Tema 2. Técnica de acceso y control de enlace

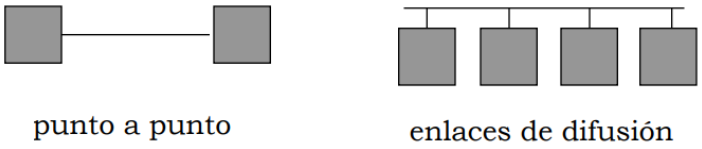
CARACTERIZACIÓN Y SERVICIOS A NIVEL DE ENLACE

OBJETIVO BÁSICO:

Transferir los datos de la capa de red de un equipo a la capa de red de otro equipo con el que tiene conexión directa.

SERVICIOS QUE OFRECE:

Acceso al medio: En enlaces de punto a punto: Se debe garantizar el envío de bits de un extremo a otro. Enlaces de difusión: Además, hay que controlar el acceso al medio compartido.



punto a punto

enlaces de difusión

Control de flujo: Se usa para evitar que el emisor envíe más datos al receptor de los que este es capaz de almacenar para su posterior tratamiento. Técnicas: Buffers, confirmaciones positivas. Protocolos: Parada y espera, Go Back-N, etc.

Control errores: Debes ser capaz de detectar tramas incorrectas. Debes ser capaz de corregir esas tramas o definir estrategias a seguir cuando se detecten errores. Técnicas detectoras: Bits paridad, CRC. Técnicas de corrección: Códigos de Hamming, confirmaciones positivas o negativas.

PROTOCOLOS BÁSICOS:

Parada y espera:

Funcionamiento: 1º Se transmite un segmento, 2º El receptor envía una confirmación, 3º El emisor no envía el siguiente segmento hasta que recibe la confirmación.

Eficiencia: Medida que indica la proporción de tiempo necesario para enviar información útil al respecto al total requerido. Lo ideal es una eficiencia de 1.

Problemas: Perdida de trama o confirmación.

Temporizadores: Se activa cuando el emisor envía una trama.

Numeración de tramas: Usa 1 bit (0 o 1) para evitar aceptación de la misma trama varias veces. La confirmación se enumera indicando la siguiente trama que espera recibir.

Ventajas: Simple de interpretar. Eficiente para mensajes de gran tamaño.

Inconvenientes: Ineficientes si usan mensajes pequeños. No siempre los mensajes pueden ser de gran tamaño.

Conceptos ventana:

Emisor: Una ventana es el conjunto de paquetes que se pueden enviar sin esperar confirmación.

Receptor: Una ventana es el conjunto de paquetes que debe estar preparado para recibir en cualquier momento.

Go Back-N:

Características: Permite al emisor tener múltiples paquetes sin confirmar, sin que el receptor tenga que almacenar los paquetes en buffer. El receptor almacena solo el paquete que espera recibir n. El receptor solo contesta si recibe la trama indicada en su ventana. En otro caso, no responde nada. La recepción de un ACK con numeración X permite al receptor confirmar todas las tramas pendientes LX. Uso de temporizadores en el emisor. Cuando se cumple se reenvían todas las pendientes de confirmación. Más eficientes que parada y espera. Menos eficiente que recepción selectiva.

Protocolo de Repetición Selectiva (SRP):

Más eficiente que parada y espera y que el Go-Back-N. Solo se transmiten tramas no confirmadas (pueden llegar tramas fuera de orden). El emisor necesita un buffer para almacenar las tramas no confirmadas (máximo ventana de envío 2^m-1). Reenviar tramas por orden del receptor o por expiración del temporizador. En el receptor es necesario un buffer para almacenar las tramas que llegan fuera de orden (máximo ventana de envío 2^m-1). Si recibe una trama fuera de orden, envía una petición de repetición (NAK, confirmación negativa) con la que esperaba recibir. Confirmación acumulada.

