24 de noviembre de 2023

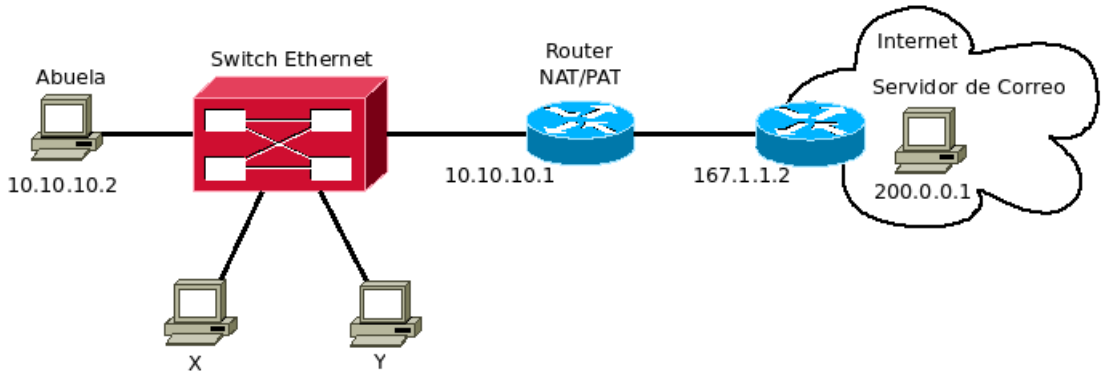
Redes de Datos 1
2do parcial – 2023
Solución

Esta es una posible solución a las preguntas planteadas. Por razones didácticas normalmente contiene bastante más información que la mínima necesaria para responder la pregunta de forma suficiente.

A pesar del esfuerzo realizado en el parcial anterior, su abuela sigue con problemas con el correo y está comenzando a dudar de la utilidad del curso de Redes 1.

Pregunta 1 (6 puntos)

La red interna de la casa de la abuela, que se esquematizó simplificadamente en el parcial 1, está en realidad implementada con un switch ethernet como se muestra en la figura.



El equipo de la abuela y el Router tienen las tablas configuradas como se indica a continuación:

Tabla de PC Abuela	
Destino	***Próximo salto***
10.10.10.0/24	*Directamente conectada*
0.0.0.0/0	*10.10.10.1*

Tabla de Router NAT/PAT	
Destino	***Próximo salto***
10.10.10.0/24	*Directamente conectada (interfaz interna)*
167.1.1.0/30	*Directamente conectada (interfaz externa)*
0.0.0.0/0	*167.1.1.2 (Router del Proveedor)*

Intentando entender el problema planteado y ahondando un poco más con su abuela, Ud. se entera que su primo gamer estuvo haciendo unas pruebas y conectó dos equipos al switch de la abuela como se representa en la figura. Los equipos X e Y se configuraron con las direcciones IP 200.0.0.1 (igual a la del servidor de correo de la abuela como se indica en la figura) y 200.0.0.2 respectivamente y al comentarle esto a su amigo, la respuesta inmediata de él es: “Ah! Claro!, encontraste el problema!”.

a) Si Ud. está de acuerdo con su amigo, explique detalladamente las decisiones y acciones que se van tomando en los equipos involucrados que justifican la veracidad de la afirmación de su amigo.

   Si Ud. no está de acuerdo con su amigo, explique detalladamente las decisiones y acciones que se van tomando en los equipos involucrados que justifican la falsedad de la afirmación de su amigo.

Nota: No es necesario explicar el funcionamiento detallado del switch (ver Pregunta 2).

La afirmación de su amigo es incorrecta.

