Capítulo 6: The link layer and LANs

Hay dos tipos de canales fundamentales distintos de la capa de enlace

- **Canales de difusión**: Hay muchos Host conectados a un mismo canal de comunicaciones por lo que se utiliza el protocolo de acceso al medio para coordinar la transmisión de las tramas. (ej wifi)
- **Canal de comunicaciones punto a punto**: dos routers conectados mediante un enlace de larga distancia.

Para qué un datagrama puede ser transferido desde el Host de origen hasta el destino debe moverse a través de cada uno de los enlaces individuales que forman la ruta extremo a extremo.

Una **trama (Frame)** consta de un campo de datos en el que se inserta el datagrama de la capa de red y de una serie de campos de cabecera.

6.1.1 Servicios proporcionados por la capa de enlace

- **Entramado (Framing)**: los protocolos de la capa de enlace encapsulan cada datagrama de la capa de red dentro de una trama de la capa de enlace antes de transmitirla a través del enlace

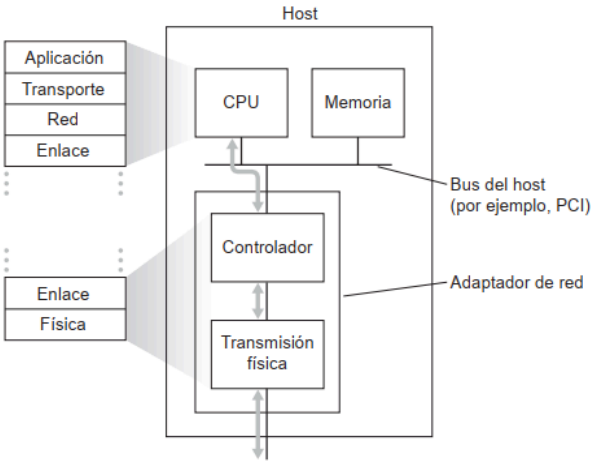
- **Acceso al enlace**: un protocolo de control de acceso al medio **Mac** especifica las reglas que se utilizan para transmitir una trama a través del enlace el emisor puede enviar una trama siempre que el enlace esté inactivo. Cuando hay varios nodos compartiendo mismo enlace de difusión el protocolo **Mac sirve para coordinar la transmisión de las tramas de los múltiples nodos**

- **Entrega fiable:** En los enlaces inalámbricos que suelen presentar altas tasas de error se utiliza el servicio de entrega fiable. Esto suele implementarse con confirmaciones y retransmisiones. (Ethernet no hace entrega fiable)

- **Detección y corrección de errores**: los protocolos de la capa de enlace proporcionan un mecanismo para detectar dichos errores de bit haciendo que el módulo transmisor incluya bits de detección de error en la trama y que el nodo receptor realice una comprobación de errores. Se implementa en Hardware

6.1.2 ¿Dónde se implementa la capa de enlace?

En su mayor parte la capa de enlace se implementa en un adaptador de red (tarjeta de interfaz de red NIC). En el “corazon” del adaptador de red se encuentra el controlador de capa de enlace; generalmente es un único chip que implementa muchos servicios de la capa de enlace.



Adaptador de red: su relación con otros componentes del host y funcionalidad de la pila de protocolos.

Buena parte de la funcionalidad del controlador de la capa de enlace se implementa por Hardware .
La parte software que se ejecuta en el CPU del host implementa el ensamblado de la información de

direccionamiento de la capa de enlace y la activacion del hardware controlador.

En el lado emisor el controlador toma un datagrama, que haya sido creado y almacenado en la memoria del Host por las capas superiores de la pila de protocolos, encapsula ese datagrama en una trama de la capa de enlace rellenando los diversos campos de la trama y luego transmite la trama al enlace de comunicaciones de acuerdo con el protocolo de acceso al enlace.

En el lado receptor un controlador recibe la trama completa y extrae el datagrama de la capa de red.

Si la capa de enlace realiza detección de errores entonces será el controlador del emisor quien se encargue de configurar los bits de detección de error en la cabecera de la trama Mientras que el controlador del receptor llevará a cabo la detección de errores

6.2 Técnicas de detección y corrección de errores

Los datos que hay que proteger Incluyen: el datagrama recibido de la capa de red para su transmisión a través del enlace y también la cabecera de la trama de enlace

El desafío del receptor es determinar si D es igual a D', dado que recibió D' y EDC'. Aunque se utilicen técnicas de detección de errores puede que queden errores de **bits no detectados** como consecuencia del receptor podría entregar un diagrama corrupto a la capa de red o no ser consciente de esto. Sucede que en general las técnicas más sofisticadas introducen mucho overhead.