DETECCIÓN Y CORRECCIÓN DE ERRORES:

Detección de errores:

Se usan técnicas de redundancia, como bits adicionales en las tramas para detectar errores. Existen dos tipos de código, detectores (bits de paridad, checksums, CRCs,etc.) y correctores (códigos haming).

Bits de paridad:

Se añade un bit de paridad al final del bloque de datos. Hay dos tipos de paridad, par (número total de unos ha de ser par) e impar (número total de unos ha de ser impar).

Comprobación de paridad:

Detecta errores de un bit o de un numero impar de ellos, no detecta los errores de pares de bits.

Sumas de comprobación (checksum):

Técnica general de detección de errores. Se suele aplicar cuando se reciben bloques de caracteres, en lugar de caracteres aislados, en la emisión y recepción (se suma cada carácter al checksum), al final de la emisión se envía el checksum al receptor y este lo comprueba con el suyo, se suele usar mas en la capa de transporte.

Códigos redundantes cíclicos:

Se conocen como CRC, su fundamento se basa en enviar k bits de info + r bits redundantes, la trama de k+r bits ha de ser divisible por un numero predeterminado, si en el receptor la división tiene de resto 0, se asume que no se ha producido ningún error. Los códigos de CRC son particularmente interesantes porque su computación se puede realizar en hardware fácilmente.

PROTOCOLOS DE ACCESO MÚLTIPLE:

En las redes de área local no se suelen usar enlaces de punto, pero si los de acceso múltiple o difusión. Ejemplos: Cable coaxial (Ethernet). Excepción: Redes token ring.

ASPECTOS A CONSIDERAR:

Pueden existir colisiones, estas colisiones se producen cuando dos tramas se transmiten simultáneamente, las colisiones son detectables (directa o indirectamente), una trama de colisiona debe de retransmitida.

Detección de portada sirve para saber si el canal esta en uso o no antes de que las estaciones envíen su mensaje. Si no se usa la detección, las emisoras transmiten libremente y después comprueban si la transmisión tuvo éxito.

CONTROL DE ACCESO AL MEDIO:

El control de los accesos a un medio compartido lo lleva a cabo un protocolo MAC (Medium Access Control). Existen dos tipos de controles, el centralizado y el distribuido. Si es un control centralizado tendremos un mayor control de los accesos, tiene una lógica de acceso relativamente sencilla y evita problemas de coordinación distribuidos. Inconvenientes: poca tolerancia de fallos, cuellos de botella.

ASIGNACIÓN DEL ENLACE:

Hay dos formas de asignar el enlace, el Estático (se dedica una capacidad dada a cada conexión, valido en conmutación de circuitos, TDM y FDM, No óptimo para LANs) y la otra es Dinámica (responde a solicitudes inmediatas).

Tres categorías de asignación dinámica: Round Robin, Reserva y competición.

Round Robin:

Cada estación tiene una oportunidad para transmitir, que puede ser utilizada o no, en cualquier caso, el turno pasará a la siguiente estación. El control puede ser centralizado o distribuido (centralizado es el sondeo y distribuido es paso de testigo). Es un método adecuado cuando varias estaciones tienen que transmitir datos durante largos periodos de tiempo.

Reserva:

El tiempo se divide en intervalos de tiempo discretos (TDM). Cuando una estación requiere transmitir reserva intervalos de tiempo para un largo periodo. Técnica válida para tráfico continuo.

Competición:

Todas las estaciones compiten por acceder al medio. Son técnicas de naturaleza distribuida. Técnica valida para trafico a ráfagas. Tienden a deteriorar las presentaciones en condiciones de alta carga.

REDES DE ACCESO MÚLTIPLE CON DETECCIÓN DE PORTADORA (ETHERNET):

PROTOCOLO ALOHA**:**

Red de comunicación de conmutación de paquetes mediante la difusión por radio construida en la universidad de Hawai al principio de los 70. Pero es aplicable a cualquier sistema en el que un conjunto de estaciones compite por un único canal compartido.

