El número de prefijos fue de $8 \times 8 \times 10$, o 640. Así, el número de oficinas finales se limita a 102.400. Este límite no es un problema.

17. Utilizando sólo los datos dados en el texto, ¿cuál es la cantidad máxima de teléfonos que el sistema existente de Estados puede manejar sin cambiar el plan de numeración o agregar equipo adicional? ¿Es posible alcanzar esta cantidad de teléfonos? Para propósitos de este problema, una computadora o máquina de fax cuenta como un teléfono. Suponga que sólo hay un dispositivo por línea de suscriptor.

R= Con un número de teléfono 10-dígitos, podría haber 1010 números, aunque muchos de los códigos de área son ilegales, como por ejemplo 000. Hay 22.000 oficinas de finales, cada una con un máximo de 10.000 líneas. Esto da un máximo de 220 millones de teléfonos. Simplemente no hay lugar para conectar más de ellos. Esto podría nunca lograrse en la práctica debido a que algunas oficinas no son de gama completa. El fin de una oficina en un pequeño pueblo de Wyoming no puede tener cerca de 10.000 clientes, de modo que esas líneas se pierden.

18. Un sistema telefónico simple consiste en dos oficinas centrales locales y una interurbana a la que está conectada cada oficina central por una troncal dúplex de 1 MHz. En promedio, cada teléfono se usa para hacer cuatro llamadas por cada jornada de 8 horas. La duración media de las llamadas es de 6 minutos. El 10% de las llamadas son de larga distancia (esto es, pasan por la oficina interurbana). ¿Cuál es la cantidad máxima de teléfonos que puede manejar una oficina central local? (Suponga que hay 4 kHz por circuito.)

R= Cada teléfono tiene 0,5 llamadas por hora a los 6 minutos cada una. Así, un teléfono ocupa un circuito durante 3 minutos por hora. Veinte teléfonos pueden compartir un circuito, a pesar de tener la carga de estar cerca del 100% ($\rho = 1$ en la cola de terminos) implica muy largos tiempos de espera). Desde el 10% de las llamadas son de larga distancia, se tarda 200 teléfonos a ocupar un tiempo del circuito de larga distancia completa. Con 200 teléfonos por circuito, una oficina final puede soportar $200 \times 250 = 50.000$ teléfonos.

19. Una compañía de teléfonos regional tiene 10 millones de suscriptores. Cada uno de sus teléfonos está conectado a una oficina central local mediante un cable de par trenzado de cobre. La longitud promedio de estos cables de par trenzado es de 10 km. ¿Cuánto vale el cobre de los circuitos locales? Suponga que la sección transversal de cada filamento es un círculo de 1 mm de diámetro, que el peso específico relativo del cobre es 9.0 y que el cobre se vende a 3 dólares por kilogramo.

R= La sección transversal de cada filamento de un par trenzado es $\pi / 4$ mm cuadrados. A 10 km-longitud de este material, con dos filamentos por cada par tiene un volumen de $2\pi / 4 \times 10^{-2}$ m³. Este volumen es de aproximadamente 15.708 cm³. Con un peso específico de 9,0, cada bucle local tiene una masa de 141 kg. La empresa de telefonía por lo tanto posee $1,4 \times 10^9$ kg de cobre. A los 3 dólares cada uno, el cobre tiene un valor de 4,2 mil millones de dólares.

20. ¿Un gasoducto es un sistema símplex, uno semidúplex, uno dúplex total, o ninguno de los antes mencionados?

R= Al igual que las vías del tren son half-duplex. El aceite puede fluir en cualquier dirección, pero no en ambos sentidos a la vez.

21. El costo de un microprocesador potente se ha reducido a tal grado que ahora es posible incluir uno en cada módem. ¿Cómo afecta esto el manejo de errores en las líneas telefónicas?

R= Tradicionalmente, los bits han sido enviados a través de la línea sin ningún tipo de corrección de errores en la capa física. La presencia de una CPU en cada módem hace posible incluir un código de corrección de errores en la capa 1 a reducir considerablemente la tasa de error efectiva vista por la capa 2. El manejo de errores por los módems puede ser hecho totalmente transparente a la capa 2. Muchos módems ahora se han construido en el error de corrección.

22. Un diagrama de constelación de módem, similar al de la figura 2-25, tiene puntos de datos en las siguientes coordenadas: (1, 1), (1, -1), (-1, 1) y (-1, -1). ¿Cuántos bps puede lograr un módem a 1200 baudios con estos parámetros?

R= Hay cuatro valores legales por baudio, por lo que la tasa de bits es el doble de la velocidad de transmisión. En 1200 baudios, la velocidad de datos es de 2400 bps.

23. Un diagrama de constelación de módem, similar al de la figura 2-25, tiene puntos de datos en (0, 1) y (0, 2). ¿El módem usa modulación de fase o modulación de amplitud?

R= El cambio de fase es siempre 0, pero dos amplitudes se utilizan, por lo que este es recto modulación de amplitud.

24. En un diagrama de constelación todos los puntos están en un círculo centrado en el origen. ¿Qué tipo de modulación se utiliza?

R= Si todos los puntos son equidistantes del origen, todos ellos tienen la misma amplitud, así la modulación de amplitud no está siendo utilizada. La modulación de frecuencia es nunca se utiliza en los diagramas de constelación, por lo que la codificación es de claves de cambio de fase pura.

25. ¿Cuántas frecuencias utiliza un módem QAM-64 de dúplex total?

R= Dos, uno para aguas arriba y aguas abajo de una. El esquema de modulación sí sólo utiliza la amplitud y fase. La frecuencia no está modulada.

26. Un sistema ADSL que utiliza DMT asigna 3/4 de los canales de datos disponibles al enlace descendente. Utiliza modulación QAM-64 en cada canal. ¿Cuál es la capacidad del enlace descendente?

R= Hay 256 canales en todo, menos 6 para POTS y 2 para el control, dejando 248 para los datos. Si 3/4 de éstos son de aguas abajo, que da 186 canales para aguas abajo. Modulación de ADSL a 4000 baudios, así que con QAM-64 (6 bits por baudio) tenemos 24.000 bps en cada uno de los 186 canales. El total ancho de banda es entonces 4.464 Mbps de descarga.

27. En el ejemplo de cuatro sectores LMDS de la figura 2-30, cada sector tiene su propio canal de 36 Mbps. De acuerdo con la teoría de encolamiento, si el canal está cargado en 50%, el tiempo de encolamiento será igual que el de descarga. Bajo estas condiciones, ¿cuánto tiempo se tarda en bajar una página Web de 5 KB? ¿Cuánto tiempo se tarda en bajar la página a través de una línea ADSL de 1 Mbps? ¿A través de un módem de 56 kbps?

R= Una página Web de 5 KB tiene 40.000 bits. El tiempo de descarga sobre un canal de 36 Mbps es de 1,1 mseg. Si el retardo de cola también es 1.1 ms, el tiempo total es de 2,2 mseg. A través de ADSL que no hay retraso de colas, por lo que el tiempo de descarga a 1 Mbps es de 40 ms. En 56 Kbps es 714 ms.

28. Diez señales, cada una de las cuales requiere 4000 Hz, se multiplexan en un solo canal utilizando FDM. ¿Cuál es el ancho de banda mínimo requerido para el canal multiplexado? Suponga que las bandas de protección tienen un ancho de 400 Hz.

R= Hay diez señales de 4000 Hz. Tenemos nueve bandas de guarda para evitar cualquier interferencia. El ancho de banda mínimo requerido es de $4000 \times 10 + 400 \times 9 = 43.600$ Hz.

29. ¿Por qué se fijó el tiempo de muestreo de PCM en 125 µseg?

R= Un tiempo de muestreo de 125 microsegundos corresponde a 8000 muestras por segundo. Según el teorema de Nyquist, esto es la frecuencia de muestreo necesaria para capturar toda la información en un canal de 4 kHz, tal como un canal telefónico. (En realidad, el ancho de banda nominal es de un poco menos, pero el corte no es en punto.)

30. ¿Cuál es el porcentaje de sobrecarga en una portadora T1?; esto es, ¿qué porcentaje de los 1.544 Mbps no se entrega al usuario final?

R= Los usuarios finales obtienen $7 \times 24 = 168$ de los 193 bits en un marco. La sobrecarga es por lo tanto, $25/193 = 13\%$.

31. Compare la tasa de datos máxima de un canal sin ruido de 4 kHz que utiliza: (a) Codificación analógica con 2 bits por muestra. (b) El sistema T1 de PCM.

R= En ambos casos 8000 muestras por segundo son posibles. Con DIBIT codificación, dos bits se envían por muestra. Con T1, 7 bits son enviados por período. Los datos respectivos las tasas son de 16 Kbps y 56.

32. Si un sistema de portador T1 pierde la pista de dónde está, trata de resincronizarse con base en el primer bit de cada trama. ¿Cuántas tramas se tendrían que inspeccionar en promedio para resincronizarse con una probabilidad de 0.001 de estar en un error?

R= Diez cuadros. La probabilidad de que algún patrón aleatorio siendo 0101010101 (en un canal digital) es 1/1024.

33. ¿Cuál es la diferencia, si la hay, entre la parte desmoduladora de un módem y la parte codificadora de un codec? (Después de todo, ambas convierten señales analógicas a digitales.)

R= Un codificador acepta una señal analógica arbitraria y genera una señal digital desde él. Un demodulador acepta una onda sinusoidal modulada única y genera una señal digital.

34. Una señal se transmite en forma digital por un canal sin ruido de 4 kHz, con una muestra cada 125 μ seg. ¿Cuántos bits por segundo se envían realmente con cada uno de los siguientes métodos de codificación? (a) CCITT, 2.048 Mbps estándar. (b) DPCM con un valor de señal relativo de 4 bits. (c) Modulación delta.

R= (A) 64 Kbps (B) 32 Kbps (C) 8 Kbps.

35. Se codifica una onda senoidal pura de amplitud A usando modulación delta, con x muestras/seg. Una salida de +1 corresponde a un cambio de señal de +A/8, y una señal de salida de -1 corresponde a un cambio de señal de -A/8. ¿Cuál es la frecuencia más alta que se puede rastrear sin error acumulativo?

R= La señal debe ir de 0 a A en un cuarto de una onda, es decir, en un tiempo $T / 4$. Con el fin de realizar un seguimiento de la señal, 8 pasos debe encajar en el cuarto de onda, o 32 muestras por onda completa. El tiempo por muestra es de $1 / x$ para todo el período debe ser tiempo suficiente como para contener 32 muestras, es decir, $T > 32 / X$ o $C_{Max} = x / 32$.

36. Los relojes de SONET tienen una tasa de arrastre de casi 1 parte en 109. ¿Cuánto tiempo tomará para que el arrastre iguale el ancho de 1 bit? ¿Cuáles son las implicaciones de este cálculo?

R= Una velocidad de deriva de los medios 10^{-9} 1 segundo en 109 segundos o 1 ns por segundo. En OC-1 velocidad, por ejemplo, 50 Mbps, por simplicidad, un poco dura 20 nseg. Esto significa que se tarda unos 20 segundos para que el reloj a la deriva en un bit. En consecuencia, los relojes deben ser sincronizados de forma continua para evitar que se vuelva demasiado muy separado. Ciertamente, cada 10 segundos, preferiblemente con mucha más frecuencia.

37. En la figura 2-37 se establece que la tasa de datos del usuario para OC-3 es de 148.608 Mbps. Demuestre cómo se puede deducir esta cantidad de los parámetros de OC-3 de SONET.

R= De las 90 columnas, 86 están disponibles para datos de usuario en OC-1. Así, el usuario la capacidad es de $86 \times 9 = 774$ bytes / marco. Con 8 bits por byte, marcos de 8000 / seg, y 3 OC-1 portadoras multiplexadas en conjunto, la capacidad total del usuario es $3 \times 774 \times 8 \times 8000$ Mbps, o 148.608.

38. Para acomodar tasas de datos menores que STS-1, SONET tiene un sistema de tributarias virtuales (VT). Una VT es una carga útil parcial que se puede insertar en una trama STS-1 y combinar con otras cargas útiles parciales para llenar la trama de datos. VT1.5 utiliza 3 columnas, VT2 utiliza 4, VT3 utiliza 6 y VT6 utiliza 12 columnas de una trama STS-1. ¿Cuál VT puede acomodar. (a) Un servicio DS-1 (1.544 Mbps)? (b) Un servicio europeo CEPT-1 (2.048 Mbps o E1)? (c) Un servicio DS-2 (6.312 Mbps)?

R= VT1.5 puede albergar 8.000 fotogramas por segundo $\times 3$ columnas $\times 9$ filas $\times 8$ bits = 1.728 Mbps Se puede utilizar para acomodar DS-1. VT2 puede acomodar 8000 fotogramas por segundo $\times 4$ columnas $\times 9$ filas $\times 8$ bits = 2,304 Mbps Se puede utilizar para dar cabida a Europa CEPT-1 de servicio. VT6 puede acomodar 8000 cuadros / seg $\times 12$ columnas $\times 9$ filas $\times 8$ bits = 6.912 Mbps Se puede utilizar para cabida a DS-2 de servicio.

39. ¿Cuál es la diferencia esencial entre la conmutación de mensajes y la de paquetes?

R= Conmutación de mensajes envía unidades de datos que pueden ser arbitrariamente largos. Paquete conmutación tiene un tamaño máximo de paquete. Cualquier mensaje más largo que se divide en paquetes múltiples.

40. ¿Cuál es el ancho de banda disponible para el usuario en una conexión OC-12c?

R= Los marcos OC-12c son $12 \times 90 = 1080$ columnas de 9 filas. De éstos, $12 \times 3 = 36$ columnas son absorbidos por la línea y la tara de sección. Esto deja una SPE de 1044 columnas. Una columna de SPE es tomado por la sobrecarga de camino, dejando 1043 columnas para datos de usuario. Puesto que cada columna contiene 9 bytes de 8 bits, un marco de OC-12c tiene 75,096 bits de datos de usuario. Con 8000 puntos por segundo, la velocidad de datos de usuario es 600.768 Mbps

41. Tres redes de conmutación de paquetes contienen n nodos cada una. La primera red tiene una topología de estrella con un conmutador central, la segunda es un anillo (bidireccional) y la tercera está interconectada por completo, con una conexión de cada nodo hacia cada uno de los otros nodos. ¿Cuáles son las rutas de transmisión óptima, media y de peor caso en saltos?

R= Las tres redes tienen las siguientes propiedades:

Estrella: mejor caso = 2, promedio de los casos = 2, peor de los casos = 2

Anillo: mejor de los casos = 1, caso promedio = $n / 4$, en el peor caso = $n / 2$

Plena interconexión: mejor caso = 1, caso promedio = 1, peor de los casos = 1

42. Compare el retardo al enviar un mensaje de x bits por una trayectoria de k saltos en una red de conmutación de circuitos y en una red de conmutación de paquetes (con carga ligera). El tiempo de establecimiento de circuito es de s segundos, el retardo de propagación es de d segundos por salto, el tamaño del paquete es de p bits y la tasa de datos es de b bps. ¿En qué condiciones tiene un retardo menor la red de paquetes?

R= Con la conmutación de circuitos, en $t = s$ el circuito está en marcha; en $t = s + x / b$ el último bit se envía, en $t = s + x / b + kd$ llega el mensaje. Con la conmutación de paquetes, el último bit se envía en $t = x / b$. Para llegar al destino final, el último paquete debe k ser retransmitido - 1 veces por los routers intermedios, de cada retransmisión de tomar p / b seg, por lo que el retardo total es $x / b + (k - 1) p / b + kd$. La conmutación de paquetes es más rápido si $s > (k - 1) p / b$.

43. Suponga que se van a transmitir x bits de datos de usuario por una trayectoria de k saltos en una red de conmutación de paquetes como una serie de paquetes, cada uno contiene p bits de datos y h bits de encabezado, donde $x = p + h$. La tasa de bits de las líneas es de b bps y el retardo de propagación es nulo. ¿Qué valor de p minimiza el retardo total?

R= El número total de paquetes necesarios es x / p , por lo que el total de datos + el tráfico de cabecera es $(P + h) x / p$ bits. La fuente requiere $(p + h) x / \text{seg}$ para transmitir estos bits. Las retransmisiones de los últimos paquetes por los routers intermedios ocupan una total de $(k - 1) (p + h) / b$ seg. Sumando el tiempo de la fuente para enviar toda la bits, más el tiempo de los routers para llevar el último paquete al destino, a fin de despejar la tubería, se obtiene un tiempo total de $(p + h) x / PB + (P + h) (k - 1) / \text{seg } b$. Reducir al mínimo esta cantidad con respecto a p , nos encontramos con $p = \sqrt{7h7x7 / 7 (K7-7717)}$.

44. En un sistema de telefónico móvil típico con celdas hexagonales se permite reutilizar una banda de frecuencia en una celda adyacente. Si están disponibles 840 frecuencias, ¿cuántas se pueden utilizar en una celda dada?

R= Cada celda tiene seis vecinos. Si la célula central se basa en un grupo de frecuencias, sus seis vecinos pueden utilizar B, C, B, C, B y C, respectivamente. En otras palabras, sólo 3 células únicas son necesarias. En consecuencia, cada célula puede tener 280 frecuencias.

45. El diseño real de las celdas rara vez es tan regular como se muestra en la figura 2-41. Incluso la forma de las celdas individuales por lo general es irregular. Dé una posible razón de por qué sucedería esto.

R= Primer despliegue, simplemente se coloca inicial de las células en las regiones donde hubo alta densidad de población humana o vehículo. Una vez allí, el operador a menudo no quiere tomarse la molestia de ponerlos. En segundo lugar, las antenas son normalmente se colocan en edificios altos o montañas. Dependiendo de la localización exacta de tales estructuras, el área cubierta por una célula puede ser irregular debido a los obstáculos cerca del transmisor. En tercer lugar, algunas comunidades o propietarios hacen no permitir la construcción de una torre en un lugar en el centro de una celda cae. En tales casos, las antenas direccionales se colocan en un lugar no en el centro de la celda.

46. Realice una estimación aproximada de la cantidad de microceldas PCS con un diámetro de 100 m que se requerirían para cubrir San Francisco (120 km²).

R= Si suponemos que cada micro célula es un círculo de 100 m de diámetro, a continuación, cada célula tiene una superficie de 2500π . Si tomamos el área de San Francisco, $1,2 \times 10^8 \text{ m}^2$ y se divide por el área de una micro célula, obtenemos 15.279 micro células. Por supuesto, es imposible tesela el plano con círculos (y San Francisco es decididamente en tres dimensiones), pero con 20.000 micro células que probablemente podría hacer el trabajo.

47. Algunas veces cuando un usuario móvil cruza el límite de una celda a otra, la llamada actual se termina de manera repentina, aunque todos los transmisores y receptores estén funcionando correctamente. ¿Por qué?

R= Las frecuencias no pueden ser reutilizados en las células adyacentes, por lo que cuando un usuario se mueve de una célula a otra, una nueva frecuencia debe ser asignado para la llamada. Si un usuario se mueve en una célula, todos de cuyas frecuencias están actualmente en uso, la llamada del usuario debe ser terminado.

48. D-AMPS tiene evidentemente una calidad de voz menor que GSM. ¿Esta es la razón por la que D-AMPS necesita tener compatibilidad hacia atrás con AMPS, y GSM no? Si no es así, explique la causa.

R= No es causado directamente por la necesidad de compatibilidad con versiones anteriores. El 30 KHz canal era de hecho un requisito, pero los diseñadores de D-AMPS no tienen para rellenar tres usuarios en él. Podían haber puesto dos usuarios en cada canal, el aumento de la carga antes de la corrección de error de $260 \times 50 = 13 \text{ Kbps}$ a $260 \times 75 = 19,5 \text{ Kbps}$ Por lo tanto, la pérdida de calidad ha sido intencionado trade-off de poner más usuarios por celda y por lo tanto salirse con grandes células.

49. Calcule el número máximo de usuarios que D-AMPS puede manejar de manera simultánea dentro de una celda. Realice el mismo cálculo para GSM. Explique la diferencia.

R= D-AMPS usa 832 canales (en cada dirección), con tres usuarios compartir una sola canal. Esto permite que D-AMPS para soportar hasta 2496 usuarios al mismo tiempo por célula. GSM utiliza 124 canales con ocho usuarios compartir una sola canal. Esto permite a GSM para soportar hasta 992 usuarios simultáneamente. Ambos sistemas utilizan aproximadamente la misma cantidad de espectro (25 MHz en cada dirección). D-AMPS utiliza $30 \text{ KHz} \times 892 = 26,76 \text{ MHz}$ GSM utiliza $200 \text{ KHz} \times 124 = 24,80 \text{ MHz}$ La diferencia puede atribuirse principalmente a la mejor discurso de calidad proporcionados por GSM (13 Kbps por usuario) a través de D-AMPS (8 Kbps por usuario).

50. Suponga que A, B y C, transmiten de manera simultánea bits 0 mediante un sistema CDMA con las secuencias de chips que se muestran en la figura 2-45(b). ¿Cuál es la secuencia de chips resultante?

R= El resultado se obtiene mediante la negación de cada uno de A, B y C y luego añadiendo el tres secuencias de chips. Alternativamente, el tres se pueden añadir y negada a continuación. El resultado es (+3 +1 +1 -1 -3 -1 -1 +1).

51. En el análisis acerca de la ortogonalidad de las secuencias de chips CDMA se dijo que si $S \cdot T = 0$, entonces $S \cdot T_{\neg}$ también es 0. Pruebe esto.

R= Por definición:

$$S \cdot T \equiv \frac{1}{m} \sum_{i=1}^m S_i T_i$$

Si T envía un bit 0 en vez de 1 bit, su secuencia de chips es negado, con el enésimo elemento cada vez - T_i . Por lo tanto,

$$S \cdot T \equiv \frac{1}{m} \sum_{i=1}^m S_i (-T_i) = -\frac{1}{m} \sum_{i=1}^m S_i T_i = 0$$

52. Considere una manera diferente de mirar la propiedad de ortogonalidad de las secuencias de chips CDMA. Cada bit en un par de secuencias puede o no coincidir. Expresé la propiedad de ortogonalidad en términos de coincidencias y falta de coincidencias.

R= Cuando dos elementos coinciden, su producto es una. Cuando no coinciden, su producto es -1. Para hacer que la suma 0, debe haber partidos como muchos como desajustes. Así, dos secuencias de chips son ortogonales si exactamente la mitad del elementos correspondientes partido y exactamente la mitad no coinciden.

53. Un receptor CDMA obtiene los siguientes chips: $(-1 +1 -3 +1 -1 -3 +1 +1)$. Suponiendo las secuencias de chips definidas en la figura 2-45(b), ¿cuáles estaciones transmitieron y qué bits envió cada una?

R= Sólo calcular los cuatro productos internos normalizados:

$$(-1 \ 1 \ -3 \ 1 \ -1 \ -3 \ +1 \ +1) \cdot (-1 \ -1 \ -1 \ +1 \ +1 \ -1 \ +1 \ +1) / 8 = 1$$

$$(-1 \ 1 \ -3 \ 1 \ -1 \ -3 \ +1 \ +1) \cdot (-1 \ -1 \ +1 \ -1 \ +1 \ +1 \ +1 \ -1) / 8 = -1$$

$$(-1 \ 1 \ -3 \ 1 \ -1 \ -3 \ +1 \ +1) \cdot (-1 \ +1 \ -1 \ +1 \ +1 \ +1 \ -1 \ -1) / 8 = 0$$

$$(-1 \ 1 \ -3 \ 1 \ -1 \ -3 \ +1 \ +1) \cdot (-1 \ 1 \ -1 \ -1 \ -1 \ -1 \ 1 \ -1) / 8 = 1$$

El resultado es que A y D enviado bits 1, B envía un bit 0, y C fue silencioso.

54. En su parte más baja, el sistema telefónico tiene forma de estrella, y todos los circuitos locales de un vecindario convergen en una oficina central local. En contraste, la televisión por cable consiste en un solo cable largo que pasa por todas las casas del mismo vecindario. Suponga que un cable de TV fuera de fibra óptica de 10 Gbps en lugar de cable de cobre. ¿Podría utilizarse para simular un modelo telefónico en el que todo mundo tuviera su propia línea privada a la oficina central local? Si esto fuera posible, ¿cuántas casas con un teléfono podrían conectarse a una sola fibra óptica?

R= Haciendo caso omiso de compresión de voz, un teléfono digital PCM necesita 64 Kbps Si dividir 10 Gbps por 64 Kbps que recibimos 156.250 viviendas por cable. Los sistemas actuales tienen cientos de casas por cable.

55. Un sistema de TV por cable tiene cien canales comerciales y todos ellos alternan programas con anuncios. ¿Esto es más parecido a TDM o a FDM?

R= Es a la vez. Cada uno de los 100 canales se le asigna su propia banda de frecuencias (FDM), y en cada canal de las dos corrientes lógicas se entremezclan por TDM. Este ejemplo es el mismo que el ejemplo de radio AM dada en el texto, pero tampoco es un fantástico ejemplo de TDM, porque la alternancia es irregular.

56. Una compañía de cable decide proporcionar acceso a Internet a través de cable en un vecindario que consiste en 5000 casas. La compañía utiliza cable coaxial y asignación de espectro que permite un ancho de banda descendente de 100 Mbps por cable. Para atraer clientes la compañía decide garantizar un ancho de banda descendente de por lo menos 2 Mbps a cada casa en cualquier momento. Describa lo que necesita hacer la compañía de cable para proporcionar esta garantía.

R= Una garantía de 2 Mbps de ancho de banda descendente a cada casa implica a lo sumo 50 viviendas por cable coaxial. De este modo, la compañía de cable tendrán que dividir el existente cable en cables coaxiales 100 y conectar cada uno de ellos directamente a un fibra nodo.

