

Capa de enlace

Arquitectura IEEE 802

Recuerda que en la arquitectura IEE 802, el nivel de enlace se divide en dos subcapas:

- LLC: se encarga de las funciones comunes de la capa independientemente del medio físico usado (ej: control de errores o de flujo). Sus funciones han sido definidas por el subgrupo 802.2.
- MAC: se encarga del acceso al medio.

En esta presentación nos ocuparemos de algunas de las funciones definidas en la subcapa MAC. Aunque haremos referencia a otros protocolos, se describirá en mayor detalle el protocolo Ethernet 802.3.

Vamos a ello



Capa de enlace

Dominios de colisión y de broadcast

Un dominio de colisión es el conjunto de segmentos de cable que interconectan una red donde, al transmitir dos o más estaciones, puede producirse una colisión.

Ejemplos de dominios de colisión son:

- Una red de cable coaxial aislada.
- Una red que utiliza un concentrador (Hub).
- Dos conjuntos de ordenadores unidos por un repetidor.
- Dos conjuntos de ordenadores unidos cada uno a un concentrador, y cada concentrador conectado al otro por un cable.



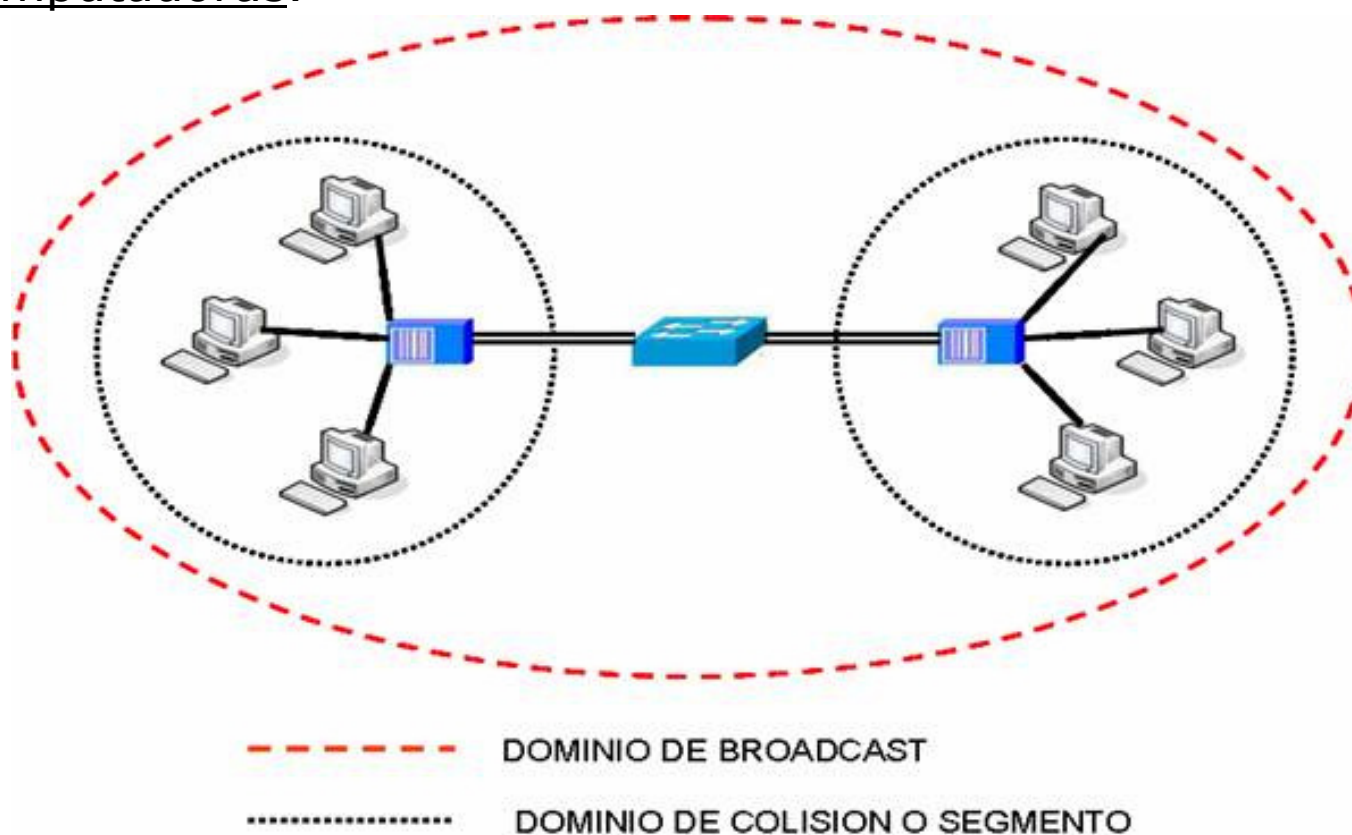
Los conmutadores evitan las colisiones entre equipos (un dominio de colisión es cada puerto del conmutador).

