4.4 IEEE 802.3 Ethernet

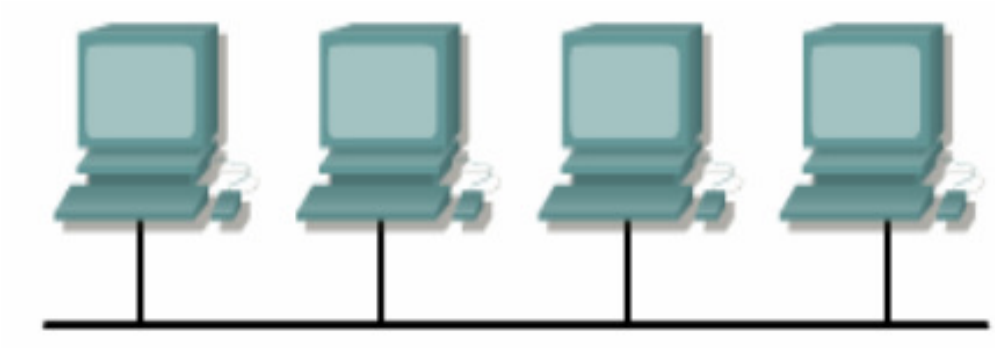
4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Orígenes

El origen de las redes Ethernet está en el desarrollo de Xerox en 1975 de la primera red local de bus común a una velocidad de 2.94 Mbps.

Posteriormente Xerox, Intel y Digital desarrollan una red Ethernet a 10 Mbps que es el fundamento del estándar IEEE 802.3.

Una red Ethernet se caracteriza por emplear un medio físico compartido entre todas las estaciones con topología de bus.



El medio físico empleado puede ser cable coaxial, cable par trenzado o fibra óptica, definiendo distintos "modelos tecnológicos" de redes Ethernet.

Debido a la necesidad de compartir el medio físico, las redes Ethernet son **semiduplex** y emplean un mecanismo denominado **CSMA/CD** para el reparto del medio físico.

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Ethernet 10Base2

Las diferentes versiones tecnológicas de Ethernet se denominan empleando la nomenclatura:

Velocidad-Señalización-Medio físico

10Base2 significa: Red Ethernet a 10 Mbps, señalización en banda base (**Manchester**) y medio físico cable coaxial fino.

Velocidad: 10 (Mbps), 100 (Mbps), 1000 (Mbps), 10G (Gbps)

Señalización: Base (banda base) o Broad (banda modulada)

Medio físico: T (cable UTP), C (cable STP), F (fibra óptica), X (soporte para varios medios físicos)

10Base2 es una de las primeras versiones de Ethernet empleando cable coaxial fino. Permite una velocidad de 10 Mbps a distancias de 185 metros.

10Base5 emplea cable coaxial grueso, permitiendo una velocidad de 10 Mbps a distancias de hasta 500 metros.

10Base2 y **10Base5** desaparecen del mercado con la introducción de los cables UTP (más tolerancia a fallos, facilidad de implantación y mejores prestaciones)

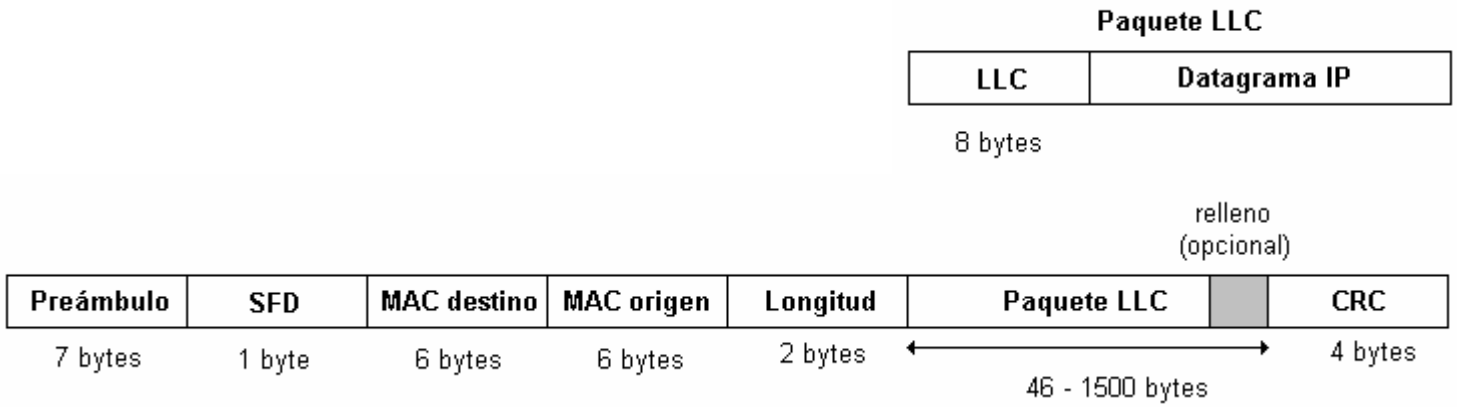
4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Formato de paquete IEEE 802.3

La normativa IEEE 802.3 establece un formato de paquete donde se especifica la cabecera MAC

Modelo TCP/IP
+
Modelo 802 IEEE



El **MTU** (tamaño máximo de paquete IP) en una red IEEE 802.3 es **1492 bytes**

Preámbulo: Secuencia de 7 bytes 10101010

SFD: Delimitador de inicio de trama 10101011

MAC destino/origen: Identificador de 48 bits para cada equipo

Longitud: Tamaño del campo de datos del paquete (máximo 1500)

CRC: Código de Redundancia Cíclica de 32 bits para detección de errores

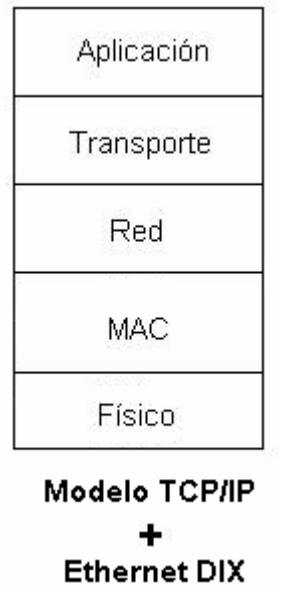
4.4 IEEE 802.3 Ethernet

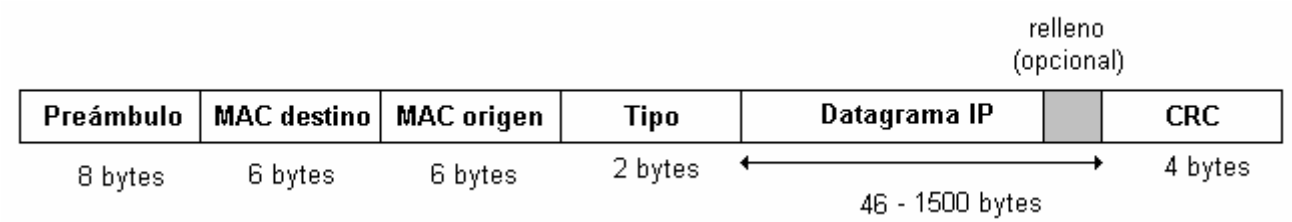
4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Formato de paquete Ethernet II

Las redes Ethernet de Digital/Intel/Xerox (Ethernet **DIX**) emplean un formato de paquete distinto

Este formato, denominado Ethernet II, no emplea la capa LLC y permite la introducción del datagrama IP en el paquete de nivel MAC





El **MTU** (tamaño máximo de paquete IP) en una red Ethernet DIX es **1500 bytes**

Este es el formato de paquete Ethernet empleado con redes TCP/IP

Preámbulo : Equivalente al campo Preámbulo + SFD del IEEE 802.3

Tipo: Código para identificar el protocolo del contenido del paquete MAC (ARP/IP)

Tipo = **0x0806** Protocolo ARP
Tipo = **0x0800** Protocolo IP

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

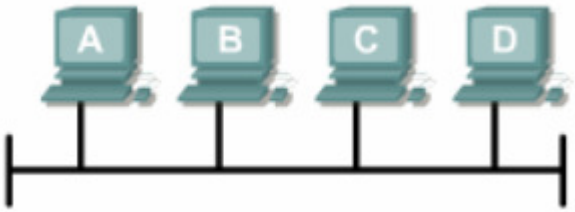
CSMA/CD – Acceso al medio con detección de portadora y de colisión

Tanto Ethernet DIX como IEEE 802.3 emplean el mismo mecanismo para compartir el bus común: CSMA/CD

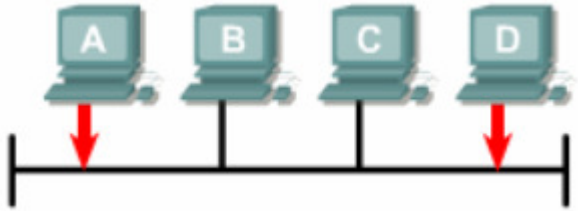
El esquema básico de funcionamiento del CSMA/CD consiste en comprobar el medio físico antes de transmitir un paquete de datos.

El esquema de funcionamiento de CSMA/CD **siempre es semiduplex**

Problema en CSMA: colisión por comprobación simultánea del bus por dos o más estaciones.



Medio físico libre

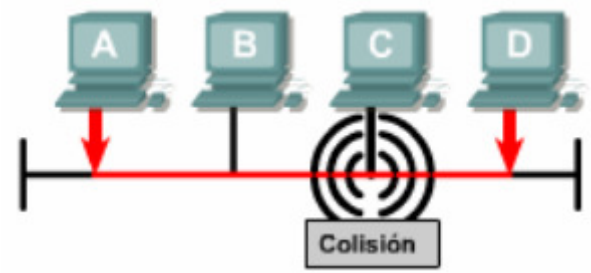


Transmisión simultánea

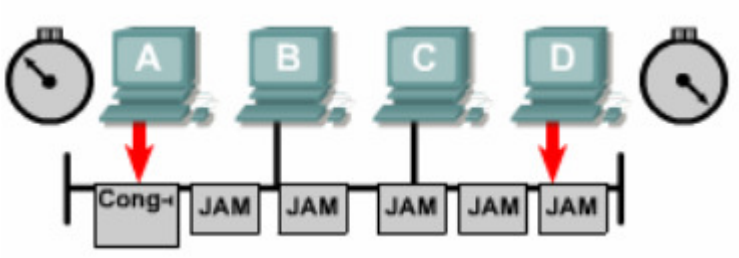
4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

CSMA/CD – Acceso al medio con detección de portadora y de colisión



Detección de colisión simultánea a la transmisión



Resolución de colisiones

Para asegurar que dos estaciones que transmiten simultáneamente detectan la colisión, es necesario que la transmisión dure lo suficiente para llegar al otro extremo.

En Ethernet se define la extensión máxima de la red (con repetidores) en 2.5 Km (5 buses de 10Base5).

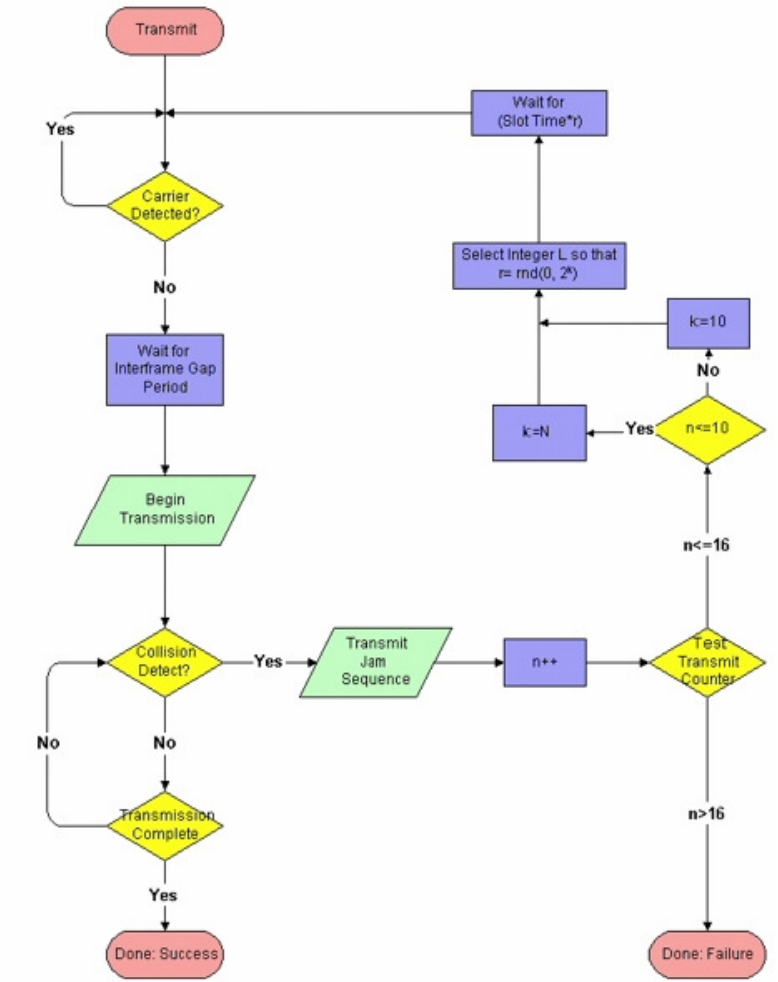
En una red a 10 Mbps y 2.5 Km de extensión, el tiempo mínimo de transmisión necesario son 512 tiempos de bit, es decir un paquete ethernet de 64 bytes (46 bytes de datos y sin tener en cuenta el preámbulo).

Al tiempo mínimo de transmisión se le denomina **ranura temporal**.

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Algoritmo CSMA/CD - Transmisión



1. Escucha del medio antes de la transmisión

2. Tiempo de espera entre tramas (96 tiempos de bit)

   Tespera = 96/10000000 = 9.6 μ segundos

3. Transmisión del paquete escuchando el medio

4. La **colisión** se detecta cuando la señal en el medio tiene una tensión anómala (superposición de señales)

5. Si una estación detecta una colisión la refuerza, transmitiendo una señal denominada **JAM** (señal de congestión)

6. El paquete que ha colisionado es reenviado hasta en 16 intentos

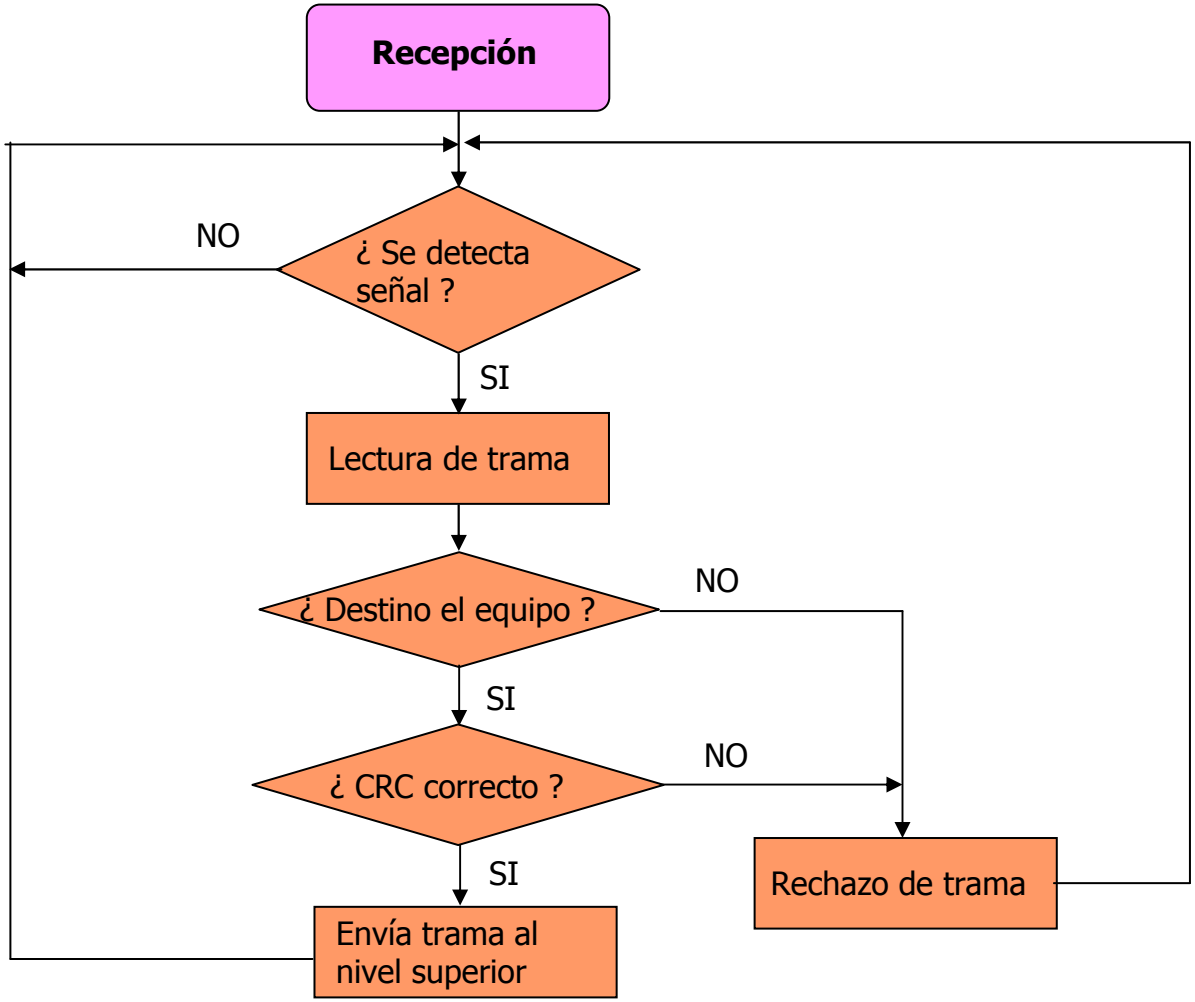
7. En cada intento se espera un número aleatorio de veces el denominado **tiempo de ranura** (regresión exponencial).