57. Tomando en cuenta la asignación espectral mostrada en la figura 2-48 y la información dada en el texto, ¿cuántos Mbps necesita asignar el sistema por cable al flujo ascendente y cuántos al flujo descendente?

R= El ancho de banda ascendente es de 37 MHz Uso de QPSK con 2 bits / Hz, se obtiene 74 Mbps de carga. Aguas abajo tenemos 200 MHz Usando QAM-64, esto es 1200 Mbps Usando QAM-256, esto es de 1600 Mbps

58. ¿Qué tan rápido un usuario de cable puede recibir datos si la red está inactiva?

R= Incluso si el canal aguas abajo funciona a 27 Mbps, el interfaz de usuario es casi siempre de 10-Mbps Ethernet. No hay manera de conseguir bits a la computadora más rápido de 10 Mbps en estas circunstancias. Si la conexión entre el PC y el módem de cable Ethernet es rápida, a continuación, los 27 Mbps completos pueden estar disponibles. Por lo general, los operadores de cable especificar Ethernet de 10 Mbps, ya que no quieren un usuario chupando el ancho de banda.

Titulo Libro	Redes de Computadoras
Titulo del Capitulo	Capitulo 3 – La Capa de Enlace de Datos
No. Ejercicios	37
Fecha de Realización	VERANO 2012

CAPITULO 3

1. Un mensaje de capa superior se divide en 10 tramas, cada una de las cuales tiene 80% de probabilidad de llegar sin daño. Si el protocolo de enlace de datos no lleva a cabo control de errores, ¿cuántas veces debe reenviarse el mensaje en promedio para conseguir que pase todo?

R= Dado que cada cuadro tiene una oportunidad de conseguir a través de 0,8, la probabilidad de que el mensaje completo es conseguir a través de 0,810, que es aproximadamente 0,107. Llame a este valor p . El número previsto de las transmisiones de un mensaje completo es entonces:

$$E = \sum_{i=1}^{\infty} ip(1-p)^{i-1} = p \sum_{i=1}^{\infty} i(1-p)^{i-1}$$

Para reducir este problema, utilice la fórmula bien conocida por la suma de un infinito serie geométrica:

$$S = \sum_{i=1}^{\infty} \alpha^i = \frac{1}{1-\alpha}$$

Diferenciar ambos lados con respecto a α para obtener:

$$S' = \sum_{i=1}^{\infty} i\alpha^{i-1} = \frac{1}{(1-\alpha)^2}$$

Ahora use $\alpha = 1 - p$ para obtener $E = 1 / p$. Por lo tanto, se necesita un promedio de 1/0.107, o Cerca de 9.3 transmisiones.

2. La siguiente codificación de caracteres se utiliza en un protocolo de enlace de datos:

A: 01000111; B: 11100011; FLAG: 01111110; ESC: 11100000

Muestre la secuencia de bits transmitida (en binario) para la trama de cuatro caracteres: A B ESC FLAG cuando se utiliza cada uno de los siguientes métodos de entramado:

- (a) Conteo de caracteres.
- (b) Bytes de bandera con relleno de bytes.
- (c) Bytes de bandera de inicio y final, con relleno de bits.

R= La solución es:

(A) 00.000.100 01.000.111 11.100.011 11.100.000 01.111.110

(B) 01111110 01000111 11100011 11100000 11100000 11100000 01111110 01111110

(C) 01.111.110 01.000.111 110.100.011 111.000.000 011.111.010 01.111.110

3. El siguiente fragmento de datos ocurre a la mitad de un flujo de datos para el cual se ha usado el algoritmo de relleno de bytes descrito en el texto: A B ESC C ESC FLAG FLAG D. ¿Cuál es la salida tras el relleno?

R= Una vez llena, tenemos AB C ESC ESC ESC ESC ESC ESC FLAG BANDERA D.

4. Uno de sus compañeros ha señalado que es un desperdicio terminar cada trama con un byte de bandera e iniciar la siguiente con otro. Un solo byte de bandera podría hacer el trabajo, por lo que un byte guardado es un byte ganado. ¿Usted está de acuerdo?

R= Si siempre se podía contar con un sinfín de marcos, un byte de marcas podría ser suficiente. Pero lo que si termina un marco (con un byte de marcas) y no hay nueva marcos durante 15 minutos. ¿Cómo el receptor sabe que el siguiente byte es en realidad el inicio de un nuevo cuadro y no sólo el ruido en la línea? El protocolo es mucho más simple, con inicio y final de bandera bytes.

5. Una cadena de bits, 011110111110111110, necesita transmitirse en la capa de enlace de datos. ¿Cuál es la cadena que realmente se está transmitiendo después del relleno de bits?

R= La salida es 011110111110011111010.

6. Cuando se usa relleno de bits, ¿es posible que la pérdida, inserción o modificación de un solo bit cause un error que la suma de verificación no detecte? Si no, ¿por qué no? Si es así, explique cómo. ¿Desempeña aquí un papel la longitud de la suma de verificación?

R= Es posible. Supongamos que el texto original contiene la secuencia de bits 01111110 como datos. Después de relleno de bits, esta secuencia se muestra como 011111010. Si el segundo 0 se pierde debido a un error de transmisión, lo que es recibido es 01111110, que el receptor ve como el extremo del bastidor. A continuación, examina justo antes del final de la trama para la suma de comprobación y verifica. Si la suma de comprobación es de 16 bits, hay una posibilidad entre 216 de que, accidentalmente, será la correcta, dando lugar a un marco correcto de ser aceptado. Cuanto más larga sea la suma de comprobación, el reducir la probabilidad de un error al obtener a través sin ser detectados, pero la probabilidad nunca es cero.

7. ¿Puede pensar en alguna circunstancia en la cual podría ser preferible un protocolo de ciclo abierto (por ejemplo, un código de Hamming) a los protocolos tipo realimentación analizados a lo largo de este capítulo?

R= Si el retardo de propagación es muy largo, como en el caso de una sonda en el espacio o cerca de Marte o Venus, la corrección de error se indica hacia adelante. También es conveniente, en una situación militar en la que el receptor no desea revelar su ubicación transmitiendo. Finalmente, en tiempo real sistemas no pueden tolerar la espera de las retransmisiones.

8. Para proporcionar mayor confiabilidad de la que puede dar un solo bit de paridad, un esquema de codificación de detección de errores usa un bit de paridad para todos los bits de número par. ¿Cuál es la distancia de Hamming de este código?

R= Hacer un cambio a cualquier carácter válido no puede generar otro carácter válido debido a la naturaleza de los bits de paridad. Hacer dos cambios para igualar bits o dos cambios en los bits impares dará otro carácter válido, por lo que la distancia es de 2.

9. Se utiliza el código de Hamming para transmitir mensajes de 16 bits. ¿Cuántos bits de verificación se necesitan para asegurar que el receptor pueda detectar y corregir errores de un solo bit? Muestre el patrón de bits transmitido para el mensaje 1101001100110101. Suponga que se utiliza paridad par en el código de Hamming.

R= Los bits de paridad son necesarios en las posiciones 1, 2, 4, 8 y 16, por lo que los mensajes que no extienden más allá de bits 31 (incluyendo los bits de paridad) en forma. Así, cinco bits de paridad son suficientes. El patrón de bits de transmisión es 011010110011001110101.

10. Un byte de 8 bits con un valor binario de 10101111 se va a codificar utilizando código de Hamming de paridad par. ¿Cuál es el valor binario que resulta de la codificación?

R= El valor codificado es 101001001111.

11. Un código de Hamming de 12 bits, cuyo valor hexadecimal es 0xE4F, llega al receptor. ¿Cuál era el valor hexadecimal original? Suponga que no más de un bit es erróneo.

R= Si el número de los bits de izquierda a derecha a partir de 1 bit, en este ejemplo, el bit 2 (un bit de paridad) es incorrecta. El valor de 12-bit transmitido (después de Hamming codificación) fue 0xA4F. El original de 8 bits de datos de valor era 0xAF.

12. Una manera de detectar errores es transmitir los datos como un bloque de n filas de k bits por fila y agregar bits de paridad a cada fila y a cada columna. La esquina inferior derecha es un bit de paridad que verifica su fila y su columna. ¿Detectará este esquema todos los errores sencillos? ¿Los errores dobles? ¿Los errores triples?

R= Un solo error hará que tanto las comprobaciones de paridad horizontal y vertical para ser mal. Dos errores también se detectan fácilmente. Si están en filas diferentes, la paridad de fila atraparlos. Si están en la misma fila, columna de la paridad será su captura. Tres errores podría deslizarse por detectada, por ejemplo, si alguna bits se invierte junto con su fila y los bits de paridad de columna. Incluso la esquina poco no coger esta.

13. Un bloque de bits con n filas y k columnas usa bits de paridad horizontales y verticales para la detección de errores. Suponga que se invierten exactamente 4 bits debido a errores de transmisión. Deduzca una expresión para la probabilidad de que el error no sea detectado.

R= Describir un patrón de error como una matriz de n filas por columnas k. Cada uno de los bits correctos es un 0, y cada uno de los bits incorrectos es un 1. Con cuatro errores por bloque, cada bloque tendrá exactamente cuatro 1s. ¿Cuántos de esos bloques son no? Hay muchas maneras nk para elegir dónde poner el primero un poco, nk - 1 maneras elegir el segundo, y así sucesivamente, de modo que el número de bloques es NK (NK-1) (NK-2) (NK-3). Los errores no detectados sólo ocurren cuando los cuatro bits 1 están en los vértices de un rectángulo. Las coordenadas cartesianas, cada bit 1 es en una coordenada (x, y), donde $0 \leq x < k$, y $0 \leq y < n$. Supongamos que el bit más cercana al origen (el vértice inferior izquierdo) está en (p, q). El número de legales rectángulos es (k - p - 1) (n - q - 1). Entonces, el número total de rectángulos puede se encuentra mediante la suma de esta fórmula para todos los posibles p y q. La probabilidad de que un error no detectado es entonces el número de tales rectángulos dividido por el número de maneras para distribuir los cuatro bits:

$$\frac{\sum_{p=0}^{k-2n-2} \sum_{q=0}^{n-1} (k-p-1)(n-q-1)}{nk(nk-1)(nk-2)(nk-3)}$$

14. ¿Qué residuo se obtiene al dividir $x^7 + x^5 + 1$ entre el polinomio generador $x^3 + 1$?

R= El resto es $x^2 + x + 1$.

15. Un flujo de bits 10011101 se transmite utilizando el método estándar CRC que se describió en el texto. El generador polinomial es $x^3 + 1$. Muestre la cadena de bits real que se transmite. Suponga que el tercer bit, de izquierda a derecha, se invierte durante la transmisión. Muestre que este error se detecta en el lado receptor.

R= El marco es 10011101. El generador es 1001. El mensaje después de anexar tres ceros es 10011101000. El resto de dividir por el 10011101000 1001 es 100. Por lo tanto, la cadena de bits reales de transmisión es 10011101100. El flujo de bits recibidos con un error en el tercer bit desde la izquierda es 10111101100. Dividiendo esta por 1001 produce un resto 100, que es diferente de cero. De este modo, el receptor detecta el error y puede solicitar una retransmisión.

16. Los protocolos de enlace de datos casi siempre ponen el CRC en un terminador, en lugar de un encabezado. ¿Por qué?

R= El CRC se calcula durante la transmisión y se añade a la secuencia de salida tan pronto como el último bit se apaga sobre el alambre. Si el CRC estaba en la cabecera, sería necesario para hacer un pase sobre el marco para calcular el CRC antes de transmitir. Esto requeriría cada byte para ser manipulados dos veces: una para la suma de comprobación y una vez que para la transmisión. Usando el remolque corta el trabajo en medio.

17. Un canal tiene una tasa de bits de 4 kbps y un retardo de propagación de 20 mseg. ¿Para qué intervalo de tamaños de trama, la parada y espera da una eficiencia de cuando menos 50%?

R= La eficiencia será del 50% a la hora de transmitir la trama es igual a la de ida y vuelta retardo de propagación. A una velocidad de transmisión de 4 bits / MS, 160 bits lleva a 40 ms. Para tamaños por encima de 160 bits, stop-and-wait es razonablemente eficiente.

18. Una troncal T1 de 3000 km de longitud se usa para transmitir tramas de 64 bytes con el protocolo 5. Si la velocidad de propagación es de 6 μ seg/km, ¿de cuántos bits deben ser los números de secuencia?

R= Para operar de manera eficiente, el espacio de secuencia (en realidad, el tamaño de la ventana de envío) debe ser suficientemente grande para permitir que el transmisor para mantener la transmisión hasta el primer reconocimiento se ha recibido. El tiempo de propagación es de 18 ms. En T1 velocidad, que es 1,536 Mbps (excluyendo el bit de cabecera 1), un bastidor 64-byte toma 0,300 ms. Por lo tanto, el primer fotograma completamente llega 18,3 mseg después de su la transmisión se inició. El reconocimiento tiene otros 18 ms para obtener espalda, además de una pequeña (insignificante) tiempo para el acuse de recibo al llegar completamente. En total, esta vez es de 36.3 ms. El transmisor debe tener suficiente ventana espacio para seguir el 36,3 ms. Un marco de toma 0,3 ms, por lo que se necesita 121 marcos para llenar la tubería. Siete bits números de secuencia son necesarios.

19. En el protocolo 3, ¿es posible que el emisor inicie el temporizador cuando éste ya está en ejecución? De ser así, ¿cómo podría ocurrir? De lo contrario, ¿por qué no es posible?

R= Puede suceder. Supongamos que el emisor envía una trama confusa y una el reconocimiento se vuelve rápidamente. El bucle principal se ejecutará un por segunda vez y un marco será enviado mientras el temporizador está en funcionamiento.

20. Imagine un protocolo de ventana corrediza que utiliza tantos bits para los números de secuencia que nunca ocurre un reinicio. ¿Qué relaciones deben mantenerse entre los cuatro límites de la ventana y el tamaño de la ventana, que es constante y el mismo tanto para el emisor como para el receptor?

R= Vamos a la ventana del emisor es (SL, D) y la del receptor será (RI, Ru). Deje que el tamaño de la ventana será W. Las relaciones que deben mantenerse son:

$$0 \leq S_u - S_l + 1 \leq W$$

$$R_u - R_l + 1 = W$$

$$S_l \leq R_l \leq S_u + 1$$

21. Si el procedimiento `between` del protocolo 5 revisara la condición $a \leq b \leq c$ en lugar de la condición $a \leq b < c$, ¿tendría esto algún efecto en la corrección o en la eficiencia del protocolo? Explique su respuesta.

R= El protocolo sería incorrecto. Supongamos que el 3-bits números de secuencia son en utilizar. Considere el siguiente escenario: Una acaba de enviar la trama 7. B recibe el marco y envía un ACK cuetas. A recibe el ACK y envía tramas 0-6, todos los cuales se pierden. B veces hacia fuera y retransmite su marco actual, con la confirmación 7. Mira la situación en un cuando el marco de `r.ack` = 7 llega. La clave variables se `AckExpected` = 0, `r.ack` = 7, y `NextFrameToSend` = 7. La modificado entre devolverá true, causando una de las tramas perdidas que fueron que se reconoce.

22. En el protocolo 6, cuando llega una trama de datos, se hace una revisión para ver si el número de secuencia es diferente del esperado y si `no_nak` es verdadero. Si ambas condiciones se cumplen, se envía una NAK. De otra manera, se arranca el temporizador auxiliar. Suponga que se omite la cláusula `else`. ¿Afectará este cambio la corrección del protocolo?

R= Sí. Ello nos podría llevar a un punto muerto. Supongamos que un lote de cuadros llegó correctamente y fueron aceptadas. A continuación, el receptor podría avanzar en su ventana. Ahora bien, supongamos que todos los reconocimientos se han perdido. El remitente finalmente el tiempo de espera y enviar el primer fotograma de nuevo. El receptor enviará una NAK. Supongamos que este se perdió. A partir de ese momento, el emisor mantendría el tiempo de espera y el envío de un marco que ya había sido aceptada, pero el receptor simplemente lo ignoran. Configuración de los resultados del temporizador auxiliares en una correcta reconocimiento de ser enviado de vuelta con el tiempo su lugar, que vuelve a sincronizar.

23. Suponga que el ciclo `while` de tres instrucciones cerca del final del protocolo 6 se elimina del código. ¿Afectará esto la corrección del protocolo o sólo su desempeño? Explique su respuesta.

R= Esto conduciría a un punto muerto porque este es el único lugar que de entrada reconocimientos se procesan. Sin este código, el emisor mantendría el tiempo de espera y no hacer ningún progreso.

24. Suponga que el caso para errores de suma de verificación fuera eliminado de la instrucción `switch` del protocolo 6. ¿Cómo afectará este cambio la operación del protocolo?

R= Se acabaría con el propósito de contar con NAK, por lo que tendría que caer de nuevo a tiempos de espera. Aunque el rendimiento se degrada, la corrección sería no se ven afectados. Las NAK no son esenciales.

25. En el protocolo 6, el código de `frame_arrival` tiene una sección que se usa para los NAKs. Dicha sección se invoca si la trama entrante es una NAK y se cumple otra condición. Describa un escenario en el que la presencia de esta otra condición sea esencial.

R= Considere el siguiente escenario. A envía 0 a B. B recibe y envía un ACK, pero la confirmación se pierde. A tiempo de espera y repeticiones 0, pero ahora espera que B 1, por lo que envía un NAK. Si una simple re-envió un `r.ack`, estaría enviando el cuadro 1, que no ha conseguido todavía.

26. Imagine que está escribiendo el software de la capa de enlace de datos para una línea que se usa para enviar datos a usted, pero no desde usted. El otro extremo usa HDLC, con un número de secuencia de tres bits y un tamaño de ventana de siete tramas. Usted podría querer almacenar en el búfer tantas tramas fuera de secuencia como fuera posible para aumentar la eficiencia, pero no se le permite modificar el software del lado emisor. ¿Es posible tener una ventana de receptor mayor que uno y aun así garantizar que el protocolo nunca fallará? De ser así, ¿cuál es el tamaño de la ventana más grande que se puede usar con seguridad?

R= No. El tamaño de la ventana de recepción máxima es de 1. Supongamos que eran 2. Inicialmente, el emisor envía marcos 0-6. Todos son recibidos y reconocidos, pero el reconocimiento se pierde. El receptor está preparado para aceptar 7 y 0. Cuando la retransmisión de 0 llega al receptor, se tamponada y 6 reconocido. Cuando se presenta en 7, 7 y 0 se pasa al locales, creando así un fallo de protocolo.

27. Considere la operación del protocolo 6 en una línea de 1 Mbps libre de errores. El tamaño máximo de trama es de 1000 bits. Se generan nuevos paquetes a intervalos aproximados de 1 segundo. El tiempo de expiración del temporizador es de 10 mseg. Si se eliminara el temporizador especial de confirmación de recepción ocurrirían terminaciones de temporizador innecesarias. ¿Cuántas veces se transmitiría el mensaje promedio?

R= Supongamos que A, B envía una trama que llegó correctamente, pero no hubo marcha atrás tráfico. Después de un tiempo sería un tiempo de espera y retransmitir. B daría cuenta de que el número de secuencia es incorrecta, ya que el número de secuencia está por debajo de `FrameExpected`. Por consiguiente, sería enviar un NAK, que lleva un número de reconocimiento. Cada cuadro se enviaría exactamente dos veces.

28. En el protocolo 6, $MAX_SEQ = 2n - 1$. Si bien esta condición es evidentemente deseable para utilizar de manera eficiente los bits de encabezado, no hemos demostrado que sea esencial. ¿Funciona correctamente el protocolo con $MAX_SEQ = 4$, por ejemplo?

R= No. Esta aplicación falla. Con $MaxSeq = 4$, obtenemos $NrBufs = 2$. La incluso números de secuencia de uso de búfer 0 y los impares usar tampón 1. Este mapeo significa que los marcos 4 y 0 tanto utilizar el mismo tampón. Supongamos que cuadros 0-3 se reciben y se reconoció. La ventana del receptor contiene ahora 4 y 0. Si se pierde 4 y llega a 0, se pondrá en tampón 0 y llegó a [0] se establece en true. Este protocolo requiere $MaxSeq$ ser extraño para funcionar correctamente. Sin embargo, otras implementaciones de los protocolos de ventana corrediza no todos tienen esta propiedad.

29. Se están enviando tramas de 1000 bits a través de un canal de 1 Mbps utilizando un satélite geoestacionario cuyo tiempo de propagación desde la Tierra es de 270 mseg. Las confirmaciones de recepción siempre se superponen en las tramas de datos. Los encabezados son muy cortos. Se usan números de secuencia de tres bits. ¿Cuál es la utilización máxima de canal que se puede lograr para:

(a) Parada y espera?

(b) El protocolo 5?

(c) El protocolo 6?

R= Sea $t = 0$ indicar el comienzo de la transmisión. En $t = 1$ mseg, el primer fotograma tiene sido completamente transmitida. En $t = 271$ mseg, el primer fotograma ha llegado completamente. En $t = 272$ ms, el marco de reconocimiento de la primera ha sido totalmente enviado. En $t = 542$ ms, la trama de confirmación de soporte ha llegado plenamente. Por lo tanto, el ciclo es 542 ms. Un total de marcos k se envían en 542 ms, para un eficiencia de $k/542$. Por lo tanto:

(A) $k = 1$, la eficiencia = $1/542 = 0,18\%$

(B) $k = 7$, la eficiencia = $7/542 = 1,29\%$

(C) $k = 4$, la eficiencia = $4/542 = 0,74\%$

30. Calcule la fracción del ancho de banda que se desperdicia en sobrecarga (encabezados y retransmisiones) para el protocolo 6 en un canal satelital de 50 kbps con carga pesada, usando tramas de datos consistentes en 40 bits de encabezado y 3960 bits de datos. Asuma que el tiempo de propagación de la señal de la Tierra al satélite es de 270 mseg. Nunca ocurren tramas ACK. Las tramas NAK son de 40 bits. La tasa de errores de las tramas de datos es de 1%, y la tasa de errores para las tramas NAK es insignificante. Los números de secuencia son de 8 bits.

R= Con un canal de 50 Kbps y números de 8 bits de la secuencia, la tubería está siempre llena. El número de retransmisiones por cuadro es de aproximadamente 0,01. Cada buen marco desechos de 40 bits de cabecera, más 1% de 4000 bits (retransmisión), además de un 40-bits NAK una vez cada 100 marcos. La sobrecarga total es de 80,4 bits por los datos de 3960 los bits, por una fracción de $80,4 / (3960 + 80,4) = 1,99$ por ciento.

31. Considere un canal satelital de 64 kbps libre de errores que se usa para enviar tramas de datos de 512 bytes en una dirección y devolver confirmaciones de recepción muy cortas en la otra. ¿Cuál es la velocidad real de transporte máxima con tamaños de ventana de 1, 7, 15 y 127? El tiempo de propagación de la Tierra al satélite es de 270 mseg.

R= La transmisión se inicia en el instante $t = 0$. En $t = 4096/64000$ seg = 64 ms, el último bit se envía. En $t = 334$ ms, el último bit llega al satélite y el muy corto ACK se envía. En $t = 604$ ms, el ACK llega a la tierra. La velocidad de datos aquí es de 4096 bits en 604 ms o 6781 bps acerca. Con un tamaño de ventana de 7 marcos, el tiempo de transmisión es 448 ms para la ventana completa, en cuyo momento el remitente tiene que parar. En 604 milisegundos, que llegue el primer ACK y el ciclo puede comenzar nuevo. Aquí tenemos $7 \times 4096 = 28.672$ bits en 604 ms. La velocidad de

datos es 47,470.2 puntos básicos. Transmisión continua sólo puede ocurrir si el emisor es aún cuando el primer envío de ACK vuelve en $t = 604$ ms. En otras palabras, si el tamaño de la ventana es mayor que 604 mseg valor de transmisión, que puede funcionar a velocidad completa. Para un tamaño de ventana de 10 o mayor, se cumple esta condición, por lo que para cualquier tamaño de ventana de 10 o mayor (por ejemplo, 15 o 127), la velocidad de datos es de 64 Kbps

32. Un cable de 100 km de longitud opera con una tasa de datos T1. La velocidad de propagación del cable es $\frac{2}{3}$ de la velocidad de la luz en el vacío. ¿Cuántos bits caben en el cable?

R= La velocidad de propagación en el cable es de 200.000 km / s, o 200 km / ms, por lo que una 100 km de cable se llenará en 500 microsegundos. Cada marco T1 es 193 bits enviados en 125 microsegundos. Esto corresponde a cuatro cuadros, o 772 bits en el cable.

33. Suponga que modelamos el protocolo 4 mediante el modelo de máquina de estados finitos. ¿Cuántos estados existen para cada máquina? ¿Cuántos estados existen para el canal de comunicaciones? ¿Cuántos estados existen para todo el sistema (dos máquinas y el canal)? Ignore los errores de suma de verificación.

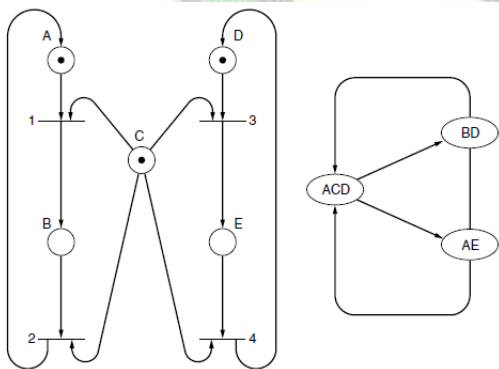
R= Cada máquina tiene dos variables clave: next3frame3to3send y frame3expected, cada uno de los cuales puede tomar los valores 0 o 1. Así, cada máquina puede estar en uno de los cuatro estados posibles. Un mensaje en el canal contiene el número de secuencia del marco que se envían y el número de secuencia del marco que se ACK. Por lo tanto, cuatro tipos de mensajes de existir. El canal puede contener 0 o 1 mensaje en cualquier dirección. Así, el número de estados del canal puede estar en es 1 con cero mensajes del mismo, de 8 con un mensaje en él, y 16 con dos mensajes sobre el mismo (un mensaje en cada dirección). En total hay $1 + 8 + 16 = 25$ estados de los canales posibles. Esto implica $4 \times 4 \times 25 = 400$ es posible estados para el sistema completo.