Los enrutadores no reenvían las tramas de enlace que reciben, con lo que separan dominios de colisión.

Capa de enlace

Dominios de colisión y de broadcast

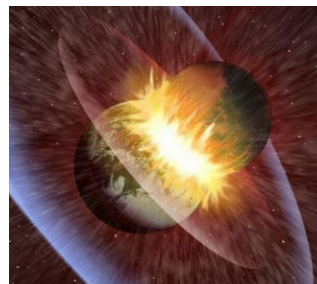
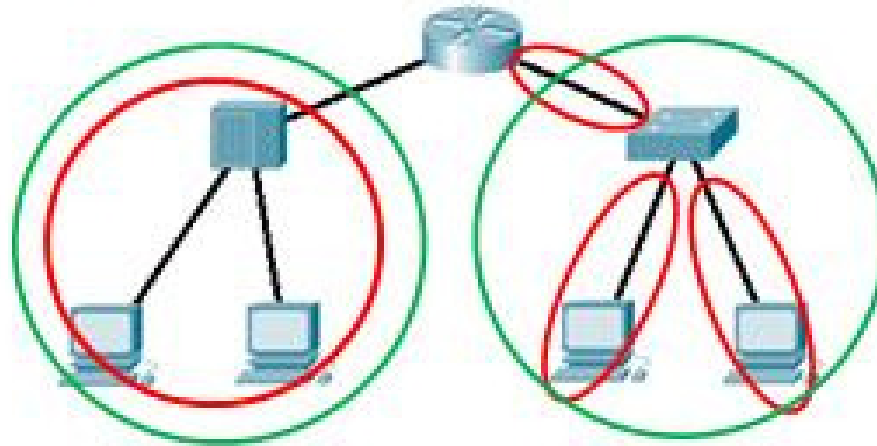
Entendemos por dominio de difusión, más conocido como dominio *broadcast* en inglés, un segmento lógico de una red de computadoras.



Capa de enlace

Dominios de colisión y de broadcast

COLLISION DOMAIN – BROADCAST DOMAIN



Capa de enlace

Compartición del medio



Al principio del curso vimos 2 tipos de redes:

- Redes de difusión.
- Redes punto a punto. No existen colisiones.

En las redes de difusión, cuyo medio de transmisión está compartido por diferentes dispositivos, hace falta un mecanismo para que cada equipo pueda usar el medio durante un tiempo suficiente.

Los protocolos se tienen que encargar de resolver los conflictos de acceso al medio.

Por esta razón, la capa de enlace de redes de difusión es más compleja que la de las redes punto a punto



Capa de enlace

Gestión de un dominio de colisión

Hay un solo canal disponible para todas las comunicaciones. Todas las estaciones pueden recibir y transmitir por él.

Si dos estaciones transmiten simultáneamente, ocurre una colisión.

Detección de portadora. Se trata de la capacidad de las estaciones transmisoras para detectar si en un determinado momento el canal está siendo ocupado por otra transmisión.

Detección de colisión. Se trata de la capacidad de las estaciones para determinar si se ha producido una colisión en el medio.

Capa de enlace

ALOHA. Precedentes de Ethernet (802.3)

Aloha. Elaborado en el 1970 por la Universidad de Hawaii.

Se manda una trama y se espera una confirmación.