8. El tiempo de ranura se determina como el doble del tiempo mínimo que tarda un bit en propagarse en la red ethernet (51.2 μ segundos)

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Algoritmo CSMA/CD – Recepción



1. El preámbulo permite sincronizar el receptor con la trama a leer (modo asíncrono)

2. La interpretación del campo dirección destino en la trama es inmediato.

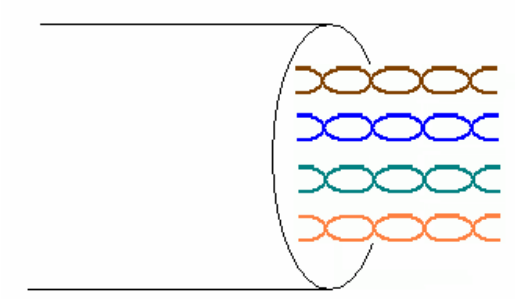
4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

10BaseT – Concentrador Ethernet (Hub)

La red 10BaseT surge con la introducción de los cables pares trenzados no blindados (UTP)

Un cable UTP comercial está formado por 4 pares de hilos trenzados



La categoría del cable UTP (3,5,6) hace referencia al ancho de banda de los pares de hilos

Categoría 3: 30 MHz

Categoría 5: 100 MHz

Categoría 6: 250 MHz

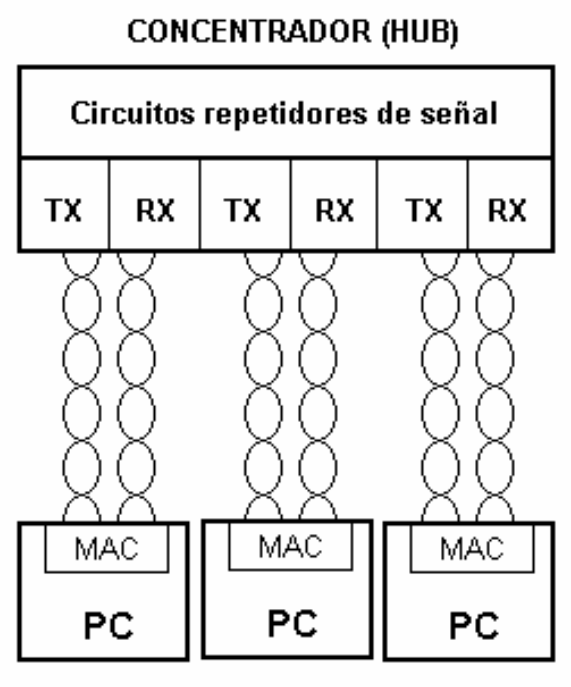
10BaseT emplea cable de categoría 3 con codificación Manchester, alcanzado sin problemas la velocidad de **10 Mbps** a distancias de **100 metros**.

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

10BaseT – Concentrador Ethernet (Hub)

La red 10BaseT emplea una topología en estrella, donde el elemento central se denomina **concentrador** o **hub**.



Las colisiones se detectan cuando se recibe una señal por el par de recepción al mismo tiempo que se transmite una trama.

La detección de problemas en el cableado es más fácil que con cable coaxial.

La distancia máxima entre equipo y concentrador debe ser inferior a 100 m.

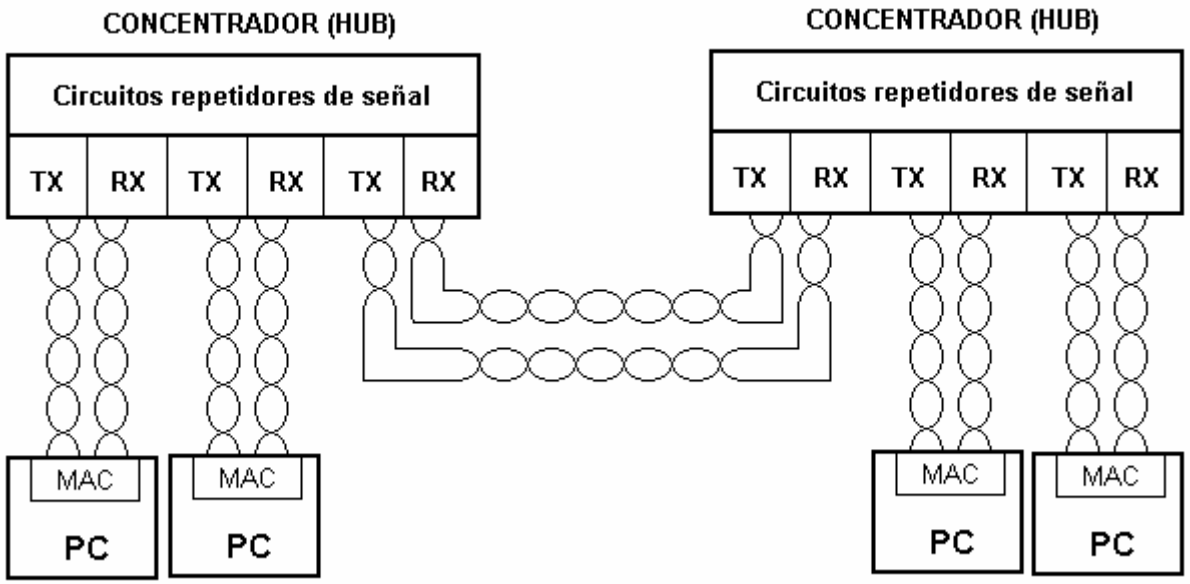
La red Ethernet puede crecer en tamaño interconectando concentradores con cables UTP cruzados (repetidores).

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Repetidores

La conexión de concentradores en cascada permite el aumento en el tamaño físico de la red Ethernet.



El número máximo de hubs que pueden colocarse en cascada (el retardo afecta al funcionamiento del CSMA/CD), está limitado por la extensión máxima de una red Ethernet que son 2.5 kilómetros (en 10Base5: 5 segmentos – 4 repetidores).

Dominio de colisión: Conjunto de dispositivos en una red que pueden colisionar al transmitir simultáneamente

Inconveniente del hub: **aumenta la probabilidad de colisiones al ser mayor el dominio de colisión**

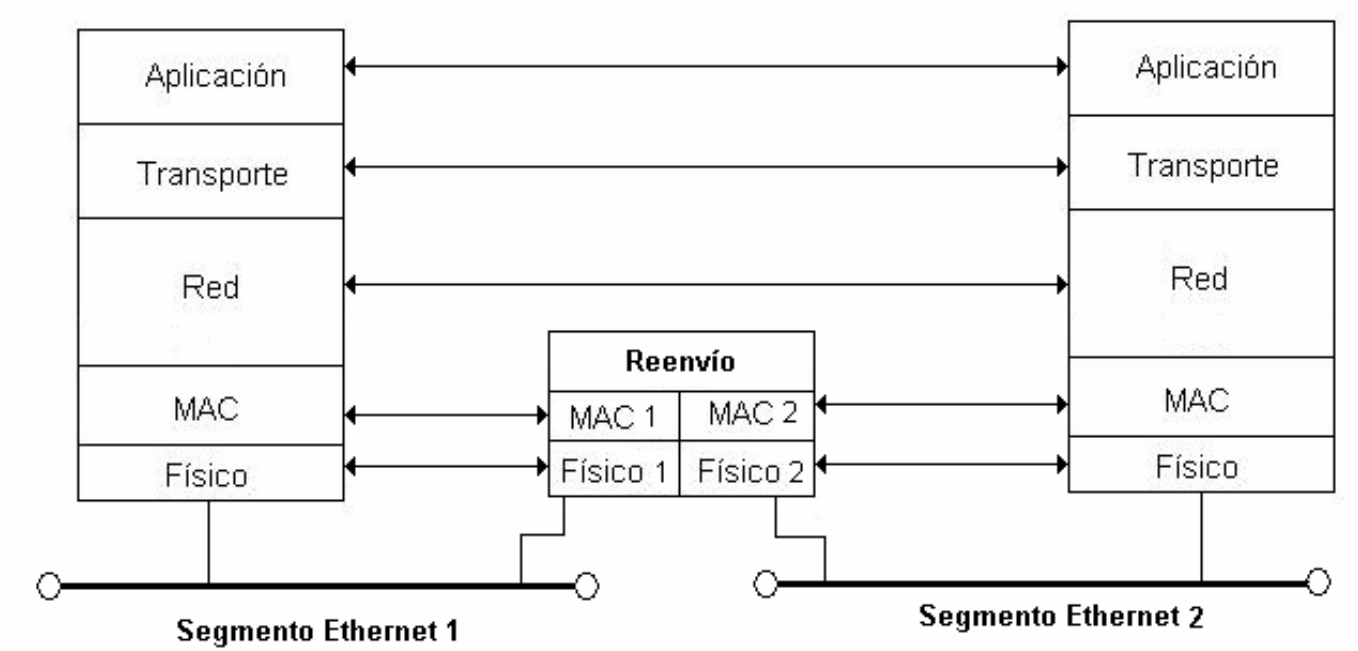
4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Puentes

La interconexión de segmentos Ethernet puede mejorarse (reducir el número de colisiones) empleando **puentes** o **bridges**.

Un puente es un dispositivo de interconexión entre dos o más segmentos Ethernet que analiza la cabecera MAC de los paquetes para determinar si hay que reenviarlos o no de un segmento a otro.



El puente divide la red en **segmentos de colisión independientes**, por lo que las LAN interconectadas con puentes no tienen limitación de extensión física al crecer.

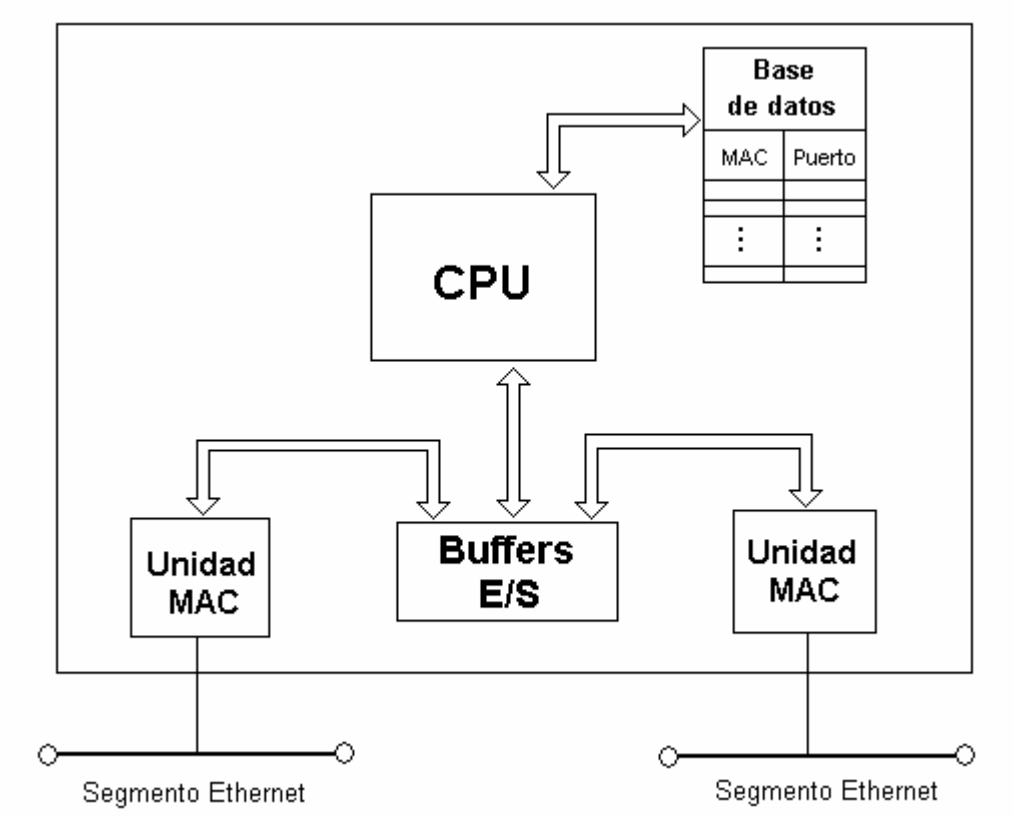
4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Puentes Transparentes

Los puentes denominados **puentes transparentes** son aquellos en los que la decisión de cómo los paquetes se intercambian entre segmentos la toman ellos (los equipos no conocen la estructura de la red)

Estructura interna de un puente transparente



CPU: Unidad de control de funcionamiento del puente (reenvío de paquetes y aprendizaje)

Buffers E/S: Unidad de almacenamiento de tramas en proceso (lectura/envío). FIFO.

Base de datos: Tabla de asociación de direcciones MAC con números de puerto **(tabla de reenvío)**.

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Puentes Transparentes

Ejemplo de tablas en puentes

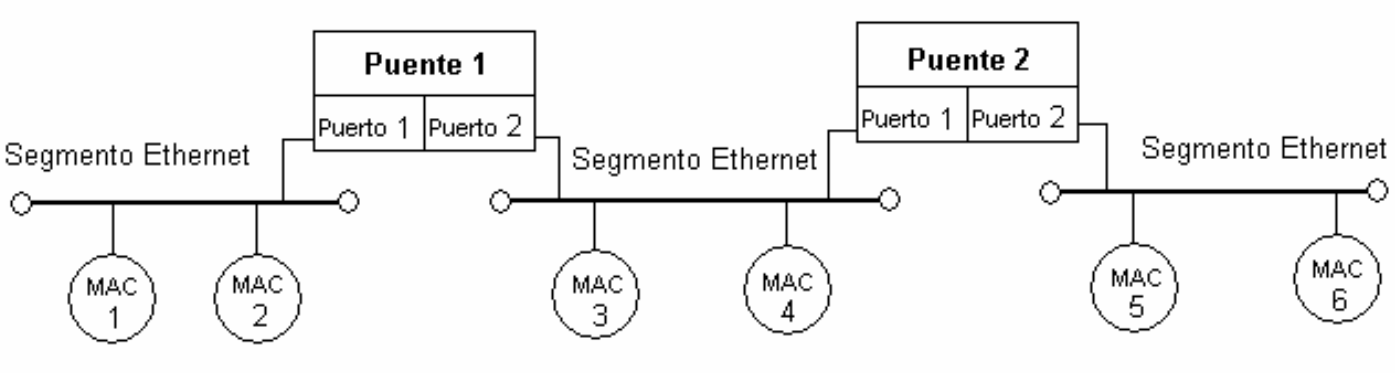


Tabla Puente 1

MAC	Puerto
1	1
2	1
3	2
4	2
5	2
6	2

Tabla Puente 2

MAC	Puerto
1	1
2	1
3	1
4	1
5	2
6	2

La inicialización de la tabla requiere de un proceso de aprendizaje automático

Un puente trabaja en dos modos simultáneamente: **modo de reenvío** y **modo de aprendizaje**

Un puente lee **todos** los paquetes recibidos por un puerto (modo promiscuo) y los almacena en un buffer para procesarlos.

El algoritmo de funcionamiento de un puente transparente se especifica en la normativa IEEE 802.1D MAC Bridge.

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Puentes Transparentes

Modo de reenvío

En el modo de reenvío se comprueba la dirección MAC de destino de cada paquete Ethernet que llega a un puerto.

Si la dirección MAC de destino se encuentra en la tabla de reenvío, el puente reenvía el paquete al puerto asociado (siempre que el puerto asociado sea distinto del puerto por donde ha llegado el paquete)

Si la dirección MAC de destino no existe en la tabla de reenvío, el paquete se reenvía a todos los puertos excepto por el que se recibió.

Los paquetes con dirección de destino la dirección de broadcast se reenvían a todos los puertos, excepto al puerto por el que se recibió el paquete de difusión.

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Puentes Transparentes

Modo de aprendizaje

En el modo de aprendizaje se comprueba la dirección MAC de origen en cada paquete Ethernet recibido en un puerto.

Si la dirección MAC de origen no se encuentra en la tabla de reenvío, el puente crea una entrada con la dirección MAC de origen y el puerto donde se ha recibido.

Durante el proceso de aprendizaje, dado que no se conocen las direcciones MAC de los equipos, la mayor parte de los paquetes son reenviados por todos los puertos, por lo que los demás puentes aprenderán información. A este fenómeno se le conoce como el nombre de inundación.

Cada entrada en la tabla de reenvío de un puente tiene asociado un temporizador (segundos) que mide el tiempo desde que se creo la entrada en la tabla.