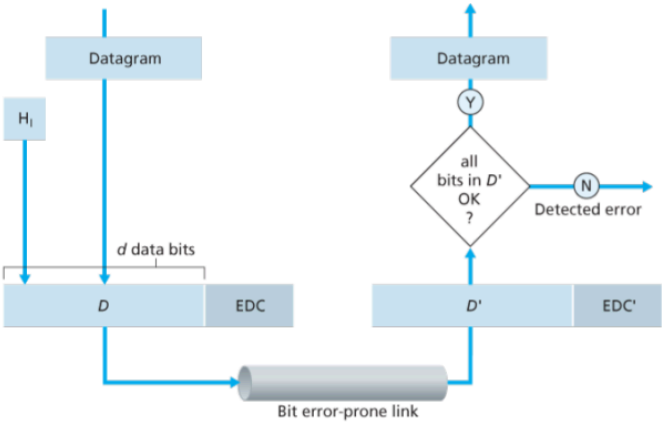


Figure 6.3 Error-detection and -correction scenario

Tecnicas para detectar errores:

6.2.1 Comprobaciones de paridad

Es la forma más simple.
Suponiendo que la data que se va a enviar, D, tiene d bits. En un esquema par, el enviador incluye un bit adicional donde elige el valor tal que el número total de 1s en los d+1 bits sea par. En un esquema impar, se elegirá tal que d+1 sea impar.
El receptor tiene que contar la cantidad de 1s recibidos en los d+1 bits, si encuentra un número impar (estando en el esquema par), entonces va a saber que hay un número impar de bits erroneos.

¿Qué pasa si encuentra un número par? no es garantía de nada, podría pasar que sea un caso donde haya errores no detectados y en esta técnica la probabilidad de ocurran errores es muy alta, asi que no es la mejor.

La capacidad de receptor para **detectar y corregir errores** a la vez se conoce con el nombre de **corrección de errores hacia adelante**. Estas técnicas se suelen utilizar en los dispositivos de almacenamiento y reproducción de audio.

6.2.2 Métodos basados en la suma de comprobación

Los d bits de datos, se toman como una secuencia de k-bits enteros. Un método simple de checksumming es el de sumar esos k-bits y usar el resultado como el bit de detección de error. El receptor verifica ese checksum calculando el complemento a 1 de la suma de lo que recibió (incluyendo el checksum) y viendo si el resultado son todos bits de 1. Si hay algún 0, es porque hay un error.

¿Por qué se utilizan checksums tanto en la capa de transporte como en la de enlace? porque los checksums de la capa de transporte están implementados en software, en cambio en la capa de enlace se implementan en hardware que rápidamente pueden resolver operaciones más complejas como CRC (cyclic redundancy checks).

6.2.3 Comprobación de redundancia cíclica (CRC)

Se conocen con el nombre de códigos polinómicos, dado que se puede ver la cadena de bits que hay que enviar como si fuera un polinomio cuyos coeficientes son los valores 0 y 1 de la cadena de bits.

Considerando la secuencia de datos de débits El emisor y receptor tienen que acordar primero un patrón de r + 1 bits conocido como **generator** = G. El bit más significativo de G tiene que ser 1. Para una data D, el enviador va a elegir r bits adicionales que va a concatenar a D tal que el patrón resultante d+r sea exactamente divisible por G usando aritmética de módulo 2.
El receptor va a dividir los d+r bits recibidos por G. Si el resto no es cero, entonces el receptor va a saber que hay un error, sino considerará que la información es correcta.

6.3 Protocolos y enlaces de acceso múltiple

Un enlace broadcast puede tener multiples senders y receivers conectados al mismo canal compartido. La idea de broadcast es que cuando un nodo transmite un frame, el canal lo difunde y cada uno de los otros nodos recibe una copia. Ejemplos son Ethernet y LANs inalámbricas.

Un tema importante es **cómo coordinar el acceso** de esos multiples nodos al canal compartido, eso se conoce como el **multiple access problem**. El problema es el de determinar **quién "habla" y cuándo**. Para regular las transmisiones existen protocolos.

Como todos los nodos son capaces de transmitir frames, dos o más nodos pueden transmitir frames al mismo tiempo. Cuando pasa eso, todos los nodos reciben multiples frames al mismo tiempo y colisionan en todos los receivers

→ Ninguno de los nuevos receptores pueden interpretar ninguna de los frames transmitidos
→ todos los frames implicados en la colisión se pierden
→ el canal broadcast es desperdiciado en el intervalo de colision.

Por eso es necesario coordinar las transmisiones de los nodos activos.

Características de un protocolo de multiples accesos de R bits por segundo :

- Cuando un solo nodo tiene data para enviar, ese nodo tiene un throughput de R bps.
- Cuando M nodos tienen data para enviar, cada uno va a tener un throughput de R/M bps.
- El protocolo es descentralizado (no hay un nodo que represente un único punto de falla).
- El protocolo es simple (fácil de implementar)

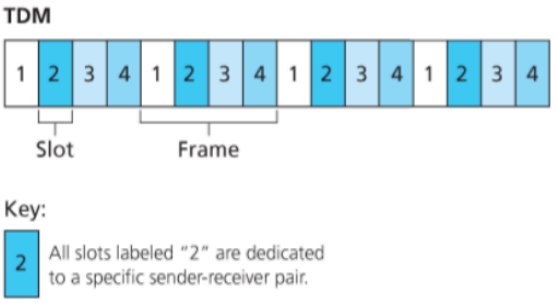
Los protocolos de multiples accesos se pueden clasificar en tres categorías:

6.3.1 Protocolos de particionamiento del canal

Time-division multiplexing (TDM) y frequency-division multiplexing (FDM) son dos técnicas que pueden usarse para particionar el bandwidth de un canal broadcast entre todos los nodos.