Si no llega la confirmación se supone que ha habido una colisión y se retransmite la trama. Uso temporizadores.

La trama retransmitida podría colisionar otra vez.

Poco eficiente.



Se mejora repartiendo el tiempo en slots. Disminuye la probabilidad de colisión.

No comprueba si el canal está libre antes de transmitir.



Capa de enlace


CSMA. Precedentes de Ethernet (802.3)

En CSMA (Carrier Sense Multiple Access). Escucha el canal antes de empezar a transmitir, para comprobar que no se está en uso.

CSMA-persistente: comprueba continuamente si el canal está libre. En cuanto detecta disponibilidad, envía. Si varios dispositivos están esperando disponibilidad del canal para realizar un envío, enviarán al mismo tiempo y se producirá colisión.

CSMA no persistente: si al intentar transmitir está ocupado, espera un tiempo aleatorio antes de intentar transmisión otra vez. Reduce las colisiones, pero aumenta el retardo con de bajo tráfico.

CSMA-CD (Collision detection). Las estaciones son capaces de detectar una colisión después de haber empezado a transmitir. Si esto ocurre, abortan la transmisión y vuelven a intentarlo después de un tiempo aleatorio.



Capa de enlace

CSMA. Precedentes de Ethernet (802.3)

CSMA-CA (Collision Avoidance). Utilizan las redes WIFI.
Se verá más adelante...



Capa de enlace

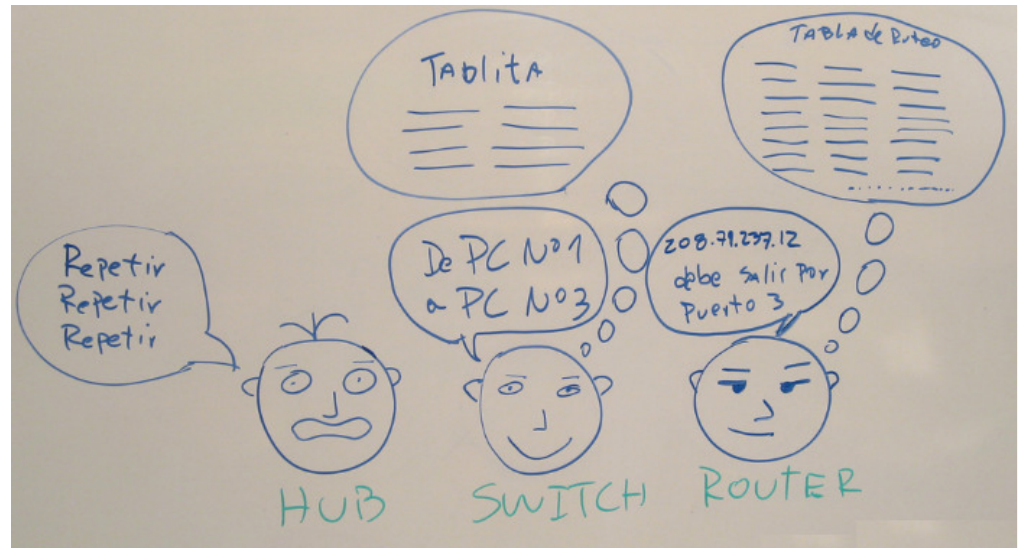
Ethernet (802.3)

Ethernet se basa sobre el CSMA/CD 1 persistente.

En las redes modernas se utilizan dispositivos que se llaman conmutadores de LAN (conocidos como Switch) que permiten la comunicación directa entre 2 estaciones conectadas a la LAN.

Utilizando los switch la LAN funciona como red punto a punto, aún si hay casos concretos en los que se parece a una red de difusión.

Si usamos concentradores (Hub), el dominio de colisión en toda la red local es único.



Capa de enlace Ethernet (802.3)

Hoy en día las ethernet más utilizadas son:

- 100 Base TX
- 1000 Base T
- Utilizan cable UTP de cat. 5e o 6.



Fast ethernet (100) usa codificación 4B/5B (NRZI, codificando 4 bits de información en 5 bits. Evita secuencias largas de ceros).

Gigabit Ethernet (1000) usa codificación 8B/10B y modulación en amplitud de pulso.