Si se recibe un paquete con una dirección MAC de origen por el puerto que se indica en la tabla de reenvío, el temporizador se inicializa a cero.

Si el temporizador alcanza un determinado valor máximo, la entrada de la tabla de reenvío se **elimina**. De esta forma las tablas de los puentes se ajustan a cambios en la estructura de la red.

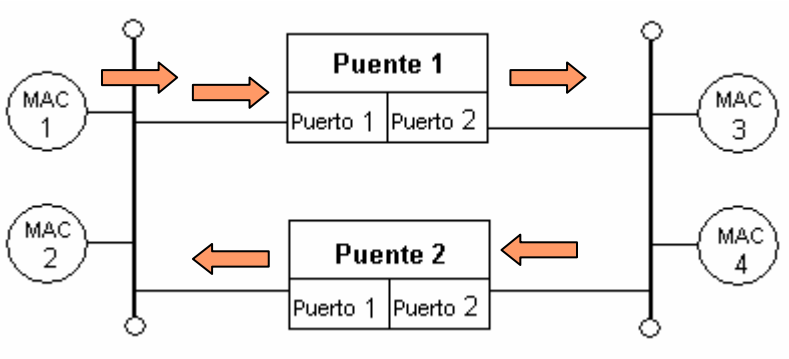
El modo de aprendizaje requiere que la LAN con puentes tenga una estructura de árbol simple **(árbol de expansión)**.

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Puentes Transparentes

Estructura de árbol de expansión



Interconexión de LAN's con bucles

Paquete de broadcast enviado por el equipo MAC 1

Los bucles provocan circulación indefinida de paquetes de broadcast y cambios continuos en las tablas de reenvío en el proceso de aprendizaje.

Algoritmo de árbol de expansión: Algortimo Spanning Tree

El algoritmo Spanning Tree define un protocolo de comunicación entre puentes que consigue una estructura de LAN's interconectadas por puentes sin existencia de bucles.

La definición de este algoritmo se encuentra en la norma IEEE 802.1D MAC Bridge.

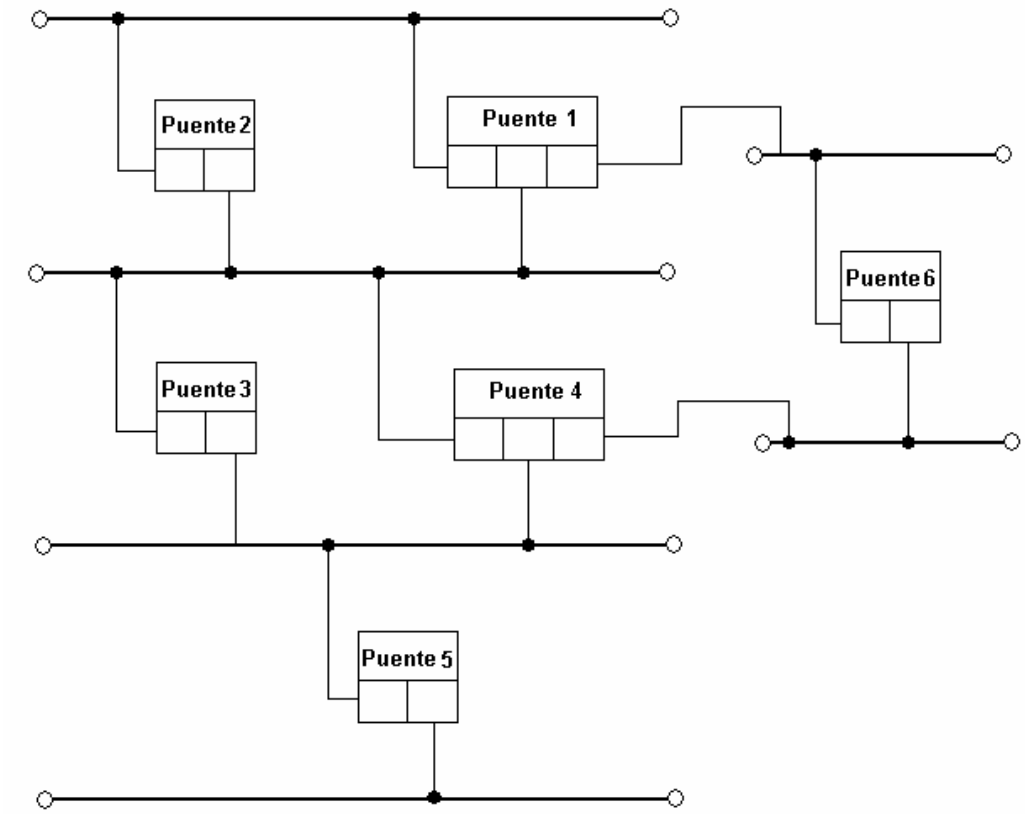
4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Puentes Transparentes

Algoritmo de árbol de expansión: Algoritmo Spanning Tree

En numerosas ocasiones, la interconexión de LAN's se realiza con puentes en una disposición tolerante a fallos (existencia de bucles).



El algoritmo elige un puente (identificador más bajo) que será la raíz de la estructura de árbol (**puente raíz**).

En cada puente se determina un coste RPC (número de redes intermedias, velocidad de transmisión) desde cada puerto al puente raíz. Al puerto con menor coste se le denomina **puerto raíz del puente**.

En cada segmento se elige un **puerto designado**. El puerto designado de un segmento es el puerto con menor valor de RPC que esté conectado al mismo.

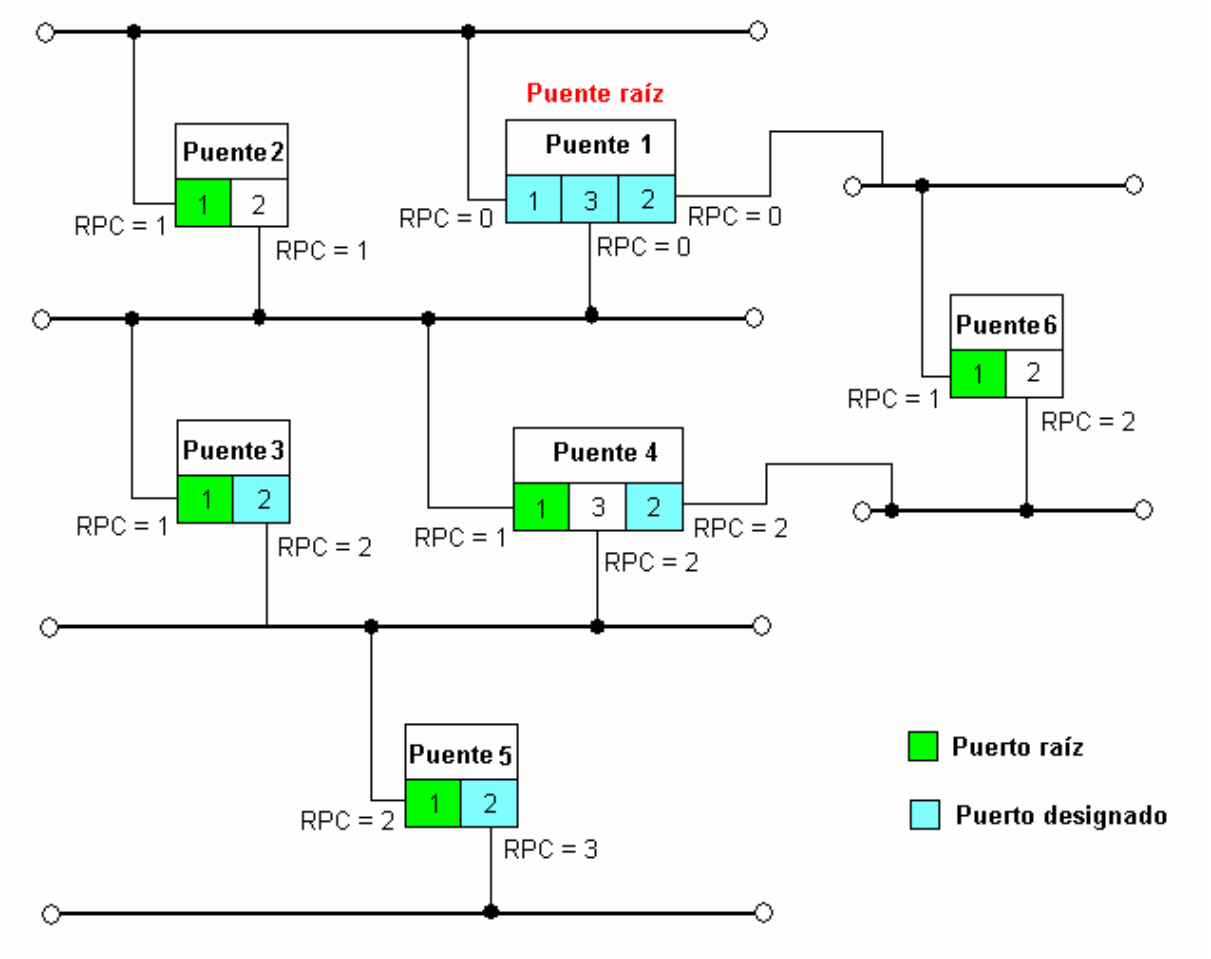
Finalmente, se activan todos los puertos raíz y designados de la red, determinando una estructura de árbol.

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Puentes Transparentes

Algoritmo de árbol de expansión: Algoritmo Spanning Tree

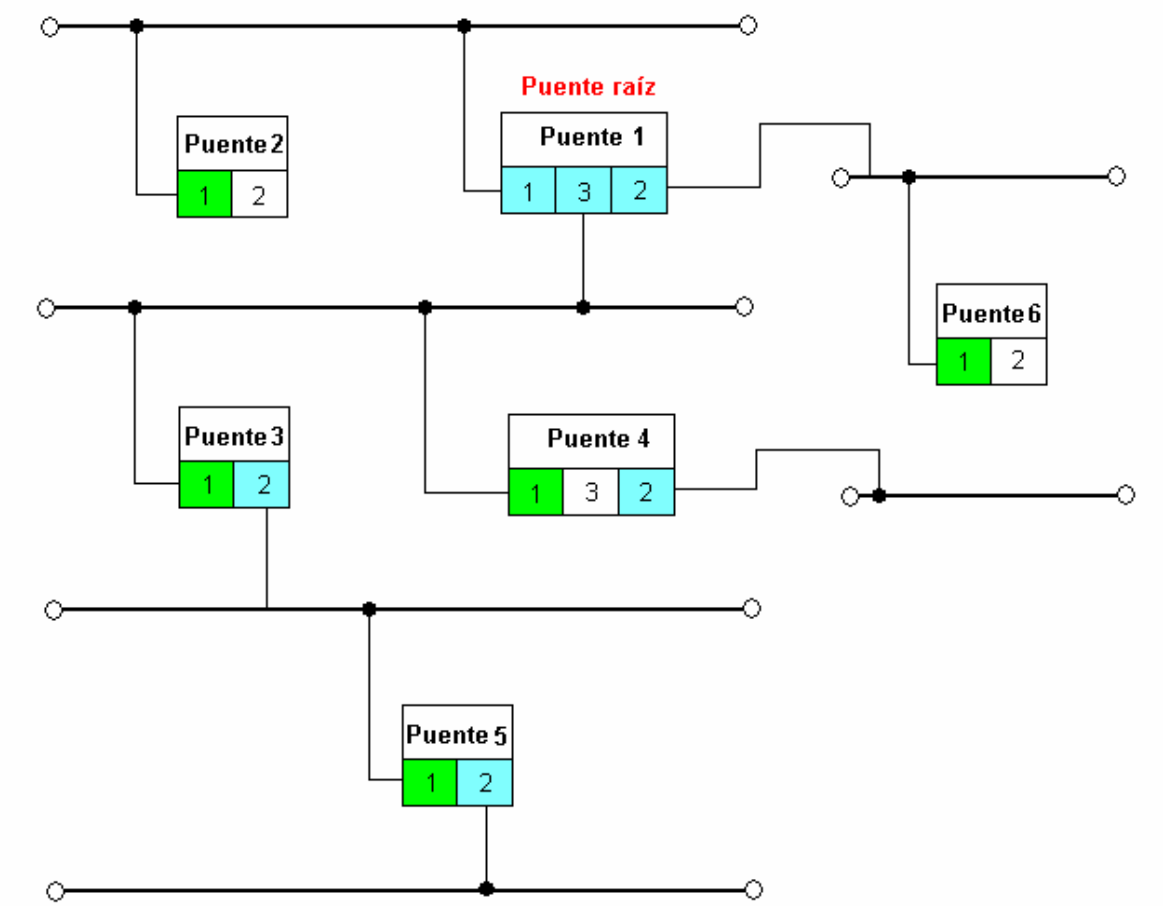


4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Puentes Transparentes

Algoritmo de árbol de expansión: Algoritmo Spanning Tree



Esta estructura se mantiene mientras que todos los puertos raíz y designados funcionen correctamente.

El puente raíz envía mensajes de control cada cierto tiempo.

Si un puente deja de recibir mensajes del puente raíz, se procederá de nuevo con el algoritmo Spanning Tree para determinar nuevos puertos raíz y designados.

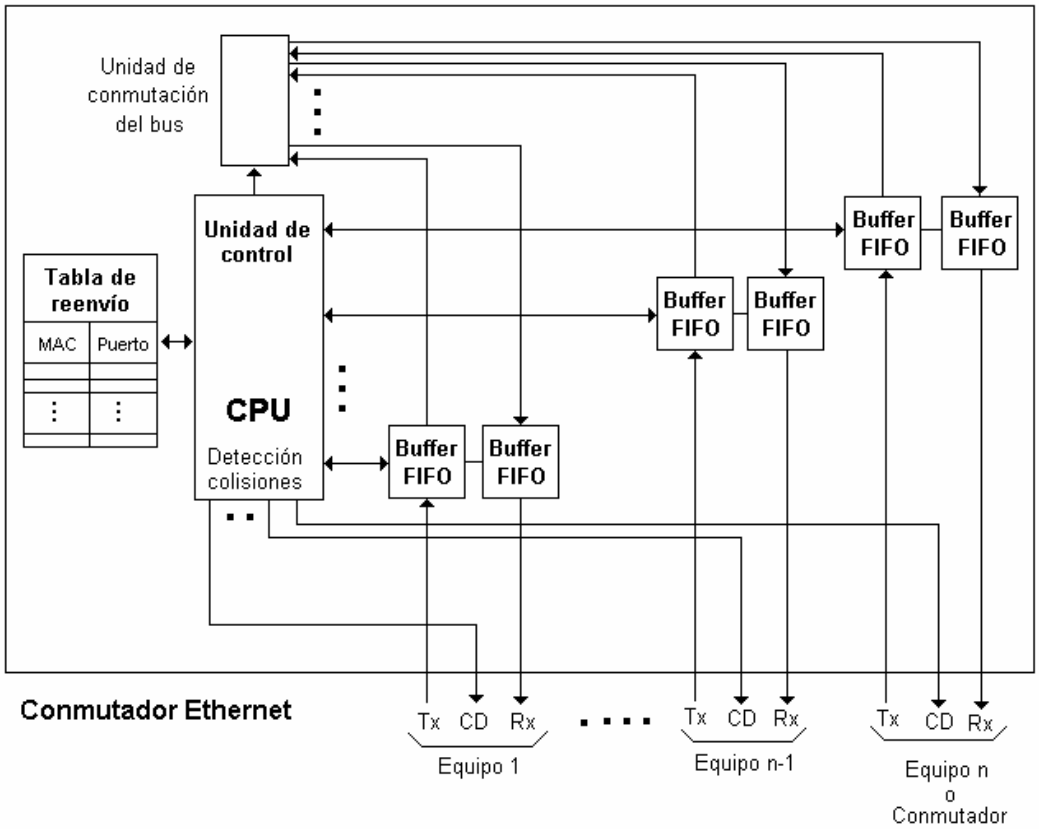
4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Ethernet Conmutada

El empleo de puentes llevó a la posibilidad de construir un puente multipuerto, donde en cada puerto se conecta un equipo en vez de un segmento de red.

Estos dispositivos se denominan **conmutadores** o **switches** definiendo las redes **Ethernet conmutadas**



Modo full-duplex: No existen colisiones (CSMA/CD no activo). Transmisión y recepción simultánea (no se emplea la línea CD).