El equipo de la abuela cuando tiene que enviar un paquete a 200.0.0.1 (servidor de correo) realiza los siguientes pasos:

i. *Consulta su tabla de forwarding utilizando el algoritmo Longest-Prefix-Match y obtiene que el próximo salto para llegar a 200.0.0.1 es la IP 10.10.10.1 del router (ruta por defecto)*
ii. *Utilizando el protocolo ARP averigua la MAC asociada a la IP 10.10.10.1 del router. Para eso envía una trama destinada a broadcast (FF:FF:FF:FF:FF:FF) conteniendo un mensaje ARP donde consulta la MAC asociada a la IP 10.10.10.1 (e incluyendo su propia asociación MAC_abuela, IP_abuela). El switch reenvía esta trama por todas las interfaces (ya que el destino es broadcast). Todos los equipos la reciben, pero solo responde el router porque es el que tiene configurada la IP buscada (10.10.10.1). La respuesta es una trama con MAC de origen la del router (MAC_R) y MAC de destino la de la PC de la abuela (MAC_abuela). Además el router guarda en su caché de ARP la correspondencia MAC_abuela, IP_abuela. El switch almacena en su tabla de macs la asociación entre la dirección MAC de origen de los mensajes y la interfaz del switch por la que ingresaron.*
iii. *Envía el paquete IP deseado usando IP de origen 10.10.10.2, IP de destino 200.0.0.1, en una trama con MAC de origen la de la interfaz ethernet del equipo de la abuela y MAC destino la del router averiguada en el paso anterior. Esa trama será por tanto recibida por el router.*

Una vez que el router recibe la trama anterior, realizará los siguientes pasos:
i. Recibirá y procesará la trama, ya que está dirigida a su dirección MAC. Enviará el contenido de la trama (el paquete IP) a su capa de red.
ii. *En capa de red, el router verá que el destino del paquete no es para él (la IP destino 200.0.0.1 no la tiene configurada en ninguna de sus interfaces), pero como es un router, su función es encaminar los paquetes hacia el destino más adecuado. Consulta por tanto su tabla de forwarding utilizando el algoritmo Longest-Prefix-Match y obtiene que el próximo salto para llegar a 200.0.0.1 es la IP 167.1.1.2 (ruta por defecto al siguiente enrutador del proveedor de servicio).*
iii. *Como cumple la función de NAT/PAT, cambiará la IP de origen del paquete por la suya pública (167.1.1.1) y el puerto de origen por uno efímero que tenga sin uso.*
iv. *Si el enlace entre los routers es ethernet, se utilizará el protocolo ARP (de forma análoga a lo explicado para la PC de la Abuela) para averiguar la MAC asociada a la IP 167.1.1.2 y se enviará el paquete. Si el enlace fuera de otra tecnología se encapsulará el paquete IP adecuadamente.*

Cuando vuelva el paquete de respuesta del servidor de correo se procederá consultando las tablas de forwarding y de NAT/PAT para enviarlo hacia el PC de la abuela. En la vuelta no es necesario enviar mensajes del protocolo ARP, ya que las correspondencias MAC,IP necesarias estarán almacenadas en el caché de ARP de los equipos.

Si bien no formaba parte de la pregunta, podemos mencionar que las máquinas X e Y pueden dialogar sin problema entre sí utilizando las direcciones 200.0.0.1 y 200.0.0.2 asignadas, pero a priori no podrán salir a internet ni comunicarse con los equipos de la red 10.10.10.0/24. Esto se debe a que tendrían que poder agregar una entrada por defecto en su tabla de forwarding hacia el router, pero el router está en una red IP diferente a la de ellos. Si se agregara una IP al router en su interfaz interna dentro del rango de direcciones utilizado por X e Y, si podría agregar una ruta por defecto hacia esa IP y podrían navegar a internet. Si se hiciera esa configuración, la comunicación del equipo de la abuela con la dirección 200.0.0.1 se perdería ya que esa IP estaría ahora directamente conectada al router y por tanto tendría una nueva entrada en su tabla de forwarding.

Pregunta 2 (9 puntos)

a) Explique cómo funcionan los switches ethernet (como el usado en la red de área local de su abuela).
En particular detalle:
i. ¿Qué función cumplen en la red?
ii. ¿Qué procesamiento realizan con los diferentes tipos de trama que pueden recibir?
iii. ¿Qué información necesitan para realizar su función? ¿cómo la obtienen? ¿cómo la usan?

