Solución Redes de Datos
2do parcial año 2010

- Las hojas se escriben de un solo lado y preguntas separadas se responden en hojas separadas.
- Letra clara y legible. Respuesta concisa.
- Nombre, número de cédula y número de pregunta en cada hoja.
- Duración del parcial 3 horas. Puntaje total 50 puntos (50% de la suma de parciales).

Pregunta 1 (10 puntos)

a)

i) a)En las redes de datagramas es necesario que cada uno de los paquetes enviados contenga
en su totalidad la dirección de origen y de destino. Por otro lado, en redes de circuitos virtuales no hace falta lo anterior, es suficiente con que cada paquete contenga un identificador del circuito virtual, que por lo general es corto y de alcance local.

ii) Tanto en las redes de circuitos virtuales como en las redes de datagramas, es necesario entontrar un camino a través de la red para llegar desde un origen a un destino. Para eso se usa una tabla de ruteo. La diferencia entre las dos arquitecturas es que en redes de circuitos virtuales, la tabla de ruteo se consulta sólo al momento de establecer el circuito virtual, mientras que en redes de datagramas se consulta en general para cada paquete a encaminar (existen mecanismos de cache para mejorar la performance en algunos enrutadores). El mecanismo para construir la tabla de rutas (con la cual se decidirá por donde armar el circuito virtual o por donde encaminar el próximo paquete) puede ser mediante ruteo estático o utilizando protocolos de ruteo dinámico en ambos casos.

iii) En las redes de datagramas, en cada uno de los saltos, se realiza el encaminamiento de los paquetes, independientemente de los paquetes anteriores y de la ruta que éstos hubieran tomado. Cada enrutador consulta su tabla de ruteo, y a partir de la dirección destino decide el próximo salto. Por otro lado, en las redes de circuitos virtuales, el encaminamiento es mucho más sencillo, dado que cada paquete contiene un identificador del CV, los enrutadores simplemente encaminan todos los paquetes de un determinado CV, hacia el proximo salto prefijado de antemano. En estas redes, previo al encaminamiento se cambia el identificador del CV que traía el paquete por el correspondiente al siguiente salto. Esto es así ya que generalmente se trabaja con identificadores de alcance local solamente (lo que posibilita que sean cortos).
Observación: Generalmente en redes de circuitos virtuales a los equipos que realizan la tarea de buscar en sus tablas de etiquetas e intercambiar la etiqueta de entrada por la de salida, se les llama switches.

iv) El control de congestión en las redes de datagramas es una tarea difícil, dado que el transmisor de los paquetes no tiene control del camino seguido por lo paquetes, no es sencillo hacer que los mismos eviten congestiones en la red. Por el contrario, en las redes de circuitos virtuales, sí es posible implementar políticas de control de congestión. Es posible realizar reservas de capacidad en los enlaces y buffers para cada CV, suficientes en todos los enrutadores (switches) de manera de evitar las congestiones. También debe realizarse control de tráfico conforme, al menos en el acceso a la red, sobre los contratos de tráfico realizados con los clientes. De esta manera se evita el exceso de tráfico no planificado.

v) La capacidad para realizar control de congestión mencionada en el item anterior, es una de las características que entran en juego si se desea proveer calidad de servicio. Por lo mencionado anteriormente y otras características, tales como la posibilidad de implementar ingeniería de tráfco de las redes de circuitos virtuales, es que las mismas permiten proveer calidad de servicio. Por lo contrario, en las redes de datagramas ofrecer

calidad de servicio es una tarea muy costosa, a menos que se desperdicien los recursos de la red de manera considerable.

vi) Las caídas de los enrutadores representa un problema relativamente serio para las redes de circuitos virtuales, mientras que no lo es para las redes de datagramas. La caída de un enrutador no tiene impacto en una red de datagramas (siempre que existan caminos alternativos), salvo por la pérdida de los paquetes durante la caída. En las redes de caminos virtuales, además de perderse los paquetes involucrados directamente en la caída, se pierden todos los CV que por dicho enrutador pasa. Esto representa un problema bastante serio, ya que dichos CV deberán reconstruirse desde el origen nuevamente, tarea que generalmente no es sencilla.