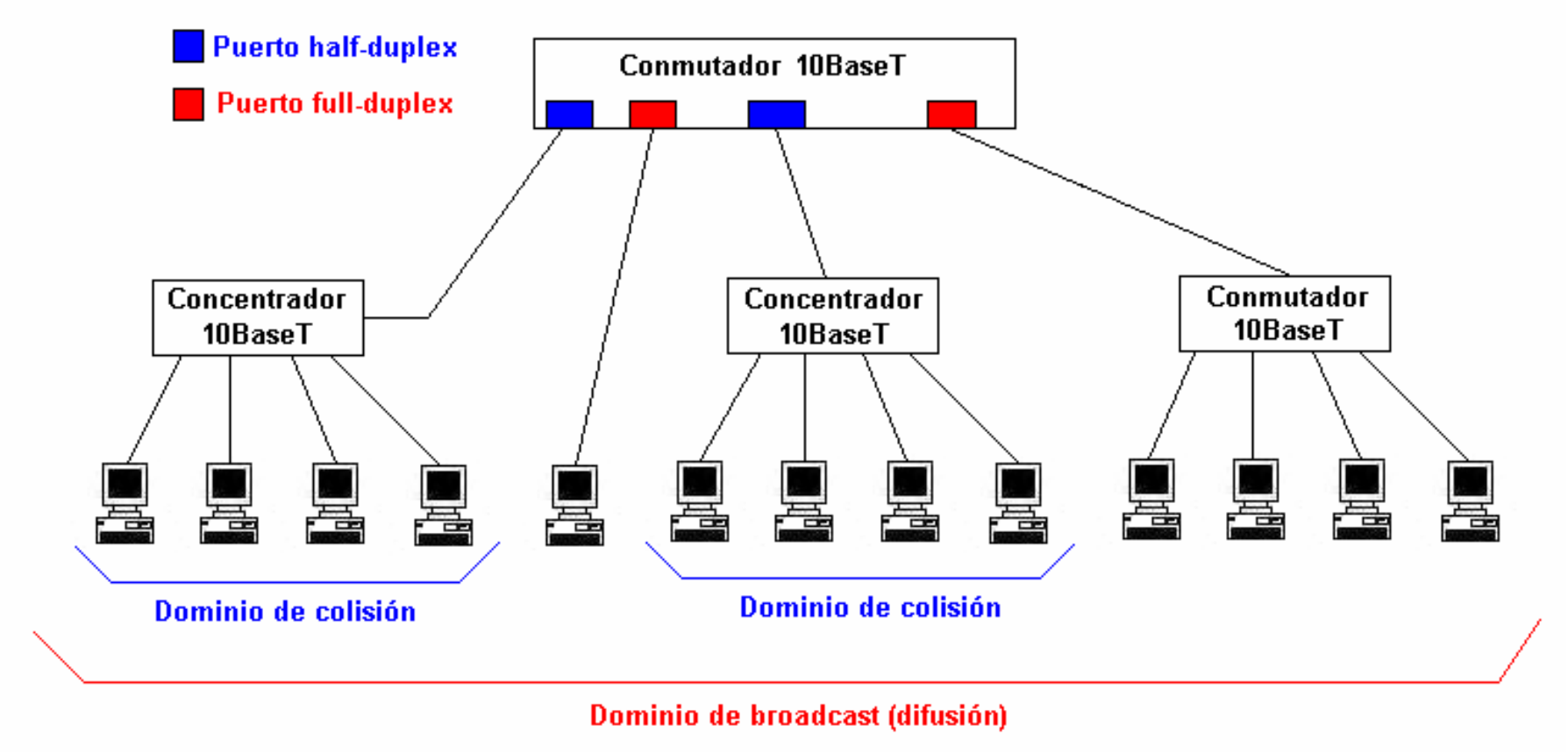
Modo half-duplex: Permite la conexión de equipos con CSMA/CD (concentrador 10BaseT). Se emplea la línea CD.

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Ethernet Conmutada

LAN Ethernet mixta de concentradores/conmutadores



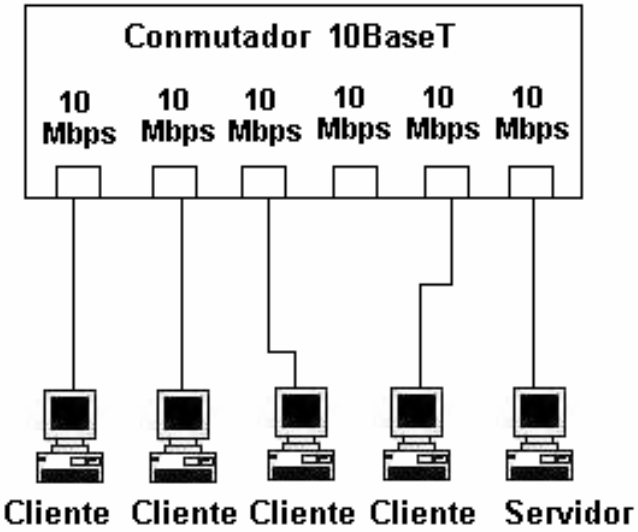
4.4 IEEE 802.3 Ethernet

4.4.2 Fast Ethernet (IEEE 802.3u)

Arquitectura cliente/servidor en Ethernet

Con el desarrollo de los conmutadores Ethernet el rendimiento que se alcanza es muy elevado si el tráfico tiene una distribución homogénea entre los equipos de la red.

En la práctica, la mayor parte de aplicaciones de red en entorno LAN (acceso a bases de datos, transferencia de archivos, web, etc.) se fundamentan en la arquitectura cliente/servidor.



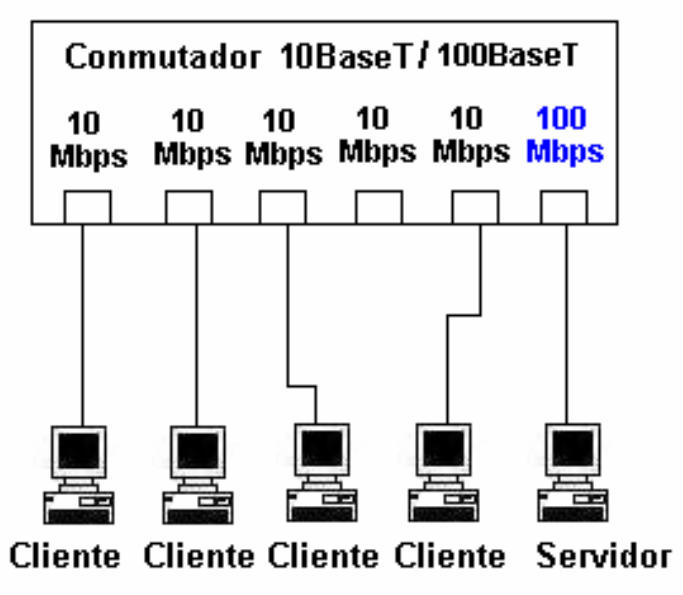
El conmutador debe emplear los buffers del puerto del servidor para repartir el tráfico de los clientes, es decir repartir el ancho de banda de 10 Mbps entre los clientes.

4.4 IEEE 802.3 Ethernet

4.4.2 Fast Ethernet (IEEE 802.3u)

Arquitectura cliente/servidor en Ethernet

Para conseguir un acceso adecuados entre clientes y servidor es necesario un puerto de mayor velocidad en el conmutador donde conectar el servidor.



Con un puerto a 100 Mbps, el servidor puede atender las peticiones y respuestas con 10 clientes a 10 Mbps de manera simultánea.

La normativa que permite la transmisión de paquetes Ethernet a 100 Mbps se denomina de forma genérica **Fast Ethernet**, existiendo diversas modalidades para la transmisión.

4.4 IEEE 802.3 Ethernet

4.4.2 Fast Ethernet (IEEE 802.3u)

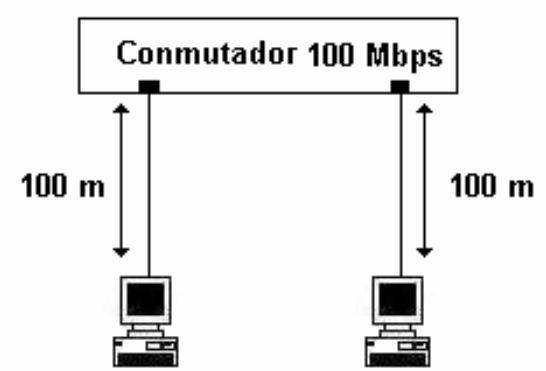
Fast Ethernet

Las redes Fast Ethernet funcionan con conmutadores, permitiendo el modo de trabajo half-duplex (CSMA/CD) y full-duplex.

Si se emplea 100 Mbps en CSMA/CD existe el problema del tamaño de paquete mínimo para la transmisión.

El tiempo mínimo de transmisión estándar en una red Ethernet con una extensión de 2.5 Km es de 51.2 μ segundos (512 bits tamaño mínimo de paquete).

En un conmutador Ethernet en modo half-duplex el dominio de colisión son 200 metros, y el tiempo mínimo de transmisión debe ser 4.1 μ segundos.



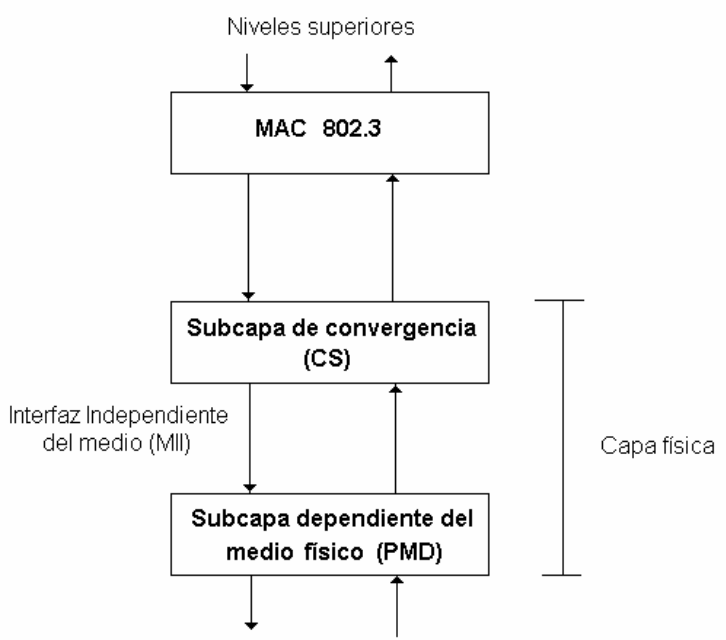
La transmisión de 512 bits a 100 Mbps supone un tiempo de 5.12 μ segundos, por lo que el tamaño mínimo de paquete es el mismo que en Ethernet 10 Mbps.

4.4 IEEE 802.3 Ethernet

4.4.2 Fast Ethernet (IEEE 802.3u)

Fast Ethernet

Para permitir la coexistencia del mismo tipo de protocolo MAC (CSMA/CD) empleando diferentes tipos de medios físicos, se introdujo una estructura de subcapas para el nivel físico.



Subcapa de convergencia: Convierte el flujo de bits de la capa MAC en grupos de 4 bits para su envío a la subcapa PMD.

Subcapa dependiente del medio físico: Transmite cada grupo de 4 bits con el mecanismo de codificación adecuado a cada tipo de medio físico.

4.4 IEEE 802.3 Ethernet

4.4.2 Fast Ethernet (IEEE 802.3u)

100BaseX

La normativa 100BaseX se desarrolló para cables UTP categoría 5, STP y fibra óptica.

El principal problema de la transmisión a alta velocidad es la sincronización emisor-receptor al transmitir la secuencia de bits.

Para introducir siempre información de sincronización en el flujo de bits, 100BaseX introduce una codificación 4B/5B.

Grupo de 4 bits	Símbolo de 5 bits
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111

Grupo de 4 bits	Símbolo de 5 bits
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

Para proporcionar una velocidad de 100 Mbps para cada grupo de 4 bits de datos, es necesario que los grupos de 5 bits se transmitan a una velocidad de 5/4*100 Mbps = 125 Mbps.

La señal de reloj para los pulsos en la capa PMD será de 125 MHz, y la codificación en pulsos será distinta si el medio es fibra óptica o cable UTP.

4.4 IEEE 802.3 Ethernet

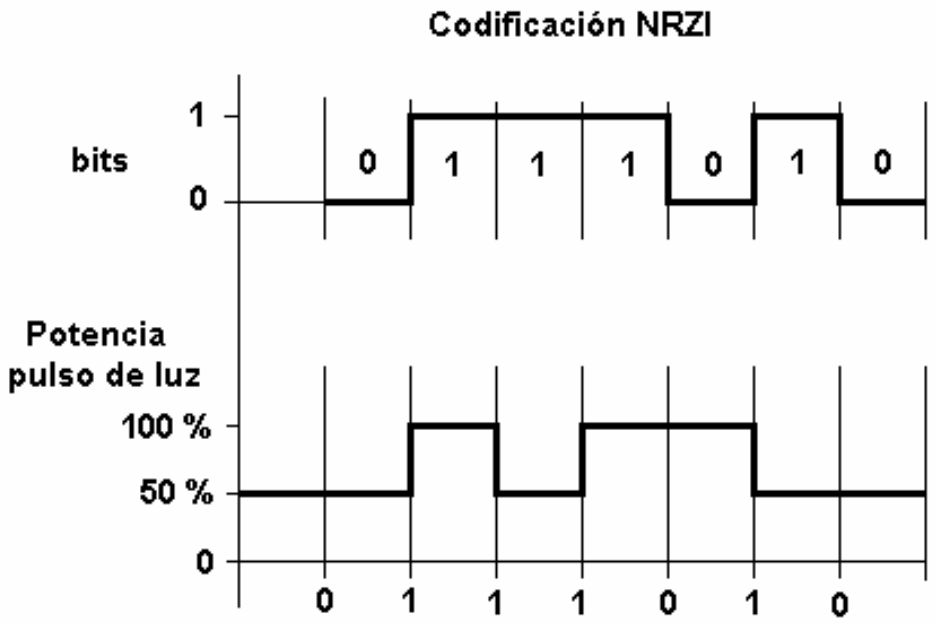
4.4.2 Fast Ethernet (IEEE 802.3u)

100BaseX

100BaseFX emplea la normativa 100BaseX de codificación 4B/5B sobre fibra óptica.

Cada símbolo de 5 bits se convierte en pulsos luminosos empleando codificación NRZI

Se definen dos niveles de amplitud para el haz de luz que incide en la fibra (50% - 100% potencia), de forma que un cambio en la amplitud del haz indica un **1** y la inexistencia de cambio de amplitud indica un **0**.



100BaseFX emplea fibra óptica multimodo y permite alcanzar distancias de hasta 400 metros entre un equipo y el conmutador.

4.4 IEEE 802.3 Ethernet

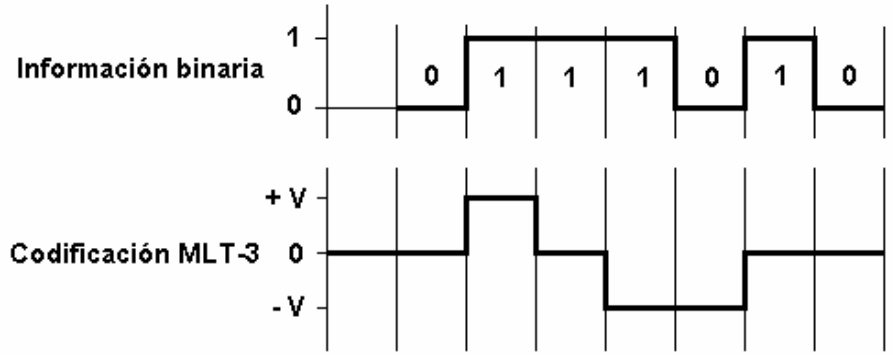
4.4.2 Fast Ethernet (IEEE 802.3u)

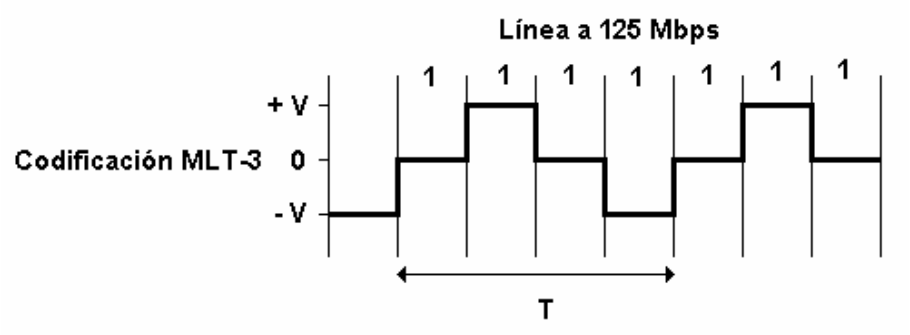
100BaseTX

100BaseTX emplea la normativa 100BaseX de codificación 4B/5B sobre cable UTP categoría 5 (máximo 100 metros).

Cada símbolo de 5 bits se convierte en pulsos eléctricos empleando la codificación MLT-3. (Si se empleara Manchester se necesitaría un cable de 125 Mhz de ancho de banda)

Se definen 3 niveles de amplitud de voltaje (-V, 0, +V). Si se transmite un bit a **1** la tensión varía aumentando o disminuyendo dependiendo de los valores anteriores. Si se transmite un bit a **0** la tensión se mantiene constante.





fo = 1/T = 1/(4 bit/125 Mbps) = 31.25 Mhz

En un par del cable UTP Cat 5 pueden transmitirse los 3 primeros armónicos de la señal.