La función de los switches Ethernet es interconectar múltiples interfaces Ethernet (posiblemente de distintas velocidades y medios físicos). Esta interconexión es mucho mejor que lo que podría implementarse con un repetidor de capa 1. El switch es un dispositivo de capa 2 (subcapa MAC) por lo que entiende el formato de las tramas. Un switch permite típicamente que varias parejas de equipos se comuniquen entre si simultáneamente y que lo puedan hacer a "velocidad de línea". Esto significa que en un switch con interfaces de 100Mbps, podría tener tráfico entre dos equipos A y B a 100Mbps y entre otros dos equipos C y D, también a 100 Mbps simultáneamente. Para esto la velocidad interna del backplane del switch debe tener la capacidad de manejar todas las parejas de equipos simultáneamente a la máxima velocidad de las interfaces.
Para lograr esto, la idea es enviar las tramas solamente a la interfaz donde se encuentra el equipo destino de la trama, evitando reenviar tramas innecesariamente a otros equipos conectados al switch, lo que a su vez requiere saber qué equipo está conectado a cada interfaz.

Para saber qué equipo (que dirección MAC) está conectada a cada interfaz sin necesidad de intervención administrativa para configurarlo, los switches Ethernet utilizan la función de autoaprendizaje para crear una tabla que asocia cada dirección MAC con la interfaz donde está conectada (tabla de direcciones MAC). El switch aprende estas asociaciones a partir de analizar la dirección MAC de origen de las tramas recibidas por cada interfaz. Las entradas en la tabla de macs, tienen un tiempo de vida, para que la tabla solamente mantenga los equipos activos, eliminándose de forma automática las entradas inactivas.
El procesamiento que realiza un switch cuando recibe una trama es:

i. *Verifica la suma de comprobación (opcional) y descarta la trama si no es válida.*
ii. *Si la dirección MAC de origen de la trama no está presente en la tabla, se agrega asociándola con la interfaz de ingreso y se establece un tiempo de validez.*
iii. *Si la dirección MAC de origen ya está en la tabla, se actualiza el tiempo de validez y se actualiza la interfaz si fuera necesario (el equipo podría haberse cambiado de interfaz por un administrador).*
iv. *Si la dirección MAC de destino es una dirección "unicast" (es de un equipo) y está en la tabla de macs, el switch sabe en qué interfaz está conectado el destino y envía la trama solamente por esa interfaz de salida. En caso que la interfaz de salida coincida con la de entrada, se descarta la trama.*
v. *Si la dirección MAC de destino es una dirección "unicast" (es de un equipo) y no está en la tabla de macs, el switch no sabe en qué interfaz está conectado el destino y por tanto envía la trama por todas sus interfaces excepto por la que ingresó.*
vi. *Si la dirección MAC de destino es broadcast (FF:FF:FF:FF:FF:FF) entonces la trama se reenvía por todos las interfaces del switch, excepto por la que ingresó.*
vii. *Si la dirección MAC de destino es multicast, el procedimiento puede variar entre switches, pero generalmente implica el reenvío por los todos los puertos restantes.*

Si el switch tiene la capacidad de implementar VLANs (Virtual LANs), la tabla de macs incluye el número de VLAN de cada interfaz, de modo que la difusión de tramas se limite a los puertos correspondientes a cada VLAN.

b) Explique qué se entiende por transmisión half-duplex o full-duplex particularmente en el contexto de los switches Ethernet. ¿Qué modalidad preferiría usar? Justifique su respuesta.

Un equipo tiene la posibilidad de transmisión en modalidad half-duplex cuando en un instante de tiempo puede enviar o recibir datos, pero no puede hacer ambas cosas simultáneamente. Si el equipo tiene capacidad para transmitir y recibir datos al mismo tiempo, entonces será capaz de transmitir en modalidad full-duplex.
Cuando conectamos un dispositivo a un switch, normalmente ambos dispositivos negocian la velocidad de transmisión (10Mbps, 100Mpbs, 1Gbps dependiendo de las capacidades de ambos equipos) y también negocian la capacidad de transmitir en full-duplex. Como en todas las versiones de Ethernet utilizando pares de cobre o fibra óptica como medio se dispone de un canal de transmisión y otro de recepción, negociarán la opción de full-duplex salvo que esté deshabilitada administrativamente, ya que permite una comunicación más rápida al disponer de canales independientes para recibir y enviar datos.