Capa de enlace

Formato de la trama (DIX-Ethernet)

- Preámbulo. Es 10101010 repetido 7 veces. Identifica el inicio de la trama.
- Direcciones MAC de destino y origen (6 bytes cada una). Todos los bits a 1 indica broadcast.
- Tipo/longitud: puede tener diferente significado en función del protocolo usado (802.3 o Ethernet-DIX). Identifica el protocolo de red de alto nivel asociado con la trama o, en su defecto, la longitud del campo de datos.
- Datos: hasta 1500 bytes, un mínimo de 64 bytes.
- CRC: código cíclico de orden 32.

Comparación entre DIX Ethernet y IEEE 802.3								
Trama DIX Ethernet	Preámbulo		Destino	Origen	Tipo	Datos	Relleno	FCS
	8 bytes		6 bytes	6 bytes	2 bytes	0 a 1500 bytes	0 a 46 bytes	2 ó 4 bytes
Trama IEEE 802.3	Preámbulo	SOF	Destino	Origen	Long	Datos	Relleno	FCS
	7 bytes	1 byte	6 bytes	6 bytes	2 bytes	0 a 1500 bytes	0 a 46 bytes	4 bytes

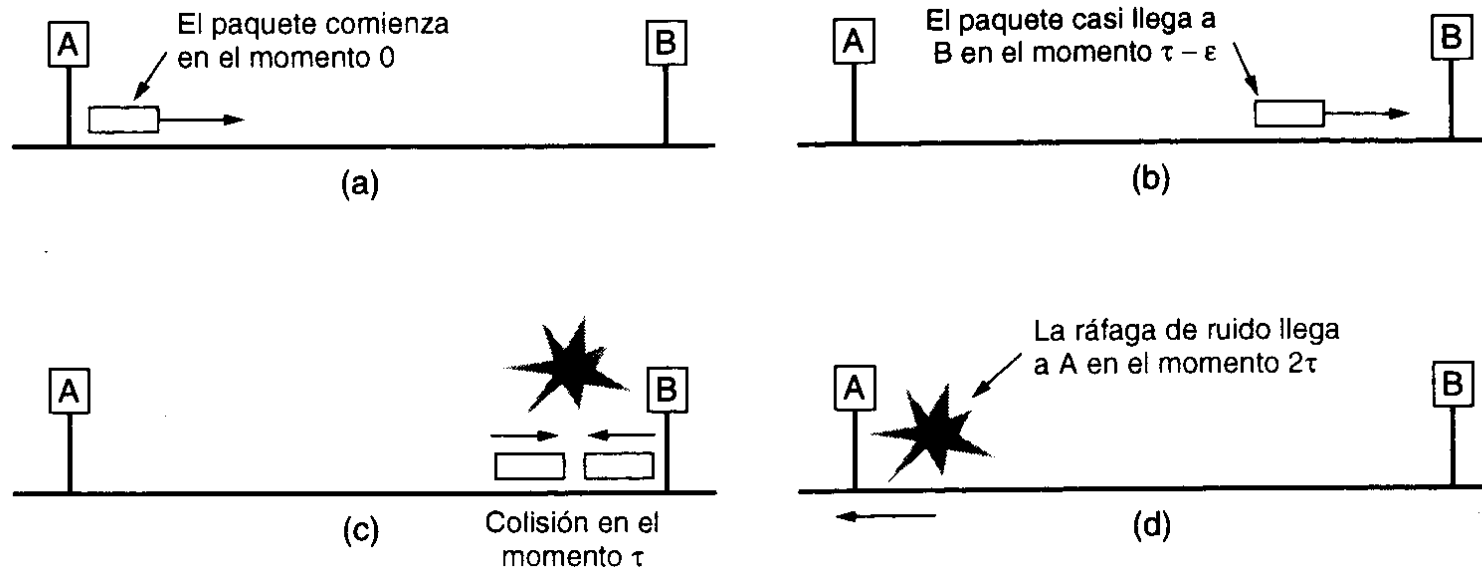
Capa de enlace


Ethernet (802.3) – Colisión de tramas

El tamaño mínimo de la trama debe ser de 64 bytes para garantizar que se detectan las colisiones de tramas.