TDM Multiplexación por división de tiempos

Dividide el tiempo en time frames y despues divide cada frame en N time slots (particiones de tiempo). Cada time slot es asignado a uno de los N nodos, cuando un nodo tiene un frame para enviar (no confundir este frame con el del time frame), transmite los bits durante su time slot asignado.



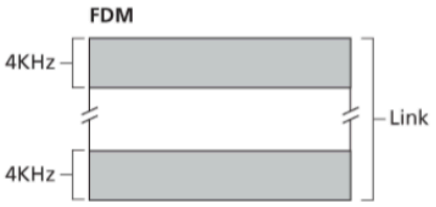
Normalmente los tamaños de partición se eligen de modo que pueden transmitirse un único paquete durante la partición de tiempo asignada.

TDM elimina las colisiones y es perfectamente equitativo. Con esta técnica, cada nodo obtiene una transmisión exclusiva de R/N bps en cada frame time.

Dos desventajas: un nodo es limitado a un rate promedio de R/N aunque sea el único nodo con paquetes para transmitir y un nodo siempre tiene que esperar por su turno en la secuencia aunque sea el único nodo con frames a enviar

FDM multiplexación por división de frecuencia

Divide el canal de R bps en diferentes frecuencias (cada una Con un ancho de banda de R/N) y asigna cada frecuencia a cada uno de los N nodos. Así, FDM crea N canales más pequeños de R/N bps a partir de un único canal disponible mayor de R bps.



CDMA (Code Division Multiple Access, Acceso múltiple por división de código)

Este protocolo asigna un código diferente a cada nodo y estos los usan para codificar los bits de datos a enviar. Los distintos nodos pueden transmitir simultáneamente y conseguir que sus respectivos receptores decodifiquen correctamente los bits de datos codificados por el emisor aunque haya interferencias provocadas por las transmisiones realizadas por los otros nodos.

6.3.2 Protocolos de acceso aleatorio

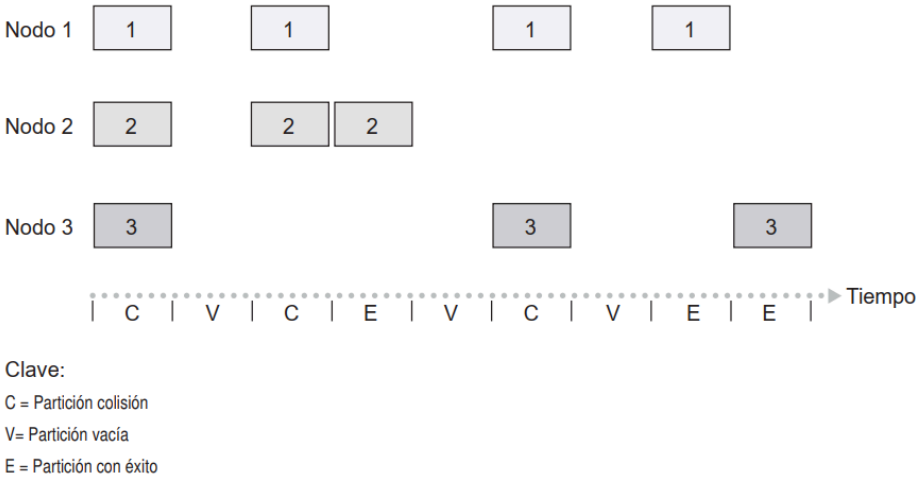
En estos protocolos, el nodo transmite al rate máximo de R bps. Cuando hay una colisión, cada nodo implicado en esa colisión retransmite su frame hasta que ese frame pase sin colisionar. Pero no es que retransmite inmediatamente después de la colisión, sino que espera un tiempo random antes de hacerlo

Slotted aloha protocol - ALOHA con particiones

Se divide el tiempo en slots de L/R segundos, donde L es la cantidad de bits por frame (todos los frames tienen la misma cantidad de bits).

Los nodos están sincronizados de modo que cada nodo sabe cuándo comienzan las particiones.
Cuando un nodo tiene un frame nuevo para mandar, espera el comienzo del siguiente slot y ahi lo envía. Si hay una colisión, se detecta antes de que termine el slot.

El nodo retransmite el frame en cada slot subsecuente con probabilidad p de que se transmita sin colisión; con probabilidad p quiere decir que decide con cierta probabilidad si retransmitir o esperar al slot siguiente.



ra 6.10 ♦ Los nodos 1, 2 y 3 colisionan en la primera partición. El nodo 2 consigue tener éxito finalmente en la cuarta partición, el nodo 1 en la octava partición y el nodo 3 en la novena.

Es un protocolo **descentralizado**, **simple** y que permite que un nodo transmita al máximo rate (R). El problema que tiene es que **no es muy eficiente** cuando hay muchos nodos con muchos frames por transmitir.

Cuando hay múltiples nodos activos, una cierta fracción de las particiones experimentará colisiones y por lo tanto se desperdiciara.
Otra fracción de las particiones estará vacía en aquellos casos en que todos los nodos activos se abstengan de transmitir. Las únicas particiones no desperdiciadas serán aquellas para las que haya exactamente un nodo transmitiendo, estas son particiones con éxito.