Pregunta 3 (9 puntos)

Durante el proceso de diagnóstico, Ud. también se preguntó: ¿Podrá haber algún error no detectado por los mecanismos de control de error de capa 2?

a) ¿Por qué es necesario implementar mecanismos de control de errores en capa 2?

T*odos los medios físicos introducen errores. La capa 2 es la primera capa en donde se hace un procesamiento de la información. Por este motivo es importante realizar el tratamiento de errores en esta capa para evitar enviar información ininteligible, corrupta o equivocada a capas superiores.*

b) ¿Qué diferencia hay entre detección de errores y corrección de errores? ¿En qué casos o contextos se preferiría usar uno u otro mecanismo?

La detección de errores consiste en identificar que existen errores en la tramas recibidas. En la corrección de errores, además de detectarlos, también se deben corregir (invertir los bits erróneos) para obtener las tramas originales.
La corrección de errores es más costosa que la detección de errores, por ende se intenta evitar pagar el precio de ella. En los casos donde las retransmisiones son muy costosas (por ejemplo medios con altos retardos o con tasas de errores elevadas), puede ser preferible utilizar corrección de errores ya que volver a enviar la trama no es la mejor opción. Además, en el caso donde las retransmisiones no son posibles (como el almacenamiento de datos en discos o CDs), se utiliza corrección de errores. En los casos donde

los errores no son frecuentes o los tiempos de retransmisión son bajos, suele alcanzar con la detección de errores y una retransmisión de aquellas tramas en las que se detectaron errores.

c) Explique detalladamente el mecanismo de control de errores conocido como códigos polinómicos o códigos de redundancia cíclica (CRC). En particular detalle:

i. Según los tipos indicados en la parte b) ¿Qué tipo de mecanismo se trata?

El mecanismo de CRC es para la detección de errores.

ii. ¿Cómo se representan los mensajes?

Para estudiar los códigos polinómicos se trata a las cadenas de bits como los coeficientes de polinomios cuyos coeficientes serán 0 o 1. A una trama de m bits se le asocia un polinomio M(x) de grado m-1 con términos que van desde x_{m-1} hasta x_0 donde el coeficiente del término x^t corresponde con el bit t de la cadena. Por ejemplo 1101 corresponde al polinomio x^3+x^2+1.

iii. ¿Qué información y con qué características deben compartir el transmisor y el receptor?
Para utilizar este método el transmisor y receptor deben ponerse de acuerdo en un polinomio generador G(x) de grado r. Dicho polinomio deberá cumplir algunas condiciones, que pueden ver en las diapositivas del teórico o en los libros recomendados para el curso.

iv. ¿Cómo se construyen los mensajes en el transmisor?

La idea es que el transmisor agregue bits de redundancia a los datos que desea transmitir de modo que el polinomio asociado a esa secuencia de bits sea divisible por G(x).
Supongamos que la trama a transmitir se asocia con el polinomio M(x) como se indicó anteriormente. El procedimiento en el transmisor es el siguiente:
• Sea r el grado de G(x). Se anexan r bits en "0" al final de la trama, con lo que se obtendrá una secuencia de m+r bits que corresponderá por tanto al polinomio: $x^rM(x)$.
• Se divide ese polinomio $x^rM(x)$ entre G(x), utilizando división módulo 2 (sumas y restas son XOR sin acarreo) y se obtiene un cociente Q(x) y un resto R(x) por lo que se puede escribir que:
$x^rM(x) = G(x)*Q(x)+R(x)$.
• Se resta el residuo (que tiene r o menos bits) a la cadena de bits correspondiente a $x^rM(x)$, utilizando resta módulo 2. Esto último es equivalente a poner los r bits del resto al final del mensaje de m bits (sustituyendo los bits en "cero" que habíamos agregado).
$T(x) = x^rM(x)-R(x) = G(x)*Q(x)$ por lo que el polinomio T(x) obviamente será divisible entre G(x) y sus coeficientes serán los bits de la trama que será enviada por el canal.
Observar que la resta o suma módulo 2 son equivalentes a XOR, por lo que sumar o restar es equivalente y además como $x^rM(x)$ tiene los r términos de menor grado en 0 y el residuo tiene grado r o menor, la resta (suma) indicada, no es más que una concatenación de M(x) con el residuo. Esto facilita la implementación en hardware del método.

v. ¿Cómo se procesan los mensajes en el receptor y cómo se controlan los errores?