El protocolo Aloha es un protocolo MAC.

La idea básica es que las estaciones transmitan paquetes de longitud fija cuando tienen datos que enviar. Teniendo en cuenta que no existe la detección de portada, los paquetes pueden colisionar.

El nodo central confirma con ACK, esto significa que si el emisor no recibe el ACK tras un timeout supone que su paquete colisiono y lo reenviará tras un retraso aleatorio.

Sin embargo, poco eficiente 18%, pero su variante Aloha Slotted llega al 37%, la baja eficiencia es debida a que no usa la detección de portada.

PROTOCOLOS BASADOS EN CSMA:

CSMA, se basa en que las estaciones escuchan para detectar si hay alguien retransmitiendo. Existen diversas variantes CSMA 1-persistente, CSMA no persistente, CSMA p-persistente y CSMA- CD.

CSMA 1-PERSISTENTE:

Cuando se va a transmitir, si el canal está ocupado la estación espera hasta que este libre, si el canal esta libre transmite. Si detecta colisión, la estación espera un tiempo aleatorio y empieza de nuevo.

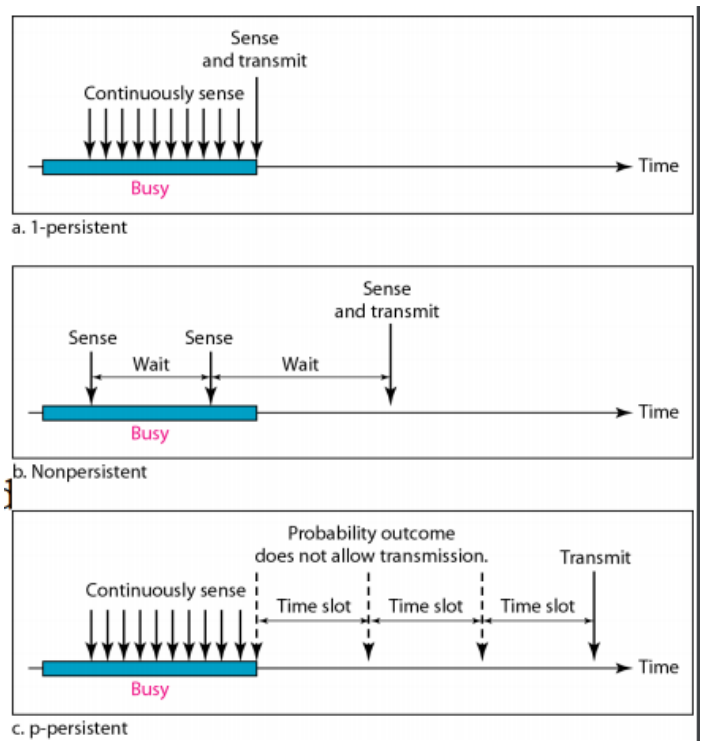
Si detecta colisión la estación espera un tiempo aleatorio y empieza de nuevo.

CSMA NO PERSISTENTE:

A diferencia del anterior, cuando se va a transmitir, si el canal está ocupado la estación espera un tiempo aleatorio antes de volver a detectar si esta libre. Intenta evitar que, si una estación transmite y dos o mas esperan, estas empiecen a transmitir justo a la vez.

CSMA P-PERSISTENTE:

Se usa cuando el tiempo se divide en intervalos (slots). Cuando se va a transmitir, si el canal esta libre, se transmite con una probabilidad p y se espera al siguiente intervalo con una probabilidad q=(1-p).



CSMA- CD:

Se basa en que las estaciones abortan la transmisión tan pronto como detecta una colisión, en los protocolos anteriores las tramas se transmiten enteras. Para que funcione, si se quiere transmitir y el canal esta libre se transmite, pero si está ocupado se espera hasta que este libre. Si se detecta colisión se transmite una señal corta de interferencia para informar al resto de estaciones y se espera un tiempo aleatorio antes de empezar de nuevo.