4.4 IEEE 802.3 Ethernet

4.4.3 Gigabit Ethernet (IEEE 802.3z)

Gigabit Ethernet

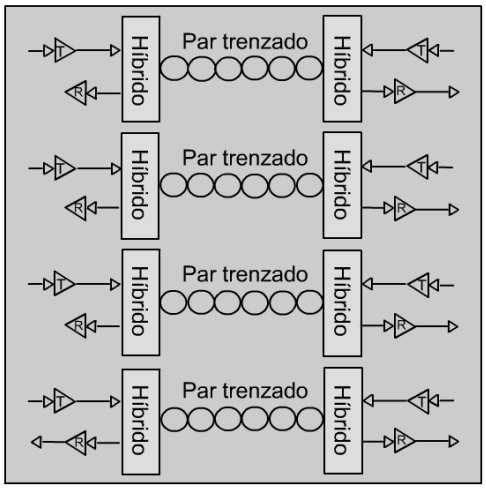
Las redes Gigabit Ethernet funcionan con conmutadores, permitiendo el modo de trabajo half-duplex (CSMA/CD) y full-duplex.

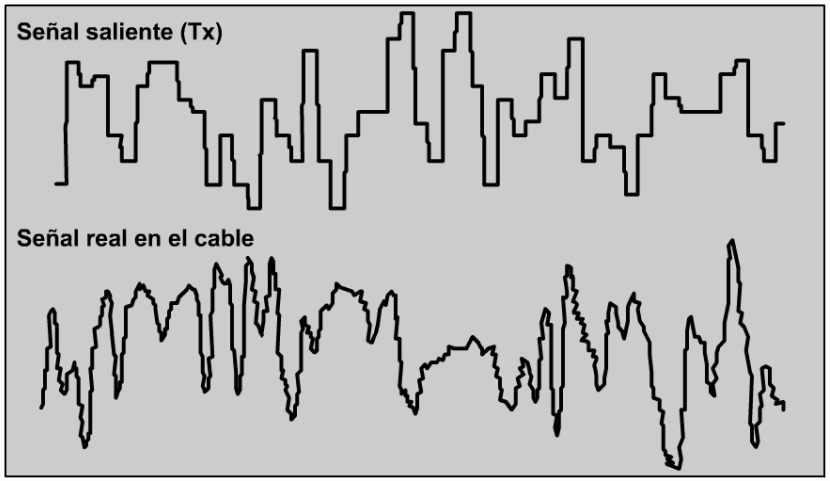
En el modo CSMA/CD, el tamaño de paquete mínimo es mayor que en Fast Ethernet, siendo de 512 bytes.

1000BaseT

Alcanzar con cable UTP categoría 5 velocidades de 1 Gbps en modo full-duplex es complejo y costoso.

1000BaseT permite alcanzar 1 Gbps a distancias de 100 metros empleando los cuatro pares de hilos para transmitir y recibir simultáneamente (cancelación de eco).





Codificación
4D-PAM5

4.4 IEEE 802.3 Ethernet

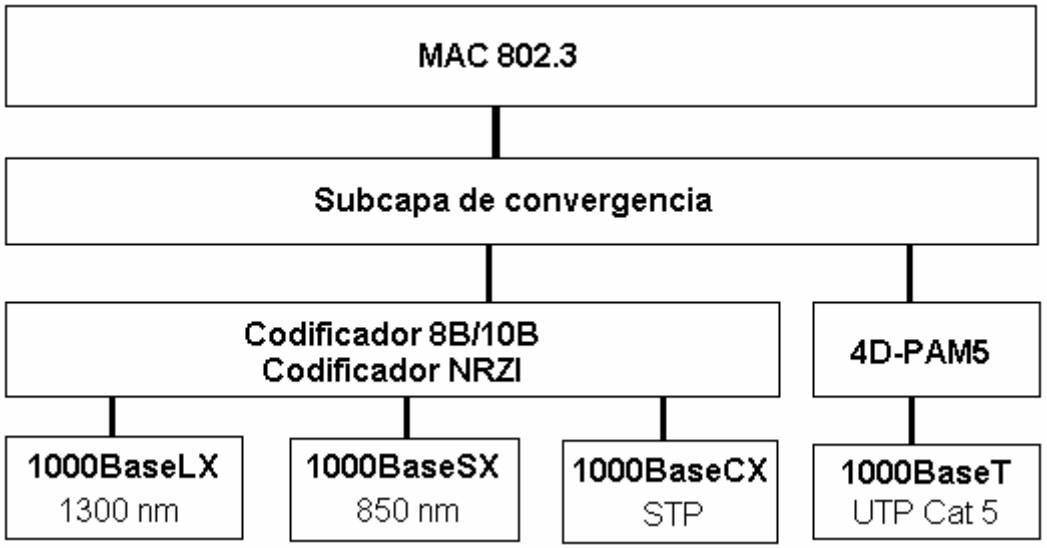
4.4.3 Gigabit Ethernet (IEEE 802.3z)

1000BaseX

La transmisión de datos a 1 Gbps por fibra óptica es menos compleja debido al enorme ancho de banda de la fibra.

Los bits del paquete Ethernet son modificados con un codificador 8B/10B, introduciendo información de sincronización para el receptor.

La señal codificada puede transmitirse por fíbra óptica o mediante cable STP (distancia máxima 25 metros)



1000BaseLX y 1000BaseSX con fibra multimodo alcanza distancias de 500 metros.

1000BaseLX permite además fibra monomodo con distancias de 5 Km.

4.4 IEEE 802.3 Ethernet

4.4.3 Gigabit Ethernet (IEEE 802.3z)

10 Gigabit Ethernet (802.3ae)

Las redes 10 Gigabit Ethernet (**10GBase-XX**) funcionan con conmutadores permitiendo **solamente** el modo de trabajo full-duplex (no existe el CSMA/CD).

El único medio físico posible es la fibra óptica pudiendo emplear el estándar de SDH para la transmisión de los paquetes Ethernet.

Empleando fibra óptica multimodo se alcanzan distancias de hasta 300 metros, pero con monomodo se consiguen hasta 40 Km.

Las aplicaciones de Ethernet hoy en día abarcan el campo LAN, MAN y WAN, pudiendo emplearlo para establecer enlaces punto a punto entre nodos de Internet.

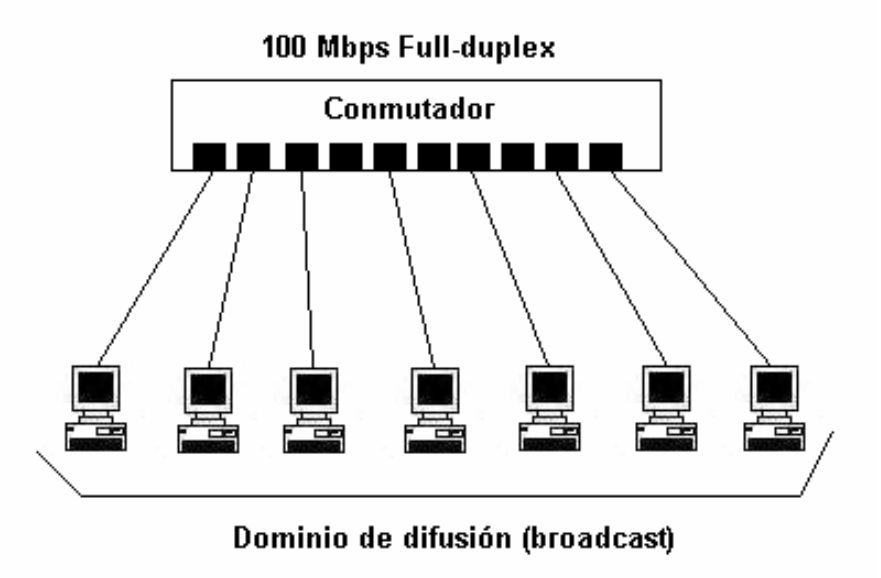
4.4 IEEE 802.3 Ethernet

4.4.4 IEEE 802.1Q. Redes de Área Local Virtuales (VLAN)

Introducción

El desarrollo de redes LAN cada vez mayores empleando conmutadores introduce problemas en cuanto a la confiabilidad de la información.

La interconexión de equipos con conmutadores elimina los dominios de colisiones, pero sigue existiendo un dominio de difusión.



Problemas de seguridad

Los paquetes de difusión son "observados" por todos los equipos del conmutador.

Cualquier equipo tiene accesibilidad física al resto.

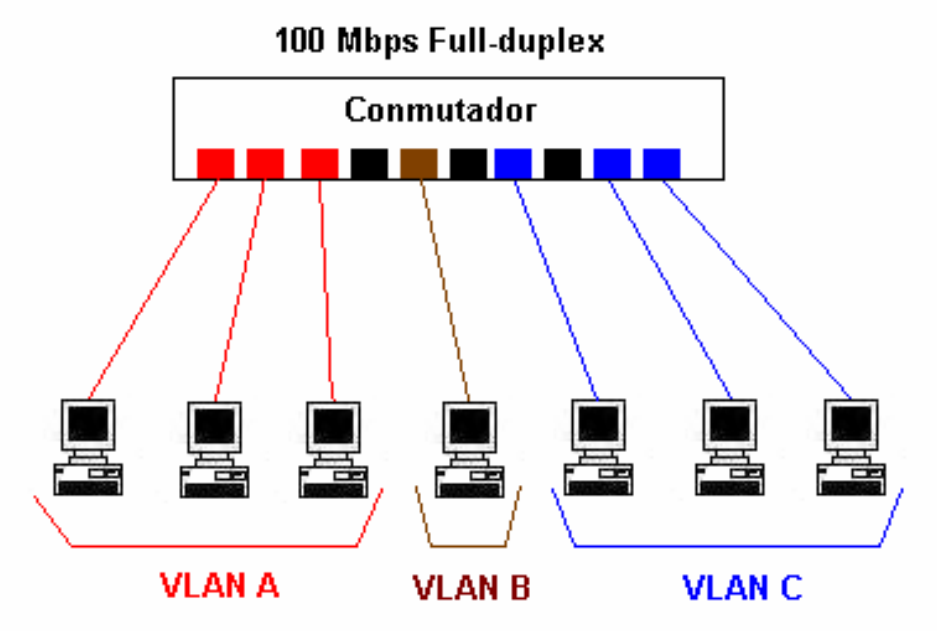
4.4 IEEE 802.3 Ethernet

4.4.4 IEEE 802.1Q. Redes de Área Local Virtuales (VLAN)

Introducción

El IEEE desarrolla una normativa (IEEE 802.1Q) para poder dividir un conmutador en varios dominios de difusión distintos.

Cada dominio de difusión independiente se denomina VLAN (Virtual Local Area Network).



4.4 IEEE 802.3 Ethernet

4.4.4 IEEE 802.1Q. Redes de Área Local Virtuales (VLAN)

IEEE 802.1Q. Funcionamiento

El funcionamiento de un conmutador VLAN es similar al de un puente, disponiendo de una tabla de reenvío.

Conmutador VLAN

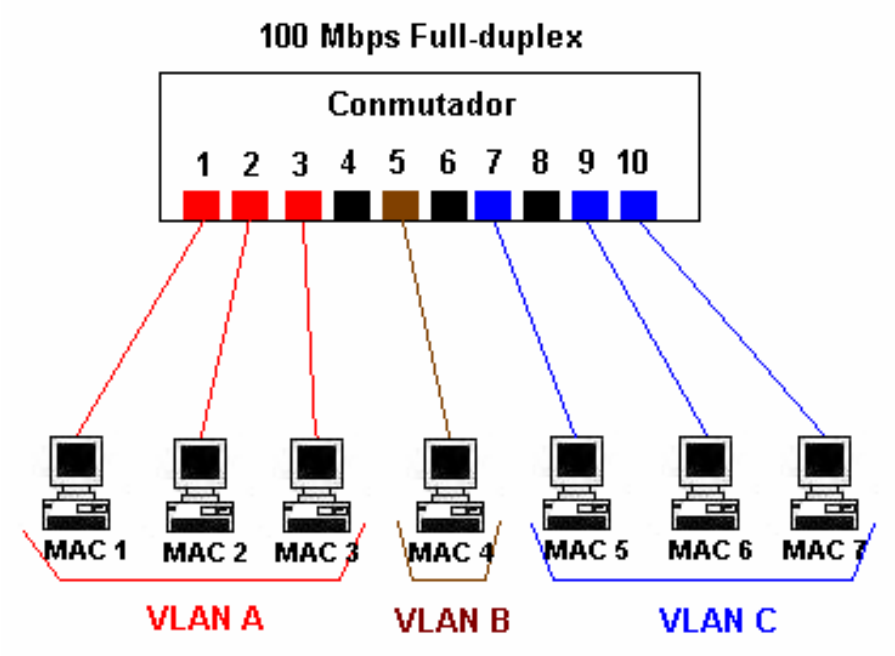


Tabla de reenvío

MAC	Id. VLAN	Puerto
1	A	1
2	A	2
3	A	3
4	B	5
5	C	7
6	C	9
7	C	10

Un conmutador VLAN reenvía las tramas de difusión de entrada en un puerto a todos los puertos etiquetados con la misma VLAN.

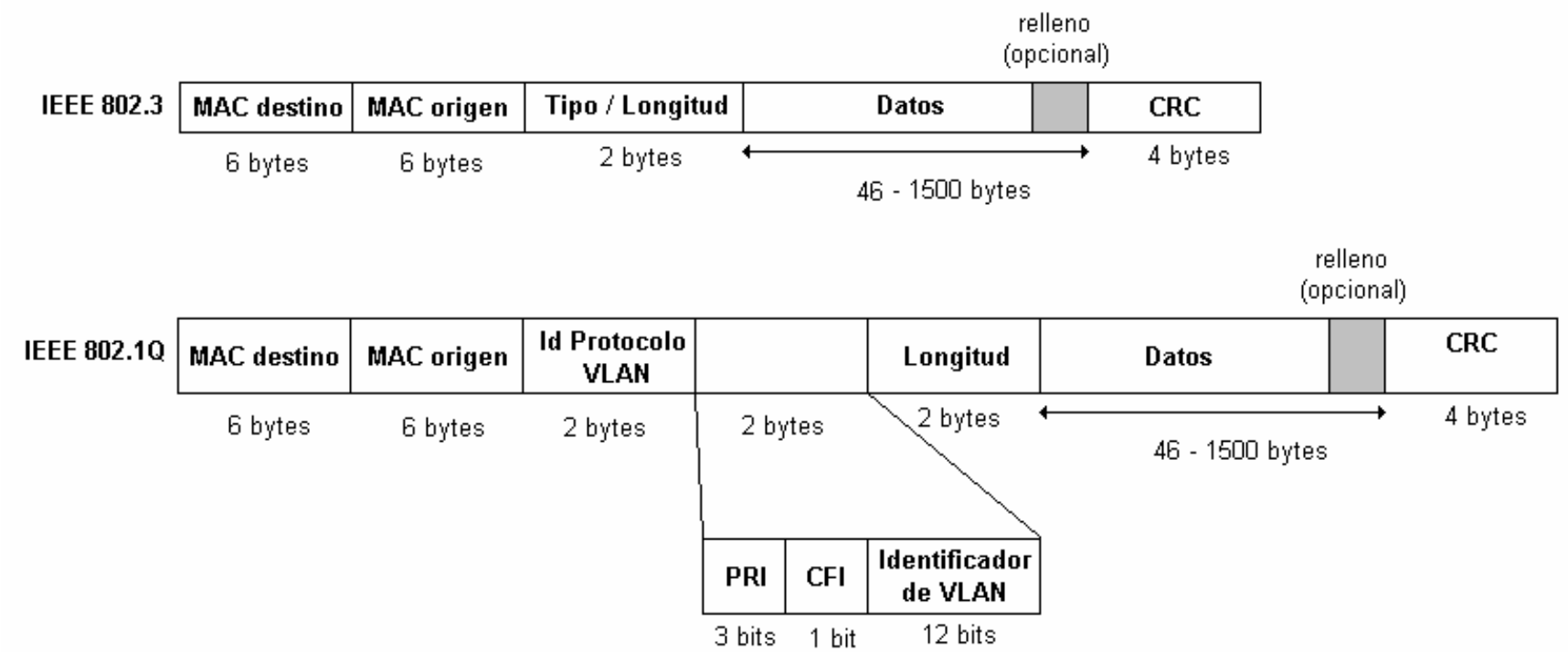
Si un equipo de una VLAN envía un paquete a una MAC que no pertenece a la misma VLAN el conmutador no lo reenvía (**Cada VLAN tiene asociada una dirección de red IP diferente para que ARP funcione**).

4.4 IEEE 802.3 Ethernet

4.4.4 IEEE 802.1Q. Redes de Área Local Virtuales (VLAN)

IEEE 802.1Q. Funcionamiento

La norma IEEE 802.1Q define un nuevo formato de paquete IEEE 802.3 cuando se emplean VLANs.



Id Protocolo VLAN: Toma el valor 0x8100 para indicar que es un paquete IEEE 802.1Q.

PRI: Bits de prioridad que pueden emplearse para conmutar unos paquetes antes que otros (voz, vídeo).