En el receptor se recibirá una secuencia de bits que corresponderá a un polinomio Q(x)=T(x)+E(x), representando E(x) el patrón de errores ocurrido en el canal y en el que serán 1 los bits alterados.
El receptor divide Q(x) entre G(x) y se toma el resto. Como T(x) es divisible por G(x), el resto obtenido será simplemente el resto correspondiente a dividir E(x) entre G(x). Por lo tanto, si la división tiene un resto diferente a cero se habrá detectado la existencia de error(es) en el canal.

vi. ¿En qué casos los errores pueden pasar inadvertidos por el mecanismo?

El resto de la división puede ser 0 concluyéndose que no hay errores si efectivamente no los hubo (E(x) es nulo) o si los hubo de tal forma que el E(x) resultó divisible entre G(x).
De modo que para que estos casos sean los mínimos, se trata de elegir G(x) de modo que no divida a los patrones de error más frecuentes en los canales.

Pregunta 4 (10 puntos)

Durante el proceso de diagnóstico, Ud. también consideró la alternativa que se tratara de un problema en el control de acceso al medio.

a) ¿Por qué en los medios compartidos se necesitan tecnologías de control de acceso? Describa brevemente cómo pueden clasificarse (taxonomía) los diferentes métodos para resolver el control de acceso.

En los medios compartidos, por definición, varios equipos pueden acceder al medio (capa física) al mismo tiempo. Surge la necesidad de repartir la utilización del medio de forma de tener garantías que las tramas puede ser transmitidas y recibidas de una forma eficiente y equitativa. Llamamos control de acceso al medio al mecanismo de cómo asignar el medio físico brindando turnos o instancias de transmisión a las diferentes estaciones que comparten el medio.

Uno de los objetivos de la gestión del acceso al medio es evitar que dos o más estaciones transmitan al mismo tiempo, interfiriéndose las señales electromagnéticas (colisionando) y determinando que el resto de las estaciones no puedan interpretar la información correctamente. Pero no siempre es posible evitar que dos estaciones intenten transmitir al mismo tiempo y se corrompa la información.

Podemos clasificar las diferentes estrategias de acceso al medio en tres grandes grupos de acuerdo con el principio de como se distribuye el medio: acceso fíjo o canal ranurado, acceso aleatorio y acceso por turnos (asignación, suscripción, etc).

***Acceso fijo:** El canal de transmisión se divide en sub-canales y a cada estación en el medio compartido se le asigna un conjunto de sub-canales para su utilización exclusiva. Ejemplos de implementación son TDMA y FDMA. Ofrece garantías de que no habrá colisiones, pero suele ser poco eficiente en la utilización de recursos, ya que si una estación no requiere transmitir, ninguna otra estación podrá utilizar los recursos asignados.*

***Acceso aleatorio:** El canal de transmisión no se divide, cualquier estación puede transmitir en cualquier momento, dando lugar a que ocurran colisiones. Se requieren métodos para detectar las colisiones y resolver que no vuelvan a colisionar en las sucesivas retransmisiones, así como medidas para disminuir la probabilidad de colisión (como CSMA, etc). Es el extremo opuesto de asignación fija, si una estación no transmite, otra puede utilizar el canal para transmitir. La desventaja es que no vamos a poder evitar que dos estaciones deseen transmitir al mismo tiempo y por ende se debe lidiar con las colisiones.*

***Acceso por turnos:** Se le asignan turnos a las diferentes estaciones para poder transmitir. La asignación de turnos o oportunidades a transmitir se puede realizar de varias maneras, por ejemplo:*
- *compartir un token o derecho de transmisión, si no necesito transmitir, le entrego el token a la siguiente estación de una lista circular.*
- *asignación de recursos (turnos) de acuerdo a la cantidad de información a enviar, como es el caso de una radio base celular cuando transmite a los móviles.*

Es un punto medio entre los extremos, "disminuye las oportunidades de colisiones" evitando que se realicen asignaciones estáticas de recursos que llevan a una utilización pobre del medio compartido.

b) Explique qué se entiende por "colisión" en las tecnologías de acceso al medio y cómo se pueden detectar.