El emisor debe estar enviando todavía datos en el momento en que se detecta la colisión. No dispone de buffer para almacenar históricos de tramas.

El siguiente dibujo ilustra una colisión y cómo es detectada.





Capa de enlace


Ethernet (802.3) – MTU

Para garantizar la detección de colisiones, el tamaño mínimo de trama ha de ser de 64 bits.

Por otro lado, el tamaño máximo es de 1500 bytes. Este máximo tamaño se denomina MTU (Maximum Transfer Unit).

La siguiente tabla muestra el MTU para diferentes tipos de redes.

Tipo de red	MTU (bytes)
Hyperchannel	65535
16 Mbits/sec token ring (IBM)	17914
4 Mbits/sec token ring (IEEE 802.5)	4464
FDDI	4352
Ethernet	1500
IEEE 802.3/802.2	1492
X.25	576
Point-to-Point (low delay)	296



Capa de enlace

Direcciones físicas. Dirección MAC

La dirección MAC se utiliza para realizar la entrega de los paquetes entre equipos pertenecientes a la misma subred. Por tanto el direccionamiento MAC corresponde a la capa de enlace.

Son números de 48 bits (6 bytes). Se suelen expresar como números hexadecimales separados por dos puntos (D4:AA:12:F3:00:C8). En ocasiones también se utiliza como separador un - (D4-AA-12-F3-00-C8).

Cada tarjeta de red tiene una dirección MAC única.

Los primeros 24 bits indican el fabricante, los siguientes 24 bits son únicos por cada fabricante.

Es posible consultar el fabricante de tu tarjeta de red desde la MAC en muchos sitios de la web, por ejemplo en:

<http://www.seguridadwireless.net/php/direccion-mac.php>

Capa de enlace

Direcciones físicas. Dirección MAC

Recuerda como en la práctica de Wireshark, se nos mostraba como parte de la MAC el nombre el fabricante

No. .	Time	Source
4	9.028195	10.0.0.109
5	9.678865	IntelCor_6e:a2:69
6	9.681088	Cisco-Li_2b:72:04
7	9.692034	IntelCor_6e:a2:69
8	9.696736	IntelCor_49:bd:93

Para saber cuál es la dirección MAC de nuestra tarjeta, se utiliza el comando:

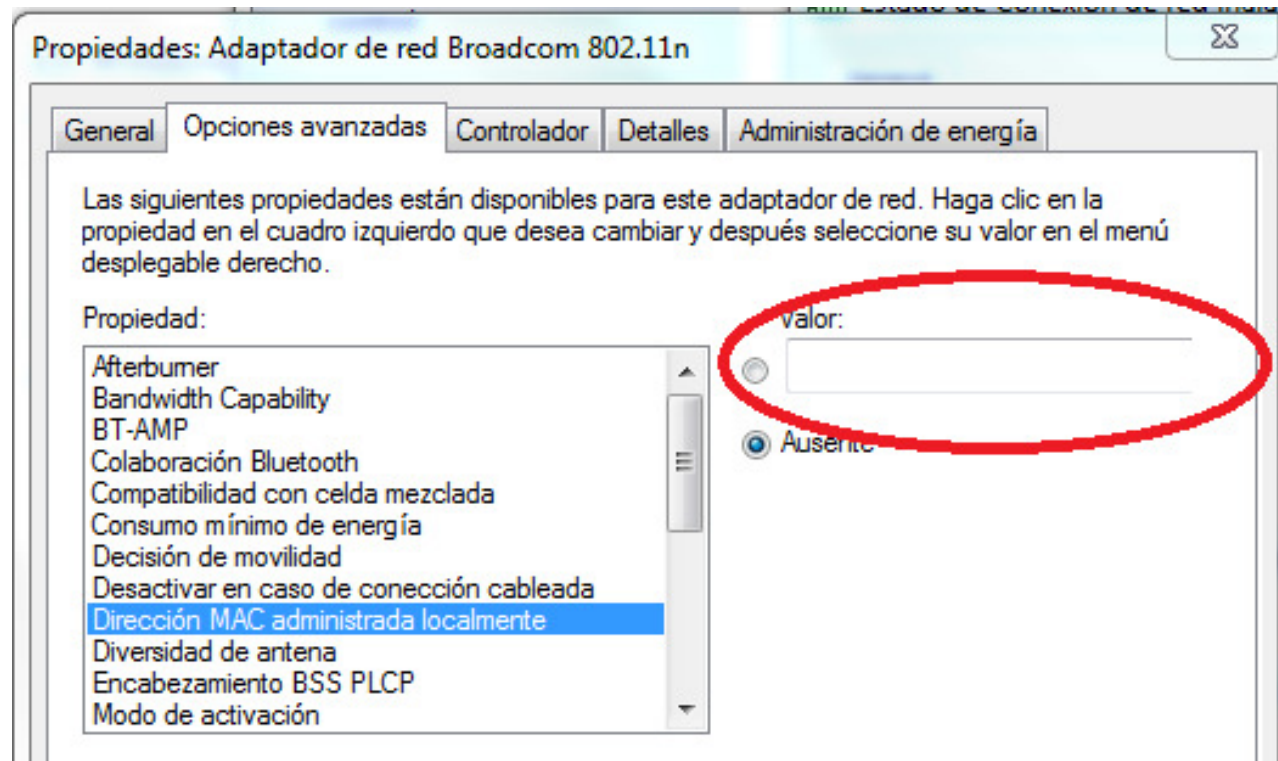
- ipconfig /all. En windows.
- ifconfig. En linux.