b) En la siguiente tabla comparativa se aprecia la diferencia de ambos protocolos en los aspectos solicitados en la pregunta:

Propiedad \ Protocolo	RIP	OSPF
¿Qué información envían?	Todas los destinos que conoce (los directamente conectados y los que aprendió en intercambios anteriores) con su distancia para llegar a ellos	Las distancias a sus enrutadores vecinos
¿A quiénes la envían?	A sus vecinos. A los enrutadores que están directamente conectados con él. El envío se hace en broadcast en RIPv1 y en multicast en RIPv2	A todos los nodos de la red que hablan OSPF en un determinado sistema autónomo. El envío se realiza mediante multicast y se realiza por inundación. Hay parámetros de control (secuencia y marcas de tiempo) de la inundación
¿Cómo se comportan frente a topologías con bucles?	RIP al ser de vector distancia tiene el problema del conteo a infinito a causa que los nodos no conocen la topología de la red. En particular en topologías con bucles puede presentarse este problema que no se soluciona por el mecanismo del horizonte dividido. RIP impone una distancia máxima de 16 saltos luego de lo que asume que el destino no es alcanzable. El problema del conteo a infinito lleva entonces a que RIP tenga una convergencia lenta en el caso de caídas.	OSPF no tiene problema con las topologías con bucles ya que los nodos conocen la topología y por tanto pueden saber si hay bucles. Esto implica que la convergencia de OSPF es más rápida frente a fallas de la red, comparada con RIP

Pregunta 2 **(15 puntos)**

a)

Para realizar el control de errores y el control de flujo de bits, es necesario que las unidades de datos de la capa de enlace sean acotadas en tamaño y que se calcule la suma de comprobación de las mismas.

Para dividir entonces el flujo de datos de capa 3 en unidades de capa 2 es necesaria la división en trozos más pequeños llamados tramas o marcos, y que se calcule la suma de comprobación para cada uno de ellos.

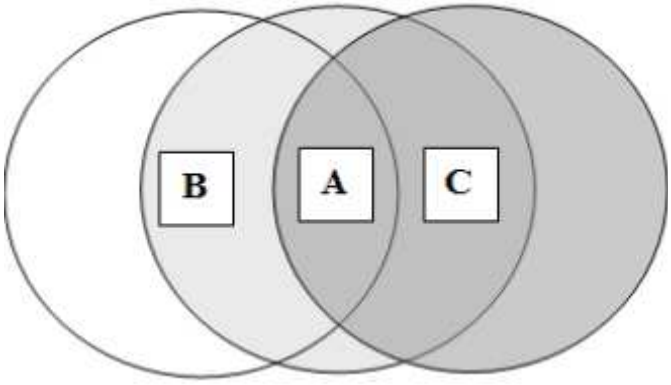
El entramado es la función que permite delimitar el comienzo y fin de estas tramas. Hay varios mecanismos para realizarlo, como ser el conteo de caracteres, las banderas de delimitación (de caracteres o de bits) y las violaciones al código de línea de la capa física.

b) i) El protocolo CSMA/CD p persistente se emplea en redes con capa de enlace ranuradas en tiempo. Cada vez que un host tiene una trama lista para enviar, este escucha el canal en caso de estar libre toma la decisión de trasmitir con probabilidad p y desiste para la siguiente ranura de tiempo con probabilidad 1-p. En caso de encontrar el medio ocupado, simplemente espera hasta la siguiente ranura de tiempo y vuelve a intentar.

ii) Las colisiones se detectan escuchando el canal, observando si la señal que un host esta imponiendo en el medio es diferente o no a lo que esta detectando del mismo. Se dice que hubo una colisión cuando difieren estas dos señales, todos los host que detectaron la colisión deben de parar lo antes posible de transmitir, esperan un tiempo aleatorio y comienzan con el mismo procedimiento para poder transmitir. Usualmente para este tiempo aleatorio se utiliza el algoritmo de exponential backoff para hacer un evento poco probable el que dos o mas estaciones vuelvan colisionar en la siguiente ranura de tiempo.