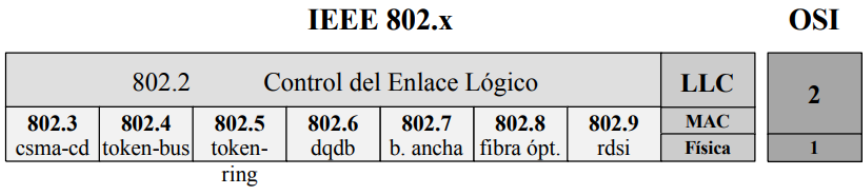
CSMA- CD: Algoritmo de retroceso exponencial binario (backoff)

Se utiliza para definir las esperas en caso de colisión. Si el paquete ha colisionado n<16 veces seguidas, el nodo selecciona un numero aleatorio k con igual probabilidad del conjunto {0,1,2,…, 2^m-1}, donde m:=min[10,n]. El nodo espera 512*k tiempo de bit (a 10Mbps, 1 tiempo de bit es 10^-7 segundos). Si n=16, se abandona la transmisión.

Si hay pocas colisiones, la espera es pequeña. Si hay muchas colisiones, espera razonable que crece poco a poco. Si el tiempo de espera fuera fijo y muy grande, pocas colisiones, pero las que hay introducen mucho retraso. Si el tiempo de espera fuera fijo y pequeño.

Las consecuencias son que las tramas deben ser suficientemente largas para que se detecte una colisión antes de que finalice la transmisión. En caso contrario, las presentaciones son las mismas que CSMA.

REDES DE ÁREA LOCAL IEEE 802:



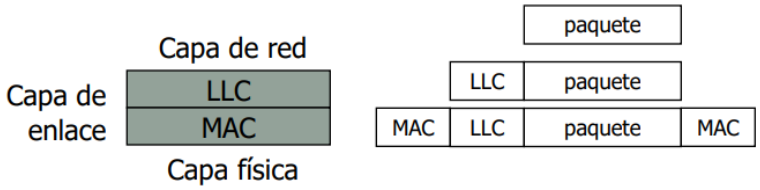
MAC = Control de Acceso Medio.

LLC = Control del Enlace Lógico.

En el estándar IEEE 802: El protocolo MAC regula el acceso al canal dando a cada nodo la posibilidad de transmitir sus paquetes. El protocolo LLC proporciona los servicios de transmisión de paquetes entre nodos, el mismo LLC puede residir sobre distintos protocolos MAC. Las LANs especificadas por el estándar IEEE 802 son compatible en los niveles superiores a LLC. Se diferencian en la capa física y en el protocolo MAC.

En general, las redes LAN y MAN ofrece un servicio de datagrama de tipo best-effort, no hay garantías de que la comunicación sea fiable.

La capa LLC ofrece una interfaz entre la capa de red y la capa MAC.

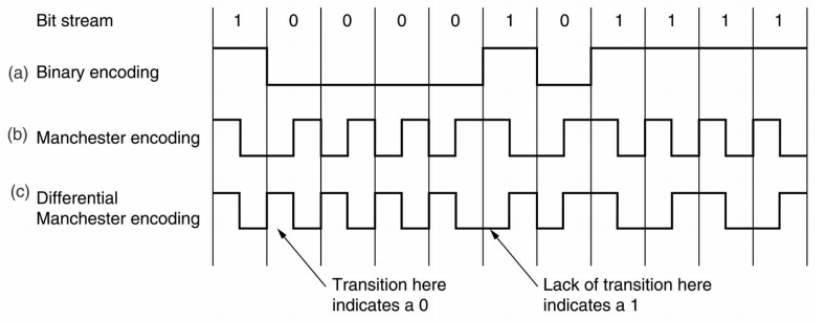


Servicios que ofrece LLC: Servicio sin conexión confirmado, no se puede enviar una trama si no se ha confirmado la anterior. Servicio sin conexión no fiable, no se garantiza que el paquete llegue bien a su destino. Servicio orientado a la conexión fiable, tiene una fase para el establecimiento de una conexión con el otro extremo.