34. Dé la secuencia de activación para la red de Petri de la figura 3-23 correspondiente a la secuencia de estado (000), (01A), (01—), (010), (01A) de la figura 3-21. Explique con palabras lo que representa la secuencia.

R= La secuencia de disparo es de 10, 6, 2, 8. Corresponde a la aceptación de un incluso estructura, la pérdida del reconocimiento, tiempo de espera por el remitente, y la regeneración del reconocimiento por parte del receptor.

35. Dadas las reglas de transición $AC \rightarrow B$, $B \rightarrow AC$, $CD \rightarrow E$ y $E \rightarrow CD$, dibuje la red de Petri descrita. A partir de esta red, dibuje el grafo de estado finito alcanzable desde el estado inicial ACD. ¿Qué concepto bien conocido modelan estas reglas de transición?

R= La red de Petri y el gráfico de estado son las siguientes:



El modelo de sistema de exclusión mutua. B y E son secciones críticas que pueden no estar activas al mismo tiempo, es decir, el estado SER no está permitido. Lugar C representa un semáforo que puede ser capturado por A o D, pero no por tanto juntos.

36. PPP se basa estrechamente en HDLC, que utiliza relleno de bits para prevenir que los bytes de bandera accidentales dentro de la carga útil causen confusión. Dé por lo menos una razón por la cual PPP utiliza relleno de bytes.

R= PPP fue claramente diseñado para ser implementado en software, no en el hardware como HDLC es casi siempre. Con una implementación de software, trabajando de manera totalmente con bytes es mucho más sencillo que trabajar con bits individuales. Además, PPP fue diseñado para ser utilizado con los módems y los módems de aceptar y transmitir los datos en unidades de 1 byte, no bit 1.

37.Cuál es la sobrecarga mínima para enviar un paquete IP mediante PPP? Tome en cuenta sólo la sobrecarga introducida por el PPP mismo, no la del encabezado IP.

R= En su más pequeño, cada cuadro tiene dos bytes de bandera, un byte de protocolo, y dos bytes de suma de comprobación, para un total de cinco bytes de cabecera por trama.

Título Libro	Redes de Computadoras
Título del Capítulo	Capítulo 4 – La Subcapa de Control de Acceso al Medio
No. Ejercicios	45
Fecha de Realización	VERANO 2012

CAPITULO 4

1. Para este problema, utilice una fórmula de este capítulo, pero primero enúnciela. Las tramas arriban de manera aleatoria a un canal de 100 Mbps para su transmisión. Si el canal está ocupado cuando arriba una trama, ésta espera su turno en una cola. La longitud de la trama se distribuye exponencialmente con una media de 10,000 bits/trama. Para cada una de las siguientes tasas de llegada de tramas, dé el retardo experimentado por la trama promedio, incluyendo tanto el tiempo de encolamiento como el de transmisión.

- (a) 90 tramas/seg.
- (b) 900 tramas/seg.
- (c) 9000 tramas/seg.

R= La fórmula es la fórmula estándar para Markov cola figuran en la sección 4.1.1, es decir, $T = 1 / (\mu C - \lambda)$. Aquí $C = 108$ y $\mu = 4.10$, por lo que $T = 1 / (10000 - \lambda)$ seg. Para los tres tipos de llegada, se obtiene (a) 0,1 ms, (b) 0,11 ms, (c) 1 mseg. Para el caso (c) estamos operando un sistema de colas con $\rho = \lambda / \mu C = 0,9$, lo que da el retardo $\times 10$.

2. Un grupo de N estaciones comparte un canal ALOHA puro de 56 kbps. La salida de cada estación es una trama de 1000 bits en promedio cada 100 seg aun si la anterior no ha sido enviada (por ejemplo, las estaciones pueden almacenar en búfer las tramas salientes). ¿Cuál es el valor máximo de N?

R= Con ALOHA puro el ancho de banda utilizable es $0,184 \times 56 \text{ Kbps} = 10,3 \text{ Kbps}$ Cada estación requiere 10 puntos básicos, por lo que $N = 10.300 / 10 = 1030$ estaciones.

3. Considere el retardo del ALOHA puro comparándolo con el ALOHA ranurado cuando la carga es baja. ¿Cuál es menor? Explique su respuesta.

R= Con ALOHA puro, la transmisión puede comenzar de inmediato. Con poca carga, no se producen colisiones se espera que la transmisión es probable que tenga éxito. Con ranurado ALOHA, tiene que esperar a la siguiente ranura. Esto introduce un tiempo medio de ranura demore.

4. Diez mil estaciones de reservaciones de una aerolínea compiten por un solo canal ALOHA ranurado. La estación promedio hace 18 solicitudes/hora. Una ranura dura 125 μ seg. ¿Cuál es la carga aproximada total del canal?

R= Cada terminal realiza una solicitud cada segundo 200, para una carga total de 50 peticiones por segundo. Por lo tanto $G = 50/8000 = 1/160$.

5. Una gran población de usuarios de ALOHA genera 50 solicitudes/seg incluidas tanto originales como retransmisiones. El tiempo se divide en ranuras de 40 mseg.

(a) ¿Cuál es la oportunidad de éxito en el primer intento?

(b) ¿Cuál es la probabilidad exacta de k colisiones y después tener éxito?

(c) ¿Cuál es el número esperado de intentos de transmisión necesarios?

R= (A) con $G = 2$, la ley de Poisson da una probabilidad de correo e^{-2} . (B) $(1 - e^{-G})^k e^{-G} = 0,135 \times 0,865^k$. (C) El número esperado de transmisiones es, por ejemplo $= 7,4$.

6. Mediciones en un canal ALOHA ranurado con una cantidad infinita de usuarios muestra que 10% de las ranuras están inactivas.

(a) ¿Qué carga, G, tiene el canal?

(b) ¿Cuál es la velocidad real de transporte?

(c) ¿El canal está subcargado o sobrecargado?

R= (A) de la ley de Poisson de nuevo, $P_0 = e^{-G}$, por lo que $G = -\ln P_0 = -\ln 0,1 = 2,3$. (B) Uso de $S = G e^{-G}$ con $G = 2,3$ y $E = G - 0,1$, $S = 0,23$. (C) Cuando $G > 1$, el canal está sobrecargado, por lo que está sobrecargado.

7. En un sistema ALOHA ranurado de población infinita, la cantidad media de ranuras que espera una estación entre una colisión y su retransmisión es de 4. Grafique la curva de retardo contra velocidad real de transporte de este sistema.

R= El número de transmisiones es $E =$ por ejemplo. Los eventos están separados por $E - 1$ intervalos de cuatro ranuras cada uno, de modo que el retardo es 4 (por ejemplo - 1). El rendimiento se da por $S = G e^{-G}$. Por lo tanto, tenemos dos ecuaciones paramétricas, uno por el retraso y una para el rendimiento, tanto en términos de G. Para cada valor de G es posible encontrar el retraso correspondiente y el rendimiento, produciendo un punto de la curva.

8. ¿Cuánto debe esperar una estación, s, en el peor de los casos, antes de empezar a transmitir su trama sobre una LAN que utiliza:

(a) el protocolo básico de mapa de bits?

(b) el protocolo de Mok y Ward con cambio de números virtuales de estación?

R= (A) El peor de los casos es la siguiente: todas las estaciones desea enviar y s es el número más bajo estación. El tiempo de espera período de bit N argumento $+(n - 1) \times d$ bits para la transmisión de de marcos. El total es $n + (n - 1) d$ veces bits. (B) El peor de los casos es la siguiente: todas las estaciones tienen marcos para transmitir y s tiene el menor número de estación virtual. Por lo tanto, s también tendrá su turno para transmitir después de la otra $N - 1$ estaciones han transmite una trama cada uno, y los períodos de contención de $N \log_2 N$ el tamaño de cada uno. El tiempo de espera es, pues, $(N - 1) \times D + n \times \log_2 \text{bits}$.

9. Una LAN usa la versión de Mok y Ward del conteo descendente binario. En cierto momento, las 10 estaciones tienen los números de estación virtual 8, 2, 4, 5, 1, 7, 3, 6, 9 y 0. Las tres estaciones siguientes que van a enviar son: 4, 3 y 9, en ese orden. ¿Cuáles son los nuevos números de estación virtual una vez que las tres han terminado sus transmisiones?

R= Cuando la estación 4 envía, se convierte en 0, y 1, 2 y 3 se incrementa en 1. Cuando la estación 3 envía, se convierte en 0, y 0 1, y 2 se incrementa en 1. Por último, cuando la estación 9 envía, se convierte en 0 y todas las otras estaciones se incrementan por 1. El resultado es 9, 1, 2, 6, 4, 8, 5, 7, 0 y 3.

10. Dieciséis estaciones contienen por un canal compartido que usa el protocolo de recorrido de árbol. Si todas las estaciones cuyas direcciones son números primos de pronto quedaran listas al mismo tiempo, ¿cuántas ranuras de bits se necesitan para resolver la contención?

R= Estaciones 2, 3, 5, 7, 11 y 13 desea enviar. Once ranuras son necesarias, con el contenido de cada ranura es como sigue:

Ranura 1: 2, 3, 5, 7, 11, 13

Ranura 2: 2, 3, 5, 7

Ranura 3: 2, 3

Ranura 4: 2

Ranura 5: 3

Ranura 6: 5, 7

Ranura 7: 5

Ranura 8: 7

Ranura 9: 11, 13

Ranura 10: 11

Ranura 11: 13

11. Un conjunto de $2n$ estaciones usa el protocolo de recorrido de árbol adaptable para arbitrar el acceso a un cable compartido. En cierto momento, dos de ellas quedan listas. ¿Cuál es el número de ranuras mínimo, máximo y medio para recorrer el árbol si $2n - 1$?

R= El número de franjas horarias necesarias depende de qué tan atrás en el árbol hay que ir para encontrar un ancestro común de las dos estaciones. Si tienen el mismo padre (es decir, un nivel de vuelta), lo que ocurre con una probabilidad de 2^{-n} , que se necesita $2n + 1$ ranuras para recorrer el árbol. Si las estaciones tienen un abuelo común, que ocurre con una probabilidad de $2^{-n} + 1$, el recorrido del árbol tiene $2n - 1$ ranuras, etc. El peor de los casos es $2n + 1$ (antepasado común), y el mejor de los casos es de tres franjas horarias diferentes (estaciones de mitades del árbol). La media, m , está dada por

$$m = \sum_{i=0}^{n-1} 2^{-(n-i)} (2n + 1 - 2i)$$

Esta expresión puede simplificarse a:

$$m = (1 - 2^{-n})(2n + 1) - 2^{-(n-1)} \sum_{i=0}^{n-1} i 2^i$$

12. Las LANs inalámbricas que estudiamos usaban protocolos como MACA en lugar de CSMA/CD. ¿En qué condiciones sería posible usar CSMA/CD?

R= Las radios no puede recibir y transmitir en la misma frecuencia al mismo tiempo, así CSMA / CD no puede ser utilizado. Si este problema podría resolverse (por ejemplo, por equipando cada estación con dos radios), todavía existe el problema de que no todos estaciones de ser dentro del alcance de radio de la otra. Sólo si estos dos problemas puede ser resuelto, es el CSMA / CD a un candidato.

13. ¿Qué propiedades tienen en común los protocolos de acceso a canal WDMA y GSM?

R= Ambos utilizan una combinación de FDM y TDM. En ambos casos dedicados frecuencia (es decir, la longitud de onda) las bandas están disponibles, y éstos, en ambos casos bandas están ranurados para TDM.

14. Seis estaciones, de A a F, se comunican mediante el protocolo MACA. ¿Es posible que dos transmisiones tengan lugar de manera simultánea? Explique su respuesta.

R= Sí. Imagínese que ellos están en una línea recta y que cada estación puede llegar sólo a sus vecinos más cercanos. Entonces A puede enviar a B, mientras que E está enviando a la F.

15. Un edificio de oficinas de siete pisos tiene 15 oficinas adyacentes por piso. Cada oficina contiene un enchufe de pared para una terminal en la pared frontal, por lo que los enchufes forman una retícula triangular en el plano vertical, con una separación de 4 m entre enchufes, tanto vertical como horizontalmente. Suponiendo que es factible tender un cable recto entre cualquier par de enchufes, horizontal, vertical o diagonalmente, ¿cuántos metros de cable se necesitan para conectar todos los enchufes usando

(a) una configuración en estrella con un solo enrutador en medio?

(b) una LAN 802.3?

R= (a) El número de los pisos 1-7. En la configuración de estrella, el router está en el centro del piso 4. Los cables son necesarios para cada uno de los $7 \times 15 - 1 = 104$ sitios. La longitud total de estos cables es:

$$4 \sum_{i=1}^7 \sum_{j=1}^{15} \sqrt{(i-4)^2 + (j-8)^2}$$

La longitud total es de unos 1832 metros. (b) Para 802.3, 7 cables horizontales 56 m de largo se necesitan, más vertical de una cable de 24 m de largo, para un total de 416 m.

16. ¿Cuál es la tasa de baudios de la Ethernet de 10 Mbps estándar?

R= La Ethernet utiliza codificación Manchester, lo que significa que tiene dos señales períodos por bit enviado. La velocidad de datos del estándar Ethernet a 10 Mbps, por lo que el velocidad de transmisión es el doble.

17. Bosqueje la codificación Manchester para el flujo de bits: 0001110101.

R= La señal es una onda cuadrada con dos valores, alto (H) y baja (L). El patrón es:

LHLHLHHLHLHLLHLLHHL.

18. Bosqueeje la codificación diferencial Manchester para el flujo de bits del problema anterior. Suponga que la línea se encuentra inicialmente en el estado bajo.

R= El patrón de este tiempo es HLHLHLLHLLHLHLHLLH.

19. Una LAN CSMA/CD (no la 802.3) de 10 Mbps y 1 km de largo tiene una velocidad de propagación de 200 m/μseg. En este sistema no se permiten los repetidores. Las tramas de datos tienen 256 bits de longitud, incluidos 32 bits de encabezado, suma de verificación y un poco más de sobrecarga. La primera ranura de bits tras una transmisión exitosa se reserva para que el receptor capture el canal y envíe una trama de confirmación de recepción de 32 bits. ¿Cuál es la tasa de datos efectiva, excluyendo la sobrecarga, suponiendo que no hay colisiones?

R= El tiempo de propagación de ida y vuelta del cable es de 10 microsegundos. Una completa transmisión tiene seis fases: transmisor apodera del cable (10 microsegundos), transmitir datos (25,6 microsegundos). Demora para la última parte para llegar a la final (5,0 microsegundos) receptor apodera cable (10 microsegundos) acuse de recibo enviado (3,2 microsegundos). Demora para la última parte para llegar a la final (5,0 microsegundos). La suma de estos es 58,8 microsegundos. En este período, 224 bits de datos se envían, por una tasa de alrededor de 3,8 Mbps

20. Dos estaciones CSMA/CD intentan transmitir archivos grandes (multitrama). Tras el envío de cada trama, contienen por el canal usando el algoritmo de retroceso exponencial binario. ¿Cuál es la probabilidad de que la contención termine en la ronda k, y cuál es la cantidad media de rondas por periodo de contención?

R= Número de intentos de la adquisición a partir de 1. Intento que se distribuye entre $2^i - 1$ ranuras. Así, la probabilidad de una colisión en intento i es $2 - (i - 1)$. La probabilidad de que las primeras k - 1 intentos fallan, seguido de un éxito en todo el k es:

$$P_k = (1 - 2^{-(k-1)}) \prod_{i=1}^{k-1} 2^{-(i-1)}$$

Que se puede simplificar a:

$$P_k = (1 - 2^{-(k-1)}) 2^{-(k-1)(k-2)/2}$$

El número previsto de rondas es entonces sólo $\sum P_k$.

21. Considere la construcción de una red CSMA/CD que opere a 1 Gbps a través de un cable de 1 km de longitud sin repetidores. La velocidad de la señal en el cable es de 200,000 km/seg. ¿Cuál es el tamaño mínimo de trama?

R= Para un cable de 1-km, el tiempo de propagación de una vía es de 5 microsegundos, por lo $2\tau = 10$ microsegundos. Para hacer CSMA / CD trabajo, debe ser imposible transmitir un marco completo en este intervalo. A 1 Gbps, todos los cuadros de menos de 10.000 bits pueden ser completamente transmitidos en virtud de 10 microsegundos, por lo que el marco mínimo es de 10.000 bits o 1250 bytes.

22. Un paquete IP que se transmitirá a través de Ethernet tiene 60 bytes de longitud, incluyendo todos los encabezados. Si no se utiliza LLC, ¿se necesita relleno en la trama Ethernet, y de ser así, cuántos bytes?

R= El mínimo de trama Ethernet es de 64 bytes, incluyendo las dos direcciones en la red Ethernet encabezado de la trama, el campo tipo / longitud, y la suma de comprobación. Desde la cabecera campos ocupan 18 bytes y el paquete es de 60 bytes, el tamaño del marco total es de 78 bytes, lo cual excede el mínimo de 64 bytes. Por lo tanto, el relleno no se utiliza.

23. Las tramas Ethernet deben tener al menos 64 bytes de longitud para asegurar que el transmisor permanezca en línea en caso de que ocurra una colisión en el extremo más lejano del cable. Fast Ethernet tiene el mismo tamaño

mínimo de trama de 64 bytes pero puede recibir los bits diez veces más rápido. ¿Cómo es posible mantener el mismo tamaño mínimo de trama?

R= La longitud máxima del cable de Fast Ethernet es 1/10 en tanto que en Ethernet.

24. Algunos libros citan que el tamaño máximo de una trama Ethernet es de 1518 bytes en lugar de 1500. ¿Están en un error? Explique su respuesta.

R= La carga útil es de 1500 bytes, pero cuando la dirección de destino, dirección de origen, los campos de tipo / longitud, y suma de comprobación se cuentan también, el total es, en efecto 1518.

25. La especificación 1000Base-SX indica que el reloj debe correr a 1250 MHz, aun cuando se supone que Gigabit Ethernet funciona a 1 Gbps. ¿Esta velocidad más alta confiere un margen adicional de seguridad? Si no es así, ¿qué está pasando?

R= La codificación es sólo el 80% de eficiencia. Se tarda 10 bits de datos transmitidos a representar 8 bits de datos reales. En un segundo, 1250 megabits se transmiten, lo que significa 125 millones de palabras de código. Cada palabra de código representa 8 bits de datos, por lo que la velocidad de datos reales, en efecto 1000 megabits por segundo.

26. ¿Cuántas tramas por segundo puede manejar Gigabit Ethernet? Reflexione con cuidado y tome en cuenta todos los casos relevantes. Sugerencia: es importante el hecho de que se trata de Gigabit Ethernet.

R= La más pequeña trama Ethernet es de 512 bits, por lo menos 1 Gbps obtenemos 1.953.125 o casi 2 millones de marcos por segundo. Sin embargo, esto sólo funciona cuando el marco de ruptura está en funcionamiento. Sin marco de ruptura, tramas cortas se rellenan hasta 4096 bits, en cuyo caso el número máximo es de 244.140. Para la mayor bastidor (12.144 bits), no puede haber tantos como 82.345 fotogramas por segundo.

27. Mencione dos redes que permitan empaquetar tramas una tras otra. ¿Por qué es importante esta característica?

R= Gigabyte Ethernet que tiene y lo mismo ocurre con 802.16. Es útil para ancho de banda eficiencia (un preámbulo, etc.), sino también cuando hay un límite inferior en el bastidor tamaño.

28. En la figura 4.27 se muestran cuatro estaciones, A, B, C y D. ¿Cuál de las dos últimas estaciones cree que está más cerca de A y por qué?

R= La estación C es el más cercano a A, ya que escuchó la estrategia en tiempo real y responde a ella por la afirmación de su señal de NAV. D, no respondían por lo que debe estar fuera de radio de una rango.

29. Suponga que una LAN 802.11b de 11 Mbps transmite tramas de 64 bytes una tras otra sobre un canal de radio con una tasa de error de 10^{-7} . ¿Cuántas tramas por segundo en promedio resultarán dañadas?

R= Una trama contiene 512 bits. La tasa de error de bit es $p = 10^{-7}$. La probabilidad de que todos ellos de 512 supervivientes correctamente es $(1 - p)^{512}$, que es aproximadamente 0,9999488. La fracción de daños es, pues, alrededor de 5×10^{-5} . El número de cuadros / seg es $11 \times 10^6 / 512$ o 21 484 acerca. Multiplicando estos dos números juntos, obtener alrededor de un chasis dañado por segundo.

30. Una red 802.16 tiene un ancho de canal de 20 MHz. ¿Cuántos bits/seg se pueden enviar a una estación suscrita?

R= Depende de lo lejos que el abonado está. Si el abonado está cerca de, QAM-64 se utiliza para 120 Mbps Para distancias medias, QAM-16 se utiliza para 80 Mbps Para las estaciones distantes, QPSK se utiliza para 40 Mbps

31. El IEEE 802.16 soporta cuatro clases de servicio. ¿Cuál es la mejor clase de servicio para enviar vídeo sin comprimir?

R= De vídeo sin comprimir tiene una tasa de bits constante. Cada marco tiene la misma número de pixeles como el cuadro anterior. Así, es posible calcular muy con precisión cómo mucho ancho de banda se necesita y cuándo. En consecuencia, servicio de velocidad de bits constante es la mejor opción.

32. Dé dos razones por las cuales las redes podrían usar un código de corrección de errores en lugar de detección de errores y retransmisión.

R= Una de las razones es la necesidad de que en tiempo real la calidad del servicio. Si un error es descubierto, no hay tiempo para obtener una retransmisión. El show debe continuar. Corrección de errores se puede utilizar aquí. Otra razón es que en muy líneas de baja calidad (por ejemplo canales, inalámbricos), la tasa de error puede ser tan alta que prácticamente todos los marcos tendría que ser retransmitido, y de la distribución del probablemente sería dañado también. Para evitar esto, corrección de errores es utilizado para aumentar la fracción de las tramas que llegan correctamente.

33. En la figura 4-35 podemos ver que un dispositivo Bluetooth puede estar en dos piconets al mismo tiempo. ¿Hay alguna razón por la cual un dispositivo no pueda fungir como maestro en ambas al mismo tiempo?

R= Es imposible para un dispositivo para ser maestro en dos piconets al mismo tiempo. Hay dos problemas. En primer lugar, sólo 3 bits de dirección están disponibles en la cabecera al mismo tiempo hasta siete esclavos podían ser en cada piconet. Por lo tanto, no habría no hay manera de abordar de forma única cada esclavo. En segundo lugar, el código de acceso al comienzo del el marco se deriva de la identidad del maestro. Así es como los esclavos dicen cuál es el mensaje que pertenece a la piconet. Si se superponen dos piconets utilizó el mismo código de acceso, no habría forma de saber que enmarca a la que pertenecía piconet. En efecto, las dos piconets se fusionarán en una piconet grande en lugar de dos separadas.

34. La figura 4-25 muestra varios protocolos de capa física. ¿Cuál de éstos está más cercano al protocolo de capa física Bluetooth? ¿Cuál es la principal diferencia entre ambos?

R= Bluetooth utiliza FHSS, al igual que lo hace 802,11. La mayor diferencia es que Bluetooth salta a una velocidad de 1600 saltos / seg, mucho más rápido que 802,11.

35. Bluetooth soporta dos tipos de enlaces entre un maestro y un esclavo. ¿Cuáles son y para qué se utiliza cada uno?

R= Un canal de ACL es asincrónica, con marcos llegan de forma irregular ya que los datos son producido. Un canal de SCO es sincrónico, con los marcos que llegan periódicamente a una velocidad bien definida.

36. Las tramas de beacon en el espectro disperso con salto de frecuencia, variante del 802.11, contienen el tiempo de permanencia. ¿Cree que las tramas de beacon análogas de Bluetooth también contienen tiempo de permanencia? Explique su respuesta.

R= Ellos no lo hacen. El tiempo de permanencia en 802,11 no está estandarizada, por lo que tiene que ser anunció que las nuevas estaciones que llegan. En Bluetooth siempre es 625 microsegundos. No hay necesidad de anunciar este. Todos los dispositivos Bluetooth que este cableado en el chip. Bluetooth fue diseñado para ser barato, y fijar el tipo de salto y moran derivaciones de tiempo a un chip sencillo.

37. Considere las LANs interconectadas que se muestran en la figura 4-44. Suponga que los hosts a y b se encuentran en la LAN 1, c está en la LAN 2 y d está en la LAN 8. En principio, las tablas de hash de todos los puentes están vacías y se utiliza el árbol de expansión que se muestra en la figura 4-44(b). Muestre la manera en que cambian las tablas de hash de los diversos puentes después de que cada uno de los siguientes sucesos ocurren en secuencia, primero (a) y a continuación (b), y así sucesivamente.

(a) a envía a d.

(b) c envía a a.

(c) d envía a c.

(d) d pasa a la LAN 6.

(e) d envía a a.