c)
i) Sean A, B y C tres estaciones inalámbricas, en donde los círculos representan las áreas de cobertura de cada una de las estaciones.
Consideremos la siguiente situación, la estación B dispone de una trama a enviar a A, esta escucha el canal lo encuentra libre y decide transmitir su trama hacia A. En un instante posterior la estación C escucha el medio, lo encuentra libre dado que C no está dentro del área de cobertura de B, por lo cual transmite con con¯anza la trama que dispone para A, produciéndoseuna colisión en la estación A.
En este tipo de redes hay que tener en cuenta que las colisiones se producen en el destino y la detección de portadora se hace en el origen. Al problema de que una estación sea incapaz de detectar una posible trama competidora en destino se llama el problema de la estación oculta.

ii: Como paliativo a este problema se implementan a nivel de capa de enlace dos tramas “cortas" de control, RTS (Request to Send) y CTS (Clear to Send). Cada estación, de acuerdo a la cantidad de datos que tenga que enviar, tiene una estimación del tiempo que va a consumir el envío de sus datos (eventualmente sus datos mas sus posibles ACK).



Utilizando el mismo ejemplo que en la parte anterior, la estación B antes de enviar la trama hacia A realiza una reserva del medio utilizando la trama RTS con destino A. Esta trama brinda información de cuanto tiempo el medio va a estar reservado para esta transmisión. La estación C no está dentro de la zona de cobertura de B, así que no se entera de esta reserva, pero A sí escucha este pedido de reserva a lo cual contesta con una trama CTS al pedido de la estación B, en la cual lleva la información de por cuanto tiempo mas queda reservado el medio para la transmisión de la trama que B dispone. Ahora C si esta en la zona de cobertura de

A, por lo cual logra escuchar la trama CTS que origina A absteniéndose se utilizar el canal por el tiempo que observo en la trama. Luego B transmite la trama hacia A .evitando la colisión.
Estos tiempos que se observan en estas tramas permiten manejar el concepto de “canal virtual". Internamente cada estación tiene un contador de tiempo, en el cual carga el valor que estimó que va a durar la comunicación (obtenido de un RTS o CTS). De no estar involucrada la estación en esa comunicación, el contador se va decrementando y hasta que este no llegue a cero no se vuelve a intentar escuchar el medio para intentar transmitir.

Pregunta 3 (10 puntos)

a) **Ventajas:**
· Baja atenuación (0.2 dB/km).
· Gran Capacidad (Actualmente equipos de 1Tbps utilizando WDM).
· Aislación ante ruido electromagnético. Esto es ventajoso en ambientes industriales y ambientes de alta seguridad.
· Permite amplificación para trasmisiones sin regeneración por varios miles de kilómetros.

Desventajas:
· Cuando se quiere instalar como solución de última milla, el costo es elevado comparado con el cobre ya instalado o soluciones inalámbricas.
· Para la operación y mantenimiento puede requerir instrumentos y capacitaciónespecializados y costosos.
· Requiere cuidados especiales cuando es doblada.

b)

I. Transmisor: 0dBm. Receptor: -25dBm.
Margen de Potencia: 25dB.
Atenuaciones: 100x0.2dB/km + 5x0.5dB=22.5dB<25dB. La comunicación es posible.

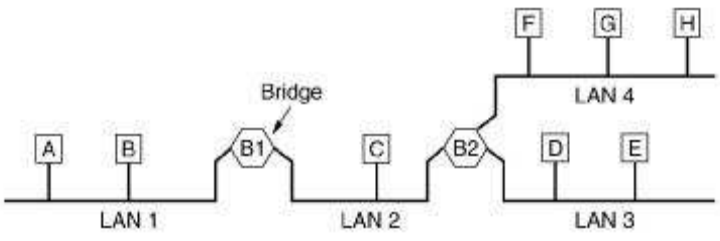
II. Ahora la atenuaciones son: 100x0.2dB/km + 5x0.5dB + 3dB=25.5dB>25dB.
La comunicación no es posible.