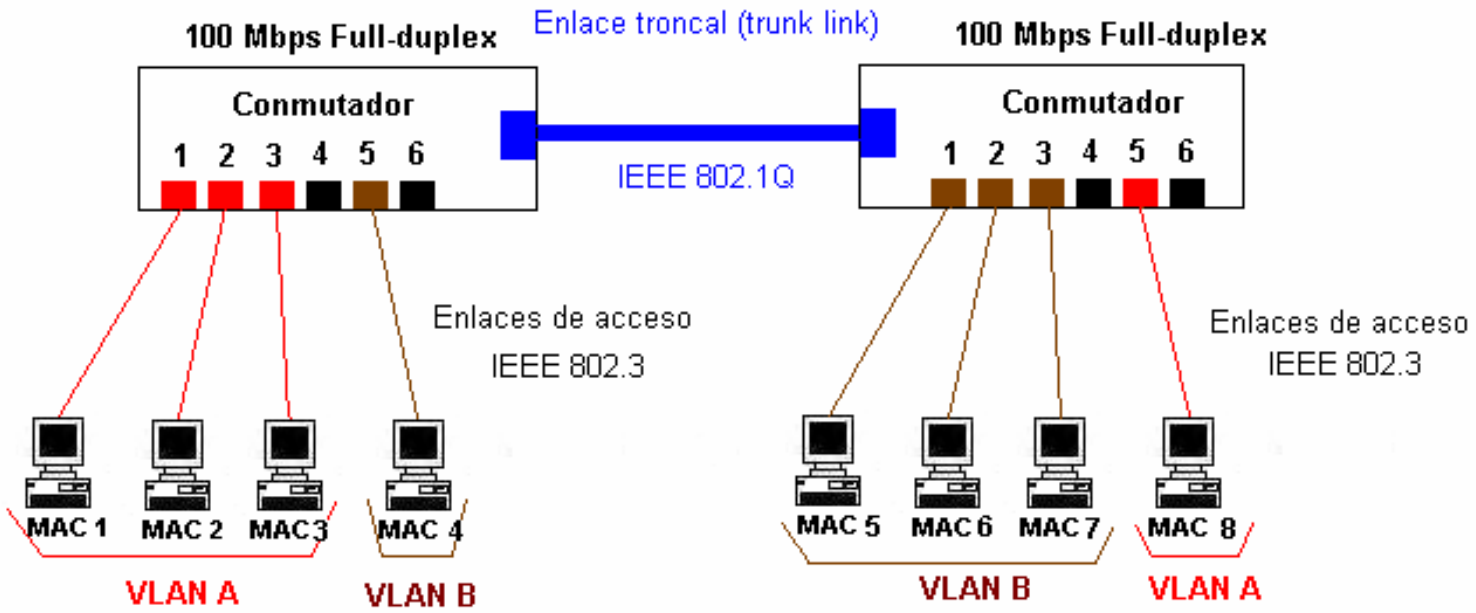
CFI: Flag para indicar que en el campo de datos hay una trama Token-Ring.

4.4 IEEE 802.3 Ethernet

4.4.4 IEEE 802.1Q. Redes de Área Local Virtuales (VLAN)

IEEE 802.1Q. Funcionamiento

El formato de trama IEEE 802.1Q se emplea cuando se interconectan conmutadores VLAN entre sí, o un router a un conmutador VLAN.



Los puertos de enlaces troncales (**trunk port**) pertenecen a varias VLAN, y a través de ellos los paquetes de diferentes VLAN se intercambian entre conmutadores distintos (debido a esto es necesario el empleo del formato IEEE 802.1Q).

4.4 IEEE 802.3 Ethernet

4.4.4 IEEE 802.1Q. Redes de Área Local Virtuales (VLAN)

IEEE 802.1Q. Funcionamiento

Un conmutador VLAN maneja de diferente forma los enlaces de acceso y los enlaces troncales.

Enlaces de acceso

En los enlaces de acceso los paquetes tienen el formato del IEEE 802.3. Cuando un paquete de un enlace de acceso se envía a un puerto troncal es necesario añadir el identificador VLAN asociado al enlace de acceso. Es decir, transformar al formato IEEE 802.1Q

Si el conmutador tiene que enviar un paquete de un puerto troncal a un puerto de acceso extrae del formato IEEE 802.1Q los datos para transformarlo en el formato IEEE 802.3.

Enlaces troncales

En los enlaces troncales los paquetes tienen el formato del IEEE 802.1Q.

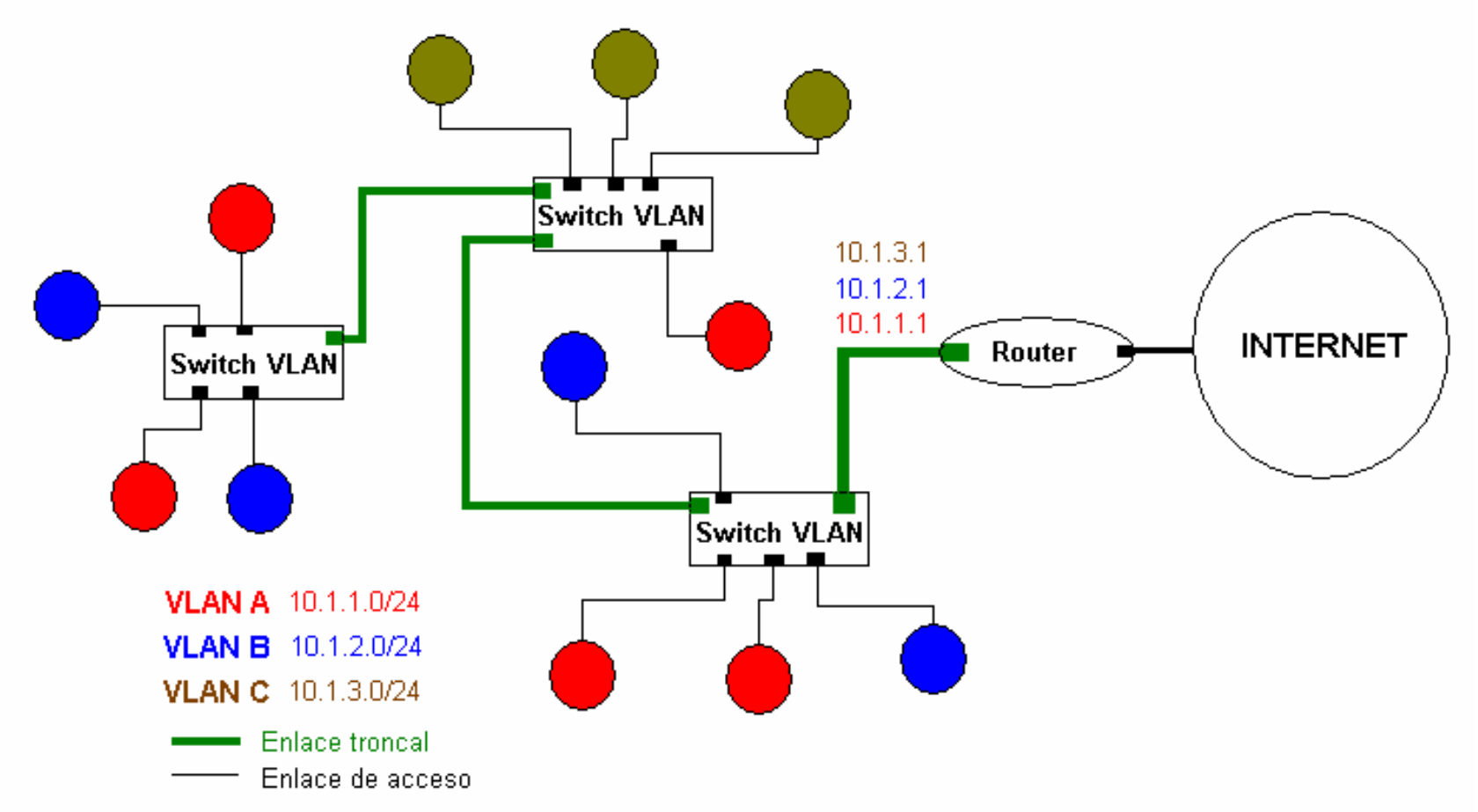
Los conmutadores VLAN emplean un protocolo denominado **GVRP (GARP VLAN Registration Protocol)** para propagar información entre los conmutadores y conocer qué VLANs hay asociadas a los puertos troncales.

Así, un conmutador, de forma automática, sabe si tiene que reenviar paquetes de una VLAN cuyo destino no está en el conmutador a otros conmutadores conectados a través de puertos troncales.

4.4 IEEE 802.3 Ethernet

4.4.4 IEEE 802.1Q. Redes de Área Local Virtuales (VLAN)

IEEE 802.1Q. Arquitectura



4.5 IEEE 802.11x. LAN Inalámbrica

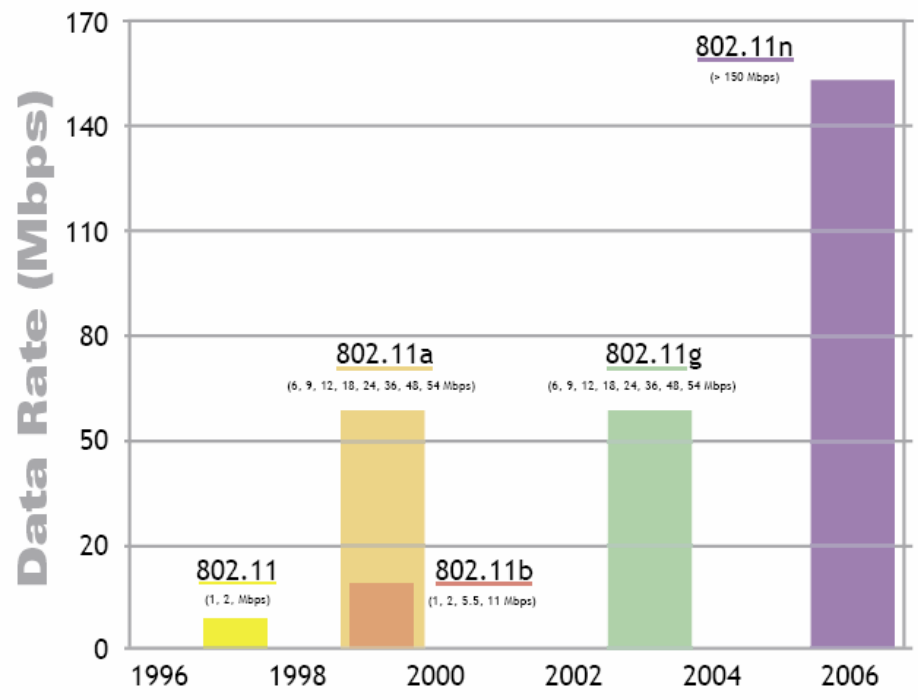
4.5.1 Introducción

Historia

Una red LAN inalámbrica es una red de área local que emplea ondas electromagnéticas como soporte físico para la comunicación de datos.

Las tecnologías de comunicación inalámbrica son más complejas y por tanto de mayor coste económico que las redes de cable.

Con el desarrollo en los años 90 de la telefonía móvil y los ordenadores portátiles se consigue una tecnología de comunicación inalámbrica con unas prestaciones competitivas a un coste razonable.



4.5 IEEE 802.11x. LAN Inalámbrica

4.5.1 Introducción

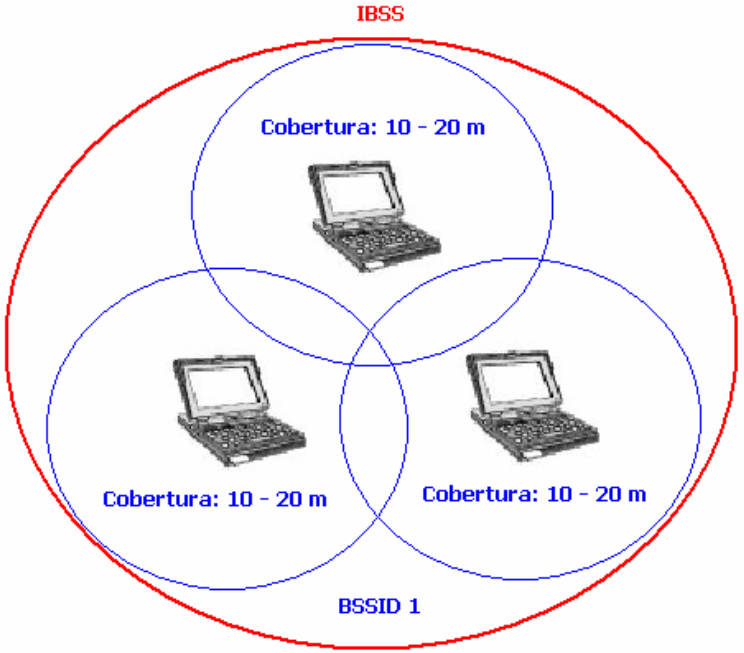
Nomenclatura

BSS (Basic Service Set): Conjunto de servicio básico. Grupo de estaciones que se comunican entre ellas.

Infraestructure BSS (**BSS**): Red inalámbrica con puntos de acceso (red de infraestructura).

Independent BSS (**IBSS**): Red inalámbrica ad-hoc.

Red Inalámbrica ad-hoc



SSID (Service Set Identifier): Identificador de un BSS. Cadena de 32 caracteres máximo.

Este identificador es el mismo para todas las estaciones de un BSS y se incluye en todos los paquetes transmitidos.

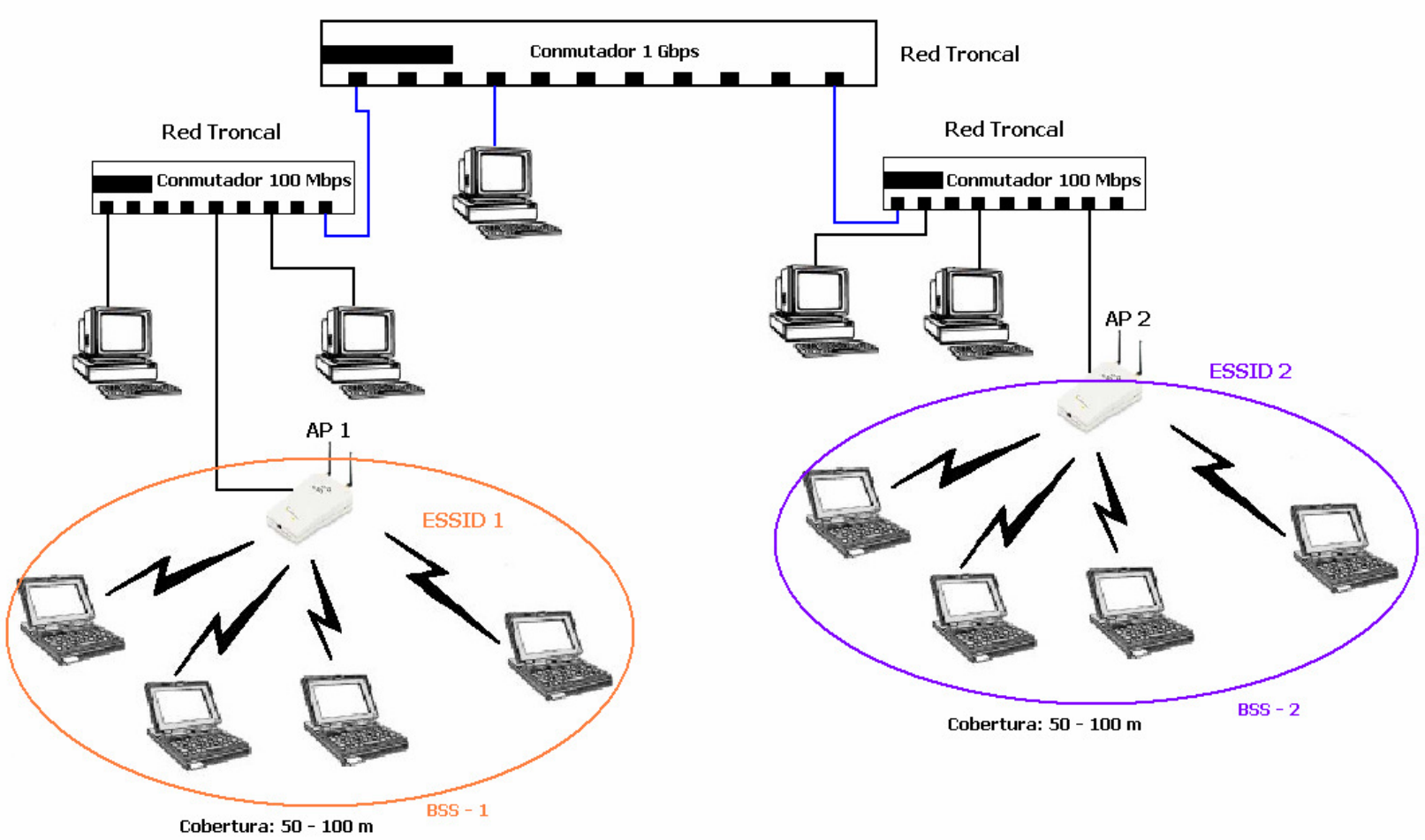
BSSID (Basic Service Set Identifier): SSID en redes ad-hoc.

ESSID (Extended Service Set Identifier): SSID en redes de infraestructura.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.1 Introducción

Red Inalámbrica de Infraestructura



AP (Access Point): Punto de Acceso. Actúa como puente entre la LAN de cable y un BSS.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.1 Introducción

Normativas de comunicación inalámbrica

El IEEE es el organismo que ha propuesto los estándares de redes LAN inalámbricas, existiendo diversas tecnologías donde destacan:

IEEE 802.11b: Comunicación inalámbrica empleando una señal portadora de 2.4 Ghz. Esta frecuencia está declarada para su uso libre, por lo que pueden existir interferencias con otros dispositivos del mercado.