R= El primer cuadro será remitida por cada puente. Después de esta transmisión, cada puente tendrá una entrada para un destino con un puerto adecuado en su tabla hash. Por ejemplo, la tabla hash D's ahora tendrán una entrada para reenviar marcos destinados a una LAN de 2. El segundo mensaje será visto por puentes B, D y A. Estos puentes añadirán una nueva entrada en su tabla hash para marcos destinados a c. Por ejemplo, la tabla hash puente de D's tendrá ahora otra entrada a los marcos futuros destinados a la c con LAN 2. El tercer mensaje se verá por puentes H, D, A y B. Estos puentes se añada un nuevo entrada en su tabla hash para los marcos destinados a d. El quinto mensaje será visto por los puentes E, C, B, D y A. Puentes E y C se añadirá una nueva entrada en su tabla hash para

los marcos destinados a la d, mientras que los puentes D, B, y una voluntad actualizar su entrada en la tabla hash para d destino.

38. Una consecuencia del uso de un árbol de expansión para reenviar tramas en una LAN extendida es que algunos puentes tal vez no participen en absoluto en el reenvío de tramas. Identifique tres puentes que se encuentren en esta situación en la figura 4-44. ¿Hay alguna razón para conservar estos puentes, aun cuando no se utilicen para el reenvío?

R= Puentes G, I y J no se utilizan para la transmisión de los marcos. La razón principal por tener bucles en una LAN extendida es para aumentar la fiabilidad. Si cualquier puente en el árbol actual que abarca falla, el que abarca (dinámico) algoritmo de árbol reconfigura el árbol de expansión en una nueva que puede incluir una o más de estos puentes, que no formaban parte del árbol de expansión anterior.

39. Suponga que un conmutador tiene tarjetas de línea para cuatro líneas de entrada. Con frecuencia, una trama que llega en una de las líneas tiene que salir en otra línea de la misma tarjeta. ¿A qué decisiones se enfrenta el diseñador del conmutador como resultado de esta situación?

R= La opción más sencilla es no hacer nada especial. Cada trama entrante se pone en el plano posterior y enviado a la tarjeta de destino, lo que podría ser la fuente tarjeta. En este caso, el tráfico intracard pasa sobre el plano posterior del interruptor. El otro la elección es el reconocimiento de este caso y tratarlo en especial, el envío de la trama directamente y no va a través del backplane.

40. Un conmutador diseñado para Fast Ethernet tiene una tarjeta madre que puede transportar 10 Gbps. ¿Cuántas tramas/seg puede manejar en el peor de los casos?

R= El peor caso es una corriente interminable de 64 bytes (512 bits) marcos. Si el plano posterior puede manejar 109 puntos básicos, el número de fotogramas que puede manejar es de $109/512$. Este es 1,953,125 cuadros / seg.

41. Considere la red de la figura 4-49(a). Si la máquina J tuviera que volverse blanca repentinamente, ¿serían necesarios cambios para el etiquetado? Si es así, ¿cuáles?

R= El puerto en B1 a LAN 3 tendría que ser re etiquetados como GW.

42. Describa brevemente la diferencia entre los conmutadores de almacenamiento y reenvío y los cutthrough.

R= Un interruptor de almacenamiento y hacia adelante almacena cada trama entrante en su totalidad, a continuación la examina y la envía. Un interruptor de corte a través comienza a transmitir entrante marcos antes de que hayan llegado completamente. Tan pronto como el destino dirección está en el desvío puede comenzar.

43. Los conmutadores de almacenamiento y reenvío tienen una ventaja sobre los cut-through en relación con las tramas dañadas. Explique cuál es.

R= Interruptores de Store-and-forward almacenar imágenes completas antes de transmitirlos. Después de un marco entra, la suma de comprobación puede ser verificada. Si el marco está dañado, se descarta de inmediato. Con corte a través de =, marcos dañados no pueden ser desechado por el conmutador porque por el momento en que el error es detectado, el marco ya se ha ido. Tratando de resolver el problema es como cerrar la puerta del establo después que el caballo se ha escapado.

44. Las tablas de configuración son necesarias en los conmutadores y los puentes para que las VLANs funcionen. ¿Qué pasaría si las VLANs de la figura 4-49(a) utilizaran concentradores en vez de cables con múltiples derivaciones? ¿Los concentradores también necesitarían tablas de configuración? ¿Por qué sí o por qué no?

R= Ejes N ° sólo tiene que conectar todas las líneas de entrada, junto eléctricamente. Hay nada que configurar. N encaminamiento se realiza en un cubo. Cada entrada en el marco el centro sale en todas las otras líneas.

45. En la figura 4-50 el conmutador del dominio final heredado en la parte derecha tiene soporte para VLAN. ¿Sería posible utilizar ahí un conmutador heredado? Si es así, ¿cómo funcionaría? En caso contrario, ¿por qué no?

R= Se iba a funcionar. Marcos que entran en el dominio básico serían todos los marcos existentes, por lo que sería hasta el interruptor principal primero en marcar. Se puede hacer esto mediante el uso de Direcciones MAC o IP. Del mismo modo, a la salida, ese cambio lo haría tienen al GANUPT marcos salientes.



Titulo Libro	Redes de Computadoras
Titulo del Capitulo	Capitulo 5 – La Capa de Red
No. Ejercicios	53
Fecha de Realización	VERANO 2012

CAPITULO 5

1. Indique dos aplicaciones de ejemplo para las cuales es adecuado un servicio orientado a conexiones. Luego dé dos ejemplos en los que el servicio sin conexiones es lo mejor.

R= La transferencia de archivos, acceso remoto, y el vídeo bajo demanda necesita orientado a la conexión servicio. Por otro lado, el crédito verificación de la tarjeta y otro punto de venta terminales de transferencia electrónica de fondos, y muchas formas de base de datos remota son inherentemente acceder sin conexión, con una consulta de una forma que va y la responder a volver a la inversa.

2. ¿Hay circunstancias en las cuales un servicio de circuito virtual entregará (o cuando menos debería entregar) paquetes en desorden? Explique.

R= Sí. Las señales de interrupción, pase directamente de los datos y se ha librado de secuencia. Un ejemplo típico se produce cuando un usuario llega a la terminal de dejar de fumar (matar) clave. El paquete generado a partir de la señal de dejar de fumar debe ser enviada inmediatamente y debe pasar directamente de los datos que están programados para el programa, es decir, datos que ya se ha escrito en el, pero no leído.

3. Las subredes de datagramas enrutan cada paquete como unidad separada, independiente de las demás. Las subredes de circuitos virtuales no tienen que hacer esto, ya que cada paquete de datos sigue una ruta predeterminada. ¿Significa esto que las subredes de circuitos virtuales no necesitan la capacidad de enrutar paquetes aislados de un origen arbitrario a un destino arbitrario? Explique su respuesta.

R= Las redes virtuales de circuito más seguro que necesitará esta capacidad con el fin de la ruta los paquetes de configuración de la conexión de una fuente arbitraria a un destino arbitrario.

4. Dé tres ejemplos de parámetros de protocolo que podrían negociarse al establecer una conexión.

R= La negociación podría establecer el tamaño de la ventana, el tamaño máximo de paquete, velocidad de datos, y valores de los temporizadores.

5. Considere el siguiente problema de diseño que concierne a la implementación del servicio de circuitos virtuales. Si los circuitos virtuales son internos a la subred, cada paquete de datos debe tener un encabezado de 3 bytes, y cada enrutador debe destinar hasta 8 bytes de almacenamiento para la identificación de circuitos. Si se usan datagramas de manera interna, se requieren encabezados de 15 bytes, pero no se requiere espacio de tabla en los enrutadores. La capacidad de transmisión cuesta 1 centavo para cada 106 bytes, por salto. Puede comprarse memoria de enrutamiento por 1 centavo por byte y se de precia en dos años (tomando en cuenta que la semana laboral es de 40 horas). Estadísticamente, la sesión promedio dura 1000 seg, tiempo durante el cual se transmiten 200 paquetes. El paquete medio requiere cuatro saltos. ¿Qué implementación es más económica, y por cuánto?

R= Cuatro saltos significa que cinco routers están implicados. La implementación de circuito virtual requiere inmovilización de $5 \times 8 = 40$ bytes de memoria para 1000 seg. La datagrama aplicación requiere la transmisión de $12 \times 4 \times 200 = 9600$ bytes de encabezado por encima de lo que la implementación de circuitos virtuales necesita. Por lo tanto, la cuestión se reduce a que el costo relativo de 40.000 bytes de memoria seg en comparación con 9600 bytes de lúpulo de la capacidad del circuito. Si la memoria no se amortiza en $2 \times 52 \times 40 \times 3600 = 1,5 \times 10^7$ seg, seg cuesta un byte $6,7 \times 10^{-8}$ centavos, y 40.000 de ellos cuestan un poco más de 2 millicentavos. Si un byte-hop cuesta 6.10 centavos de dólar, 9.600 de ellos costará 9,6 millicentavos. Los circuitos virtuales son más baratos para este conjunto de parámetros.

6. Suponiendo que todos los enrutadores y hosts están trabajando de manera adecuada y que el software de ambos está libre de errores, ¿hay alguna posibilidad, por pequeña que sea, de que un paquete sea entregado al destino equivocado?

R= Sí. Una ráfaga de ruido grande podría mutilar un paquete mal. Con una suma de comprobación k bits, hay una probabilidad de 2^{-k} que el error es detectado. Si el destino campo o, equivalentemente, el número de circuito virtual, se cambia, el paquete será entregado a un destino equivocado y aceptado como genuino. Dicho de otra palabras, una ráfaga de ruido ocasional podría cambiar un paquete perfectamente legal para un destino en un paquete perfectamente legal para otro destino.

7. Considere la red de la figura 5-7, pero ignore los pesos de las líneas. Suponga que dicha red utiliza la inundación como algoritmo de enrutamiento. Si un paquete enviado mediante A a D tiene una cuenta máxima de salto de 3, liste todas las rutas que éste tomará. También mencione cuántos saltos merecedores de ancho de banda realiza.

R= Se seguirán todas las rutas siguientes: ABCD, ABCF, ABEF, ABEG, AGHD, AGHF, AGEH, y AGEF. El número de saltos utilizados es 24.

8. Dé una heurística sencilla para encontrar dos rutas a través de una red de origen dado a un destino dado que pueda sobrevivir a la pérdida de cualquier línea de comunicación (suponiendo que existen dos de tales rutas). Los enrutadores se consideran lo bastante confiables, por lo que no es necesario preocuparse por la posibilidad de caída de los enrutadores.

R= Elija una ruta utilizando el camino más corto. Ahora eliminar todos los arcos utilizados en el camino acaba de encontrar, y ejecutar el algoritmo de ruta más corta de nuevo. El segundo camino será capaz de sobrevivir a la falta de cualquier línea en la primera ruta, y viceversa. Es concebible, sin embargo, que esta heurística puede fallar a pesar de que dos líneas disjuntos caminos existen. Para resolverlo correctamente, un algoritmo de flujo máximo-debe ser utilizado.

9. Considere la subred de la figura 5-13(a). Se usa enrutamiento por vector de distancia y acaban de llegar los siguientes vectores al enrutador C: de B: (5, 0, 8, 12, 6, 2); de D: (16, 12, 6, 0, 9, 10), y de E: (7, 6, 3, 9, 0, 4). Los retardos medios a B, D y E son 6, 3 y 5, respectivamente. ¿Cuál es la nueva tabla de enrutamiento de C? Indique tanto la línea de salida a usar como el retardo esperado.

R= Yendo a través de B da (11, 6, 14, 18, 12, 8).

Yendo a través de D da (19, 15, 9, 3, 9, 10).

Yendo a través de E da (12, 11, 8, 14, 5, 9).

Tomando el mínimo de cada destino, salvo C da (11, 6, 0, 3, 5, 8).

Las líneas salientes son (B, B, -, D, E, B).

10. Si en una red de 50 enrutadores los retardos se registran como números de 8 bits y se intercambian vectores de retardo dos veces por segundo, ¿qué ancho de banda por línea dúplex total es consumido por el algoritmo de enrutamiento distribuido? Suponga que cada enrutador tiene tres líneas a los demás enrutadores.

R= La tabla de enrutamiento es de 400 bits. Dos veces por segundo este cuadro está escrito en cada la línea, por lo que se necesitan 800 puntos básicos en cada línea en cada dirección.

11. En la figura 5-14 el OR booleano de los dos grupos de bits ACF es de 111 en cada fila. ¿Es éste un mero accidente, o es cierto para todas las subredes en todas las circunstancias?

R= Siempre se mantiene. Si el paquete ha llegado en una línea, hay que reconocer. Si sin paquete ha llegado en una línea, éste debe ser enviado allí. Los casos 00 (no tiene llegó y no se enviará) y 11 (ha llegado y será enviado de vuelta) son lógicamente incorrecta y por lo tanto no existen.

12. Para un enrutamiento jerárquico con 4800 enrutadores, ¿cuál región y tamaños de clúster deberían elegirse para minimizar el tamaño de la tabla de enrutamiento para una jerarquía de tres capas? Un buen lugar de inicio es la hipótesis de que una solución k clústeres de k regiones de k enrutadores está cerca de ser óptima, lo que significa que k es aproximadamente la raíz cúbica de 4800 (cerca de 16). Utilice la prueba y el error para verificar las combinaciones en las que los tres parámetros están en el límite de 16.

R= El mínimo se produce en 15 grupos, cada uno con 16 regiones, cada región tiene 20 routers, o una de las formas equivalentes, por ejemplo, 20 grupos de 16 regiones de 15 routers. En todos los casos el tamaño de la tabla es $15 + 16 + 20 = 51$.

13. En el texto se indicó que, cuando un host móvil no está en casa, los paquetes enviados a su LAN base son interceptados por su agente de base en esa LAN. En una red IP de una LAN 802.3, ¿cómo logra esta intercepción el agente de base?

R= Es concebible que podría ir en modo promiscuo, la lectura de todos los fotogramas en la LAN, pero esto es muy ineficiente. En su lugar, lo que normalmente se hace es que los trucos de agente de origen del router para que piense que es el anfitrión móvil responder a las peticiones ARP. Cuando el router recibe un paquete IP destinado a él host móvil, emite una petición ARP preguntando por el 802.3 del nivel MAC la dirección de la máquina con esa dirección IP. Cuando el host móvil no está cerca, el agente de origen responde a la ARP, por lo que los socios del router los dirección IP del usuario de telefonía móvil con 802,3 agente de la casa MAC de nivel de dirección.

14. Viendo la subred de la figura 5-6, ¿cuántos paquetes se generan por una difusión de B, usando:

(a) reenvío por ruta invertida?

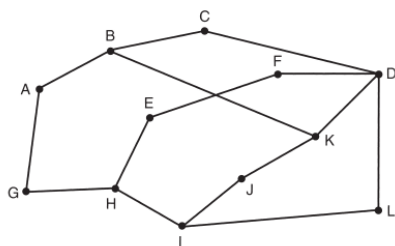
(b) árbol sumidero?

R= (a) El algoritmo de transmisión vía inversa tiene cinco rondas para el final. La los destinatarios de paquetes en estas rondas son de CA, DFIJ, DEGH IJKN, GHKN, y OVM, respectivamente. Un total de 21 paquetes se generan. (b) El árbol sumidero necesita cuatro rondas y los paquetes 14.

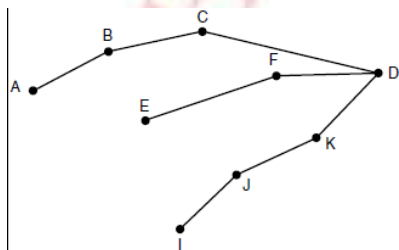
15. Considere la red de la figura 5-16(a). Imagine que entre F y G se agrega una línea nueva pero el árbol sumidero de la figura 5-16(b) permanece sin cambios. ¿Qué cambios ocurren en la figura 5-16(c)?

R= Nodo F en la actualidad tiene dos descendientes, A y D. En la actualidad adquiere una tercera, G no, un círculo, porque el paquete que sigue IFG no está en el árbol sumidero. El nodo G adquiere un descendiente segunda, además de D, con la etiqueta F. Esto, también, no se rodeó ya que no vienen en el árbol sumidero.

16. Calcule un árbol de expansión multidifusión para el enrutador C de la siguiente subred para un grupo con miembros en los enrutadores A, B, C, D, E, F, I y K.



R= Varios árboles de expansión son posibles. Uno de ellos es:



17. En la figura 5-20, ¿los nodos H o I difunden alguna vez en la búsqueda mostrada iniciada en A?

R= Cuando H recibe el paquete, que se transmite. Sin embargo, sabe cómo llegar al yo, por lo que no transmite.

18. Suponga que el nodo B de la figura 5-20 ha reiniciado y no tiene información de enrutamiento en sus tablas. De repente necesita una ruta a H. Envía difusiones con TTL establecido a 1, 2, 3, etcétera. ¿Cuántas rondas da para encontrar la ruta?

R= Nodo H es de tres saltos de B, por lo que toma de tres rondas para encontrar la ruta.

19. En la versión más simple del algoritmo Chord para búsqueda de igual a igual, las búsquedas no utilizan la tabla finger. En su lugar, se ejecutan en forma lineal alrededor del círculo, en cualquier dirección. ¿Puede un nodo predecir de manera precisa en qué dirección debe buscar? Explique su respuesta.

R= Puede hacerlo aproximadamente, pero no exactamente. Supongamos que hay 1024 nodos identificadores. Si el nodo 300 está buscando para el nodo 800, es probable que sea mejor ir hacia la derecha, pero podría suceder que hay 20 nodos reales entre 300 y 800 va hacia la derecha y sólo 16 nodos reales entre ellos van en sentido contrario. El propósito de la función hash criptográfico SHA-1 es producir una distribución muy uniforme de modo que la densidad de nodos es aproximadamente la misma todo lo largo del círculo. Pero siempre habrá fluctuaciones estadísticas, por lo que en la elección directa puede ser malo.

20. Considere el círculo Chord de la figura 5-24. Suponga que el nodo 10 de repente se activa. ¿Esto afecta la tabla finger del nodo 1; de ser así, cómo?

R= El nodo de entrada de 3 interruptores de 12 a 10.

21. Como posible mecanismo de control de congestión en una subred que usa circuitos virtuales internamente, un enrutador podría abstenerse de confirmar la recepción de un paquete hasta que (1) sabe que su última transmisión por el circuito virtual se recibió con éxito y que (2) tiene un búfer libre. Por sencillez, suponga que los enrutadores usan un protocolo de parada y espera y que cada circuito virtual tiene un búfer dedicado a él para cada destino del tráfico. Si se quieren T seg para transmitir un paquete (de datos o de confirmación de recepción) y hay n enrutadores en la ruta, ¿cuál es la velocidad con que se entregan paquetes al host de destino? Suponga que los errores de transmisión son poco frecuentes y que la conexión host-enrutador es infinitamente rápida.

R= El protocolo es terrible. Deje que el tiempo ser colocado en unidades de T segundos. En la ranura 1 router de origen envía el primer paquete. Al comienzo de la ranura 2, el segundo router ha recibido el paquete, pero no puede reconocer todavía. Al comienzo de la ranura 3, el router tercera ha recibido el paquete, pero no se puede reconocer bien, por lo que todos los routers detrás de él todavía se aferran. El primer reconocimiento sólo puede ser enviado cuando el host de destino tiene el paquete desde el destino router. Ahora comienza el reconocimiento de multiplicación de nuevo. Toma completa de dos los tránsitos de la subred, $2(n - 1)T$ segundos, antes de que el

enrutador de origen puede enviar el segundo paquete. Por lo tanto, el rendimiento es un paquete de cada $2(n - 1)T$ seg.

22. Una subred de datagramas permite que los enrutadores puedan deshacerse de paquetes cuando lo necesiten. La probabilidad de que un enrutador descarte un paquete es de p . Considere el caso de un host de origen conectado al enrutador de origen, que está conectado al enrutador de destino, y por él al host de destino. Si cualquiera de los enrutadores descarta un paquete, el host de origen tarde o temprano termina la temporización e intenta de nuevo. Si tanto las líneas host-enrutador como enrutador-enrutador se cuentan como saltos, ¿cuál es la media de:

(a) saltos que da un paquete por transmisión?

(b) transmisiones que hace un paquete?

(c) saltos requeridos por paquete recibido?

R= Cada paquete emitido por el host de origen hace que el sector del lúpulo ya sea 1, 2, ó 3. La probabilidad que hace un salto es p . La probabilidad de que hace dos saltos es $p(1 - p)$. La probabilidad de que hace 3 saltos es $(1 - p)^2$. El camino medio longitud de un paquete se puede esperar para viajar es la suma ponderada de estos tres probabilidades o $P_2 - 3P + 3$. Tenga en cuenta que para $p = 0$, la media es de 3 saltos y para $p = 1$, la media es de 1 salto. Con $0 < p < 1$, las transmisiones pueden ser múltiples necesario. El número medio de transmisiones se pueden encontrar por darse cuenta de que el probabilidad de una transmisión con éxito todo el camino es $(1 - p)^2$, que se llamar a α . El número esperado de transmisiones es sólo

$$\alpha + 2\alpha(1 - \alpha) + 3\alpha(1 - \alpha)^2 + \dots = \frac{1}{\alpha} = \frac{1}{(1 - p)^2}$$

Por último, el total de lúpulo utilizado es justo $(p^2 - 3p + 3) / (1 - p)^2$.

23. Describa dos diferencias principales entre el método de bit de advertencia y el método RED.

R= En primer lugar, el método poco advertencia explícita envía una notificación de congestión a la fuente mediante el establecimiento de un poco, mientras que el rojo implícita notifica a la fuente, simplemente caer una de sus paquetes. En segundo lugar, el método poco advertencia cae un paquete sólo cuando no hay espacio en el buffer a la izquierda, mientras que RED descarta paquetes antes de que todo el buffer se han agotado.

24. Cite una razón por la que el algoritmo de cubeta con goteo debe tener sólo un paquete por intervalo, independientemente del tamaño del paquete.

R= El router tiene que ver aproximadamente la misma cantidad de trabajo una cola de paquetes, no importa lo grande que es. No hay duda de que el procesamiento de 10 paquetes de 100 bytes cada uno es mucho más trabajo que el procesamiento de un paquete de 1000 bytes.

25. La variante de conteo de bytes del algoritmo de cubeta con goteo se usa en cierto sistema. La regla es que pueden enviarse por intervalo un paquete de 1024 bytes, dos paquetes de 512 bytes, etcétera. Indique una restricción sería de este sistema que no se menciona en el texto.

R= No es posible enviar cualquier paquete mayor que 1024 bytes, de la historia.

26. Una red ATM usa un esquema de cubeta con tokens para la conformación de tráfico. Se pone un token nuevo en la cubeta cada 5 μ seg. Cada token cabe en una celda, que contiene 48 bytes de datos ¿Cuál es la tasa de datos máxima sustentable?

R= Con una señal cada 5 microsegundos, las células $200.000 / \text{seg}$ se puede enviar. Cada célula contiene 48 bytes de datos o bits 384. La velocidad de datos neta es entonces de 76,8 Mbps

27. Una computadora de una red de 6 Mbps se regula mediante una cubeta con tokens. La cubeta con tokens se llena a razón de 1 Mbps. Inicialmente está llena a su capacidad máxima de 8 megabits. ¿Durante cuánto tiempo puede la computadora transmitir a 6 Mbps?

R= La respuesta ingenua, dice que a los 6 Mbps que se necesita 4.3 segundos para drenar un megabit 8 cubo. Sin embargo, esta respuesta es incorrecta, ya que durante ese intervalo, más fichas de llegar. La respuesta correcta puede obtenerse mediante la fórmula $S = C / (M - \rho)$. Sustituyendo, obtenemos $S = 8 / (6-1)$ o 1,6 segundos.

28. Imagine una especificación de flujo que tiene un tamaño máximo de paquete de 1000 bytes, una tasa de cubeta con tokens de 10 millones de bytes/seg, un tamaño de cubeta con tokens de 1 millón de bytes y una tasa máxima de transmisión de 50 millones de bytes/seg. ¿Cuánto tiempo puede durar una ráfaga a la velocidad máxima?

R= Llama la longitud de la ráfaga Dt intervalo máximo. En el caso extremo, el cubo está lleno al comienzo del intervalo (1 Mbyte) y otros Mbyte $10\Delta t$ vienen en durante el intervalo. La salida durante la ráfaga de transmisión contiene $50\Delta t$ Mbyte. Igualando estas dos cantidades, se obtiene $1 + = 10\Delta t$ $50\Delta t$. Resolviendo esta ecuación, obtenemos t es 25 ms.

29. La red de la figura 5-37 utiliza RSVP con árboles de multidifusión para los hosts 1 y 2. Suponga que el host 3 solicita un canal de ancho de banda de 2 MB/seg para un flujo del host 1 y otro canal de ancho de banda de 1 MB/seg para un flujo del host 2. Al mismo tiempo, el host 4 solicita un canal de ancho de banda de 2 MB/seg para un flujo del host 1 y el host 5 solicita un canal de ancho de banda de 1 MB/seg para un flujo del host 2. ¿Cuánto ancho de banda se reservará para estas solicitudes en los enrutadores A, B, C, E, H, J, K y L?

R= Los anchos de banda en MB / seg son como sigue: A: 2, B: 0, C: 1, E: 3, H: 3, J: 3, K: 2, y L: 1.

30. La CPU de un enrutador puede procesar 2 millones de paquetes/seg. La carga que se le ofrece es 1.5 millones de paquetes/seg. Si una ruta del origen al destino contiene 10 enrutadores, ¿cuánto tiempo tardan las CPUs en encolar y dar servicio?

R= Aquí μ es de 2 millones y λ es de 1,5 millones, por lo que $\rho = \lambda / \mu$ es de 0,75, y de la cola teoría, cada paquete sufre un retraso de cuatro veces más de lo que sería en un ralenti sistema. El tiempo en un sistema inactivo es de 500 ns, aquí es de 2 microsegundos. Con 10 routers a lo largo de un camino, el tiempo de cola además de un servicio es de 20 microsegundos.

31. Considere el usuario de los servicios diferenciados con reenvío expedito. ¿Hay alguna garantía de que los paquetes expeditos experimenten un retardo más pequeño que los paquetes regulares? ¿Por qué sí o por qué no?