Pregunta 4 **(15 puntos)**

a) Los puentes son dispositivos que trabajan a nivel de capa de enlace (capa 2, sub capa MAC), entre las principales funciones que realizan podemos encontrar:
- interconectar redes de área local con diferentes capas MAC (ej redes 802.3 con redes 802.11);
- interconectar redes a más distancia de largo de cable que la permitida en la norma (a diferencia de los repetidores que amplifican la señal analógica, un bridge regenera la trama a nivel digital);
- cuando la carga de una red aumenta (hay mas equipos intentando transmitir simultáneamente)

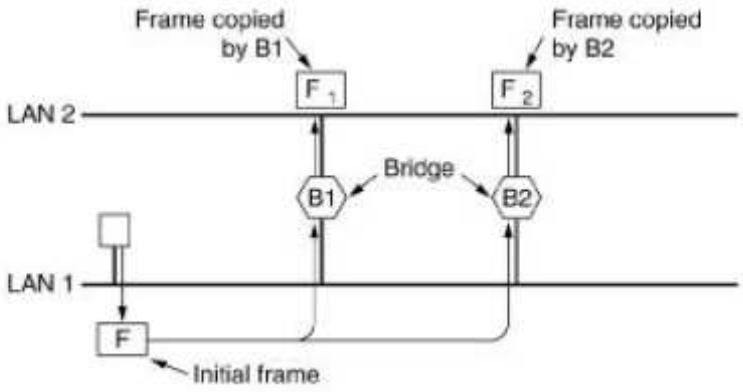
permite “segmentar” la red y separa en diferentes dominios de colisión;
- facilitan el diagnostico de fallas en los segmentos y pueden mejorar la seguridad seleccionando que tramas “forwardear” y que tramas no.

b) Los puentes transparentes normalmente funcionan sin necesidad de configuración previa, funcionan en modo promiscuo observando todas las tramas del medio compartido, de esta manera aprenden en cuál de las interfaces se encuentran los equipos en base a las direcciones MAC origen que observa en las tramas. En caso de no conocer o no tener información previa opta por hacer “flooding” o inundación, esto quiere decir que repite la trama por todas las interfaces salvo por la cual ingresó originalmente la trama.