La eficiencia de un protocolo de acceso múltiple con particiones se define como la fracción, calculada a largo plazo, de **particiones con éxito** cuando existe un gran número de nodos activos, cada uno de los cuales tiene siempre una gran cantidad de frames que enviar . (Solo el 0,37% de las particiones lograra ser transmitidas con exito. => La tasa efectiva de transferencia de este canal sera inferior a 37 Mps)

ALOHA

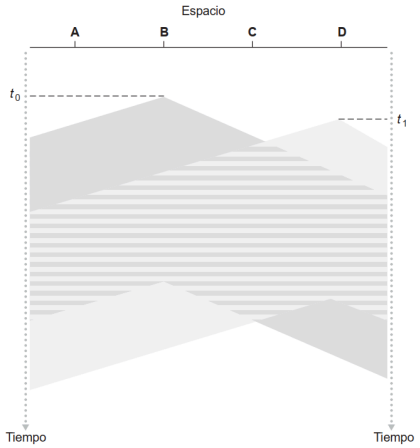
No tiene slots. Apenas llega un frame, se transmite al canal de broadcast. Si hay colisión, se va a retransmitir inmediatamente con probabilidad p. En caso contrario el nodo esperará durante un tiempo equivalente al tiempo total de transmisión de un frame.

CSMA (Carrier sense multiple access)

En los anteriores, la decisión de transmitir o no era independiente de los demás nodos. Acá aparecen dos reglas:

- **Escuchar antes que hablar**: Sondeo de portadora (carrier sensing) Cada nodo escucha el canal antes de transmitir. Si tiene que transmitir algo, espera hasta detectar que no haya otras transmisiones.

Si B comienza a transmitir (t0) va a pasar un tiempo hasta que D se entere que B esta transmitiendo, entonces D creera que no hay nadie transmitiendo y comienza a transmitir (t1), entonces luego B y D colisionan. Por eso el **delay de propagacion de canal extremo a extremo** de un canal de difusion desempeña un papel fundamental en el rendimiento del canal.

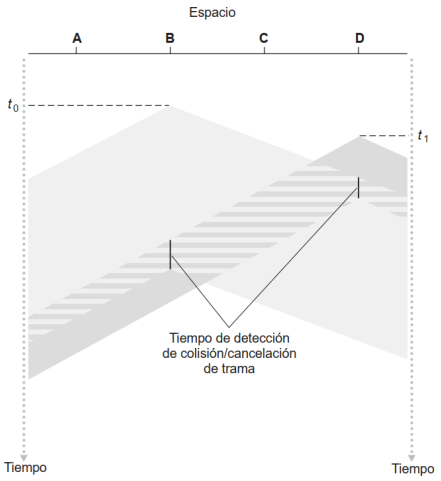


CSMA/CD (Carrier-Sense Multiple Access con deteccion de colisiones)

- **Escuchar antes que hablar**: Sondeo de portadora (carrier sensing) Cada nodo escucha el canal antes de transmitir. Si tiene que transmitir algo, espera hasta detectar que no haya otras transmisiones.

- **Si alguien comienza a hablar al mismo tiempo hay que dejar de hablar**: Colission Detection. Un nodo que está transmitiendo, escucha el canal mientras transmite. Si se detecta qué otro nodo está transmitiendo se deja de transmitir y espera una cantidad aleatoria de tiempo antes de repetir el ciclo de detectar y transmitir sin inactividad. La performance queda atada al delay de propagación del canal.

Funcionamiento desde la perspectiva de un adaptador en un nodo Conectado a un canal de difusión:



1. El adaptador obtiene un datagrama de la capa de red, prepara un frame de la capa de enlace y la coloca en el buffer del adaptador
2. Si el Adaptador detecta que el canal está inactivo comienza a transmitir el frame. Si está ocupado espera hasta comprobar que no hay intensidad de señal y luego comenzar a transmitir frame.
3. Mientras está transmitiendo el adaptador monitoriza la presencia de señales de otros adaptadores.
4. Si el adaptador transmite la trama completa sin detectar otra señal, termina el trabajo con ese frame. Pero si el adaptador detecta intensidad de señal procedente de otros adaptadores mientras se está transmitiendo, cancela la transmisión
5. Después de abortar la misión del frame, el adaptador espera una cantidad de tiempo aleatoria y vuelve al paso 2

El intervalo de espera será corto cuando el número de nodos que colisionan es pequeño y largo cuando el número de nodos que colisionan sea grande.

6.3.3 Protocolos de toma de turnos

Lo que le falta a los protocolos de ALOHA y CSMA es la propiedad de que cuando hay M nodos activos, todos tengan un throughput de R/M bps.

Protocolo de sondeo (Polling protocol)

Requiere que uno de los nodos sea designado como el nodo “maestro”. El nodo maestro va eligiendo cada uno de los nodos al estilo **round-robin**. El nodo maestro elige al nodo uno y le dice que puede transmitir hasta un cierto número de paquetes de frames, y asi continuamente con los otros nodos de forma ciclica.
Desventajas: el delay que introduce esto de estar eligiendo nodos y que si el nodo maestro falla, todo el canal se vuelve inoperativo.

Token-passing protocol Protocolo de paso de testigo

El token es un pequeño frame que se intercambia entre los nodos en un determinado orden. Cuando un nodo recibe el token, se lo queda sólo si tiene datos para transmitir, sino se lo pasa al siguiente nodo. Si el nodo sí tiene datos para transmitir, envía hasta un número máximo de frames y después le pasa el token al nodo siguiente. Esta técnica es descentralizada y eficiente, pero tiene un problema: la falla de un nodo puede afectar a todo el canal, o si algun nodo se apodera del token seria necesario invocar algun procedimiento de recuperacion.