Una colisión es cuando dos o más estaciones coinciden transmitiendo al mismo tiempo en el medio compartido, generando en el receptor una interferencia de las ondas electromagnéticas de las señales generadas por cada estación (que efectivamente transmitió). Esta superposición de señales en la estación receptora hace que no le sea posible distinguir en la señal recibida un mensaje válido. De acuerdo a la taxonomía de la parte a), las colisiones son relevantes en los protocolos con acceso aleatorio al medio.

En el caso del transmisor, la detección de colisiones se basa en la capacidad de poder "escuchar" el medio compartido y confirmar que no recibimos una señal que difiera de lo que estamos transmitiendo. En el caso de las estaciones que reciben la señal la detección se da ya sea porque observamos violaciones al código de línea correspondiente, o porque el chequeo de errores nos indica que la trama no es válida. En la práctica la estrategia final depende de cual sea el medio compartido y si soy una de las estaciones que participó en la colisión u otra de las estaciones.

Por ejemplo, en Aloha, la estación terrena finaliza en envío de la trama, unos instantes más tarde observa si la estación repetidora transmite su trama. En CSMA/CD es posible conocer si hubo o no colisión antes de finalizar el envío de la trama, para ello se suelen utilizar estrategias de codificación de canal que le agrega una propiedad a la transmisión, si se detecta una violación a la codificación se asume colisión. También disponemos de un código de detección de errores (por ejemplo CRC) el cual en última instancia nos permite detectar una colisión, aunque hay otras causas que también pueden generar errores en el CRC. En redes WiFi, disponemos de mensajes de control agregados que permiten el reconocimiento (ACK) de las tramas.

c) En las redes cableadas que utilizan el protocolo CSMA/CD persistente 1, como 802.3 o ethernet:

1. ¿qué significa que sean CSMA? ¿cómo se comporta un transmisor que tiene una trama para enviar si el canal se encuentra ocupado? ¿y si está libre?

2. ¿Cómo se comporta si mientras está transmitiendo hay una colisión? ¿Qué diferencia hay con el caso en que se utiliza CSMA (sin CD)?

1. *La sigla CSMA significa Carrier Sense Multiple Access (Acceso Multiple con detección de portadora), es una estrategia que se utiliza en la capa MAC en la cual antes de transmitir una trama, se verifica si hay otra estación transmitiendo en el medio compartido utilizando la detección de una portadora (señal de otra estación).*
   Portadora: Las señales digitales (los 0 y 1) se codifican en señales electromagnéticas analógicas que cumplen con determinadas características, por ejemplo, que siempre exista una transición de nivel alto a nivel bajo y el nivel de continua del medio. A estas características son las que llamamos portadora.
   En CSMA si un estación desea transmitir lo primero que hace es sensar el canal,
   - *si el canal está ocupado (portadora) no transmite (de lo contrario generaría una colisión). En el caso de 1-persistente, el transmisor se queda escuchando el canal (la portadora) hasta que se libere (se haya terminado la trama anterior). En cuanto se libere (deje de detectar la portadora) comienza a transmitir.*
   - *si el canal está libre comienza a transmitir.*

   Observar que CSMA hace referencia a la acción de sensar el canal antes de transmitir, pero no se hace referencia a la detección de colisiones.
2. *CSMA/CD. La sigla CD significa collision detection o detección de colisiones. Debemos escuchar el canal mientras estamos transmitiendo de forma de confirmar que lo que estamos viendo en el canal es lo mismo que estamos transmitiendo. En caso de no ser así, implica una colisión y la transmisión se finaliza cuanto antes (para liberar el canal).*