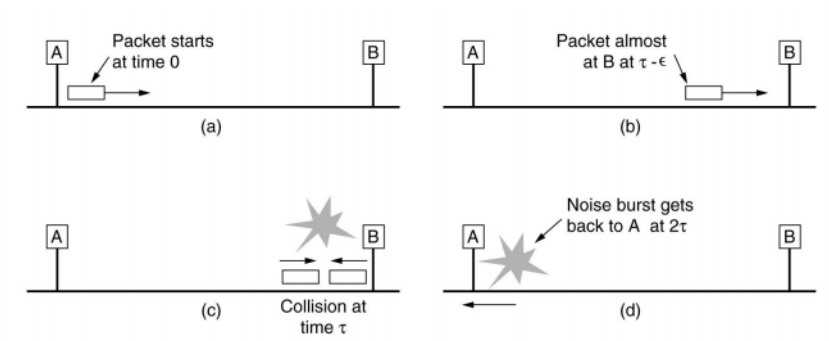
EL ESTÁNDAR IEE 802.3 (ETHERNET):

Es la red más usada hoy día, fue desarrollada por Xerox en los años 70, la red tiene topología de bus y usa un protocolo MAS de tipo CSMA-CD.

Codificación Manchester:



Análisis: Para implementar CSMA/CD, las tramas tienen que ser lo suficiente largas como para detectar colisiones.



En la red Ethernet, la velocidad de transmisión (10Mbps), la longitud máxima del cable (2500 metros con 4 repetidores), round trip time (50 microsegundos en el peor caso). La trama tiene que transmitirse al menos durante 50 microsegundos, a 10MBPS, un bit se transmite en 100 nseg, la trama debe tener 500 bits, se redondea a 512 (64 bytes), la longitud es de 18 y el pad de 46 bytes. Si se quiere aumentar la velocidad (por ejemplo 100 Mbps), hay dos opciones, mantener la distancia (2500 metros) multiplicar por 10 el tamaño de la trama (640 bytes) o mantener el tamaño de la trama (64 bytes) y dividir por 10 la distancia máxima (250 metros).

IEEE 802.3 a 100 Mbps y compatible con la Ethernet clásica.

IEEE 802.3 a 1 Gbps, su objetivo es multiplicar la velocidad por 10.

IEEE 802.3 a 10 Gbps, fibra óptica.

REDES DE PASO DE TESTIGO:

Características básicas:

Suelen emplearse en redes con enlaces punto a punto. Existe una trampa especial llamada testigo. Cada nodo solo puede enviar si posee el testigo. En la actualidad no se suelen utilizar. Ejemplos Token Ring o FDDI.

TOKEN RING y IEEE 802.5:

Utiliza una topología lógica en anillo con paso de testigo. Funcionamiento básico: El testigo va circulando por la red, si una estación recibe un testigo y quiere enviar, lo "elimina" y envia los datos, mientras los datos circulan en el anillo, no existe otro testigo, los datos circulan en el anillo hasta que localiza la estación destino que copia la información para poder procesar, la información circula por el anillo y finalmente es borrada cuando regresa al nodo origen y restablece el testigo. Los posibles problemas son la perdida del testigo, la caída del enlace y la circulación indefinida de los datos.

FDDI:

Se basa en token ring, pero incorpora dos para ser tolerante a fallos. Usa fibra óptica (hay versión con cable de cobre CDDI). Permite diseñar redes de gran alcance (100/200 km) a alta velocidad (100/200 Mbps). Se utiliza como backbones en redes WAN.