Realmente no se emplea un única portadora, si no que existen 13 portadoras entre los 2.4 y 2.5 GHz. Cada una de estas portadoras define un canal, de forma que todos los equipos que pertenecen a un BSS deben emplear la misma portadora.

El AP debe configurarse para emplear una canal que no tenga interferencias en la zona. Así, es necesaria una política de gestión de canales cuando se utilizan varios AP.

La norma IEEE 802.11b emplea modulación de múltiples niveles (amplitud y fase) en cada canal, permitiendo alcanzar velocidades de 1, 2, 5.5 y 11 Mbps.

IEEE 802.11g: Comunicación inalámbrica empleando una señal portadora de 2.4 Ghz. Con esta normativa se consigue alcanzar velocidades de hasta 54 Mbps.

IEEE 802.11 Super G: Empleando la misma portadora de 2.4 GHz permite alcanzar 108 Mbps.

IEEE 802.11n: Permite emplear la portadora de 2.4 GHz y una de 5 GHz consiguiendo velocidades de 600 Mbps.

La velocidad de transmisión con wireless no es fija, le afecta el ruido del entorno de trabajo.

4.5 IEEE 802.11x. LAN Inalámbrica

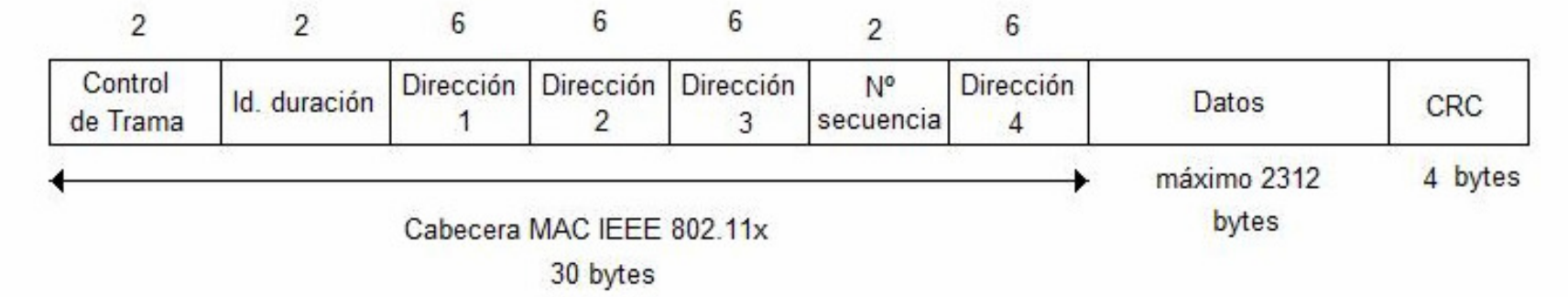
4.5.2 Acceso al medio

Características

Las redes LAN 802.11 se caracterizan por presentar una elevada tasa de error en el medio físico. Este problema condiciona cuál es el mecanismo de reparto del uso del medio físico.

La elevada tasa de error en el medio introduce dos necesidades:

1. Tamaño de paquete pequeño. Es necesario un tamaño de paquete más pequeño, pues los errores provocarán reenvíos más pequeños de datos. Los paquetes del nivel superior (LLC) serán fragmentados por el protocolo MAC del 802.11. La norma 802.11 especifica un tamaño máximo de datos de 2312 bytes.



2. Protocolo MAC 802.11 confirmado. Debido a la elevada tasa de error, es necesario que el protocolo de control de acceso al medio sea capaz de confirmar los paquetes transmitidos en el medio inalámbrico. Así, los reenvíos necesarios se realizarán rápidamente.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.2 Acceso al medio

El protocolo MAC del 802.11 distingue entre dos modos de funcionamiento para el uso del medio físico:

1. **DCF (Función de coordinación distribuida)**

   Empleadas en wireless de infraestructura y ad-hoc.

2. **PCF (Función de coordinación centralizada)**

   Empleadas en wireless de infraestructura, donde el AP controla el acceso al medio compartido.

DCF – Función de coordinación distribuida

En el modo DCF cada estación compite por el uso del medio físico. El mecanismo de reparto empleado es el **CSMA/CA** (Acceso al medio con detección de portadora y evitación de colisiones).

Las estaciones comprueban si el medio físico está libre detectando una señal denominada **CCA** (Estimación de desocupación del canal). Esta señal la transmiten los dispositivos en escucha en la red.

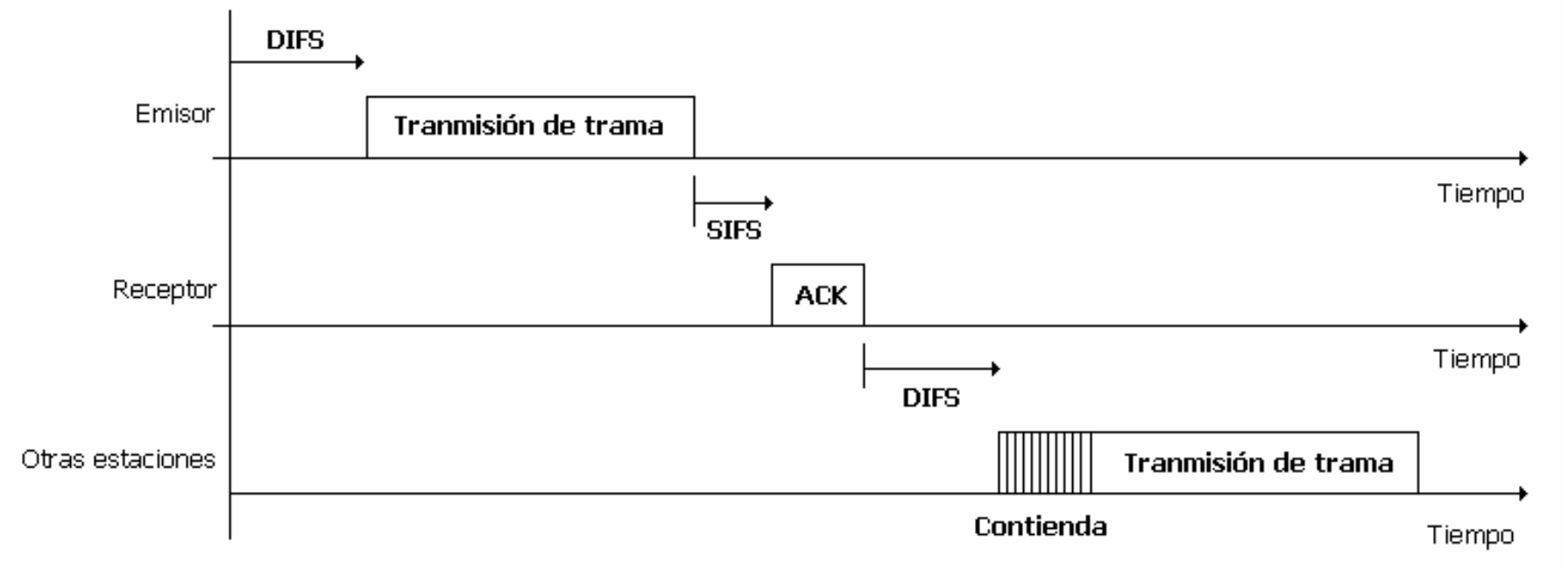
Si una estación encuentra el medio libre durante un tiempo denominado DIFS (espacio de tiempo entre la transmisión de tramas en DCF), entonces transmitirá el paquete de datos. Si recibe una confirmación del envío se considerará que la transmisión ha sido correcta.

Si la estación detecta que el medio físico está ocupado, espera a que se detecte de nuevo el medio físico libre durante un tiempo DIFS. Al expirar este tiempo, el equipo entra en una situación de contienda esperando un tiempo aleatorio. Al finalizar el tiempo aleatorio, si el medio físico está libre transmitirá, y si no esperará un nuevo periodo de contienda.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.2 Acceso al medio

DCF – Función de coordinación distribuida



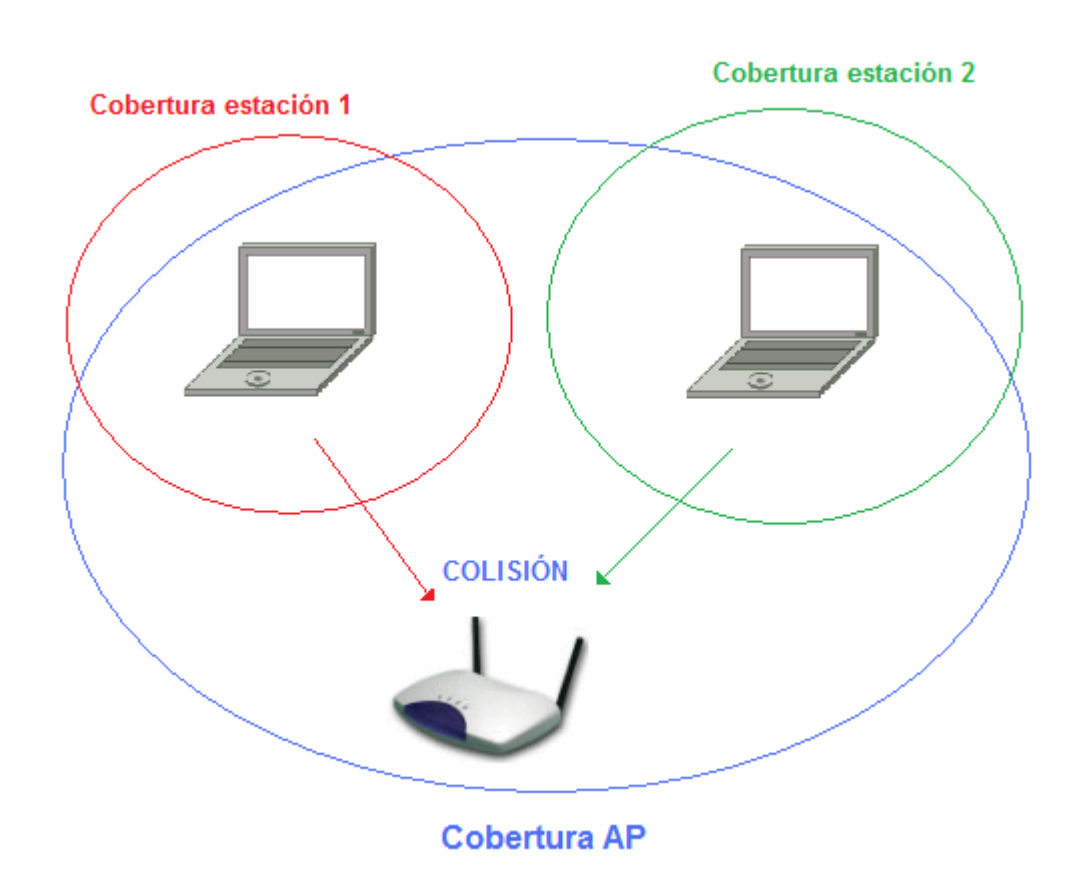
CSMA/CA

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.2 Acceso al medio

DCF – Función de coordinación distribuida

El problema de la estación oculta



4.5 IEEE 802.11x. LAN Inalámbrica

4.5.2 Acceso al medio

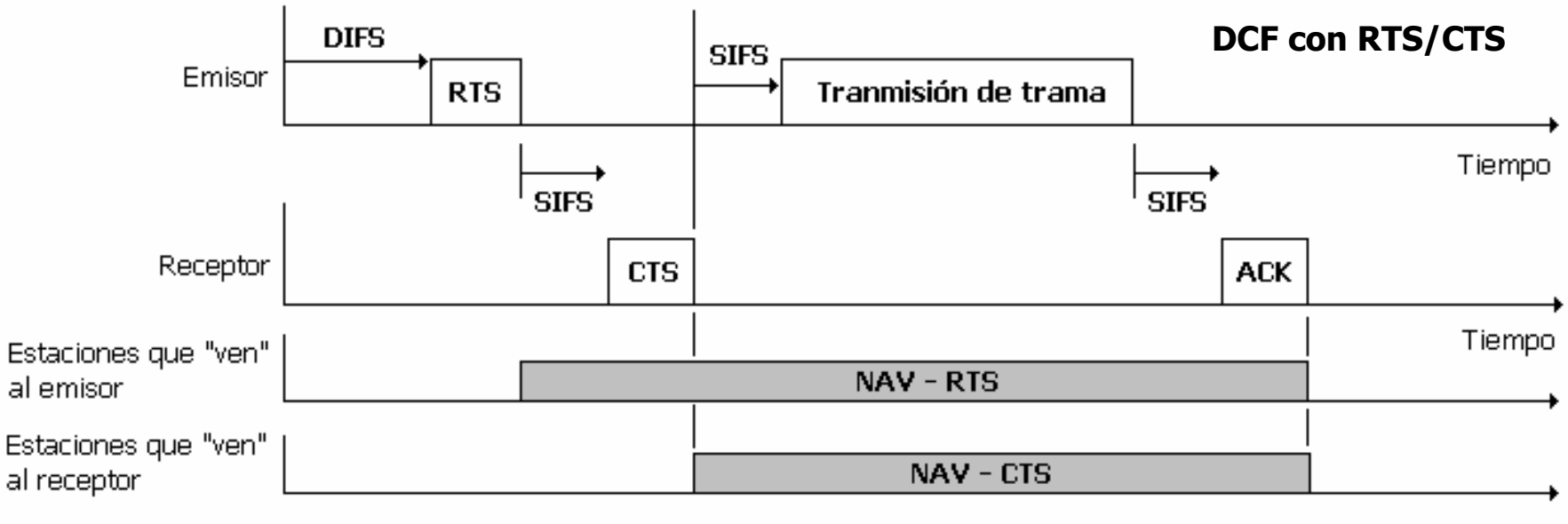
DCF – Función de coordinación distribuida

Variante DCF con RTS/CTS

Para evitar el problema de la estación oculta (un AP detecta dos estaciones, pero las estaciones no se detectan entre ellas) se introduce un mecanismo de reserva de la red.

La estación que transmite envía un paquete de tipo **RTS** que indica a las demás estaciones "visibles" el tiempo durante el que no pueden transmitir (**NAV – Vector de reserva de red**).

El receptor confirma el paquete RTS con un paquete de tipo **CTS** que indica a las demás estaciones "visibles" el tiempo durante el que no pueden transmitir.



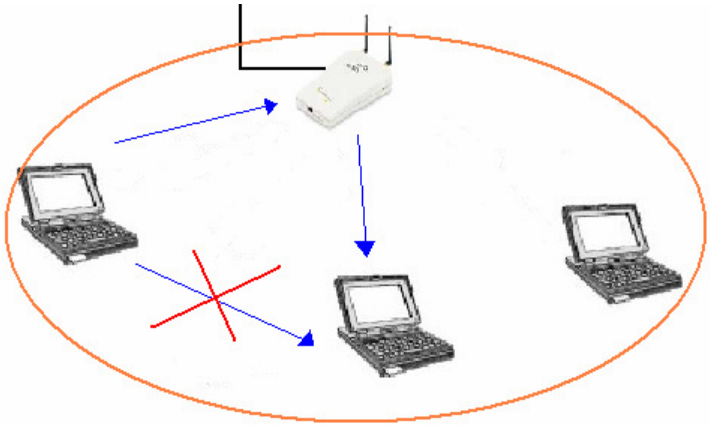
4.5 IEEE 802.11x. LAN Inalámbrica

4.5.2 Acceso al medio

PCF – Función de coordinación centralizada

Este modo de funcionamiento está definido sólo para las redes de infraestructura, pues precisa de la existencia de un punto de acceso **AP**.

Cuando existe un AP todas las comunicaciones se realizan a través de él. Es decir, si una estación quiere transmitir un paquete a otra estación, se enviará la información al AP y éste lo reenviará a la estación destino.



El AP divide el tiempo de transmisión en la red en celdas de tiempo denominadas **supertramas**.

Cada supertrama se divide en dos periodos de tiempo:

Un periodo en el que no hay colisiones y el AP controla el uso del medio (selección de equipos a transmitir)

Un periodo de contienda donde se emplea CSMA/CA o CSMA/CA con RTS/CTS.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.2 Acceso al medio

PCF – Función de coordinación centralizada

Periodo de no colisión

En el periodo de no colisión, el AP envía a una estación un paquete solicitando que le envíe un bloque de datos.

Cuando el bloque de datos es recibido por el AP, envía otra solicitud a otra estación.

Este proceso finaliza cuando el AP envía un paquete de finalización del periodo libre de colisiones. El resto de tiempo de la supertrama emplea la contienda para transmitir información entre el AP y las estaciones.

Durante el periodo de no colisión se realizan también las funciones de gestión de la red wireless, que básicamente son **añadir/eliminar un equipo de la red wireless**.

Para añadir un equipo en la red (registrar un equipo en el AP) el AP envía cada cierto tiempo un paquete denominada **trama de baliza o señalización** (beacon frame).

Cuando una estación recibe una trama de invitación a registrarse contesta, pudiendo el AP aceptarla o no (filtrado por MAC).