R= No hay ninguna garantía. Si los paquetes son demasiados acelerado, su canal puede tienen un desempeño aún peor que el canal regular.

32. ¿Es necesaria la fragmentación en interredes de circuitos virtuales concatenados o sólo en los sistemas de datagramas?

R= Se necesita en ambos. Incluso en un concatenado de circuito virtual de la red, algunos redes a lo largo de la ruta de acceso puede aceptar los paquetes de 1024 bytes, y el poder que otros sólo aceptar 48-byte paquetes. La fragmentación sigue siendo necesaria.

33. El entunelamiento a través de una subred de circuitos virtuales concatenada es directo: el enrutador multiprotocolo en un extremo sólo establece un circuito virtual al otro extremo y pasa los paquetes a través de él. ¿El entunelamiento también puede utilizarse en las subredes de datagramas? ¿De ser así, cómo?

R= No hay problema. Sólo encapsular el paquete en el campo de carga útil de un datagrama perteneciente a la subred que pasa a través y enviarlo.

34. Suponga que el host A está conectado a un enrutador R 1, R 1 está conectado a otro enrutador, R 2, y R 2 está conectado al host B. Suponga que un mensaje TCP que contiene 900 bytes de datos y 20 bytes de encabezados TCP se pasa al código IP en el host A para entregarlo a B. Muestre los campos Longitud total, Identificación, DF, MF y Desplazamiento del fragmento del encabezado IP en cada paquete transmitido a través de los tres enlaces. Suponga que el enlace A-R1 puede soportar un tamaño máximo de trama de 1024 bytes, así como un encabezado de trama de 14 bytes; el enlace R1-R2 puede soportar un tamaño máximo de trama de 512 bytes, así como un encabezado de trama de 8 bytes, y el enlace R2-B puede soportar un tamaño máximo de trama de 512 bytes, incluyendo un encabezado de trama de 12 bytes.

R= El primer datagrama IP se fragmenta en dos datagramas IP en I1. No fragmentación otro va a producir. Enlace A-R1: Longitud = 940; ID = x, df = 0; MF = 0; offset = 0 Enlace R1-R2: (1) Longitud = 500; ID = x, df = 0; MF = 1; offset =

0 (2) Longitud = 460; ID = x, df = 0; MF = 0; offset = 60 Enlace R2-B: (1) Longitud = 500; ID = x, df = 0; MF = 1; offset = 0: (2) Longitud = 460; ID = x, df = 0; MF = 0; offset = 60.

35. Un enrutador está eliminando paquetes IP cuya longitud máxima (datos más encabezado) es de 1024 bytes. Suponiendo que los paquetes vivan por 10 seg, ¿cuál es la velocidad máxima a la que el enrutador puede operar sin el peligro de desbordar el espacio de números ID del datagrama IP?

R= Si la tasa de bits de la línea es b, el número de paquetes / seg que el router puede emitir es $b/8192$, por lo que el número de segundos que se tarda en emitir un paquete es de $8192 / b$. Para apagar 65.536 paquetes toma $229 / b$ seg. Igualando esto a la máxima paquete de por vida, tenemos $229 / b = 10$. Entonces, b es aproximadamente 53.687.091 bps.

36. Un datagrama IP que utiliza la opción Enrutamiento de origen estricto tiene que fragmentarse. ¿Cree que la opción se copia en cada fragmento, o con colocarlo en el primer fragmento es suficiente? Explique su respuesta.

R= Dado que la información que se necesita para dirigir cada fragmento, la opción debe aparecer en cada fragmento.

37. Suponga que en lugar de usar 16 bits para la parte de red de una dirección clase B, se hubieran usado 20 bits. ¿Cuántas redes clase B habría?

R= Con un prefijo 2-bits, no habría sido de 18 bits sobrantes para indicar la red. En consecuencia, el número de redes habría sido 218 o 262.144. Sin embargo, todos los 0s y 1s todos son especiales, por lo que sólo 262.142 están disponibles.

38. Convierta la dirección de IP cuya representación hexadecimal es C22F1582 a notación decimal con puntos.

R= La dirección es 194.47.21.130.

39. Una red en Internet tiene una máscara de subred de 255.255.240.0. ¿Cuál es la cantidad máxima de hosts que puede manejar?

R= La máscara es de 20 bits de largo, por lo que la parte de red es de 20 bits. El restante 12 bits son para el anfitrión, por lo que existen 4096 direcciones de host.

40. Hay una gran cantidad de direcciones IP consecutivas, comenzando en 198.16.0.0. Suponga que cuatro organizaciones, A, B, C y D, solicitan 4000, 2000, 4000, y 8000 direcciones, respectivamente, y en ese orden. Dé la primera dirección asignada, la última dirección IP asignada y la máscara en la notación w.x.y.z/s para cada una de ellas.

R= Para empezar, todas las solicitudes se redondean hacia arriba a una potencia de dos. La partida dirección, dirección de acabar, y la máscara son los siguientes: A: 198.16.0.0 - 198.16.15.255 escrito como 198.16.0.0/20 B: 198.16.16.0 - 198.23.15.255 escrito como 198.16.16.0/21 C: 198.16.32.0 - 198.47.15.255 escrito como 198.16.32.0/20 D: 198.16.64.0 - 198.95.15.255 escribir como 198.16.64.0/19.

41. Un enrutador acaba de recibir las siguientes nuevas direcciones IP: 57.6.96.0/21, 57.6.104.0/21, 57.6.112.0/21 y 57.6.120.0/21. Si todas éstas utilizan la misma línea de salida, ¿se pueden agregar? De ser así, ¿a qué? Si no, ¿por qué?

R= Pueden ser agregados a 57.6.96/19.

42. El conjunto de direcciones IP de 29.18.0.0 a 29.18.128.255 se ha agregado a 29.18.0.0/17. Sin embargo, hay un hueco de 1024 direcciones sin asignar de 29.18.60.0 a 29.18.63.255 que de repente se asignan a un host que utiliza una línea de salida diferente. Ahora es necesario dividir la dirección agregada en sus bloques constituyentes, agregar el nuevo bloque a la tabla y, después, ver si es posible alguna reagregación? Si no lo es, ¿qué se puede hacer en lugar de eso?

R= Basta con añadir una nueva entrada de la tabla: 29.18.0.0/22 para el nuevo bloque. Si un paquete entrante coincide con 29.18.0.0/17 y 29.18.0.0./22, el más largo uno gana. Esta regla permite asignar un bloque grande para una salida línea, sino hacer una excepción con uno o más bloques pequeños dentro de su rango.

43. Un enrutador tiene las siguientes entradas (CIDR) en su tabla de enrutamiento:

Dirección/máscara Siguiendo salto

135.46.56.0/22 Interfaz 0

135.46.60.0/22 Interfaz 1

192.53.40.0/23 Enrutador 1

Predeterminada Enrutador 2

Para cada una de las siguientes direcciones IP, ¿qué hace el enrutador si llega un paquete con esa dirección?

(a) 135.46.63.10

(b) 135.46.57.14

(c) 135.46.52.2

(d) 192.53.40.7

(e) 192.53.56.7

R= Los paquetes se enrutan como sigue:

(A) Interfaz 1

(B) Interfaz 0

(C) Router 2

(D) Router 1

(E) Router 2

44. Muchas compañías tienen la política de contar con dos (o más) enrutadores que conecten a la compañía a Internet para proporcionar alguna redundancia en caso de que una de ellas falle. ¿Esta política aún es posible con NAT? Explique su respuesta.

R= Después de NAT está instalado, es crucial que todos los paquetes que pertenezcan a una sola conexión a entrar y salir de la empresa a través del mismo router, ya que es donde la asignación se mantiene. Si cada router tiene su propia dirección IP y todo el tráfico perteneciente a una conexión dada puede ser enviado al mismo router, el asignación se puede hacer correctamente y multihoming con NAT se pueden hacer para trabajar.

45. Usted explica el protocolo ARP a un amigo. Cuando usted termina su explicación, él dice: "Ya entiendo. ARP proporciona un servicio a la capa de red, por lo que es parte de la capa de enlace de datos". ¿Qué le diría a su amigo?

R= Usted dice que ARP no proporciona un servicio a la capa de red, es parte de la capa de red y ayuda a proporcionar un servicio a la capa de transporte. La cuestión de las direcciones IP no se produce en la capa de enlace de datos. Datos de los protocolos de capa de enlace son como los protocolos de 1 a 6 en el Cap. 3, HDLC, PPP, etc. Ellos se mueven los bits desde un extremo de una línea a otra.

46. ARP y RARP asignan direcciones de un espacio a otro. En este sentido, son similares. Sin embargo, sus implementaciones son esencialmente diferentes. ¿En qué aspecto fundamental son diferentes?

R= RARP tiene un servidor RARP que responde a las peticiones. ARP no tiene esta. Los propios anfitriones responder a las consultas ARP.

47. Describa una forma de reensamblar fragmentos IP en el destino.

R= En el caso general, el problema no es trivial. Los fragmentos pueden llegar fuera del orden y algunos pueden no estar disponibles. En una retransmisión, el datagrama puede ser fragmentado en trozos de diferentes tamaños. Además, el tamaño total no es conocido hasta el último fragmento llega. Probablemente, la única forma de manejar re ensamblaje es para amortiguar todas las piezas hasta el último fragmento llega y el tamaño que se conoce. A continuación, construir un búfer del tamaño adecuado, y poner los fragmentos en el tampón, manteniendo un mapa de

bits con un bit por 8 bytes para seguir la pista de que octetos están presentes en el tampón. Cuando todos los bits en el mapa de bits son 1, el datagrama es completo.

48. La mayoría de los algoritmos de reensamble de datagramas IP tienen un temporizador para evitar que un fragmento perdido enlace búferes de reensamble por siempre. Suponga que un datagrama se divide en cuatro fragmentos. Los primeros tres fragmentos llegan y el cuarto se retrasa. En algún momento, el temporizador termina, por lo que se descartan los tres fragmentos de la memoria del receptor. Un poco más tarde, llega el último fragmento. ¿Qué se debería hacer con él?

R= En cuanto al receptor se refiere, esta es una parte de la nueva datagrama, ya que no se otras partes del mismo son conocidos. Por lo tanto, se pondrán en cola hasta que el resto presenta. Si no lo hacen, éste será el tiempo de espera también.

49. Tanto en IP como en ATM, la suma de verificación cubre sólo el encabezado y no los datos. ¿Por qué supone que se eligió este diseño?

R= Un error en la cabecera es mucho más grave que un error en los datos. Una mala dirección, por ejemplo, podría resultar en un paquete que se entrega al mal de acogida. Muchos anfitriones no comprueban si un paquete entregado a ellos es, de hecho, en realidad para ellos. Ellos asumen que la red no les dará los paquetes destinados a otro host. Los datos a veces no es la suma de comprobación por haciendo así que es caro, y capas superiores a menudo se hacen de todos modos, por lo que es redundante aquí.

50. Una persona que vive en Boston viaja a Minneapolis, y lleva su computadora portátil. Para su sorpresa, la LAN de su destino en Minneapolis es una LAN IP inalámbrica, por lo que no tiene que conectarse. ¿Para que el correo electrónico y otro tipo de tráfico llegue de manera correcta aún es necesario todo el proceso con los agentes de base y foráneos?

R= Sí. El hecho de que la red LAN inalámbrica de Minneapolis es no hacer que los paquetes que llegan a ella en Boston para saltar de repente a Minneapolis. El hogar agente en Boston debe túnel al agente foráneo en la LAN inalámbrica en el Minneapolis. La mejor manera de pensar de esta situación es que el usuario tiene conectado a la LAN de Minneapolis, de la misma manera todos los demás Minneapolis los usuarios tienen. Que utiliza la conexión de radio en lugar de un cable es irrelevante.

51. IPv6 utiliza direcciones de 16 bytes. Si un bloque de 1 millón de direcciones se asigna cada picosegundo, ¿cuánto tardará la dirección?

R= Con 16 bytes que hay 2128 o $3,4 \times 10^{38}$ direcciones. Si les asigne a un tasa de 1.018 por segundo, que tendrá una duración de 1013 años. Este número es 1000 veces la edad del universo. Por supuesto, el espacio de direcciones no es plana, de modo que no se asignan de forma lineal, sino que muestra este cálculo que incluso con una asignación esquema que tiene una eficiencia de 1/1000 (0,1 por ciento), uno nunca se quedará a cabo.

52. El campo Protocolo utilizado en el encabezado IPv4 no está presente en el encabezado IPv6 fijo. ¿Por qué?

R= El campo Protocolo indica el host de destino, que el controlador de protocolo para dar la Paquete IP. Routers intermedios no necesitan esta información, por lo que no es necesaria en la cabecera principal. En realidad, está ahí, pero disfrazado. El Siguiendo campo de cabecera de la última (extensión) de cabecera se utiliza para este propósito.

53. Cuando se introduce el protocolo IPv6, ¿tiene que cambiarse el protocolo ARP? De ser así, ¿los cambios son conceptuales o técnicos?

R= Conceptualmente, no hay cambios. Técnicamente, las direcciones IP solicitada son ahora más grandes, por lo que grandes campos son necesarios.



Título Libro	Redes de Computadoras
Título del Capítulo	Capítulo 6 – La Capa de Transporte
No. Ejercicios	42
Fecha de Realización	VERANO 2012

CAPITULO 6

1. En nuestras primitivas de ejemplo de la figura 6-2, LISTEN es una llamada bloqueadora. ¿Es estrictamente necesario esto? De no serlo, explique cómo debe usarse una primitiva no bloqueadora. ¿Qué ventaja tendría esto respecto al esquema descrito en el texto?

R= La llamada LISTEN podría indicar una voluntad de establecer nuevas conexiones, pero no bloquee. Cuando un intento de conexión se hizo, la persona que llama se podría dar una señal. A continuación, se ejecutaría, por ejemplo, Aceptar o Rechazar para aceptar o rechazar la conexión. En nuestro plan original, esta flexibilidad no existe.

2. En el modelo de la figura 6-4, se supone que la capa de red puede perder paquetes y, por tanto, su recepción se debe confirmar individualmente. Suponga que la capa de red es 100% confiable y que nunca pierde paquetes. ¿Qué cambios, si acaso, se necesitarán en la figura 6-4?

R= La línea discontinua desde el establecimiento PASIVA PENDIENTE a ESTABLECIDO ya no es contingente en un acuse de llegar. La transición puede suceder de inmediato. En esencia, el ESTABLECIMIENTO DE PASIVO Estado pendiente de que desaparezca, ya que nunca es visible a cualquier nivel.

3. En las dos partes de la figura 6-6 hay un comentario de que los valores de SERVER_PORT deben ser los mismos en el cliente y en el servidor. ¿Por qué es tan importante?

R= Si el cliente envía un paquete a SERVER3PORT y el servidor no está escuchando a ese puerto, el paquete no será entregada al servidor.

4. Suponga que el esquema operado por reloj para generar números de secuencia iniciales se usa con un contador de reloj de 15 bits de ancho. El reloj pulsa una vez cada 100 mseg, y el tiempo de vida máximo de un paquete es de 60 seg. ¿Con qué frecuencia ocurre la resincronización (a) en el peor caso? (b) cuando los datos consumen 240 números de secuencia/min?

R= (A) El reloj lleva 32768 garrapatas, es decir, 3276,8 seg a alrededor de ciclo. En la generación cero caso, el remitente entrar en la zona prohibida en 3276,8 a $60 = 3216,8$ seg. (B) A 240 números de secuencia por minuto, el número de secuencia real es $4t$, donde t es en segundos. El borde izquierdo de la región prohibida es de 10 ($t - 3.216,8$). Igualando estas dos fórmulas, nos encontramos con que se cruzan en el instante $t = 5361,3$ segundos.

5. ¿Por qué tiene que ser el tiempo de vida máximo de paquete, T , lo bastante grande para asegurar que han desaparecido no sólo el paquete, sino también sus confirmaciones de recepción?

R= Mira el paquete duplicado en segundo lugar en la fig. 6-11 (b). Cuando ese paquete llega, sería un desastre si los reconocimientos a los y todavía estaban flotando alrededor.

6. Imagine que se usa un acuerdo de dos vías en lugar de uno de tres vías para establecer las conexiones. En otras palabras, no se requiere el tercer mensaje. ¿Son posibles ahora los bloqueos irreversibles? Dé un ejemplo o demuestre que no pueden existir.

R= Interbloqueos son posibles. Por ejemplo, un paquete llega a un fuera del azul, y A la reconoce. El reconocimiento se pierde, pero una ya está abierta mientras que B no sabe nada en absoluto sobre lo que ha sucedido. Ahora lo mismo pasa a B, y ambos están abiertos, pero esperando diferentes números de secuencia. Tiempos de espera que se introdujo para evitar los callejones sin salida.

7. Imagine un problema de n -ejércitos generalizado, en el que el acuerdo de dos de los ejércitos azules es suficiente para la victoria. ¿Existe un protocolo que permita ganar a los azules?

R= No. El problema es esencialmente el mismo con más de dos ejércitos.

8. Considere el problema de la recuperación después de una caída del host (es decir, la figura 6-18). Si el intervalo entre la escritura y el envío de una confirmación de recepción, o viceversa, puede hacerse relativamente pequeño, ¿cuáles son las mejores estrategias emisor-receptor para reducir al mínimo la posibilidad de una falla del protocolo?

R= Si el tiempo de AW o WA es pequeño, el CA eventos (W) y WC (A) es poco probable eventos. El emisor debería retransmitir en S1 del Estado; forma que el receptor no lo hace materia.

9. ¿Son posibles los bloqueos irreversibles con la entidad de transporte descrita en el texto (figura 6-20)?

R= Sí. Ambas partes al mismo tiempo podría ejecutar RECIBIR.

10. Por curiosidad, el implementador de la entidad de transporte de la figura 6-20 ha decidido incluir contadores en el procedimiento sleep para obtener estadísticas sobre el arreglo conn. Entre éstas están la cantidad de conexiones en cada uno de los siete estados posibles, n_i ($i = 1, \dots, 7$). Tras escribir un enorme programa en FORTRAN para analizar los datos, nuestro implementador descubrió que la relación $\sum n_i = \text{MAX_CONN}$ parece ser verdadera siempre. ¿Hay otras invariantes en las que intervengan sólo estas siete variables?

R= Sí, $n_2 + n_3 + n_6 + n_7 = 1$. Los estados de escucha, de espera, enviar y recibiendo todos implica que el usuario está bloqueado y por lo tanto no puede también estar en otro estado.

11. ¿Qué ocurre cuando el usuario de la entidad de transporte dada en la figura 6-20 envía un mensaje de longitud cero? Explique el significado de su respuesta.

R= Un mensaje de longitud cero es recibida por el otro lado. Podría ser utilizado para la señalización final del archivo.

12. Por cada evento que puede ocurrir en la entidad de transporte de la figura 6-20, indique si es legal o no cuando el usuario está durmiendo en el estado sending.

R= Ninguno de los primitivos se puede ejecutar, porque el usuario está bloqueado. Por lo tanto, sólo los eventos de llegada de paquetes son posibles, y no todos ellos, tampoco. CallReq, ClearReq, DataPkt, y el crédito son los únicos legales.

13. Explique las ventajas y desventajas de los créditos en comparación con los protocolos de ventana corrediza.

R= La ventana corrediza es más sencilla, teniendo solamente un conjunto de parámetros (la ventana y los bordes) para la gestión. Además, el problema de una ventana que es aumentada y luego disminuida, con las TPDU que llegan en el orden equivocado, no se produce. Sin embargo, el plan de crédito es más flexible, permitiendo una gestión dinámica de la memoria intermedia, separado de los acuses de recibo.

14. ¿Por qué existe el UDP? ¿No habría bastado con permitir que los procesos de usuario enviaran paquetes IP en bruto?

R= Paquetes IP no contiene direcciones IP, que especifican una máquina de destino. Una vez que un paquete llega, ¿cómo el controlador de red sabe qué proceso para darle a? Paquetes UDP contiene un puerto de destino. Esta información es esencial para que puedan ser entregados al proceso correcto.

15. Considere un protocolo de nivel de aplicación simple construido encima de UDP que permite a un cliente recuperar un archivo desde un servidor remoto que reside en una dirección bien conocida. El cliente primero envía una solicitud con el nombre del archivo, y el servidor responde con una secuencia de paquetes de datos que contienen diferentes partes del archivo solicitado. Para asegurar la confiabilidad y una entrega en secuencia, el cliente y el servidor utilizan un protocolo de parada y espera. Ignorando el aspecto de desempeño obvio, ¿ve usted un problema con este protocolo? Piense cuidadosamente en la posibilidad de la caída de los procesos.

R= Es posible que un cliente puede obtener el archivo incorrecto. Supongamos que el cliente A envía una solicitud de F1 archivo y luego se bloquea. Otro cliente B a continuación, utiliza el mismo protocolo solicitar un nuevo archivo f2. Supongamos cliente B, que se ejecuta en el mismo máquina A (con la misma dirección IP), se une a su socket UDP al mismo puerto una que estaba usando anteriormente. Por otra parte, supongamos solicitud B se pierde. Cuando el respuesta del servidor (a A la petición) llega, el cliente B va a recibir y asumir que es una respuesta a su propia solicitud.

16. Un cliente envía una solicitud de 128 bytes a un servidor localizado a 100 km de distancia a través de una fibra óptica de 1 gigabit. ¿Cuál es la eficiencia de la línea durante la llamada a procedimiento remoto?

R= El envío de 1.000 bits sobre una línea de 1 Gbps es de 1 mseg. La velocidad de la luz en fibra la óptica es de 200 km / ms, por lo que se necesita 0,5 ms para la solicitud de llegar y otro 0,5 ms para la respuesta para volver. En total, 1000 bits han sido transmitidas en 1 ms. Esto es equivalente a 1 megabit / seg, o 1/10 de 1% eficiencia.

17. Considere nuevamente la situación del problema anterior. Calcule el tiempo de respuesta mínimo posible para la línea de 1 Gbps y para una de 1 Mbps. ¿Qué conclusión puede obtener?

R= En 1 Gbps, el tiempo de respuesta está determinada por la velocidad de la luz. Lo mejor que se puede lograr es 1 mseg. A 1 Mbps, se tarda alrededor de 1 ms para bombear los 1024 bits, 0,5 ms para el último en llegar al servidor y, a ms de 0,5 la respuesta para volver en el mejor de los casos. El tiempo de RPC mejor posible es entonces 2 mseg. La conclusión es que la mejora de la velocidad de la línea por un factor de 1000 sólo ha sufrido un factor de dos en el rendimiento. A menos que la línea de gigabyte es increíblemente barato, es probable que no vale la pena tener para esta aplicación.

18. Tanto UDP como TCP utilizan números de puerto para identificar la entidad de destino cuando entregan un paquete. Dé dos razones por las cuales estos protocolos inventaron un nuevo ID abstracto (números de puerto), en lugar de utilizar IDs de proceso, que ya existían cuando se diseñaron estos protocolos.

R= Aquí hay tres razones. En primer lugar, los identificadores de proceso son específicos del sistema operativo. Uso de los identificadores de proceso habría hecho estos protocolos OS-dependiente. En segundo lugar, un solo proceso puede establecer múltiples canales de comunicación. Un proceso de identificación individual (por proceso) como el identificador de destino no puede ser utilizado para distinguir entre estos canales. En tercer lugar, con los procesos de escuchar en puertos conocidos es fácil, pero bien conocidos los identificadores de proceso son imposibles.

19. ¿Cuál es el tamaño total de la MTU mínima de TCP, incluyendo la sobrecarga de TCP e IP pero no la de la capa de enlace de datos?

R= El segmento por defecto es 536 bytes. TCP añade 20 bytes, y lo mismo ocurre con IP, por lo que la configuración predeterminada de 576 bytes en total.

20. La fragmentación y el reensamble de datagramas son manejados por IP y son transparentes para TCP. ¿Esto significa que TCP no tiene que preocuparse porque los datos lleguen en el orden equivocado?

R= A pesar de que cada datagrama llega intacto, es posible que los datagramas lleguen en el orden equivocado, por lo que TCP tiene que estar preparado para volver a montar las partes de un mensaje correctamente.

21. RTP se utiliza para transmitir audio con calidad de CD, el cual crea un par de muestras de 16 bits, 44,100 veces/seg, una muestra por cada uno de los canales de estéreo. ¿Cuántos paquetes por segundo debe transmitir RTP?

R= Cada muestra ocupa 4 bytes. Esto da un total de 256 muestras por paquete. Hay 44.100 muestras por segundo, así que con 256 muestras de paquetes, se necesita $44100/256$ o de 172 paquetes para transmitir la pena un segundo de música.

22. ¿Sería posible colocar el código RTP en el kernel del sistema operativo junto con el código UDP? Explique su respuesta.

R= Claro. La persona que llama tiene que proporcionar toda la información necesaria, pero no hay ninguna razón RTP no podía estar en el núcleo, al igual que UDP.

23. Un proceso del host 1 se ha asignado al puerto p, y un proceso del host 2 se ha asignado al puerto q. ¿Es posible que haya dos o más conexiones TCP entre estos dos puertos al mismo tiempo?

R= No. Una conexión se identifica sólo por sus órbitas. Por lo tanto, (1, p) - (2, q) es la única conexión posible entre estos dos puertos.

24. En la figura 6-29 vimos que además del campo Confirmación de recepción de 32 bits, hay un bit ACK en la cuarta palabra. ¿Esto agrega realmente algo? ¿Por qué sí o por qué no?

R= El bit ACK se usa para saber si el campo de 32 bits se utiliza. Pero si no fuera allí, el campo de 32-bit siempre tendría que ser utilizado, si es necesario reconocer un byte que ya había reconocido. En resumen, no es absolutamente esencial para el tráfico de datos normal. Sin embargo, desempeña un papel crucial durante la conexión establecimiento, donde se utiliza en los mensajes de la segunda y tercera del Trió apretón de manos.