REDES INALÁMBRICAS:

PROTOCOLOS PARA REDES INALÁMBRICAS:

Las redes locales inalámbricas son cada vez mas habituales. Todas comparten el medio: onda de radio. Al mas alto nivel, podemos clasificar las redes inalámbricas de acuerdo a dos criterios: Si un paquete cruza la red inalámbrica exactamente en un salto (inalámbrico)(single hop) o en múltiples saltos (inalámbricos)(multiple hop). Si hay una infraestructura, como una estación base, en la red.

	Single hop	Multiple hops
Infraestructura	WIFI, WIMAX, 3G	ZIGBEE red MESH (de malla) de sensores
Sin Infraestructura	Bluetooth WIFI ad hoc	Redes MANET y VANET

REDES DE ÁREA LOCAL INALÁMBRICAS – WIFI:

Sin embargo, CSMA-CD no es aplicable directamente:

Dificultades para implementar detecciones de colisiones. Para poder detectar la colisión es necesario poder enviar y recibir a la vez. Es costoso de implementar en las tarjetas inalámbricas.

Problemas de cobertura, no existentes en las redes cableadas. Problema de la estación oculta y de la estación expuesta.

IEE 802.11: Define las especificaciones del nivel físico y de enlace de datos para una LAN inalámbrica.

Medio físico: Ondas de radio en la banda ISM de 2.4 GHz, velocidad de transmisión (IEE 802.11b -11Mbps, IEE 802.11g- 54Mbps, IEE 802.11ª- 54 Mbps y IEE 802.11n – hasta 600 Mbps)

Enlace de datos:

CSMA/CA: Se adaptan las técnicas de control de acceso para intentar evitar la colisión y resolver problemas propios de las redes inalámbricas.

Se definen dos modos de acceso/transmisión en la red, uno centralizado otro distribuido.

REDES IEE 802.11 – Concepto de BSS:

Un conjunto de servicios básicos BSS es el bloque constructivo de una WLAN. Un BSS se compone de estaciones móviles o fijas y una estación base opcional. Arquitectura ad hoc, es un conjunto BSS sin AP, es una red aislada y no puede enviar datos a otros BSS y las estaciones pueden formar una red, localizarse y acordar formar una BSS. Red con infraestructura BSS con AP.

Modo ad hoc.

REDES IEEE 802.11:

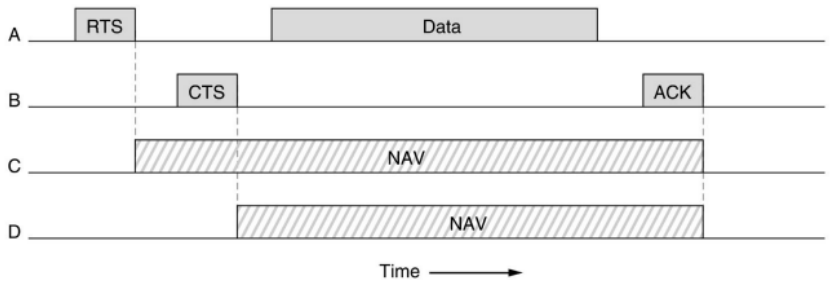
Arquitectura: modo infraestructura. Con dos o mas BSS puede unirse a través de un sistema de distribución para formar un ESS.

REDES IEEE 802.11 SUBNIVEL MAC:

La función de coordinación distribuida utiliza una variante de CSMA/CA como método de acceso, dos modos de comprobación del canal. La funcion de coordinación puntual, mecanismo de acceso centralizado el punto de acceso.

PROTOCOLO MAC DCF MODO: VIRTUAL CHANNEL SENSING:

La idea básica: informar previamente con un pequeño paquete indicado que se quiere enviar un paquete de datos por parte del emisor y confirmar por parte del receptor. Las estaciones que oyen el RTS o el CTS esperan para no interferir.