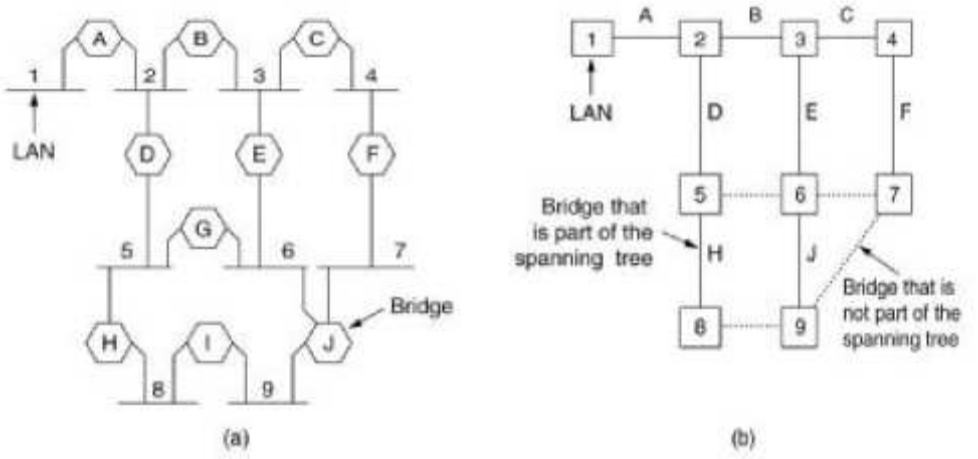


Supongamos entonces que el Host A quiere transmitir una trama con destino el Host H (más exactamente a la dirección MAC del Host H), el Host A compite por el medio y coloca la trama en la LAN 1. Como la LAN 1 es un medio compartido, el puente B1 es una estación más en este medio y por lo tanto escucha esta trama. La primera vez el punte B1 no tiene conocimiento de donde se encuentra la dirección MAC de H, por lo que este decide enviarlo por el resto de la interfaces (en este caso solamente la LAN 2). Lo que puede deducir el puente B1 es que la MAC A se encuentra en la LAN 1, el puente B1 guarda esta asociación en una tabla. Una vez que el puente B1 forwardea la trama a la LAN 2, el puente B2 la observa, como este aun no conoce donde se encuentra la MAC de H decide hacer flooding, por lo cual genera una trama en la LAN 3 y otra en la LAN 4. En este momento el puente B2 conoce que para alcanzar la MAC A tiene que utilizar la interfaz que se encuentra en la LAN 2. En el último paso le llega la trama al Host H, este contesta, cuando contesta el puente B2 aprende que para llegar a la MAC de H debe utilizar la interface de la LAN 4, como B2 ya conoce por que interfaz salir para llegar hacia la MAC de A no realiza flooding, directamente coloca la trama en la LAN 2. Esta trama es observada por el puente B1, se da cuenta que la dirección MAC de destino es la MAC de A y este conoce que “se encuentra” en la LAN 1. De esta manera el puente B1 aprende que para alcanzar la MAC de H debe utilizar la interface de la LAN 2. Por último la trama respuesta le llega al Host A.

El gran problema de los puentes transparentes es que en muchas situaciones se desea tener enlaces redundantes entre LANes (es mas correcto utilizar el termino segmentos de una red).



Dado el ejemplo de la figura tengo dos redes unidas por dos puentes, ambos puentes se acaban de prender. Cuando un Host en la LAN 1 envíe una trama F, ambos puentes la observan, al no poseer información previa optan por realizar “flooding” de la trama hacia la LAN 2 por turnos (recordar que es un medio compartido y pueden haber colisiones). Por lo cual en la LAN 2 se generan dos tramas, la F1 (forward del puente B1 de la trama F) y la F2 (forward del puente B2 de la trama F). A su vez como los puntes B1 y B2 siguen sin conocer donde se encuentra el equipo destino vuelven a forwardear las tramas F1 y F2 hacia la LAN1, generando así dos nuevas tramas, una por cada una de las anteriores, y se repite el ciclo de forma indefinida. Es evidente que esto genera funcionamientos no deseados en la red como colisiones excesivas. A este problema se lo suele llamar loops (bucles) de capa 2.
Para resolver este problema se realiza una abstracción de la topología a un grafo para luego obtener un árbol libre de loops. Primero se decide la raíz del árbol (root brdige) y luego cada uno de los restantes puentes agrega sus respectivos enlaces (como ramas) al grafo. Hasta aquí solamente se realizo la abstracción de la topología, luego para poder evitar loops, se decide en el grafo que los puentes solo tengan un camino para acceder al root bridge (Dijkstra), y los restantes caminos alternativos se deshabilitan administrativamente de forma temporal. De esta manera del grafo original se obtiene un árbol sin loops. Normalmente esta solución tiene el costo de que podemos no estar utilizando el camino mas optimo entre dos puentes (o entre dos redes). En caso de una modificación de la topología como la caída de un enlace, el mismo protocolo se encarga de detectar los cambios, propagarlos, modificar el árbol y volver a generar el árbol libre de loops. En este último caso en donde entran en juego los enlaces redundantes. Este protocolo se llama spanning-tree.



d)
i) SI es posible. Las tramas enviadas del Host A al Host C, primero son “almacenadas en el puente”, luego se observa la dirección MAC de destino, en base a esto se elije la interfaz de salida, por último las trama tiene que competir por el medio multiacceso (en nuestro caso el Hub) para poder transmitir hacia el Host C. Es en este momento en que puede colisionar con las tramas intercambiadas entre los Host B y Host D.

ii) El Host B pude llegar a conocer las direcciones MAC de todas las placas ethernet que esten en su mismo dominio de broadcast, es decir todas las direcciones MAC de los equipos que ven los pedidos de ARP. Las direcciones MAC que puede llegar a ver el Host B son:

- MAC del Host A
- MAC del Host B
- MAC del Host C
- MAC del Host D
- MAC del router If1 (interfaz 1)

La MAC del Host E y la MAC del router If2 no van a ser conocidas por el Host B, dado que en el router termina o no es forwardeado los broadcast de capa2.

iii) Los broadcast de capa 2 generados por el Host C nunca sean vistos por el Host E. Los Hosts queven el pedido ARP son:

- Host A
- Host B
- Host C
- Host D
- Mac del router If1 (aunque la letra dice Host)