25. La máxima carga útil de un segmento TCP son 65,495 bytes. ¿Por qué se eligió ese extraño número?

R= Todo el segmento TCP debe caber en el campo de carga útil 65.515 bytes de una dirección IP paquete. Desde la cabecera TCP es un mínimo de 20 bytes, sólo 65.495 bytes se dejan de datos TCP.

26. Describa dos formas de entrar en el estado SYN RCVD de la figura 6-33.

R= Una forma comienza con un LISTEN. Si se recibe un paquete SYN, el protocolo entra en el SYN RECD estado. La otra forma se inicia cuando un proceso intenta hacer un activa abierta y envía un paquete SYN. Si el otro lado se abre también, y es un SYN recibido, el estado SYN RECD también se introduce.

27. Indique una desventaja potencial del uso del algoritmo de Nagle en una red muy congestionada.

R= A pesar de que el usuario está escribiendo a una velocidad uniforme, los personajes serán se hizo eco en ráfagas. El usuario puede pulsar varias teclas con nada que aparece en la pantalla, y luego, de repente, la pantalla se pone al día con la escritura. La gente puede encontrar este molesto.

28. Considere el efecto de usar arranque lento en una línea con un tiempo de ida y vuelta de 10 mseg sin congestionamientos. La ventana receptora es de 24 KB y el tamaño máximo de segmento es de 2 KB. ¿Cuánto tiempo pasará antes de poder enviar la primera ventana completa?

R= Los primeros contienen ráfagas 4K 2K, 8K, 16K y bytes, respectivamente. El próximo uno es de 24 KB y se produce después de 40 ms.

29. Suponga que la ventana de congestionamiento del TCP está ajustada a 18 KB y que ocurre una expiración del temporizador. ¿Qué tan grande será la ventana si las siguientes cuatro ráfagas de transmisiones tienen éxito? Suponga que el tamaño máximo de segmento es de 1 KB.

R= La siguiente transmisión será de 1 tamaño máximo de segmento. Entonces 2, 4 y 8. Así que después de cuatro éxitos, será de 8 KB.

30. Si el tiempo de ida y vuelta del TCP, RTT, actualmente es de 30 mseg y las siguientes confirmaciones de recepción llegan después de 26, 32 y 24 mseg, respectivamente, ¿cuál es la nueva estimación de RTT utilizando el algoritmo de Jacobson? Use $\alpha = 0.9$.

R= Las estimaciones sucesivas son 29,6, 29,84, 29,256.

31. Una máquina TCP envía ventanas de 65,535 bytes por un canal de 1 Gbps que tiene un retardo de 10 mseg en un solo sentido. ¿Cuál es la velocidad real de transporte máxima que se puede lograr? ¿Cuál es la eficiencia de la línea?

R= Una ventana se puede enviar cada 20 ms. Esto da 50 ventanas / seg, para una velocidad de datos máxima de unos 3,3 millones de bytes por segundo. La eficiencia de la línea es entonces 26.4 Mbps/1000 Mbps o 2,6 por ciento.

32. ¿Cuál es la velocidad máxima de línea a la que un host puede enviar cargas útiles TCP de 1500 bytes con un tiempo de vida máximo de paquete de 120 seg sin que los números de secuencia den vuelta? Tome en cuenta la sobrecarga TCP, IP y Ethernet. Suponga que las tramas Ethernet se pueden enviar de manera continua.

R= El objetivo es enviar 232 bytes de 120 segundos o 35,791,394 bytes de carga útil / seg. Esto es 23.860 1500-byte cuadros / seg. La sobrecarga de TCP es de 20 bytes. La IP sobrecarga es de 20 bytes. La sobrecarga de Ethernet es de 26 bytes. Esto significa que para 1500 bytes de carga útil, 1566 bytes deben ser enviados. Si vamos a enviar a 23.860 marcos de 1566 bytes por segundo, necesitamos una línea de 299 Mbps Con cualquier cosa más rápido que esto se corre el riesgo de dos diferentes segmentos TCP con el mismo número de secuencia, al mismo tiempo.

33. En una red que tiene un tamaño máximo de TPDU de 128 bytes, un tiempo de vida máximo de TPDU de 30 seg, y un número de secuencia de 8 bits, ¿cuál es la tasa máxima de datos por conexión?

R= Un emisor no puede enviar más de 255 TPDU's, es decir, $255 \times 128 \times 8$ bits, en el 30 seg. La velocidad de datos es por lo tanto no más de 8.704 Kbps

34. Suponga que usted está midiendo el tiempo para recibir una TPDU. Cuando ocurre una interrupción, lee el reloj del sistema en milisegundos. Cuando la TPDU se ha procesado por completo, lee nuevamente el reloj. Mide 0 mseg 270,000 veces y 1 mseg 730,000 veces. ¿Cuánto tarda en recibir una TPDU?

R= Calcular la media: $(270.000 \times 730.000 \times 0 + 1 \text{ ms}) / 1000000$. Se necesita 730 microsegundos.

35. Una CPU ejecuta instrucciones a la tasa de 1000 MIPS. Los datos pueden copiarse 64 bits a la vez, y cada palabra toma diez instrucciones para copiarse. Si un paquete entrante tiene que copiarse cuatro veces, ¿puede este sistema manejar una línea de 1 Gbps? Por simplicidad, suponga que todas las instrucciones, incluso aquellas que leen o escriben en la memoria, se ejecutan a la tasa total de 1000 MIPS.

R= Lleva $4 \times 10 = 40$ instrucciones para copiar 8 bytes. Cuarenta instrucciones que llevan 40 nseg. Por lo tanto, cada byte requiere de 5 ns de tiempo de CPU para la copia. El sistema es por tanto capaz de manejar 200 MB / seg o 1600 Mbps Puede manejar una de 1 Gbps la línea si no hay otro cuello de botella está presente.

36. Para resolver el problema de los números de secuencia repetidos mientras que los paquetes anteriores aún existen, se podrían utilizar números de secuencia de 64 bits. Sin embargo, teóricamente, una fibra óptica puede ejecutarse a 75 Tbps. ¿Cuál es el tiempo de vida máximo de paquete que se requiere para asegurarse de que las futuras redes de 75 Tbps no tengan problemas de números de secuencia que den vuelta incluso con los números de secuencia de 64 bits? Suponga que cada byte tiene su propio número de secuencia, al igual que TCP.

R= El tamaño del espacio de secuencia es de 2^{64} bytes, que es aproximadamente 2×10^{19} bytes. A 75 Tbps transmisor utiliza el espacio de secuencia a una velocidad de 9.375×10^{12} secuencia de números por segundo. Se necesita 2 millones de segundos para envolver. Puesto que hay son 86.400 segundos en un día, tomará más de 3 semanas para envolver, incluso en 75 Tbps. Un tiempo de vida máximo de paquete de menos de 3 semanas evitará que el problema. En definitiva, va a 64 bits es probable que funcione por un tiempo.

37. Mencione una ventaja de RPC sobre UDP en comparación con el TCP para transacciones. Mencione una ventaja del T/TCP sobre RPC.

R= RPC a través de UDP tiene sólo dos paquetes en vez de tres. Sin embargo, RPC tiene una problema si la respuesta no cabe en un paquete.

38. En la figura 6-40(a) vimos que para completar el RCP se necesitan 9 paquetes. ¿Hay alguna circunstancia en la que se necesiten exactamente 10 paquetes?

R= Sí. Paquete de 6 reconoce tanto la solicitud y la aleta. Si cada uno se reconocido por separado, tendríamos 10 paquetes en la secuencia. Alternativamente, Paquete de 9, que reconoce la respuesta, y la aleta podría ser también dividido en dos paquetes separados. Así, el hecho de que hay nueve paquetes es sólo se debe a la buena suerte.

39. En la sección 6.6.5 calculamos que una línea de gigabits descarga 80,000 paquetes/seg en el host, y éste dispone de sólo 6250 instrucciones para procesarlos, lo que deja la mitad del tiempo de CPU para las aplicaciones. Para este cálculo se tomó un tamaño de paquete de 1500 bytes. Rehaga el cálculo para un paquete de tamaño ARPANET (128 bytes). En ambos casos, suponga que los tamaños de paquete dados incluyen toda la sobrecarga.

R= Con un paquete de 11,72 veces más pequeño, se obtiene 11.72 veces más por segundo, por lo que cada paquete sólo se $6250/11.72$ o 533 instrucciones.

40. Para una red de 1 Gbps que opera sobre 4000 km, el retardo es el factor limitante, no el ancho de banda. Considere una MAN con un promedio de 20 km entre el origen y el destino. ¿A qué tasa de datos el retardo de ida y vuelta debido a la velocidad de la luz iguala el retardo de transmisión para un paquete de 1 KB?

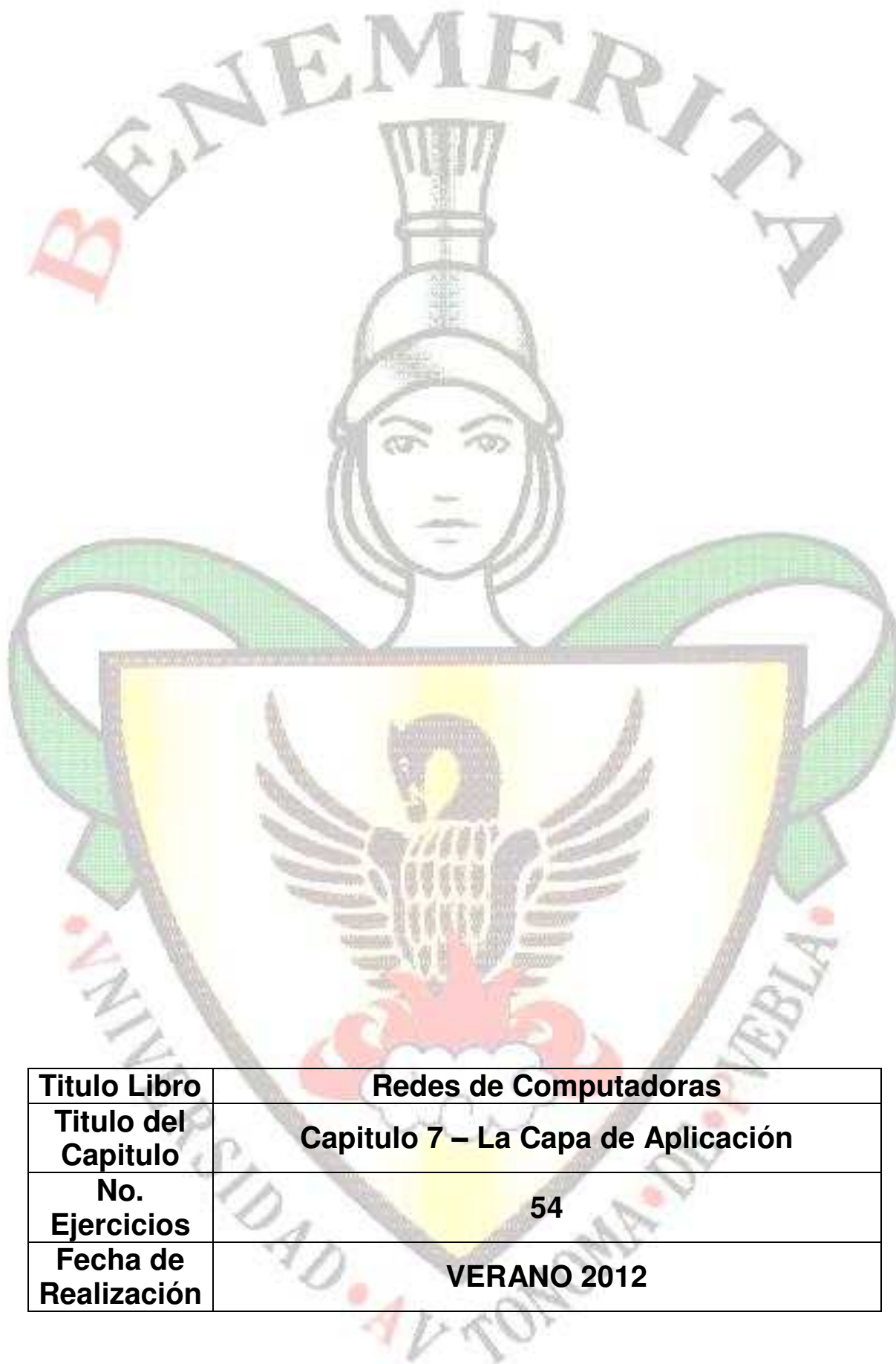
R= La velocidad de la luz en la fibra y el cobre es de unos 200 km / ms. Para una de 20 km línea, la demora es de 100 microsegundos de una manera y de ida y vuelta 200 microsegundos. Un paquete de 1 KB tiene 8192 bits. Si el tiempo de enviar 8192 bits y obtener el reconocimiento es 200 microsegundos, los retrasos en la transmisión y propagación son iguales. Si B es el bit tiempo, entonces tenemos $8192B = 2 \times 10^{-4}$ s. La velocidad de datos, $1/B$, es entonces sobre 40 Mbps

41. Calcule el producto de retardo de ancho de banda para las siguientes redes: (1) T1 (1.5 Mbps), (2) Ethernet (10 Mbps), (3) T3 (45 Mbps) y (4) STS-3 (155 Mbps). Suponga un RTT de 100 mseg. Recuerde que un encabezado TCP tiene 16 bits reservados para el tamaño de ventana. ¿Cuáles son sus implicaciones a la luz de sus cálculos?

R= La respuesta son: (1) 18,75 KB, (2) 125 KB, (3) 562,5 KB, (4) 1.937 MB. A 16-bit tamaño de la ventana significa que un remitente puede enviar un máximo de 64 KB antes de tener que esperar a una confirmación. Esto significa que un remitente no puede transmitir continuamente utilizando TCP y mantener lleno el tubo si la tecnología de red utilizada es Ethernet, T3, o STS 3-.

42. ¿Cuál es el producto de retardo de ancho de banda para un canal de 50 Mbps en un satélite geoestacionario? Si todos los paquetes son de 1500 bytes (incluyendo la sobrecarga), ¿qué tan grande debería ser la ventana en los paquetes?

R= El retraso de ida y vuelta es de aproximadamente 540 milisegundos, por lo que con un canal de 50 Mbps de la ancho de banda-retardo es producto de 27 megabits o bytes 3.375.000. Con los paquetes de 1500 bytes, que toma 2250 paquetes para llenar la tubería, por lo que la ventana debe estar a menos de 2250 paquetes.



Título Libro	Redes de Computadoras
Título del Capítulo	Capítulo 7 – La Capa de Aplicación
No. Ejercicios	54
Fecha de Realización	VERANO 2012

CAPITULO 7

1. Muchas computadoras de negocios tienen tres identificadores únicos en todo el mundo. ¿Cuáles son?

R= Ellos son el nombre DNS, la dirección IP y la dirección Ethernet.

2. De acuerdo con la información que se dio en la figura 7-3, ¿little-sister.cs.vu.nl corresponde a una red A, B o C?

R= Su dirección IP comienza con 130, por lo que está en una red de clase B. Véase el capítulo. 5 para la asignación de dirección IP.

3. En la figura 7-3, ¿hay un punto después de rowboat? ¿Por qué no?

R= No es un nombre absoluto, pero en relación con. Cs.vu.nl. En realidad es un atajo notación para rowboat.cs.vu.nl.

4. Adivine qué significa: -X (algunas veces se escribe como :-#).

R= Es decir: mis labios están sellados. Se utiliza en respuesta a una solicitud para mantener un secreto.

5. DNS utiliza UDP en lugar de TCP. Si se pierde un paquete DNS, no hay recuperación automática. ¿Esto causa un problema, y si es así, cómo se resuelve?

R= DNS es idempotente. Las operaciones se pueden repetir sin daño. Cuando un proceso hace una petición DNS, se inicia un temporizador. Si el tiempo se agota, sólo hace la solicitud de nuevo. No se hace daño.

6. Además de ser propensos a perderse, los paquetes UDP tienen una longitud máxima, potencialmente tan baja como 576 bytes. ¿Qué pasa cuando un nombre DNS que se va a buscar excede esta longitud? ¿Se puede enviar en dos paquetes?

R= El problema no se produce. Nombres DNS debe ser inferior a 256 bytes. La norma exige. Por lo tanto, todos los nombres DNS caber en un solo paquete.

7. ¿Una máquina con un solo nombre DNS puede tener múltiples direcciones IP? ¿Cómo puede ocurrir esto?

R= Sí. De hecho, en la figura. 7-3 vemos un ejemplo de una dirección IP duplicada. Recuerde que una dirección IP se compone de un número de red y un host número. Si una máquina tiene dos tarjetas Ethernet, puede estar en dos redes separadas, y si es así, se necesitan dos direcciones IP.

8. ¿Una computadora puede tener dos nombres DNS que pertenecen a dominios de nivel superior diferentes? De ser así, dé un ejemplo razonable. De lo contrario, explique por qué no.

R= Es posible. www.large-bank.com y www.large bank.ny.us-podría tener la misma dirección IP. Por lo tanto, una entrada en .com y en uno de los países dominios es ciertamente posible (y común).

9. El número de compañías con un sitio Web ha crecido de manera explosiva en los años recientes. Como resultado, miles de compañías están registradas con el dominio com, lo que causa una carga pesada en el servidor de nivel superior de este dominio. Sugiera una manera de aliviar este problema sin cambiar el esquema de nombres (es decir, sin introducir nuevos nombres de dominio de nivel superior). Es válido que su solución requiera cambios al código cliente.

R= Hay muchos enfoques, obviamente. Una de ellas es desactivar el servidor de nivel superior en una granja de servidores. Otra es tener 26 servidores separados, uno para los nombres que empiezan con una, una para b, y así sucesivamente. Para un cierto período de tiempo (por ejemplo, 3 años) después la introducción de los nuevos servidores, el viejo podría seguir funcionando para dar la gente la oportunidad de adaptar su software.

10. Algunos sistemas de correo electrónico soportan un campo de encabezado Content Return:. Especifique si el cuerpo de un mensaje se va a regresar en caso de que no se entregue. ¿Este campo pertenece al sobre o al encabezado?

R= Pertenece a la envoltura debido a que el sistema de entrega necesita conocer su valor para gestionar el correo electrónico que no se puede entregar.

11. Los sistemas de correo electrónico necesitan directorios a fin de que se puedan buscar las direcciones de correo electrónico de las personas. Para construir tales directorios y para que la búsqueda sea posible, los nombres deben dividirse en componentes estándar (por ejemplo, nombre, apellido). Mencione algunos problemas que deben resolverse a fin de que un estándar mundial sea aceptable.

R= Esto es mucho más complicado de lo que piensas. Para empezar, sobre la mitad del mundo, escribe los nombres que se dan en primer lugar, seguido por el nombre de la familia, y la otra mitad (por ejemplo, China y Japón) lo hacen en sentido contrario. Un sistema de nombres habría que distinguir un número arbitrario de nombres que se dan, además de una familia nombre, aunque este último podría tener varias partes, como en John von Neumann. Luego están las personas que tienen la inicial del segundo, pero no tiene segundo nombre. Varios títulos, como el Sr., Srta., Sra., Dr., Prof., o Señor, pueden agregar un prefijo de nombre. La gente viene de generaciones, de modo Jr., Sr., III, IV, etc. tienen que ser incluido. Algunas personas usan sus títulos académicos en sus nombres, así que necesitamos BA, B.Sc., MA, M.Sc., Ph.D., y otras titulaciones. Por último, hay personas que incluyen los premios y honores determinados en su nombre. Un miembro de la Real Sociedad en Inglaterra podría agregar FRS, por ejemplo. Por ahora debemos ser capaz de satisfacer incluso a los sabios: Prof. Dr. Abigail Barbará Cynthia Doris E. de Vries III, Ph.D., FRS.

12. La dirección de correo electrónico de una persona es su nombre de inicio de sesión + @ + el nombre de un dominio DNS con un registro MX. Los nombres de inicio de sesión pueden ser nombres de pila, apellidos, iniciales y todos los tipos de nombres. Suponga que una compañía grande decidió que se estaba perdiendo mucho correo debido a que las personas no sabían el nombre de inicio de sesión del receptor. ¿Hay alguna forma de que dicha compañía arregle este problema sin cambiar el DNS? De ser así, dé una propuesta y explique cómo funciona. De lo contrario, explique por qué no es posible.

R= Es factible y relativamente sencillo. Cuando el correo electrónico entrante llega, el SMTP demonio que lo acepta tiene que buscar el nombre de usuario en el mensaje RCPT TO. Ciertamente, hay un archivo o base de datos donde se encuentran estos nombres. Ese archivo podría ampliarse para tener alias de la forma "" que Ellen. Johnson señalar al buzón de la persona. A continuación, el correo electrónico siempre puede ser enviado a través del nombre real de la persona.

13. Un archivo binario tiene una longitud de 3072 bytes. ¿Qué longitud tendrá si se codifica mediante base64, y se inserta un par CR+LF después de cada 80 bytes enviados y al final?

R= La codificación de base 64 se romperá el mensaje en 1024 unidades de 3 bytes cada uno. Cada uno de éstos se codifica como 4 bytes, para un total de 4096 bytes. Si estos A continuación se divide en líneas de 80 bytes, 52 líneas tales será necesario, añadiendo 52 CR y LF 52. La longitud total será entonces 4200 bytes.

14. Considere el esquema de codificación MIME entrecomillado-imprimible. Mencione un problema que no se analiza en el texto y proponga una solución.

R= Si una secuencia comienza con un signo igual y seguido por dos hexadecimal dígitos pasa a aparecer en el texto, por ejemplo, = FF, esta secuencia será erróneamente interpretarse como una secuencia de escape. La solución es codificar la igualdad firma en sí, por lo que todos los signos de igualdad siempre empiezan las secuencias de escape.

15. Nombre cinco tipos MIME que no se listan en este libro. Puede verificar su navegador o Internet para obtener información.

R= Algunos ejemplos son posibles y ayudantes de aplicación / msexcel (Excel), application / PPT (PowerPoint), de audio / MIDI (de sonido MIDI), image / tiff (cualquier vista previa de los gráficos), video / x-dv (QuickTime Player).

16. Suponga que desea enviar un archivo MP3 a un amigo, pero el ISP de éste limita a 1 MB la cantidad de correo entrante y el archivo MP3 es de 4 MB. ¿Hay alguna forma para manejar esta situación utilizando el RFC 822 y MIME?

R= Sí, utilizar el mensaje / external-body subtipo y envíanos la dirección URL del archivo en lugar del archivo real.

17. Suponga que alguien establece un demonio de vacaciones y que después envía un mensaje justo antes de terminar su sesión. Desgraciadamente, el receptor ha estado de vacaciones una semana y también tiene un demonio de vacaciones en su lugar. ¿Qué sucede a continuación? ¿Las respuestas grabadas se enviarán y regresarán hasta que alguien regrese?

R= El mensaje enviado justo antes de salir va a generar una respuesta enlatada. Su llegada también va a generar una respuesta enlatada. Suponiendo que cada máquina se conecta por e-mail direcciones a las que ya ha respondido, no hay respuestas más lata será enviada.

18. En cualquier estándar, como el RFC 822, se necesita una gramática precisa de lo que está permitido de manera que diferentes implementaciones puedan interactuar. Incluso los elementos simples se tienen que definir con cuidado. Los encabezados SMTP permiten espacios en blanco entre los tokens. Dé dos definiciones de alternativas razonables de espacios en blanco entre los tokens.

R= El primero es cualquier secuencia de uno o más espacios y / o tabuladores. La segunda es cualquier secuencia de uno o más espacios y / o fichas y / o retrocesos sujetos a la condición de que el resultado neto de la aplicación de todas las teclas de retroceso aún deja al por lo menos un espacio o una tabulación más.

19. ¿El demonio de vacaciones es parte del agente de usuario o del agente de transferencia de mensajes? Por supuesto, se establece con el agente de usuario, pero ¿éste envía realmente las respuestas? Explique.

R= Las respuestas reales tienen que ser realizada por el agente de transferencia de mensajes. Cuando un Conexión SMTP entrante, el agente de transferencia de mensaje tiene que comprobar si un demonio de vacaciones está configurado para responder a la entrada de correo electrónico, y en caso afirmativo enviar, una respuesta. El agente de transferencia de usuario no puede hacer esto porque ni siquiera será invoca hasta que el usuario regresa de sus vacaciones.

20. POP3 permite que los usuarios obtengan y bajen correo electrónico de un buzón remoto. ¿Esto significa que el formato interno de los buzones debe estandarizarse para que cualquier programa POP3 en el cliente pueda leer el buzón en cualquier servidor de correo? Explique su respuesta.

R= No. El programa de POP3 no llegan a tocar el buzón de correo remoto. Se envía órdenes al demonio POP3 en el servidor de correo. Mientras que el demonio entiende el formato de buzón, que puede funcionar. Por lo tanto, un servidor de correo podría cambiar de un formato a otro durante toda la noche sin decirles a sus clientes, como mientras que al mismo tiempo cambia su demonio POP3 por lo que entiende el nuevo formato.

21. Desde el punto de vista de un ISP, POP3 e IMAP tienen diferencias importantes. Por lo general, los usuarios de POP3 vacían sus buzones todos los días. Los usuarios de IMAP mantienen su correo electrónico en el servidor de manera indefinida. Imagine que se le pide a usted que aconseje a un ISP sobre cuáles protocolos debe soportar. ¿Qué aspectos tomaría en cuenta?