Si una estación es registrada puede aplicarse un proceso adicional de autenticación (opcional pero muy recomendable) antes de que sea permitido el envío de paquetes de datos.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.3 Seguridad en redes Wi-Fi™

Wi-Fi Alliance

Wi-Fi Alliance es una asociación de fabricantes de tecnología de red inalámbrica basada en la norma IEEE 802.11x (Cisco, Microsoft, Nokia, Intel, Dell, etc). http://www.wi-fi.org/

Esta asociación ha desarrollado la marca Wi-Fi™ para identificar sistemas de comunicación LAN inalámbricos que son compatibles, pues emplean las normas del IEEE 802.11x.

Uno de los campos de normalización de la Wi-Fi Alliance es la seguridad en redes Wi-Fi.

Principios de seguridad

La seguridad en una red Wi-Fi se fundamenta en dos principios:

Autenticación: Una estación (cliente) debe identificarse como un usuario autorizado de la red Wi-Fi.

Existen diferentes mecanismos de autenticación, cada uno de ellos con un nivel inherente de seguridad.

Integridad de la información: La información debe transmitirse cifrada para evitar espías (sniffers).

Existen diferentes mecanismos de cifrado en redes Wi-Fi, desarrollados en base a vulnerabilidades de seguridad que se han ido detectando.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.3 Seguridad en redes Wi-Fi™

Autenticación

Cuando una estación desea conectarse a una red Wi-Fi inicia un proceso de registro en el AP de la red.

Para realizar el registro, la estación debe conocer el SSID de la red. Aquí es posible introducir un mecanismo de seguridad.

Los AP transmiten cada cierto tiempo un paquete de señalización indicando cuál es su SSID e invitando a equipos a añadirse. Esta acción puede deshabilitarse en el AP, de forma que los equipos no "ven" la red y sólo pueden conectarse si conocen el SSID.

Si la estación conoce el SSID puede registrarse en el AP. Un nivel de seguridad adicional consiste en permitir solamente el registro de estaciones con una dirección MAC almacenada en una lista del AP.

Finalizado el proceso de registro, es posible llevar a cabo un proceso de autenticación (opcional).

En general, los AP no suelen realizar este control de acceso en el registro de la estación, pues la flexibilidad de los sistemas Wi-Fi radica en que cualquier estación pueda registrarse. El proceso de control de acceso suele llevarse a cabo en la autenticación.

Sólo en sistemas muy controlados (redes LAN personales o de hogar, redes LAN corporativas con pocos equipos) el sistema de control de acceso por dirección MAC es empleado.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.3 Seguridad en redes Wi-Fi™

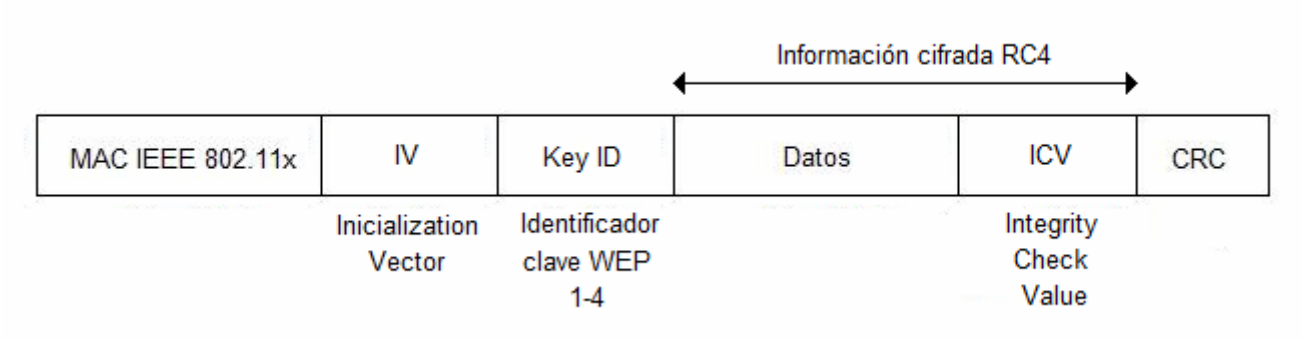
Autenticación y cifrado WEP

WEP (Wired Equivalente Privacy) fue el primer protocolo de encriptación empleado en el estándar IEEE 802.11x hacia 1999 y que se basa en el algoritmo de cifrado RC4.

El funcionamiento de WEP está basado en el conocimiento de una misma clave secreta por parte de la estación y el AP (PSK – Pre-Shared Key)

El mecanismo de autenticación consiste en que la estación proporcione una información cifrada al AP con la clave secreta. Si la información es cifrada correctamente el AP permite la conexión de la estación a la red Wi-Fi.

El objetivo de WEP no es tanto la autenticación como el cifrado de todos los paquetes intercambiados entre la estación y el AP.



La seguridad de WEP se fundamenta en una clave secreta de 64 o 128 bits, pero que no es suficiente. Actualmente, WEP está obsoleto pues es posible descubrir cualquier clave en unos pocos minutos con el software apropiado.

4.5 IEEE 802.11x. LAN Inalámbrica

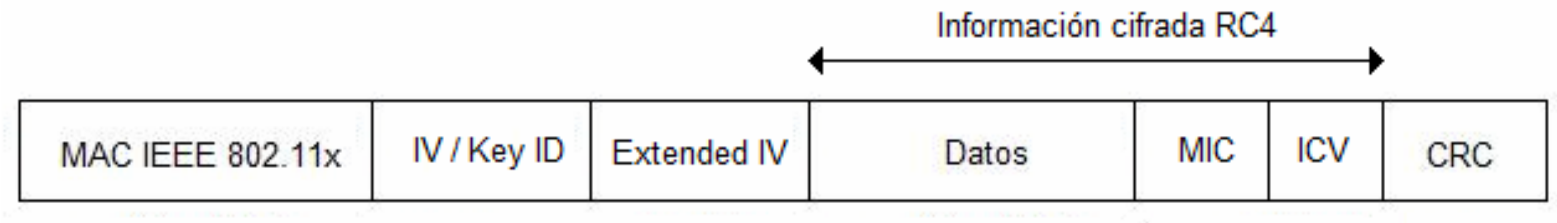
4.5.3 Seguridad en redes Wi-Fi™

Autenticación y cifrado WPA

WPA (Wi-Fi Protected Access) fue desarrollado por la Wi-Fi Alliance en 2003 para sustituir a WEP.

La principal vulnerabilidad de WEP es la capacidad de obtener la clave de cifrado. Así, WPA mantiene el mismo algoritmo de cifrado de WEP (RC4), pero introduce el mecanismo TKIP (*Temporal Key Integrity Protocol*).

TKIP modifica la clave de cifrado entre el cliente y el AP cada cierto tiempo, además de introducir un mecanismo de verificación de la integridad de los paquetes cifrados (MIC – *Message Integrity Code*).



Al aumentar el tamaño del campo IV, proporciona una mayor entropía (aleatoriedad) en el proceso de cifrado, y unido a la variación de la clave de cifrado, una mayor seguridad.

En la actualidad, el cifrado WPA basado en TKIP se ha roto. Por tanto, no se seguro emplearlo aunque dado que se requiere unos 15 minutos para descubrir una clave, puede configurarse TKIP para cambiar claves cada 2 minutos o menos (esto puede afectar al rendimiento). En septiembre 2009, investigadores de la Universidad de Hiroshima han conseguido romper un cifrado WPA en 1 minuto.

Otra solución es emplear WPA2.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.3 Seguridad en redes Wi-Fi™

Autenticación y cifrado WPA

En el procedimiento de autenticación, WPA admite dos mecanismos:

WPA–Personal o WPA-PSK: En este mecanismo, cliente y AP disponen de una clave de acceso prefijada para permitir el acceso a la red inalámbrica (mismo mecanismo de WEP). La clave PSK inicial es modificada posteriormente en el cifrado al emplear TKIP.

Al emplear este mecanismo de autenticación, la vulnerabilidad principal es la fortaleza de la clave prefijada ante ataque por fuerza bruta.

Debido a la vulnerabilidad de WPA indicada anteriormente, este mecanismo de autenticación sólo es asumible en entornos no críticos (redes personales o de hogar) .

WPA–Enterprise: En este mecanismo, cada cliente autentica su acceso al AP empleando un servidor de autenticación (RADIUS). La gestión de la autenticación se realiza empleando el estándar IEEE 802.1x.

La base del funcionamiento del 802.1x es el protocolo de autenticación EAP (*Extensible Authentication Protocol*).

EAP se emplea en otros entornos, como las redes VPN, y permite realizar la autenticación de un cliente contra un servidor de autenticación (en general suele emplearse Radius).

El potencial de EAP es que permite múltiples mecanismos de autenticación (CHAP, Kerberos, certificados de seguridad, autenticación con clave pública, etc.)

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.3 Seguridad en redes Wi-Fi™

Autenticación y cifrado WPA

WPA–Enterprise

Los mecanismos de autenticación empleados más frecuentemente en WPA son tres:

EAP/TLS: Autenticación basada en un certificado de servidor y cliente (requiere una infraestructura de clave públicas por parte de la entidad gestora del AP).

EAP/TTLS o PEAP: Autenticación basada en un certificado de servidor. El cliente se valida con un nombre de usuario y contraseña en un servidor RADIUS. (Ejemplo: acceso Wi-Fi en la Universidad de Alicante).

LEAP (*Lightweight* EAP): Autenticación propietaria de Cisco Systems y que no emplea certificados de seguridad. La autenticación de un cliente se realiza empleando alguno de los mecanismos de autenticación que soporte un servidor RADIUS donde se almacenan los usuarios autorizados. Uno de los mecanismos que soporta RADIUS es CHAP, que permite el intercambio de la contraseña del usuario cifrada.

El objetivo de estos tres mecanismos es proporcionar a un usuario autorizado la denominada MK – *Master Key*, clave primaria con la que se inicia el mecanismo de cifrado TKIP.

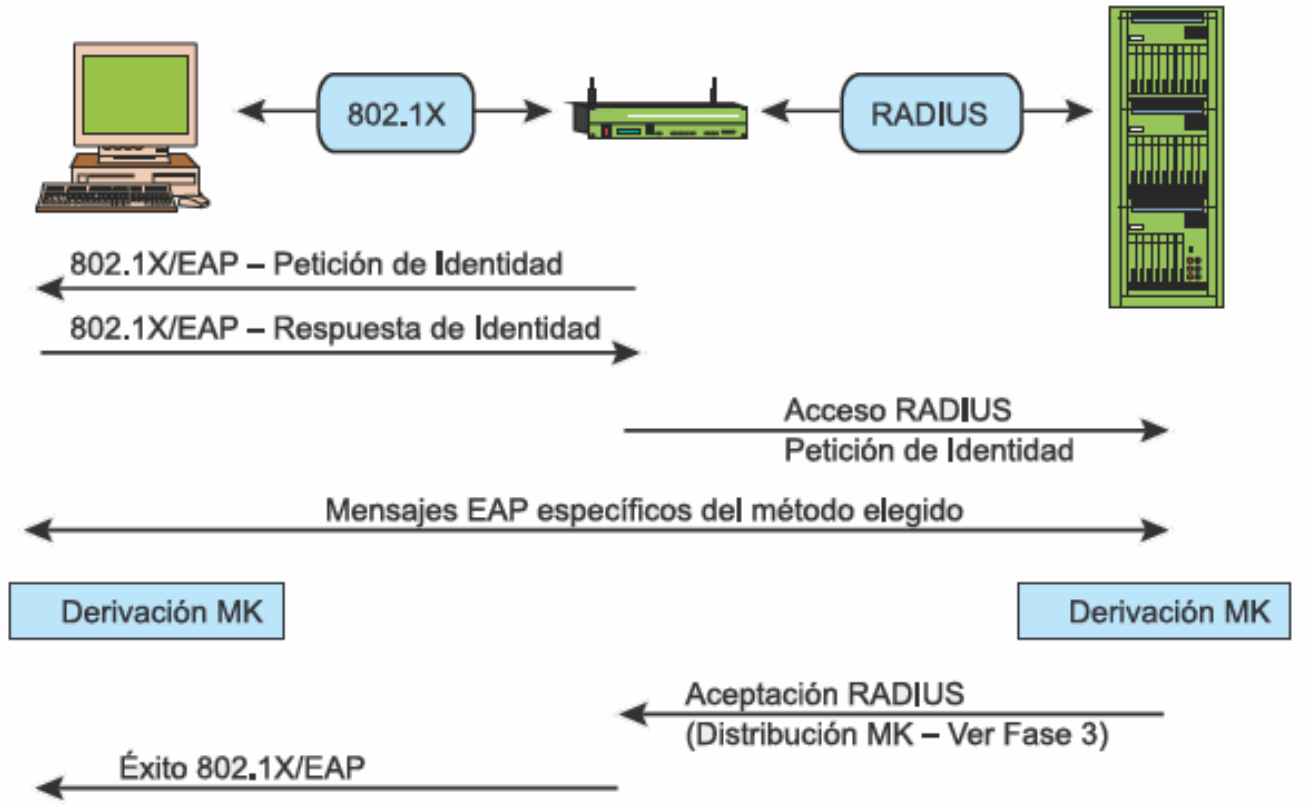
4.5 IEEE 802.11x. LAN Inalámbrica

4.5.3 Seguridad en redes Wi-Fi™

Autenticación y cifrado WPA

WPA–Enterprise

Esquema del mecanismo de autenticación 802.1x



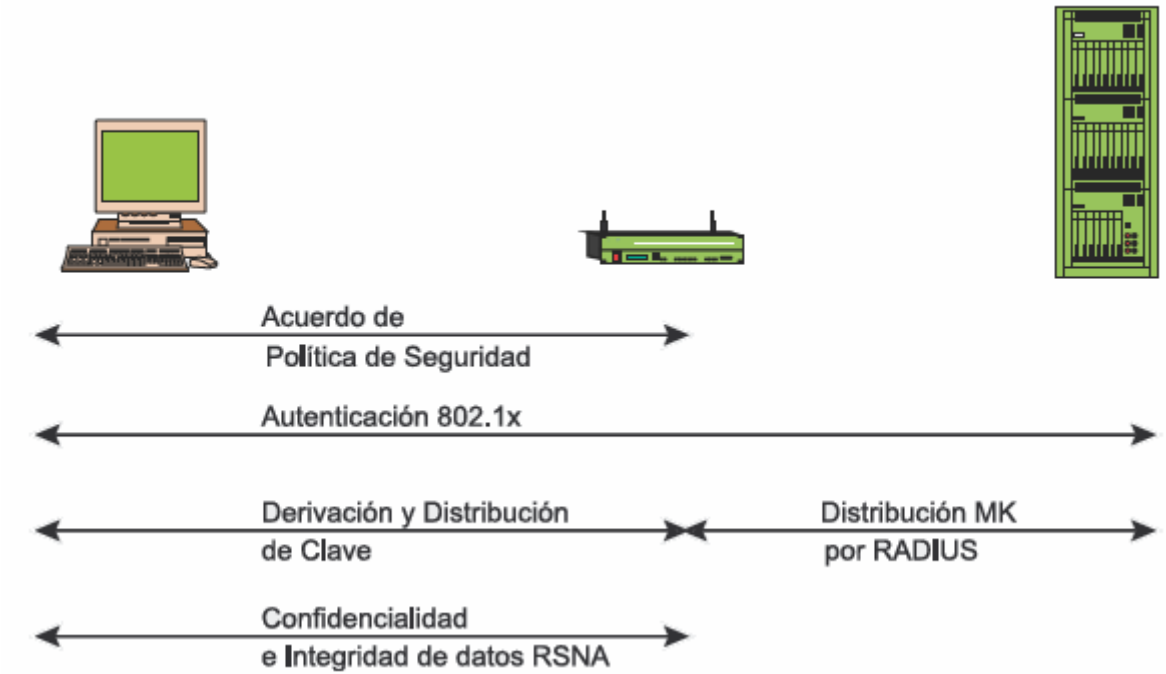
4.5 IEEE 802.11x. LAN Inalámbrica

4.5.3 Seguridad en redes Wi-Fi™

IEEE 802.11i – WPA2™

Durante la implantación de WPA para superar los críticos problemas de seguridad de WEP, la Wi-Fi Alliance estaba desarrollando un sistema de seguridad Wi-Fi que completa en 2004 en la normativa IEEE 802.11i o WPA2 como marca comercial.

WPA2 introduce un paradigma de seguridad Wi-Fi, basado en toda la tecnología desarrollada para WPA.



RSNA – Robust Security Network Association. Proporciona un sistema con integridad y confidencialidad.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.3 Seguridad en redes Wi-Fi™

IEEE 802.11i – WPA2™

WPA2 no introduce variaciones en los mecanismos de autenticación empleados en WPA (se denominan WPA2-Personal y WPA2-Enterprise), pero sí permite mejorar la seguridad del cifrado.

WPA2 permite emplear, además de TKIP, otro mecanismo de cifrado denominado **AES** (Advanced Encryption Standard).

AES es un estándar de cifrado del NIST (Instituto Nacional de Estándares de EEUU) adoptado como mecanismo estándar de cifrado por el gobierno de EEUU.

AES emplea claves de cifrado de 128 bits cuando se emplea en WPA2. En la actualidad, este esquema de cifrado no se ha roto y por tanto es el más recomendable para accesos Wi-Fi.