6.3.4 DOCSIS: el protocolo de la capa de enlace para acceso a Internet por cable

sabemos que una red de acceso por cable suele conectar varios miles
de módems domésticos de acceso por cable a un sistema de terminación de módem por cable (CMTS, Cable Modem Termination System).
DOCSIS utiliza FDM para dividir los segmentos de red de bajada y de subida en múltiples canales de frecuencia. Cada canal de subida y de bajada es un canal de difusión. como hay un único CMTS transmitiendo a través del canal de bajada, no existen problemas de acceso múltiple. en la subida múltiples modems por cable comparten el mismo canal (frecuencia) hacia el CMTS, por lo que aca si podrían producirse colisiones.
El CMTS concede explícitamente permiso a los modems por cable individuales para transmitir durante ciertas mini-particiones específicas.

6.4 Redes de área local conmutadas

Switched Local Area Networks

MAC Addresses

Además de la/s dirección/es de red, los hosts y routers (sus adaptadores aka interfaces de red) tienen multiples direcciones de enlace asociadas.

Los switches no tienen dirección de enlace asociada, solo los hosts y routers.
Una dirección de enlace puede llamarse MAC address.

Una propiedad interesante es que no puede haber dos adaptadores con la misma dirección. La IEEE gestiona el espacio de direcciones MAC. A diferencia de la dirección IP, la dirección MAC no cambia, sin importar el lugar físico en el que se encuentre el adaptador.

Cuando un adaptador quiere enviar un frame, inserta la dirección MAC del adaptador destino en el frame y lo manda a la LAN. Entonces cuando un adaptador recibe un frame, verifica que la dirección destino que tiene coincida con la propia. Si no coincide, lo descarta.

Existe una dirección MAC especial de broadcast para cuando se quiere que el frame lo reciban todos los adaptadores. En LANs con direcciones de 6 bytes es FF-FF-FF-FFFF-FF.

Address Resolution Protocol (ARP)

Se encarga de la traducción entre direcciones IP y direcciones MAC.

ARP recibe como input una dirección IP que esté en la **misma** LAN y devuelve la correspondiente dirección MAC. Esto se necesita para enviar datagramas dentro de una misma subnet porque quien envía solo tiene la dirección IP destino.
Se parece a DNS porque traduce IP a MAC PERO a diferencia de DNS, **ARP solo resuelve dir IP** para las interfaces de los hosts y routers **de una misma subred**

Cada host y cada router tienen una **tabla ARP** en su memoria, conteniendo los mapeos de **IP↔MAC** y un **TTL** que determina después de cuánto tiempo se tiene que borrar el mapeo de la tabla.

Si un host quisiera enviar un datagrama a otro teniendo la IP destino, necesita la dirección MAC entonces primero se fija en la tabla ARP si tiene ese dato, si no lo tiene va a usar el protocolo ARP para calcularlo. Esto último consiste en que quien envía tiene que construir un paquete ARP.

Un paquete ARP tiene varios campos, entre ellos las direcciones IP y MAC destino y origen. La **idea** es pedirle a todos los demás hosts y routers de la subred que chequeen si su dirección IP coincide con la direccion IP destino del paquete ARP, la que coincida va a enviar un paquete ARP de respuesta indicandole el mapeo.

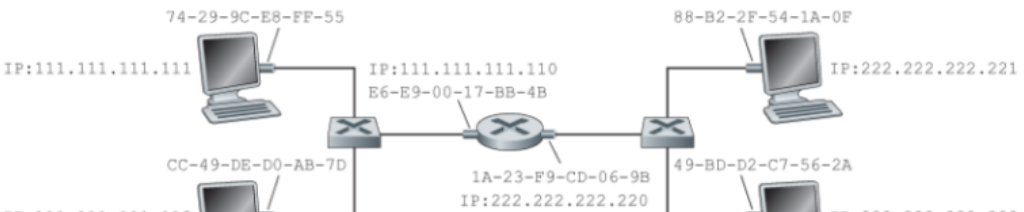
El Frame que contiene la consulta ARP es recibida por todos los demás adaptadores existentes en la Subred y gracias a la dirección de broadcast cada adaptador pasa la consulta arp contenida en el frame a su módulo arp . El único nodo en el que se produzca la coincidencia devolverá al nodo que ha realizado la consulta una respuesta ARP con la correspondencia deseada.

Notar que el mensaje ARP de consulta se envía dentro de un frame de broadcast, mientras que el mensaje ARP de respuestas se envía dentro de un frame estándar.

ARP es un protocolo que se encuentra entre la capa de red y la de enlace

Envío de un datagrama fuera de la subred

Un Host de una subred desea enviar un datagrama de la capa de red a un Host que está fuera de la subred:



Notar que un router tiene dos adaptadores, dos direcciones IP, dos modulos ARP y cada adaptador tiene su dirección MAC.
Si se quisiera enviar un paquete desde la subnet de la izquierda a la de la derecha, primero se tendría que enviar el datagrama a la interfaz del router 111.111.111.110, entonces al frame se le indicaría la dirección MAC E6-E9-00-17-BB-4B. Para mover el datagrama del router a la interfaz que corresponde, el router chequea en su tabla de forwarding: 222.222.222.220. Esta interfaz le pasa el datagrama a su adaptador que lo va a encapsular en un frame para enviarlo a la subnet2. La dirección MAC destino la obtiene el router de su tabla ARP.