La mayor diferencia entre CSMA/CD y CSMA es que en el primer caso, en cuanto detectamos una colisión (no coincide lo que se lee del canal con lo que se está enviando), se finaliza la transmisión. En CSMA no vamos a detectar una colisión. Si pensamos que una trama puede tener 1500 bytes y el tamaño mínimo de trama es de 64 bytes. CSMA/CD se entera si hubo una colisión antes de finalizar los primeros 64 bytes de la trama. En CSMA, las estaciones "receptoras" (todas aquellas diferentes a las que estaban transmitiendo) primero leen una trama de hasta 1500 bytes, para luego verificar el CRC y confirmar que hubieron errores. CSMA/CD entonces optimiza el tiempo de uso de canal, finalizando el uso del canal lo antes posible.
En CSMA las estaciones que transmiten finalizan de transmitir la trama sin saber si efectivamente hubo colisión (no pueden transmitir y escuchar al mismo tiempo), se requiere un mecanismo adicional que detecte este escenario y retransmita la trama. Podemos delegar la responsabilidad a las capas superiores, por ejemplo capa de transporte, otra alternativa es implementar un protocolo en capa de enlace que permita enviar ACK (como es el caso de WiFi).

***Nota:** Formalmente lo que se escucha del canal es que no ocurran violaciones de código de línea, no necesariamente leer la misma trama que se envía, requiere que la estación pueda transmitir y escuchar el medio al mismo tiempo, algo que suele ser costoso de implementar en redes inalámbricas.*

d) En las redes inalámbricas se utiliza un protocolo diferente, CSMA/CA. ¿Por qué no se usa CSMA/CD? Justifique su respuesta.

CSMA/CD se basa en la premisa que lo que transmite una estación debe llegarle al resto de las estaciones del medio compartido, con niveles de señal equivalentes, y que que es posible transmitir y escuchar al medio al mismo tiempo. Por la naturaleza de los medios inalámbricos, resulta difícil recibir la transmisión de todas las otras estaciones y fabricar un radio económico que pueda "escuchar" cuando se transmite. Las señales puede estar atenuadas porque estamos lejos (mayor atenuación en el aire), las colisiones pueden llegar con niveles de señal atenuados y no ser perceptibles.
Al comenzar a transmitir interesa que se pueda sensar el medio y confirmar que nadie más está transmitiendo, pero una vez que se está transmitiendo, las colisiones nos interesan cuando ocurren cerca del destinatario de la trama y no cerca de la estación que transmite. El problema de la estación oculta ejemplifica muy bien el escenario descripto.

El problema de la estación oculta es cuando teniendo tres o más estaciones (A,B,C, …), A-B están en zona de cobertura (si A transmite la señal alcanza a B, si B transmite la señal alcanza a A), B-C están en zona de cobertura (si C transmite la señal alcanza a B, si B transmite la señal alcanza a C), pero A y C no se ven entre sí. Cuando A y C desean transmitir, sensan el medio y no detectan portadora (A y C no están a distancia de alcance), A comienza a transmitir y C también comienza a transmitir, ninguno detectaría

colisión, pero si nos concentramos en lo que recibe B, este recibe la suma de ambas señales, por lo que ocurre una colisión en B.

Por este motivo se cambia la estrategia /CD por otra que busca evitar las colisiones utilizando la funcionalidad llamada CA Collision Avoidance o evitar las colisiones, donde lo que se intenta es poder evitar las colisiones de tramas largas, reservando el medio por determinado tiempo. Para esto se utilizan dos mensajes, RTS (Request to send) y CTS (Clear to send). Esto no evita las colisiones en los mensajes RTS y CTS, pero si se logra finalizar la reserva hay "garantías" de que no habrá colisiones.
El uso de reserva del medio mediante RTS/CTS es opcional, CSMA/CA implementa también ACK en capa de enlace, habíamos mencionado que el emisor no detecta las colisiones, por ello depende de los reconocimientos de capa de enlace para saber si debe retransmitir. La otras estaciones dependerán del CRC para descartar una trama inútil.