La dirección MAC: FF:FF:FF:FF:FF:FF es de broadcast, e implica que los destinatarios del paquete enviado son todos los equipos de la subred.

Capa de enlace

Direcciones físicas. Dirección MAC

Bien a través de ciertos programas o desde el sistema operativo es posible “camuflar” tu verdadera dirección MAC e identificar tu interfaz de red con una dirección introducida manualmente:



Capa de enlace

Protocolo ARP



Es un protocolo que se encuentra en la frontera de las capas de red y enlace, aunque generalmente aparece como protocolo de red.

Permite determinar la dirección MAC de un equipo de nuestra misma subred conocida su dirección IP, para hacer la entrega de la trama localmente. Esta tarea la realiza el sistema operativo de nuestra máquina de forma transparente al usuario.

Cada vez que se hace una consulta para determinar la dirección física, el sistema operativo almacena temporalmente en una tabla la correspondencia de las direcciones IP y MAC para evitar repetir el proceso en futuros envíos.

Capa de enlace

Protocolo ARP

Desde una sesión de consola, podemos consultar la información actual de la tabla ARP con el comando: `arp -a`.

Otros parámetros aceptados por el comando `arp` son:

- `arp -d`. Borra entradas en la tabla `arp`.
- `arp -s`. Permite introducir entradas estáticas en la tabla `arp`.
- Consulta el resto de opciones disponibles introduciendo el comando `arp` sin parámetros.

```
C:\Users\Moreno>arp -a

Interfaz: 192.168.1.164 --- 0xb
Dirección de Internet      Dirección física      Tipo
192.168.1.1                30-39-f2-6d-0b-e5    dinámico
192.168.1.255              ff-ff-ff-ff-ff-ff    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
255.255.255.255            ff-ff-ff-ff-ff-ff    estático

Interfaz: 192.168.56.1 --- 0x12
Dirección de Internet      Dirección física      Tipo
192.168.56.255             ff-ff-ff-ff-ff-ff    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
```

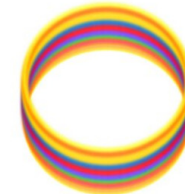
Capa de enlace

Otros estándares

802.5 Token ring: utiliza el algoritmo de paso de testigo para regular el acceso al medio.

El testigo pasa de ordenador a ordenador (conectados en anillo) y si un ordenador quiere transmitir, puede hacerlo (por un tiempo limitado) cuando posee el testigo

Usa codificación Manchester diferencial
Existen especificaciones para lograr 1Gbps.



802.4 Token bus: es una mezcla entre ethernet y token ring. Se utiliza el paso de testigo en una red que tiene topología bus