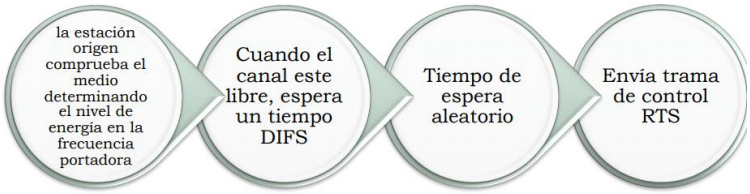


PROTOCOLO MAC DCF MODO: PHYSICAL CHANNEL SENSING:

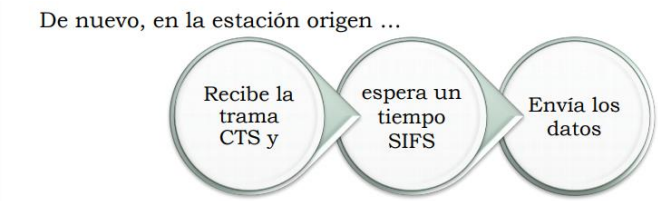
Si no hay NAV activo en una estación, se escucha el medio. La transmisión se basa en un algoritmo CSMA/CA que incluye: Tiempo de espera entre tramas, retroceso exponencial binario antes de transmitir y confirmaciones (ACK).

IEEE 802.11 Variante de CSMA/CA:

Cuando una estación quiere transmitir antes de enviar la trama…



Mientras la estación destino…



¿CÓMO EVITAR LA COLISIÓN?

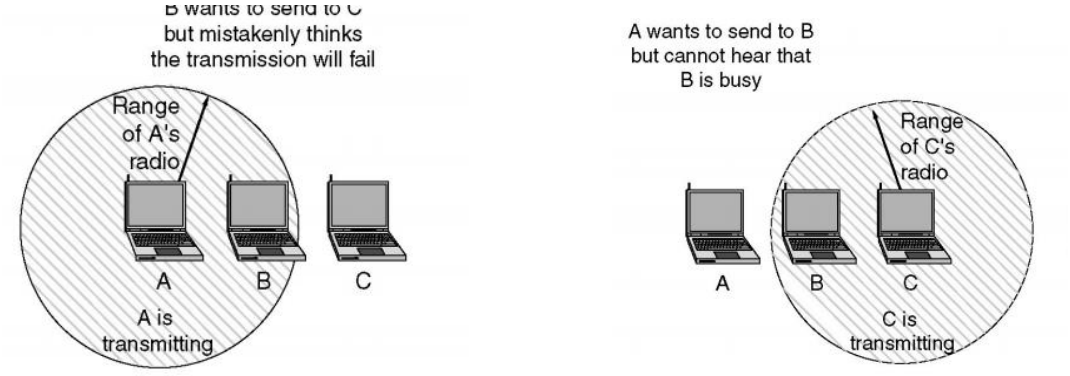
¿Cómo aplaza una estación el envio de datos si una estación adquiere el acceso? Mediante el vector de asignación de red (NAV -> NETWORK ACCESS VECTOR). Cuando una estación envia un RTS, incluye el tiempo que necesita ocupar el canal. Las estaciones que quieres transmitir crean un temporizador denominado NAV que determina cuanto tiempo debe pasar antes de poder comprobar si el canal esta libre. Cada vez que una estación envia un RTS, otras inician su NAV. Por tanto, antes de comprobar si el medio esta libre, comprueba su NAV para ver si ha expirado.

¿QUÉ OCURRE SI HAY COLISIÓN MIENTRAS LAS TRAMAS RTS/CTS ESTÁN EN TRANSICIÓN?

Dos o más estaciones pueden enviar tramas RTS al mismo tiempo y pueden colisionar. Debido a que no hay forma de evitar la colisión, el Emisor asume que se ha producido si no recibe una trama CTS del Receptor. Se espera un tiempo según la estrategia de espera aleatoria y se comienza de nuevo.

Además, dado que el numero de colisiones puede ser alto y para minimizar el impacto de la retransmisión, los paquetes se pueden fragmentar, se usa un protocolo de parada y espera.