CA proporciona grandes mejoras pero no resuelve todos los problemas, en la práctica no se evitan las colisiones sino que se disminuye la probabilidad de que ocurran colisiones. En un medio inalámbrico las estaciones puede moverse, una estación puede pasar a zona de cobertura de otra, pueden aparecer estaciones nuevas (algo usual en un WiFi abierto), la interferencia de las señales cambia porque hay objetos moviéndose, etc. Si bien el tiempo de transmisión de una trama es chico del orden de milésimas de segundo (asumiendo 10 Mbps y trama de 1500 bytes), las condiciones puede cambiar y ocurrir colisiones aun habiendo reservado el canal.

Pregunta 5 (8 puntos)

Cuando ya las ideas de cómo resolver el problema de la abuela escaseaban, Ud. se pregunta si habrán *hackeado* a su abuela!!

a) Explique los siguientes objetivos de la seguridad: secreto, autenticación, integridad y no repudio.

Secreto: Busca que la información transmitida sea incomprensible para cualquier persona no autorizada. Se logra mediante el uso de técnicas como la criptografía, donde se emplean algoritmos para cifrar y descifrar la información con claves, de forma que solo quien(es) posea(n) la clave adecuada pueda obtener el mensaje en texto plano.

Autenticación: Tiene como objetivo verificar la identidad de uno o más de los participantes en una comunicación. Asegura que los mensajes provengan realmente de quien afirman ser y no de un impostor.

Integridad: El control de integridad permite verificar si la información recibida no ha sido modificada ni alterada durante su envío.

No repudio: Busca impedir que una de las partes niegue su participación en una comunicación o en una transacción. Permiten que un tercero (por ejemplo un juez) pueda realizar la verificación. Por ejemplo pueden utilizarse firmas digitales.

b) Describa los principios de funcionamiento de un algoritmo de clave asimétrica o clave pública.

En los algoritmos de clave asimétrica se utilizan dos algoritmos, uno para cifrar y otro para descifrar, y un par de claves distintas, una pública y una privada. Los algoritmos de cifrado y descifrado son inversos cuando se utilizan las claves correspondientes de un mismo par. La clave pública se puede compartir abiertamente, mientras que la clave privada debe mantenerse en secreto. Es computacionalmente inviable encontrar la clave privada a partir de la clave pública, así como descifrar mensajes que hayan sido cifrados con la clave pública sin disponer de la clave privada (tampoco es viable generar mensajes cifrados que se descifren correctamente con la clave pública, sin poseer la clave privada correspondiente). Por lo tanto al cifrar algo con la clave pública de un par sabemos que solo quien disponga de la clave privada correspondiente podrá descifrarlo. De la misma manera, un mensaje que se descifra correctamente con la clave pública sabemos que fue generado utilizando la clave privada correspondiente.

c) Explique cómo se puede cumplir con el objetivo de secreto utilizando un algoritmo de clave asimétrica. Indique qué clave debe utilizar el emisor y cuál el receptor. Explique por qué con este procedimiento se obtiene el secreto.

El emisor utiliza la clave pública del receptor para cifrar el mensaje. Solo el receptor, que es el único poseedor de la clave privada correspondiente, puede descifrar el mensaje. De esta manera, el emisor

asegura que solo el receptor pueda acceder al contenido del mensaje, ya que solo él tiene la clave privada necesaria para descifrarlo.

Esta técnica proporciona secreto porque el mensaje cifrado con la clave pública solo puede ser descifrado por el receptor que posee la clave privada asociada. Ninguna otra persona, incluso si tiene acceso a la clave pública, puede descifrar el mensaje sin la clave privada correspondiente, garantizando así la confidencialidad de la comunicación.

FIN

Después de todo el análisis y las verificaciones realizadas por Ud. en base a los conocimientos adquiridos en el curso y considerando las consultas a sus "asesores", finalmente el problema fue resuelto por su hermanito menor!!
Carlitos descubrió que el teclado de la abuela tenía la tecla "}" rota, carácter que su abuela había incluido en su contraseña de correo, haciendo caso a sus recomendaciones sobre la fortaleza de las contraseñas.
Para salir en su defensa …. digamos que era difícil de diagnosticar ese problema desde Italia!!