6.4.2 Ethernet

Es la tecnología de LAN cableado más prevalente hoy en día. Ethernet con una topología de bus es una LAN de broadcast.

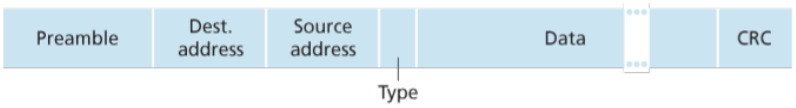


Figure 6.20 Ethernet frame structure

Campos de un frame Ethernet:

- **Data field**: transporta el datagrama IP. Si el datagrama excede los 1500 bytes, se va a tener que fragmentar. Si el datagrama contiene menos de 46 bytes, se tiene que rellenar.
- **Destination address**: Contiene la dirección MAC del adaptador destino. Cuando el adaptador destino recibe el frame, le pasa los contenidos del campo de data a la capa de red.
- **Source address**: Contiene la dirección MAC del adaptador que transmite el frame a la LAN.
- **Type field**: Permite multiplexar protocolos de la capa de red (tener en cuenta que se podria usar un protocolo que no sea IP)
- **Cyclic redundancy check** (CRC): Sirve para permitir al adaptador receptor, detectar errores de bits en el frame.
- **Preamble**: Los primeros 7 bytes sirven para "**despertar**" a los adaptadores receptores y sincronizar sus clocks al clockdel emisor. Esta sincronización es para que la transferencia que se da a una cierta tasa de transmisión, tenga en consideración el drift que puede haber con respecto al target rate.

Todas las tecnologías de Ethernet proveen un servicio **conectionless** para la capa de red. Esto es, cuando el adaptador A quiere enviar un datagrama al adaptador B, el adaptador A encapsula el datagrama en un frame Ethernet y envia el frame a la LAN, sin ningún handshaking inicial con el adaptador B. Este servicio conectionless de capa 2 es análogo al servicio de datagrama de IP en capa 3, o UDP en capa 4.

Las tecnologías Ethernet proveen un **servicio no confiable** en la capa de red. Corre el frame a lo largo de un check CRC, pero no envia un ACK cuando un frame pasa el check CRC, ni tampoco envia un NACK cuando un frame falla. Cuando un frame falla el check CRC, el adaptador B simplemente **descarta el frame**. Esta falta de transporte confiable ayuda a Ethernet a ser **simple y barato**, pero también significa que el stream de datagramas pasados a la capa de red puede tener gaps.

Si hay gaps entre frames Ethernet descartados, entonces la aplicación en el Host B ve gaps también? Esto dependerá de si se utiliza UDP o TCP.

Historia de ethernet:

En la época de las topologías de bus y de las topologías en estrella basadas en hub, Ethernet era claramente un enlace de difusión en el que se producían colisiones entre tramas cuando los nodos transmitían al mismo tiempo. Para tratar estas colisiones, el estándar Ethernet incluyó el protocolo CSMA/CD.

Hoy día de Ethernet es una topología en estrella basada en switches, que utiliza la conmutación de paquetes de almacenamiento y reenvío, un switch coordina sus transmisiones y nunca reenvía más de una trama a la misma interfaz en un determinado instante. Además, los switches modernos son full-duplex, por lo que un switch y un nodo pueden enviarse tramas entre sí simultáneamente sin interferir. En otras palabras, en una red LAN Ethernet basada en switches no se producen colisiones y, por tanto, no se necesita un protocolo MAC.

6.4.3 Switches de la capa de enlace

La función de un switch es recibir las tramas de la capa de enlace entrantes y reenviarlas a los enlaces de salida.
Un host/router dirige una trama a otro host/router (en lugar de dirigirla al switch) y la envía a la red LAN, sin ser consciente de que un switch recibirá la trama y la reenviará.

Como la velocidad a la que llegan los frames a cualquiera de las interfaces de salida del switch puede ser temporalmente mayor que la capacidad del enlace de dicha interfaz, las interfaces de **salida del switch disponen de buffers**.

Reenvío y filtrado

- El **filtrado** es la función del switch que determina si una trama debe ser **reenviada** a alguna interfaz o debe ser **descartada**.
- El **reenvío** es la función del switch que determina las interfaces a las que una trama debe dirigirse y luego envía la trama a esas interfaces.

Las funciones de filtrado y reenvío del switch se realizan utilizando la **tabla de conmutación.** Esta tabla contiene entradas para algunos de los hosts y routers de la LAN

Una entrada de la tabla de conmutación contiene:
- Una dirección MAC
- La interfaz del switch que lleva hacia dicha dirección MAC
- El instante en el que la entrada fue incluida en la tabla.

Es importante resaltar que los switches (conmutadores) reenvían los paquetes basándose en las direcciones MAC, en lugar de en las direcciones IP

Cuando una tabla de switching se indexa con una MAC Address hay **3 casos posibles**:

- **No hay entrada para la MAC Address**: Si no hay entrada en el address destino, entonces el switch realiza broadcast del frame
- **Hay una entrada en la tabla, asociando a la MAC Address con la interfaz X**: En este caso, el frame viene del segmento LAN que contiene a la MAC Address destino. El switch realiza la función de filtering y descarta el frame ya que no tiene necesidad de reenviar.