R= El almacenamiento de los usuarios de correo electrónico de toma espacio en el disco, que cuesta dinero. Este factor argumenta a favor de usar POP3. Por otro lado, el ISP podría cobrar por disco de almacenamiento por encima de unos pocos megabytes, convirtiendo el correo electrónico en una máquina de hacer dinero. La este último argumenta a favor de IMAP para animar a los usuarios para mantener el correo electrónico en el servidor (y pagar por el espacio en disco).

22. ¿Webmail utiliza POP3, IMAP o ninguno? Si utiliza alguno de éstos, ¿por qué se eligió? Si no se utiliza ninguno, ¿cuál está más cerca de ser usado?

R= No utilizar cualquiera de ellas. Sin embargo, es bastante similar en espíritu a IMAP, porque tanto de ellos permiten que un cliente remoto para examinar y gestionar un buzón de correo remoto. Por el contrario, POP3 sólo envía al buzón del cliente para el procesamiento de allí.

23. Cuando se envían las páginas Web, se les anteponen encabezados MIME. ¿Por qué?

R= El navegador tiene que ser capaz de saber si la página es de texto, audio, vídeo u otra cosa. Los encabezados MIME proporcionar esta información.

24. ¿Cuándo son necesarios los visores externos? ¿Cómo sabe un navegador cuál utilizar?

R= Si el navegador recibe una página con un tipo MIME que no puede manejar, se llama un visor externo para visualizar la página. Se encuentra el nombre del espectador en una tabla de configuración, o que se obtiene del usuario.

25. ¿Es posible que cuando un usuario haga clic en un vínculo con Netscape se inicie una aplicación auxiliar en particular, y que cuando haga clic en el mismo vínculo en Internet Explorer se inicie una aplicación auxiliar completamente diferente, aunque el tipo MIME regresado en ambos casos sea idéntico? Explique su respuesta.

R= Sí, es posible. Lo que se ha iniciado auxiliar depende de la configuración mesas en el interior del navegador, y Netscape e Internet Explorer puede haber sido configurado de manera diferente. Por otra parte, es decir, tiene la extensión de archivo más en serio que la Tipo MIME y la extensión de archivo puede indicar una ayuda diferente a la Tipo MIME.

26. Un servidor Web de múltiples subprocesos está organizado como se muestra en la figura 7-21. Tarda 500 μ seg en aceptar una solicitud y verificar el caché. La mitad del tiempo es para encontrar el archivo en el caché y para regresarlo de inmediato. En la otra mitad del tiempo, el módulo tiene que bloquearse por 9 msec mientras su solicitud de disco se coloca en la cola y se procesa. ¿Cuántos módulos debe tener el servidor para mantener ocupada todo el tiempo a la CPU (suponiendo que el disco no es un cuello de botella)?

R= Si un módulo tiene dos solicitudes, una será un éxito y una memoria caché será una caché perderse en promedio. El tiempo total de CPU que se consume es de 1 ms, y la espera total tiempo es de 9 ms. Esto da una utilización de la CPU 10%, por lo que con 10 módulos de los La CPU se mantiene ocupado.

27. El URL http estándar da por hecho que el servidor Web está escuchando en el puerto 80. Sin embargo, es posible que un servidor Web escuche en otro puerto. Diseñe una sintaxis razonable para que un URL acceda a un archivo en un puerto no estándar.

R= El funcionario de RFC 1738 forma de hacer esto es `http://dns-name:port/file`.

28. Aunque no se mencionó en el texto, una forma alternativa de un URL es utilizar una dirección IP en lugar de su nombre DNS. Un ejemplo del uso de una dirección IP es `http://192.31.231.66/index.html`. ¿Cómo sabe el navegador si el nombre que sigue al esquema es un nombre DNS o una dirección IP?

R= Los nombres DNS no puede terminar con un dígito, lo que no hay ambigüedad.

29. Imagine que alguien del Departamento de Computación de Stanford acaba de escribir un nuevo programa que desea distribuir mediante FTP. Esa persona coloca el programa en el directorio `ftp/pub/freebies/-newprog.c` de FTP. ¿Cuál será el URL más probable de este programa?

R= La dirección URL es probablemente `ftp://www.cs.stanford.edu/ftp/pub/freebies/newprog.c`

30. En la figura 7-25, `www.aportal.com` mantiene un registro de las preferencias del usuario en una cookie. Una desventaja de este esquema es que las cookies están limitadas a sólo 4 KB, de manera que si las preferencias son grandes —por ejemplo, muchas acciones, equipos de deportes, tipos de noticias, el clima de varias ciudades, ediciones especiales de varias categorías de productos, etcétera— puede alcanzarse el límite de 4 KB. Diseñe una forma alternativa para mantener el registro de las preferencias que no tengan este problema.

R= Hacerlo de la manera toms-casino hace: sólo hay que poner un ID de cliente en la cookie y la tienda las preferencias en una base de datos en el servidor de indexado por ID de cliente. Qué manera el tamaño del registro es ilimitado.

31. El Banco Sloth desea que sus clientes flojos puedan utilizar con facilidad su banca en línea, por lo que después de que un cliente firma y se autentica mediante una contraseña, el banco regresa una cookie que contiene un número de ID del cliente. De esta forma, el cliente no tiene que identificarse a sí mismo o escribir una contraseña en visitas futuras a la banca en línea. ¿Qué opina de esta idea? ¿Funcionará? ¿Es una buena idea?

R= Técnicamente, funciona, pero es una idea terrible. Todo el cliente tiene que hacer es modificar la cookie para obtener acceso a la cuenta bancaria de otra persona. Tener el galletas proporcionar la identidad del cliente está a salvo, pero el cliente debe ser necesario introducir una contraseña para probar su identidad.

32. En la figura 7-26, el parámetro ALT se establece en la etiqueta ``. ¿Bajo qué condiciones lo utiliza el navegador, y cómo?

R= Si el usuario ha desactivado el automático de la visualización de imágenes, o si las imágenes no pueden Se mostrará por alguna otra razón, entonces el texto que figura en la ALT es muestra en lugar de la imagen. Además, si el puntero del ratón sobre la imagen, la texto puede ser mostrado.

33. ¿Cómo utiliza HTML a fin de que se pueda hacer clic en una imagen? Dé un ejemplo.

R= Un hipervínculo consiste en `` y ``. Entre ellos está el hacer clic en texto. También es posible poner una imagen aquí. Por ejemplo: ` `

34. Muestre la etiqueta `<a>` que se necesita para hacer que la cadena "ACM" sea un hipervínculo a `http://www.acm.org`.

R= Sería ` ACM `.

35. Diseñe un formulario para que la nueva compañía Interburger permita ordenar hamburguesas a través de Internet. Dicho formulario debe incluir el nombre, la dirección y la ciudad del cliente, así como opciones que permitan seleccionar el tamaño (gigante o inmensa) y si llevará queso. Las hamburguesas se pagarán en efectivo a la entrega por lo que no se necesita información de tarjeta de crédito.

R= Aquí está una manera de hacerlo.

```
<html>
<head> <title> INTERBURGER </ title> </ head>
<body>
forma <h1> Interburger de pedidos </ h1>
<form METHOD=POST> action="http://interburger.com/cgi-bin/burgerorder"
Nombre <p> <input name="customer" size=46> </ p>
Dirección Calle <p> <input name="address" size=40> </ p>
Ciudad <p> <input name="city" size=20> </ p>
Tamaño de la hamburguesa gigante <input name="size" type=radio value="gigantic">
Inmenso <input name="size" type=radio value="immense">
Queso <input name="cheese" type=checkbox>
<p> <input type=submit value="submit order"> </ p>
</ form>
</ body> </ html>
```

36. Diseñe un formulario que pida al usuario que teclee dos números. Cuando el usuario haga clic en el botón de envío, el servidor regresará la suma de dichos números. Escriba el servidor como una secuencia de comandos PHP.

R= La página que muestra el formulario es el siguiente:

```
<html>
<head> <title> Adder </ title> </ head>
<body>
<form action="action.php" method="post">
<p> Por favor, introduzca el primer número: <input type="text" name="first"> </ p>
<p> Por favor, introduzca el segundo número: <input type="text" name="second"> </ p>
<input type="submit">
</ form>
</ body>
</ html>
```

El script PHP que hace el proceso es el siguiente:

```
<html>
<head> <title> adición </ title> </ head>
<body>
La suma es <php echo $ primero + $ segundo;?>
</ body>
</ html>
```

37. Para cada una de las siguientes aplicaciones, indique si sería (1) posible y (2) mejor utilizar una secuencia de comandos PHP o una JavaScript y por qué.

(a) Desplegar un calendario por cada mes solicitado desde septiembre de 1752.

(b) Desplegar la agenda de vuelos de Ámsterdam a Nueva York.

(c) Graficar un polinomio a partir de coeficientes proporcionados por el usuario.

R= (a) Hay sólo 14 calendarios anuales, dependiendo del día de la semana en 01 de enero, que las caídas y si el año es un año bisiesto. Por lo tanto, un Java Script el programa podría contener todos los 14 calendarios y una pequeña base de datos de los cuales año se qué calendario. Una secuencia de comandos PHP también podría ser utilizado, pero sería más lento. (b) Esto requiere una gran base de datos. Hay que hacerlo en el servidor mediante el uso de PHP. (c) Tanto el trabajo, pero Java Script es más rápido.

38. Escriba un programa en JavaScript que acepte un entero mayor que 2 e indique si es un número primo. Observe que JavaScript tiene instrucciones if y while con la misma sintaxis que C y Java. El operador de módulo es %. Si necesita la raíz cuadrada de x, utilice Math.sqrt (x).

R= Hay muchas soluciones posibles, obviamente. Aquí está uno.

```
<html>
<head> <title> Java Script prueba </ title> </ head>
<script language="JavaScript" type="text/JavaScript">
función de respuesta (test3form) {
var n = 2;
has3factors var = 0;
var = número eval (test3form.number.value);
var = límite Math.sqrt (número);
mientras que (n + + <límite) if (numero% n == 0) has3factors = 1;
document.open ();
document.writeln ("<body> <html>");
if (has3factors > 0) document.writeln (número, "no es un número primo");
if (has3factors == 0) document.writeln (número, "es un número primo");
document.writeln ("</ body> </ html>");
document.close ();
}
</ script>
</ head>
<body>
<form name="myform">
Por favor, introduzca un número: <input type="text" name="number">
<input type="button" onclick="response(this.form)" value="compute primality"
</ form>
</ body>
</ html>
```

Claramente, esto se puede mejorar de varias maneras, pero éstos requieren un poco más conocimiento del Java script.

39. Una página HTML es como sigue:

```
<html> <body>
<a href="www.info-source.com/welcome.html"> Haga clic aquí para obtener información </a>
</body> </html>
```

Si el usuario hace clic en el hipervínculo, se abre una conexión TCP y se envía una serie de líneas al servidor. Liste todas las líneas enviadas.

R= Los comandos enviados son los siguientes: GET / HTTP/1.1 welcome.html. Host: www.info-source.com. Tenga en cuenta la línea en blanco al final. Es obligatorio.

40. Es posible utilizar el encabezado If-Modified-Since para verificar si una página almacenada en caché aún es válida. Las solicitudes pueden realizarse para obtener páginas que contengan imágenes, sonido, vídeo, HTML, etcétera. ¿Cree que la efectividad de esta técnica es mejor o peor para imágenes JPEG en comparación con HTML? Piense con cuidado sobre lo que significa "efectividad" y explique su respuesta.

R= La mayoría de las páginas HTML que puedan cambiar más a menudo que los archivos JPEG. Muchos de los sitios jugar con el código HTML todo el tiempo, pero no cambian las imágenes mucho más. Pero la eficacia se refiere a no sólo la tasa de aciertos, pero también la recompensa del. Hay diferencia no tanto entre conseguir un mensaje 304 y 500 líneas de conseguir HTML. El retardo es esencialmente el mismo en ambos casos porque los archivos HTML son tan pequeños. Los archivos de imágenes son grandes, así no tener que enviar a uno es una gran victoria.

41. El día en que se celebra un evento deportivo importante, como el juego de campeonato de la NFL, muchas personas visitan el sitio Web oficial. ¿Es ésta una aglomeración instantánea en el mismo sentido que con las elecciones en Florida del 2000? ¿Por qué sí o por qué no?

R= Día N ° En el caso de los deportes, que se conoce de antemano que habrá un gran público en el sitio web y las réplicas se pueden construir por todo el lugar. La esencia de una multitud de flash es que es inesperado. Había una gran multitud en el Sitio web de la Florida, pero no en los sitios de Iowa o Minnesota. Nadie podría tener predicho de antemano.

42. ¿Tiene sentido que un solo ISP funcione como una CDN? De ser así, ¿cómo funcionaría? De lo contrario, ¿qué está mal con esa idea?

R= Claro. El proveedor de Internet va a un número de proveedores de contenido y se pone su permiso para replicar el contenido en el sitio del ISP. El proveedor de contenido puede incluso pagar por esto. La desventaja es que es un montón de trabajo por el ISP para póngase en contacto con muchos proveedores de contenido. Es más fácil dejar que un CDN hacer esto.

43. ¿Bajo qué condiciones es una mala idea utilizar una CDN?

R= Es una mala idea si el contenido cambia rápidamente. Páginas llenas de arriba a la segunda resultados deportivos o cotizaciones de bolsa no son buenos candidatos, por ejemplo. Páginas que se generan de forma dinámica no son adecuadas.

44. Las terminales de los sistemas inalámbricos Web tienen un ancho de banda bajo, lo cual provoca que la codificación eficiente sea importante. Diseñe un esquema para transmitir texto en inglés de manera eficiente a través de un enlace inalámbrico a un dispositivo WAP. Puede asumir que la terminal tiene algunos megabytes de ROM y una CPU con potencia moderada. Sugerencia: piense en transmitir japonés, en el que cada símbolo es una palabra.

R= Cada kanji japonés (palabra) se le ha asignado un número. Hay alrededor de 20.000 de ellos en Unicode. Para un sistema todo-Inglés, sería posible asignar las 65.000 palabras más comunes de un código de 16 bits y transmitir sólo el código. El terminal automáticamente agregar un espacio entre palabras. Palabras no en la lista, se recogería en ASCII. Utilizando este esquema, la mayoría de las palabras tomaría 2 bytes, mucho menos que su transmisión carácter a carácter. Otros programas podrían incluir el uso de códigos de 8 bits de las palabras más comunes y la prolongación de los códigos de los códigos menos frecuentes (primitiva Huffman).

45. Un disco compacto contiene 650 MB de datos. ¿La compresión se utiliza para CDs de audio? Explique su respuesta.

R= Audio necesita 1,4 Mbps, que es de 175 KB / seg. En un dispositivo de 650 MB, hay espacio para 3714 segundos de audio, que es un poco más de una hora. CDs nunca más se encuentran de una hora larga, así que no hay necesidad de compresión y que no se utiliza.

46. En la figura 7-57(c) el ruido de cuantización ocurre debido al uso de muestras de 4 bits para representar nueve valores de señal. La primera muestra, en 0, es exacta, pero las siguientes no lo son. ¿Cuál es el porcentaje de error para las muestras en 1/32, 2/32 y 3/32 del periodo?

R= Los verdaderos valores son $\sin(2\pi i / 32)$ para i desde 1 a 3. En términos numéricos, estos senos son 0,195, 0,383, y 0,556. Ellos son representados como 0,250, 0,500 y 0,500, respectivamente. Así, los errores por ciento son 28, 31 y 10 por ciento, respectivamente.

47. ¿Es posible utilizar un modelo psicoacústico para reducir el ancho de banda necesario para la telefonía de Internet? De ser así, ¿cuáles condiciones, si las hay, se tendrían que cumplir para que funcionara? De lo contrario, ¿por qué no es posible?

R= En teoría, podría ser utilizado, pero la telefonía por Internet es en tiempo real. Para la música, no hay ninguna objeción a pasar 5 minutos para codificar una canción de 3 minutos. Para en tiempo real del habla, que no funcionaría. La compresión psicoacústica posible trabajar para la telefonía, pero sólo si existe un chip que podría hacer la compresión sobre la marcha con un retraso de alrededor de 1 ms.

48. Un servidor de flujo continuo de audio tiene una distancia de una sola vía de 50 mseg con un reproductor de medios. Tiene una salida de 1 Mbps. Si el reproductor de medios tiene un búfer de 1 MB, ¿qué puede decir acerca de la posición de la marca de agua baja y de la alta?

R= Se tarda 50 ms para obtener un comando de pausa para el servidor, en el que el tiempo 6250 bytes se llega, por lo que la línea de bajamar debe ser muy por encima de 6250, probablemente 50.000 para estar seguro. De manera similar, la marca alta de agua debe ser de al menos 6250 bytes desde el principio, sino, digamos, 50.000 estarían más seguros.

49. El algoritmo de entrelazado de la figura 7-60 tiene la ventaja de que puede resolver la pérdida de un paquete ocasional sin introducir un hueco en la reproducción. Sin embargo, cuando se utiliza para la telefonía de Internet, también tiene una pequeña desventaja. ¿Cuál es?

R= Se introduce un retardo adicional. En el esquema sencillo, después de 5 ms tienen transcurrido, el primer paquete puede ser enviado. En este esquema, el sistema tiene que esperar hasta 10 ms hasta que se puede mandar las muestras para los primeros 5 ms.

50. ¿La voz sobre IP tiene los mismos problemas con los servidores de seguridad que el audio de flujo continuo? Explique su respuesta.

R= Depende. Si la persona que llama no está detrás de un firewall y el destinatario se encuentra en un regular teléfono, no hay problema en absoluto. Si la persona que llama está detrás de un firewall y el firewall no es exigente con lo que abandona el sitio, sino que también va a funcionar. Si el destinatario de la llamada está detrás de un firewall que no le dejará los paquetes UDP a cabo, no va a funcionar.

51. ¿Cuál es la tasa de bits para transmitir tramas de color sin comprimir de 800×600 píxeles con 8 bits/ -píxel a 40 tramas/seg?

R= El número de bits por segundo se encuentra a sólo $800 \times 600 \times 40 \times 8$ ó 153,6 Mbps

52. ¿Un error de 1 bit en una trama MPEG puede dañar más que la trama en la que ocurrió el error? Explique su respuesta.

R= Sí. Un error en un I-frame se producirán errores en la reconstrucción de la siguiente Fotogramas P y B-frames. De hecho, el error seguirá para propagar hasta el siguiente cuadro I.

53. Considere un servidor de vídeo de 100,000 clientes, en donde cada cliente ve dos películas por mes. La mitad de las películas se proporcionan a las 8 p.m. ¿Cuántas películas tiene que transmitir a la vez el servidor durante este periodo? Si cada película requiere 4 Mbps, ¿cuántas conexiones OC-12 necesita el servidor para la red?

R= Con 100.000 clientes cada uno recibiendo dos películas al mes, los productos de servidor 200.000 películas por mes o alrededor de 6.600 por día. Si la mitad de estos se encuentran en PM, el servidor debe manejar alrededor de 3.300 películas a la vez. Si el servidor tiene que transmitir películas en 3300 a los 4 Mbps cada uno, el ancho de banda requerido es de 13,2 Gbps. Uso de conexiones OC-12, con una capacidad de SPE de 594 Mbps cada uno, por lo menos 23 conexiones serán necesarios. Una máquina que sirve al mismo tiempo las películas de 3300 más de 23 conexiones OC-12 no es una máquina pequeña.

54. Suponga que la ley de Zipf se cumple para acceder un servidor de vídeo con 10,000 películas. Si el servidor mantiene las 1000 películas más populares en un disco magnético y las restantes 9000 en un disco óptico, dé una expresión para la fracción de todas las referencias que estarán en un disco magnético. Escriba un pequeño programa para evaluar esta expresión de manera numérica.

R= La fracción de todas las referencias a las primeras películas de r viene dada por:

$$C/1 + C/2 + C/3 + C/4 + \cdots + C/r$$

Así, la relación de la primera 1000 a la primera es 10.000:

$$\frac{1/1 + 1/2 + 1/3 + 1/4 + \cdots + 1/1000}{1/1 + 1/2 + 1/3 + 1/4 + \cdots + 1/10000}$$

Debido a que el C se anula. La evaluación de esta forma numérica, se obtiene 7.486/9.788. Por lo tanto, alrededor de 0,764 de todas las solicitudes será a las películas en el disco magnético. Es de destacar que la ley de Zipf implica que una cantidad sustancial de la distribución está en la cola, en comparación, por ejemplo, al decaimiento exponencial.



Titulo Libro	Redes de Computadoras
--------------	-----------------------

Titulo del Capitulo	Capitulo 8 – Seguridad en Redes
No. Ejercicios	45
Fecha de Realización	VERANO 2012

CAPITULO 8

1. Rompa el siguiente cifrado monoalfabético. El texto llano, que consiste sólo en letras, es un fragmento bien conocido de un poema de Lewis Carroll.

kfd ktbd fzm eubd kfd pzyiom mztz ku kzyg ur bzha kfthcm
ur mftnm zhx mfudm zhx mdzythc pzq ur ezsszcdm zhx gthcm
zhx pfa kfd mdz tm sutythc fuk zhx pfdkfdi ncm fzld pthcm
sok pztz z stk kfd uamkdim eitdx sdruidd pd fzld uoi efzk
rui mubd ur om zid ouk ur sidzkh zhx zyy ur om zid rzk
hu foia mztz kfd ezindhkdi kfda kfzhgdx ftb boef rui kfzk

R= ha llegado el momento de la morsa, dijo que hablar de muchas cosas de los zapatos, barcos y lacre de las coles y reyes y por qué hierve el mar tan caliente y si los cerdos tienen alas pero esperar un poco gritaron las ostras antes de que tengamos nuestro chat para algunos de nosotros están fuera de la respiración y todos nosotros somos la grasa no tiene prisa.

2. Rompa el siguiente cifrado de transposición columnar. El texto llano proviene de un libro de texto de computadoras muy popular, por lo que “computadora” es una palabra probable. El texto llano consiste por completo en letras (sin espacios). Para mayor claridad, el texto cifrado está dividido en bloques de cinco caracteres.

aaun cvlre runn dltme aeepb ytust iceat npmey iicgo gorch srsoc
nntii imiha oofpa gsvit tpsit lbolr otoex

R= El texto es el siguiente: una computadora digital es una máquina que puede resolver los problemas de la gente por llevar a cabo las instrucciones dadas a la misma. Desde Organización de Computadoras estructurado por AS Tanenbaum.

3. Encuentre un relleno de una sola vez de 77 bits que genere el texto “Donald Duck” a partir del texto cifrado de la figura 8-4.

R= Es: 1011111 0000100 1110000 1011011 1001000 1100010 0001011 0010111 1001101 1110000 1101110.

4. La criptografía cuántica requiere tener un arma de fotones que pueda disparar a solicitud un solo fotón que transporte 1 bit. En este problema, calcule cuántos fotones transporta un bit en un enlace de fibra de 100 Gbps. Suponga que la longitud de un fotón es igual a su longitud de onda, que por propósitos de este problema, es 1 micra. La velocidad de la luz en la fibra es de 20 cm/nseg.

R= A 100 Gbps, un poco toma 10-11 segundos para ser transmitidos. Con la velocidad de la luz siendo 2×10^8 metros por segundo, en tiempo de bit 1, el pulso de luz alcanza una longitud de 2 mm o 2000 micras. Puesto que un fotón es de aproximadamente 1 micra de longitud, el pulso es 2000 fotones largos. Por lo tanto, estamos muy lejos de un fotón por bit, incluso en 100 Gbps. Sólo a 200 Tbps logramos un poco por fotón.

5. Si Trudy captura y regenera fotones cuando está en uso la criptografía cuántica, obtendrá algunos fotones erróneos y causará errores en el relleno de una sola vez de Bob. ¿En promedio qué fracción de los bits de relleno de una sola vez de Bob serán erróneos?

R= La mitad del tiempo de Trudy acertará. Todos los bits se regenerará correctamente. La otra mitad se va a adivinar equivocado y entrega bits aleatorios a Bob. La mitad de ellos se equivocan. Así, el 25% de los bits se pone la fibra estar equivocado. De una sola vez de Bob plataforma será, pues, el 75% bien y el mal 25%.

6. Un principio fundamental de criptografía indica que todos los mensajes deben tener redundancia. Pero también sabemos que la redundancia ayuda a que un intruso sepa si una clave adivinada es correcta. Considere dos formas de redundancia. Primero, los n bits iniciales de texto llano contienen un patrón conocido. Segundo, los bits n finales del mensaje contienen un hash en el mensaje. Desde un punto de vista de seguridad, ¿estos dos son equivalentes? Analice su respuesta.

R= Si el intruso tenía potencia de cálculo infinito, que sería el mismo, pero ya que no es el caso, el segundo es mejor. Obliga a que el intruso que hacer un cálculo para ver si cada tecla tratado es la correcta. Si este cálculo es caro, será más lento que el intruso hacia abajo.

7. En la figura 8-6, se alternan las cajas P y S. Aunque este arreglo es estético, ¿es más seguro que primero tener todas las cajas P y después todas las S?

R= Sí. Una secuencia contigua de P-cajas puede ser reemplazada por una sola P-caja. Lo mismo ocurre con las cajas-S.

8. Diseñe un ataque a DES con base en el conocimiento de que el texto llano consiste exclusivamente en letras ASCII mayúsculas, más espacio, coma, punto, punto y coma, retorno de carro y avance de línea. No se sabe nada sobre los bits de paridad de texto llano.

R= Para cada posible clave de 56 bits, descifrar el primer bloque de texto cifrado. Si el resultante texto es legal, intente el siguiente bloque, etc. Si el texto es ilegal, trata de la siguiente tecla.

9. En el texto calculamos que una máquina para romper cifrado con mil millones de procesadores que pueden analizar una clave en 1 picosegundo podría tardar sólo 1010 años para romper la versión de 128 bits de AES. Sin embargo, las máquinas actuales podrían tener 1024 procesadores y tardar 1 mseg en analizar una clave, por lo que necesitamos un factor de mejora en rendimiento de 1015 sólo para obtener una máquina de rompimiento AES. Si la ley de Moore (el poder de cómputo se duplica cada 18 meses) sigue vigente, ¿cuántos años se necesitarían tan sólo para construir la máquina?