El problema de estación oculta se soluciona con RTS Y CTS.



El problema de la estación expuesta.

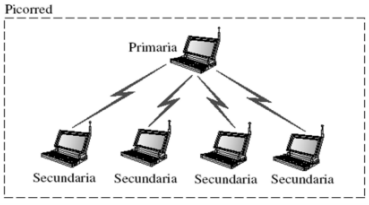
LANs INALÁMBRICAS DE ÁREA PERSONAL (PAN):

BLUETOOTH:

Tecnología de LAN inalámbrica de área personal. Permite la conexión de dispositivos variados: teléfonos, portátiles, cámaras, impresoras, …, reemplazar cables en conexión de teclados, ratones o impresoras, sensores conectados con dispositivos de monitorización para control de salud. Originalmente, proyecto de compañía Ericsson, posteriormente se estandarizo como 802.15.1. Red ad hoc: se forma de manera espontánea, dispositivos se encuentran unos a otros, forma una picorred.

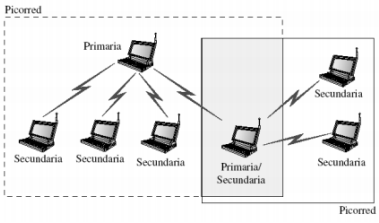
Arquitectura picorred:

- Máximo 8 estaciones
- 1 estación actúa de primaria, el resto secundarias.



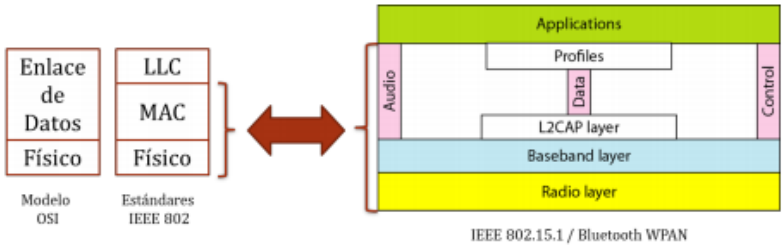
Arquitectura Red Dispersa

- Combinación de picorredes
- Una estación secundaria en una picorred actúa de primaria en otra
- Una estación puede ser miembro de dos picorredes



NIVELES EN BLUETOOTH:

No se corresponden exactamente con el modelo de internet.



Nivel de radio: Aproximadamente equivalente a nivel físico. Emplea banda de 2.4 GHZ, dividida en 79 canales de 1 MHz. Utiliza técnica de espectro ensanchado por salto de frecuencias, los dispositivos cambian de frecuencias 1600 veces por segundo, cada frecuencia es solo utilizada durante 1/1600s (625us) antes de salvar a otra, evita con otras redes. Requiere que todos los dispositivos de la picorred estén sincronizados.

PROTOCOLO DE CONTROL DE ENLACE DE ALTO NIVEL (PPP):

PROTOCOLO PPP:

Introducción: Protocolo muy extendido para el acceso punto a punto.

Aspectos definidos por ppp: formato de la trama a intercambiar, como negociar establecimiento del enlace e intercambio de datos, como encapsular datos de nivel de red, autentificación entre dispositivos, soporte de múltiples protocolos y servicios a nivel de red, configuración de direcciones de red.

Aspectos no definidos por ppp: control de flujo, control de error mínimo: CRC para detección de error. Sin numeración de secuencia.

Funcionamiento básico:

- **Muerto**: Línea en silencio, no hay portadora activa
- **Establecer**: Comienza comunicación. Negociación de opciones
- **Autenticar**: Opcional. Si acordada, debe superarse con éxito para pasar a fase de red.
- **Red**: Negociación de los protocolos a nivel de red. Necesaria dado que PPP soporta múltiples protocolos de red.
- **Abierto**: Comienza el intercambio de paquetes de datos. Transferencia de datos
- **Terminar**: Se cierra el enlace y finaliza la conexión.