- **Hay una entrada en la tabla que asocia la MAC destino con la interfaz Y distinta de X**. En este caso, el frame necesita ser forwardeado al segmento LAN ligado a la interfaz Y. El switch realiza su función de forwarding poniendo el frame en un output buffer que precede a la interfaz Y.

Self-Learning
Una propiedad del switch es que se construye automatica y dinámicamente, y de forma autonoma.

Esto se logra con lo siguiente:

1. La tabla de switching inicialmente está vacía.
2. Por cada frame que viene recibido en una interfaz, el switch guarda en su tabla
    a. La MAC Address en el campo de frame source address
    b. La interfaz de la cual arribó
    c. El tiempo actual.

    Entonces, si cada host envía un frame en la LAN, entonces cada host eventualmente tendrá un registro en la tabla.

3. El switch borra una dirección en la tabla si ningún frame es recibido con esa dirección como dirección fuente luego de un periodo de tiempo (AGING TIME).

Los switches son dispositivos **plug-and-play** porque no requieren intervención ni de un administrador de redes ni de los usuarios.

Los switches también permiten la comunicación **full-duplex**, lo que significa que cualquier interfaz del switch puede enviar y recibir al mismo tiempo

Propiedades de la conmutación de la capa de enlace

- **Eliminación de Colisiones**: No se desperdicia el ancho de banda por colisiones xq Los switches tienen un buffer donde van guardando los frames y **nunca transmiten más de un frame a un segmento al mismo tiempo**.
  Como con un router, el maximo throughput agregado de un switch es la suma de todos los ratios de las interfaces del switch. Por lo tanto, los switches proveen una mejora significante de performance sobre una LAN con enlaces de broadcast.

- **Enlaces Heterogéneos**: Debido a que un switch aísla un enlace del otro, los diferentes enlaces en la LAN pueden operar a diferentes velocidades y pueden correr en diferentes medios.

- **Administración**: Un switch también facilita la administración de redes. Si detecta que un adaptador está funcionando mal, puede desconectarlo automáticamente. También recolectan estadísticas del uso de bandwidth, colisiones, tráficos, etc.

Switches vs routers

Los routers son dispositivos de conmutación de paquetes de almacenamiento y reenvío que reenvían los paquetes utilizando direcciones de la capa de red. Aunque un **switch** también es un dispositivo de conmutación de paquetes de almacenamiento y reenvío, es diferente de un router porque **reenvía los paquetes utilizando direcciones MAC**

Los switches son de capa 2 y los routers son de capa 3. Aunque los switches modernos "correspondencia-acción" pueden usarse tanto para reenviar una trama de la capa 2 según la dirección MAC de destino como un datagrama de la capa 3 usando la dirección IP de destino del datagrama

pros y contras de los Switches:

- los switches son dispositivos plug-and-play,
- Los switches también ofrecen tasas de filtrado y reenvío relativamente altas
- los switches tienen que procesar las tramas solo hasta la capa 2
- Los switches no ofrecen ninguna protección frente a las tormentas de difusión haciendo que toda la red colapse

pros y contras de los routers

- Los paquetes no seguirán ciclos a través de los routers
- los routers no tienen la restricción del árbol de recubrimiento
- proporcionan protección mediante firewalls frente a las tormentas de difusión de la capa 2
- no son dispositivos plug-and-play (ellos, y los hosts conectados a ellos, necesitan que sus direcciones IP sean configuradas)
- suelen tener un tiempo de procesamiento por paquete mayor que los switches, ya que tienen que procesar campos hasta la capa 3

Conclu: Los switches son suficientes para las redes pequeñas, ya que localizan el tráfico y aumentan la tasa de transferencia agregada sin necesidad de configurar direcciones IP. Pero las redes de mayor tamaño que constan de miles de hosts suelen incluir routers dentro de la red (además de switches). Los routers proporcionan un aislamiento más robusto del tráfico, controlan las tormentas de difusión y utilizan rutas más "inteligentes" entre los hosts de la red.

6.4.4 Redes de área local virtuales (VLAN)

Generalmente las LANs institucionales están configuradas jerárquicamente: Las redes LAN institucionales modernas suelen estar configuradas de forma jerárquica, teniendo cada departamento su propia red switched LAN conectada a las redes switched LAN de los otros grupos a través de una jerarquía de switches.