R= La ecuación $2^n = 1015$ nos dice n , el número de duplicar períodos necesarios. Resolviendo, obtenemos $n = 15$ $n = \log_2 10$ o 50 períodos de duplicación, que es 75 años. Sólo la construcción de esta máquina es bastante lejos, y la ley de Moore no puede continuar por 75 años más.

10. AES soporta una clave de 256 bits. ¿Cuántas claves tiene AES-256? Vea si puede obtener algún número en física, química o astronomía de aproximadamente el mismo tamaño. Utilice Internet para buscar números grandes. Elabore una conclusión a partir de su investigación.

R= La ecuación que tenemos que resolver es $2^{256} = 10^n$. Tomando logaritmos comunes, obtener $n = 256 \log 2$, por lo que $n = 77$. El número de teclas es, pues, 1077. El número de estrellas en nuestra galaxia es de unos 1012 y el número de galaxias está a punto 108, por lo que hay alrededor de 1.020 estrellas en el universo. La masa del Sol, una típica estrella, es de 2×10^{33} gramos. El sol está compuesto principalmente de hidrógeno y el número de de átomos en un gramo de hidrógeno es de aproximadamente 6×10^{23} . Tan el número de átomos en el sol es de aproximadamente $1,2 \times 10^{57}$. Con 1020 estrellas, el número de átomos en todas las estrellas en el universo es de unos 1077. Así, el número de claves de 256 bits AES es igual al número de átomos en el conjunto universo (haciendo caso omiso de la materia oscura). Conclusión: romper AES-256 por la bruta la fuerza no es probable que suceda en el corto plazo.

11. Suponga que un mensaje se ha encriptado utilizando DES en modo de encadenamiento de bloque de texto cifrado. Un bit de texto cifrado en el bloque C_i se transforma accidentalmente de 0 a un 1 durante la transmisión. ¿Cuánto texto llano se obtendrá como resultado?

R= DES mezcla los bits bastante a fondo, por lo que un solo bit de error en el bloque C_i de bloques completos al garble P_i . Además, un poco se equivoca en el bloque 1 P_i . Sin embargo, todos los siguientes bloques de texto plano será la correcta. Un error de bit único por lo tanto sólo afecta a dos bloques de texto plano.

12. Ahora considere nuevamente el encadenamiento de bloque de texto cifrado. En lugar de que un solo bit 0 sea transformado en un bit 1, un bit 0 extra se inserta en el flujo de texto cifrado después del bloque C_i . ¿Cuánto texto llano se distorsionará como resultado?

R= Por desgracia, cada bloque de texto plano a partir de P_i será un mal ahora, ya que todas las entradas a las cajas de XOR se equivocan. Un error de encuadre es, pues, mucho más grave que un poco de arriba abajo.

13. Compare el encadenamiento de bloque cifrado con el modo de retroalimentación de cifrado en términos del número de operaciones de encriptación necesarias para transmitir un archivo grande. ¿Cuál es más eficiente y por cuánto?

R= Encadenamiento de Bloque Cifrado produce 8 bytes de la producción por el cifrado. Cifra modo de realimentación produce un byte de salida por el cifrado. Por lo tanto, cifrado en bloque encadenamiento es ocho veces más eficientes (es decir, con el mismo número de ciclos puede cifrar en ocho ocasiones como texto sin formato mucho más).

14. Utilizando el criptosistema de clave pública RSA, con $a = 1$, $b = 2$, etcétera,

(a) Si $p = 7$ y $q = 11$, liste cinco valores legales para d .

(b) Si $p = 13$, $q = 31$ y $d = 7$, encuentre e .

(c) Utilizando $p = 5$, $q = 11$ y $d = 27$, encuentre e y encripte "abcdefghij".

R= A) Para estos parámetros, $z = 60$, por lo que debe elegir d ser primos entre sí a 60. Los valores posibles son: 7, 11, 13, 17 y 19. (B) Si el correo satisface la ecuación $7e = 1 \pmod{360}$, 7 de correo debe ser 361, 721, 1081, 1441, etc. Dividiendo cada uno de éstos a su vez por 7 para ver que es divisible por 7, nos encontramos con que $721/7 = 103$, por lo tanto, $e = 103$. (C) Con estos parámetros, $e = 3$. Para cifrar P se utiliza la función $C = P^3 \pmod{55}$. Para $p = 1$ a 10, $C = 1, 8, 27, 9, 15, 51, 13, 17, 14$ y 10, respectivamente.

15. Suponga que un usuario, María, descubre que su clave privada RSA (d_1, n_1) es la misma que la clave pública RSA (e_2, n_2) de otro usuario, Frances. En otras palabras, $d_1 = e_2$ y $n_1 = n_2$. ¿María debe considerar cambiar sus claves pública y privada? Explique su respuesta.

R= María debe considerar el cambio de las llaves. Esto es debido a que es relativamente fácil para Francés de averiguar la clave privada de María de la siguiente manera. Francés sabe Clave pública de María es (e_1, n_1). Francés avisa de $n = 2n - 1$. Francés ahora puede Supongo que la clave privada de María (d_1, n_1) por simple enumeración de las diferentes soluciones de la ecuación $d_1 \times 1 = 1 \pmod{n}$.

16. Considere el uso del modo de contador, como se muestra en la figura 8-15, pero con $IV = 0$. ¿El uso de 0 amenaza la seguridad del cifrado en general?

R= No. La seguridad se basa en tener un fuerte algoritmo de cifrado y una clave de longitud. El IV no es realmente esencial. La clave es lo que importa.

17. El protocolo de firma de la figura 8-18 tiene la siguiente debilidad. Si Bob falla, podría perder el contenido de su RAM. ¿Qué problemas causa esto y qué puede hacer él para evitarlos?

R= Los RAS desde el último mensaje todavía puede estar en la RAM. Si esto se pierde, puede Trudy tratar de reproducir el mensaje más reciente a Bob, con la esperanza de que no va a ver que es un duplicado. Una solución es que Bob para escribir la evaluación del riesgo de cada mensaje entrante en el disco antes de hacer el trabajo. En este caso, el ataque de reproducción no se trabajar. Sin embargo, ahora existe el peligro de que si una petición se escribe en el disco seguido poco después por un accidente, la solicitud nunca se lleva a cabo.

18. En la figura 8-20 vimos la forma en que Alice puede enviar a Bob un mensaje firmado. Si Trudy reemplaza P , Bob puede detectarlo. Pero, ¿qué sucede si Trudy reemplaza tanto P como la firma?

R= Si Trudy reemplaza ambas partes, cuando Bob se aplica la clave pública de Alice para la firma, va a conseguir algo que no es la síntesis del mensaje del texto. Trudy se puede poner en un mensaje falso y que pueda hash, pero no puede firmar con la clave privada de Alice.

19. Las firmas digitales tienen una debilidad potencial debido a los usuarios flojos. En las transacciones de comercio electrónico podría suscribirse un contrato y el usuario podría solicitar la firma de su hash SHA-1. Si el usuario no verifica que el contrato y el hash correspondan, firmará de manera inadvertida un contrato diferente. Suponga que la mafia trata de explotar esta debilidad para ganar algo de dinero. Los mafiosos establecen un sitio Web no gratuito (por ejemplo, de pornografía, apuestas, etcétera) y piden a los nuevos clientes un número de tarjeta de crédito. Después envían al cliente un contrato en el que estipulan que éste desea utilizar su servicio y pagar con tarjeta de crédito y le pide que lo firme, a sabiendas de que la mayoría de los clientes simplemente firmarán sin verificar que el contrato y el hash correspondan. Muestre la forma en que la mafia puede comprar diamantes de un joyero legítimo de Internet y pueda cargarlos a clientes inocentes.

R= Cuando un cliente, digamos, Sam, indica que quiere comprar juegos de azar, o lo que sea, el fin de la mafia un diamante en la tarjeta de crédito de Sam de un joyero. Cuando el joyero envía un contrato que deberá firmar (probablemente incluyendo el número de tarjeta de crédito y un puesto de la mafia de taquilla como la dirección), la Mafia envía el hash del mensaje de la joyería a Sam, junto con un contrato la firma de Sam como el cliente de juego. Si Sam sólo señala a ciegas, sin darse cuenta de que el contrato y la firma no coinciden, la mafia de remitir la firma en el joyero, que luego las envía el diamante. Si Sam más tarde afirma que no ordenó un diamante, la joyería será capaz de producir un contrato firmado que muestra lo que hizo.

20. Una clase de matemáticas tiene 20 estudiantes. ¿Cuál es la probabilidad de que por lo menos dos estudiantes tengan la misma fecha de nacimiento? Suponga que nadie nació en año bisiesto, por lo que hay posibles 365 fechas de nacimiento.

R= Con 20 estudiantes, hay $(20 \times 19) / 2 = 190$ pares de estudiantes. La probabilidad que los estudiantes de cualquier par tienen el mismo cumpleaños es de $1/365$, y la probabilidad que tienen diferentes cumpleaños es $364/365$. La probabilidad de que todos 190 parejas tienen diferentes cumpleaños es, pues, $(364/365)^{190}$. Este número es de aproximadamente 0,594. Si la probabilidad de que todos los pares son desajustes es 0,594, entonces la probabilidad que uno o más pares tienen el mismo cumpleaños es de aproximadamente 0,406.

21. Después de que Ellen confiesa a Marilyn que la engañó en el asunto de Tom, Marilyn decide evitar este problema dictando el contenido de los mensajes futuros en una máquina de dictado y dárselos a su nueva secretaria para que los teclee. A continuación, Marilyn planea examinar los mensajes en su terminal después de que la secretaria los haya tecleado para asegurarse de que contengan sus palabras exactas. ¿La nueva secretaria aún puede utilizar el ataque de cumpleaños para falsificar un mensaje, y de ser así, cómo? Sugerencia: Ella puede hacerlo.

R= El secretario puede tomar un cierto número (por ejemplo, 32) espacios en la carta, y, potencialmente, sustituir a cada uno de ellos por el espacio, la tecla de retroceso, el espacio. Cuando se visualiza en el terminal, todas las variantes que se parecen, pero todo tiene un mensaje diferente digiere, por lo que el ataque del cumpleaños todavía funciona. Alternativamente, la adición de espacios en el extremo de líneas y espacios de intercambio entre las pestañas y también se puede utilizar.

22. Considere el intento fallido de Alice para obtener la clave pública de Bob en la figura 8-23. Suponga que Bob y Alice ya comparten una clave secreta, pero Alice aún quiere la clave pública de Bob. ¿Hay ahora una forma para obtenerla de manera segura? De ser así, ¿cómo?

R= Es factible. Alicia encripta un nonce con la clave compartida y la envía a Bob. Bob envía un mensaje cifrado con la clave compartida que contenga la nonce, nonce su propia, y la clave pública. Trudy no se puede forjar este mensaje, y si se envía basura al azar, cuando se descifra no contendrá Alice nonce. Para completar el protocolo, Alice envía nonce Bob cifrado con la clave pública de Bob.

23. Alice se quiere comunicar con Bob, utilizando la criptografía de clave pública. Ella establece una conexión con alguien que espera sea Bob. Le pide su clave pública y él se la envía en texto llano junto con un certificado X.509 firmado por la raíz CA. Alice ya tiene la clave pública de la raíz CA. ¿Qué pasos debe realizar Alice para verificar que está hablando con Bob? Suponga que a Bob no le importa con quién está hablando (por ejemplo, Bob es algún tipo de servicio público).

R= El paso 1 es para verificar el certificado X.509 utilizando la clave pública del CA raíz. Si es genuina, ella ahora tiene la clave pública de Bob, a pesar de que debe comprobar si la CRL hay una. Pero para ver si es Bob en el otro extremo de la conexión, se necesita saber si Bob tiene la clave privada correspondiente. Ella toma un nonce y lo envía a él con su clave pública. Si Bob puede enviar de nuevo en texto plano, está convencida de que es Bob.

24. Suponga que un sistema utiliza PKI con base en una jerarquía con estructura de árbol de CAs. Alice desea comunicarse con Bob y recibe un certificado de Bob firmado por un CA X después de establecer el canal de comunicación con Bob. Suponga que Alice nunca ha escuchado sobre X. ¿Qué pasos debe realizar Alice para verificar que está hablando con Bob?

R= En primer lugar Alicia establece un canal de comunicación con X y X para una pregunta certificado para verificar su clave pública. Supongamos que X proporciona un certificado firmado por otra Y. CA Si Alicia no sabe Y, repite el paso anterior con Y. Alice continúa haciendo esto, hasta que recibe un certificado acreditando el público clave de un Z CA firmado por A y Alice lo sabe de una clave pública. Nótese que este puede continuar hasta que se alcanza una raíz, es decir, A es la raíz. Después de esto Alicia verifica las claves públicas en orden inverso a partir de la certificación de que Z proporcionado. En cada paso durante la verificación, se comprueba también la CRL para hacer

Asegúrese de que el certificado a que no han sido revocadas. Finalmente, después de verificar Clave pública de Bob, Alice asegura que ella es de hecho de hablar con Bob utilizando el mismo método que en el problema anterior.

25. ¿Es posible utilizar en modo de transporte IPsec con AH si alguna de las máquinas está detrás de una caja NAT? Explique su respuesta.

R= N° AH en modo de transporte incluye la cabecera IP en la suma de comprobación. El NAT cambia la dirección de origen, arruinando la suma de comprobación. Todos los paquetes será percibe como errores.

26. Dé una ventaja de HMACs con respecto del uso de RSA para firmar hashes SHA-1.

R= HMAC son mucho más rápidos computacionalmente.

27. Dé una razón por la cual se configuraría un firewall para inspeccionar el tráfico entrante. Dé una razón por la cual se configuraría para inspeccionar tráfico saliente. ¿Cree que las inspecciones sean exitosas?

R= El tráfico entrante puede ser inspeccionada por la presencia de virus. Saliente el tráfico puede ser inspeccionado para ver si la información confidencial de la compañía tiene una fuga a cabo. Comprobación de los virus podría funcionar si un buen programa antivirus se utiliza. Comprobar el tráfico de salida, que puede ser encriptada, es casi imposible en contra de un serio intento de fuga de información.

28. En la figura 8-31 se muestra el formato de paquetes WEP. Suponga que la suma de verificación es de 32 bits, calculada mediante la aplicación de OR exclusivos a todas las palabras de 32 bits en la carga útil. También suponga que los problemas con RC4 se corrigen reemplazándolo con un cifrado de flujo que no tiene debilidad y que los de IV se extienden a 128 bits. ¿Hay alguna forma para que un intruso espíe o interfiera con el tráfico sin ser detectado?

R= Si Jim no quiso revelar quién se está comunicando con alguien que (Incluyendo a su propio administrador del sistema, a continuación, Jim tiene que utilizar más mecanismos de seguridad. Recuerde que la VPN proporciona seguridad para la comunicación Sólo a través de Internet (fuera de la organización). No proporciona ninguna seguridad para la comunicación dentro de la organización. Si Jim sólo quiere mantener su comunicación a salvo de personas ajenas a la empresa, es una VPN suficiente.

29. Suponga que una organización utiliza VPN para conectar de manera segura sus sitios a Internet. ¿Hay alguna necesidad de que un usuario, Jim, de esta organización utilice la encriptación o cualquier otro mecanismo de seguridad para comunicarse con otro usuario, Mary, de la organización?

R= Sí. Supongamos que Trudy XOR una palabra al azar con el inicio de la carga útil y luego XOR la misma palabra con la suma de comprobación. La suma de comprobación todavía se ser correcta. Por lo tanto, Trudy es capaz de mutilar a los mensajes y no los han ser detectado porque se puede manipular la suma de comprobación a través de la encriptación.

30. Cambie ligeramente un mensaje del protocolo de la figura 8-34 para hacerlo resistente al ataque de reflexión. Explique por qué funcionaría su modificación.

R= En el mensaje 2, puesto RB en el interior del mensaje cifrado en lugar de fuera de ella. En de esta manera, Trudy no será capaz de descubrir RB y el ataque reflexión no funciona.

31. El intercambio de claves de Diffie-Hellman se utiliza para establecer una clave secreta entre Alice y Bob. Alice envía a Bob (719, 3, 191). Bob responde con (543). El número secreto de Alice, x , es 16. ¿Cuál es la clave secreta?

R= Bob sabe que $g^x \bmod n = 191$. Se calcula $191^{15} \bmod 719 = 40$. Alicia sabe que $G^y \bmod n = 543$. Se calcula $543^{16} \bmod n = 40$. La clave es 40. La forma más sencilla de hacer los cálculos anteriores es utilizar el programa de UNIX antes de Cristo.

32. Si Alice y Bob no se conocen, no comparten secretos ni tienen certificados, de cualquier manera pueden establecer una clave secreta compartida utilizando el algoritmo de Diffie-Hellman. Explique por qué es muy difícil protegerse contra un ataque de hombre en medio.

R= No hay nada que Bob sabe que Trudy no lo sabe. Cualquier respuesta Bob puede dar, Trudy también se puede dar. Bajo estas circunstancias, es imposible para Alicia para saber si ella está hablando con Bob o de Trudy.

33. En el protocolo de la figura 8-39, ¿por qué A se envía en texto llano junto con la clave de sesión encriptada?

R= El KDC necesita alguna manera de decirle que envió el mensaje, por lo tanto, que descifrado clave para aplicar a la misma.

34. En el protocolo de la figura 8-39, señalamos que iniciar cada mensaje de texto llano con 32 bits 0 es un riesgo de seguridad. Suponga que cada mensaje comienza con un número aleatorio por usuario, efectivamente una segunda clave secreta conocida sólo por su usuario y el KDC. ¿Esto elimina el ataque de texto llano conocido? ¿Por qué?

R= No. Todos los Trudy tiene que hacer es capturar dos mensajes desde o hacia el mismo usuario. A continuación, puede tratar de descifrar tanto de las personas con la misma clave. Si el azar campo de número, tanto de ellos es el bingó mismo, tiene la clave correcta. Todo este esquema no es aumentar su carga de trabajo por un factor de dos.

35. En el protocolo Needham-Schroeder, Alice genera dos desafíos, RA y RA2 . Esto parece excesivo. ¿Uno solo no podría haber sido suficiente?

R= Los dos números aleatorios se utilizan para diferentes propósitos. RA se utiliza para convencer a Alice ella está hablando con el KDC. RA 2 se utiliza para convencer a Alice que es hablando con Bob más adelante. Ambos son necesarios.

36. Suponga que una organización utiliza Kerberos para la autenticación. En términos de seguridad y disponibilidad de servicio, ¿cuál es el efecto si AS o TGS se desactivan?

R= Si AS baja, los nuevos usuarios legítimos no podrán autenticarse, es decir, conseguir un billete de TGS. Así, no será capaz de acceder a cualquier servidor de la organización. Los usuarios que ya cuentan con un billete de TGS (que se obtiene de AS antes de caer) puede seguir teniendo acceso a los servidores hasta su TGS vida vale caduca. Si TGS va hacia abajo, sólo a aquellos usuarios que ya tener un billete de servidor (obtenido a partir de TGS antes de caer) para un servidor de S será capaz de acceder a S hasta que su vida boleto expira el servidor. En tantos casos, no se producirá violación de la seguridad.

37. En el protocolo de autenticación de clave pública de la figura 8-43, en el mensaje 7, RB se encripta con KS. ¿Esta encriptación es necesaria, o podría haber sido adecuado regresarla en texto llano? Explique su respuesta.

R= No es esencial para enviar RB encriptada. Trudy no tiene forma de saberlo, y no se utiliza de nuevo, por lo que no es realmente secreto. Por otro lado, haciendo de esta manera permite una puesta a punto de KS para estar doblemente seguro de que todo está bien antes del envío de datos. Además, ¿por qué darle información gratuita acerca de Trudy aleatoria de Bob generador de números? En general, cuanto menos, enviadas en texto plano, el mejor, y desde el costo es tan bajo aquí, Alice también podría cifrar RB.

38. Las terminales de punto de ventas que utilizan tarjetas con banda magnética y códigos PIN tienen una falla fatal: un comerciante malicioso puede modificar su lector de tarjetas para capturar y almacenar toda la información de la tarjeta, así como el código PIN a fin de realizar posteriormente transacciones adicionales (falsas). La siguiente generación de terminales de punto de ventas utilizará tarjetas con una CPU completa, teclado y una pequeña pantalla en la tarjeta. Diseñe un protocolo para este sistema que los comerciantes maliciosos no puedan romper.

R= El banco envía un desafío (un número aleatorio de largo) a la computadora del comerciante, que luego se le da a la tarjeta. La CPU de la tarjeta, entonces se transforma de un modo complejo que depende de un código PIN introducido directamente en la tarjeta. El resultado de esta transformación se da a la computadora del comerciante para la transmisión al banco. Si el comerciante llama a la orilla de nuevo para ejecutar otra transacción, el banco le enviará un nuevo reto, por lo que con pleno conocimiento del viejo no sirve para nada. Incluso si el comerciante conoce el algoritmo utilizado por las tarjetas inteligentes, que no sabe código PIN del cliente, ya que se escribe directamente en la tarjeta. La pantalla de la tarjeta es necesaria para evitar que el comerciante de muestra: "El precio de compra es 49,95", pero dice que el banco es 499,95.

39. Dé dos razones por las cuales PGP comprime mensajes.

R= La compresión ahorra ancho de banda, pero lo más importante, sino que también acaba con la frecuencia y la información en el texto original (por ejemplo, que la " e " es la más carta común en el texto de Inglés). En efecto, convierte el texto en la basura, el aumento de la cantidad de trabajo que el criptoanalista debe hacer para romper el mensaje.

40. Suponiendo que todos en Internet utilizaron PGP, ¿un mensaje PGP puede enviarse a una dirección arbitraria y decodificarse de manera correcta por todos los interesados? Explique su respuesta.

R= No. Supongamos que la dirección era una lista de correo. Cada persona tendría su o su propia clave pública. Cifrado de la clave de IDEA con una sola llave pública sería no funciona. Se tendría que ser codificado con múltiples claves públicas.

41. El ataque mostrado en la figura 8-47 omite un paso. Éste no es necesario para que el falsificador trabaje, pero incluyéndolo podría reducir la sospecha potencial después del hecho. ¿Cuál es el paso faltante?

R= En el paso 3, el ISP pide `www.trudy-la-intruder.com` y nunca se suministra. Sería mejor para suministrar la dirección IP para ser menos visible. El resultado se debe marcar como no almacenable en caché para que el truco puede ser utilizado más adelante si es necesario.

42. Se ha propuesto hacer que la falsificación DNS fracase utilizando la predicción ID haciendo que el servidor coloque un ID aleatorio en lugar de utilizar un contador. Discuta los aspectos de seguridad de este método.

R= El código de DNS es pública, por lo que el algoritmo utilizado para la generación de ID es público. Si es un generador de números aleatorios, usando identificaciones aleatorias difícilmente ayuda en absoluto. Por mediante el ataque spoofing mismo como se muestra en el texto, Trudy puede aprender el actual (al azar) de identificación. Como generadores de números aleatorios son completamente deterministas, Trudy, si conoce una identificación, se puede calcular fácilmente el siguiente. Si el número aleatorio generado por el algoritmo se XOR con el tiempo, que hace que sea menos predecible, excepto que Trudy también conoce el tiempo. XOR el número aleatorio con el tiempo y también con el número de operaciones de búsqueda del servidor ha hecho en el último minuto (Trudy algo que no sabe) y luego tomar el hash SHA-1 de este es mucho mejor. El problema aquí es que SHA-1 toma una cantidad no trivial de tiempo y el DNS tiene que ser rápido.

43. El protocolo de transporte de datos SSL involucra dos marcas aleatorias, así como una clave premaestra. ¿Cuál valor, en caso de que haya, tiene el uso de las marcas aleatorias?

R= Los nonces protegerse contra ataques de repetición. Dado que cada parte contribuye a la clave, si un intruso intenta reproducir los mensajes antiguos, la nueva clave generada no coincidir con el anterior.

44. La imagen de la figura 8-55(b) contiene el texto ASCII de cinco obras de Shakespeare. ¿Sería posible ocultar música entre las cebras en lugar de ocultar texto? De ser así, ¿cómo funcionaría y cuánto podría ocultar en esta imagen? Si no es posible, explique por qué.

R= Fácil. La música es sólo un archivo. No importa lo que está en el archivo. Hay espacio para 294,912 bytes en los bits de orden inferior. MP3 requiere aproximadamente 1 MB por minutos, por lo que alrededor de 18 segundos de la música podría encajar.

45. Alicia era usuario de un retransmisor de correo anónimo de tipo 1. Ella podía publicar muchos mensajes en su grupo de noticias favorito, `alt.fanclub.alice`, y todos sabían que tales mensajes provenían de Alice porque todos llevaban el mismo pseudónimo. Suponiendo que el retransmisor de correo funcionaba de manera correcta, Trudy no podía suplantar a Alice. Después de que los retransmisores de correo de tipo 1 desaparecieran, Alice cambió a un retransmisor cypherpunk e inició un nuevo subproceso en su grupo de noticias. Diseñe una manera para que Alice evite que Trudy la suplante y publique nuevos mensajes en el grupo de noticias.

R= Alicia pudo hash de cada mensaje y lo firme con su clave privada. Luego se podría añadir el hash firmado y su clave pública al mensaje. Personas Podríamos comparar verificar la firma y comparar la clave pública a la que se Alice usó la última vez. Si Trudy trató de hacerse pasar por Alice y se adjuntará Clave pública de Alicia, ella no sería capaz de obtener el derecho de hash. Si se utiliza su propia clave pública, la gente vería que no era la misma que la última vez.