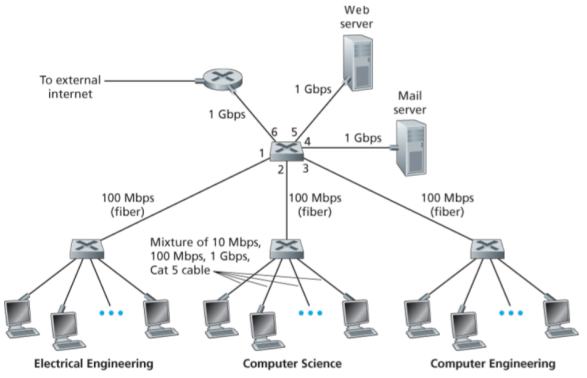


Figure 6.15 An institutional network connected together by four switches

En la Figura podemos identificar tres desventajas:

- **Falta de aislamiento del tráfico**: El tráfico de broadcast tienen que atravesar toda la red. Limitar el ámbito del tráfico de broadcast mejoraría el rendimiento de la LAN. Esto se podría solucionar reemplazando el switch del medio por un router
- **Uso ineficiente de los switches.** Si en lugar de tres grupos la institución tiene 10 grupos, entonces se necesitarían 10 switches de primer nivel. Si cada uno de los grupos es pequeño entonces un único switch de 96 puertos sería lo suficientemente grande
- **Gestión de los usuarios**. Si un empleado se mueve entre grupos, el cableado físico debe modificarse para conectar al empleado a un switch diferente.

Estas dificultades se pueden resolver utilizando un switch que soporte **VLANs: es un switch que permite definir múltiples redes de área local virtuales sobre una única infraestructura de red de área local física.**

Los hosts de una VLAN se comunican entre sí como si solo ellos (y ningún otro host) estuvieran conectados al switch.

En una VLAN basada en puertos, el administrador de la red divide los puertos (interfaces) del switch en grupos. Cada grupo constituye una VLAN, con los puertos de cada VLAN formando un dominio de difusión -> **el tráfico de difusión de un puerto solo puede llegar a los demás puertos del grupo**

Los fabricantes de switches hacen que dicha tarea de configuración resulte sencilla para los administradores de red, incorporando en un único dispositivo un switch VLAN y un router, con lo que no es necesario utilizar un router externo separado

Troncalización VLAN
Un puerto especial de cada switch se configura como un puerto troncal para interconectar los dos switches VLAN. El puerto troncal pertenece a todas las VLAN y las tramas enviadas a cualquier VLAN son reenviadas a través del enlace troncal hacia el otro switch. El switch del lado emisor de un enlace troncal VLAN añade la etiqueta VLAN a la trama, la cual es analizada y eliminada por el switch del lado receptor del enlace troncal

En las VLAN basadas en direcciones MAC, el administrador de la red especifica el conjunto de direcciones MAC que pertenece a cada VLAN. Las redes VLAN también pueden abarcar varios routers IP, lo que permite conectar islas de redes LAN con el fin de formar una única VLAN que podría abarcar todo elglobo

6.5 Virtualización de enlaces: la red como una capa de enlace

6.5.1 Conmutación de etiquetas multiprotocolo (MPLS)

MPLS Multiprotocol Label Switching, Conmutación de etiquetas multiprotocolo

MPLS es una red de circuitos virtuales de conmutación de paquetes de pleno derecho. Tiene sus propios formatos de paquete y comportamientos de reenvío. MPLS es de la capa de enlace xq que sirve para **interconectar dispositivos IP.**
Idea inicial: Expandir la infraestructura existente etiquetando selectivamente los datagramas y permitiendo a los routers reenviar esos datagramas basándose en etiquetas de longitud fija

Un frame ampliado MPLS solo se puede intercambiar entre routers compatibles con MPLS.
Routers de conmutación de etiquetas: Los routers compatibles con MPLS, reenvían las tramas MPLS buscando la etiqueta MPLS en su tabla de reenvío y luego pasando inmediatamente el datagrama a la interfaz de salida apropiada. El router compatible con MPLS no necesita extraer la dirección IP de destino

MPLS tiene una cabecera MPLS pequeña, que se añade entre la cabecera de la capa 2 (por ejemplo, Ethernet) y la cabecera de la capa 3 (es decir, IP)

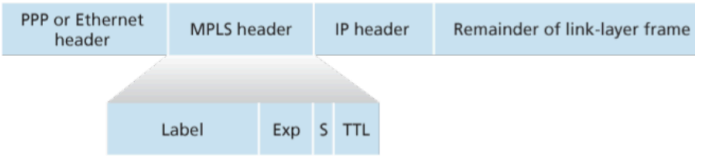


Figure 6.28 MPLS header: Located between link- and network-layer headers

La ventaja que trae es que provee la habilidad de reenviar paquetes por rutas que no serían posibles siguiendo un protocolo IP estandar, esto es una forma de “ingenieria de trafico” donde se puede sobreescribir el ruteo IP y forzar el tráfico por otros caminos.

También se usa MPLS para implementar VPNs. Envia un paquete y en mlps le dice que saltos hacer, une ips a traves de un tunel mpls

6.6 Redes para centros de datos

Cada data center tiene su propia red que interconecta los hosts entre sí e interconecta al data center con Internet. Esta red soporta dos tipos de tráficos: entre clientes externos y hosts internos, y entre hosts internos. Para manejar los flujos con clientes externos existen los border routers

Tres propiedades:
Balanceador de carga - Load balancing: Todas las solicitudes externas pasan primero por un balanceador de carga cuyo trabajo es **distribuir las solicitudes de los hosts**, balanceando la carga entre los hosts en función de su carga actual. Además, provee una función tipo NAT traduciendo la IP pública a la IP interna, asi se previene a los clientes de contactar directamente al host.

Hierarchical architecture. En general tienen una jerarquia de routers y switches jerarquizada

Tendencias en las redes para centros de datos: sustituir la jerarquía de switches y routers por una topología completamente conectada