Redes y comunicaciones

Resumen teorías - Capa de enlace

Clase 1 - Introducción a la capa de enlace

Terminología

Hosts y routers son nodes

Los canales de comunicación que conectan nodos adyacentes a través de caminos de comunicación son links:

- Enlaces cableados
- Enlaces inalámbricos
- LANs

PDU

La PDU de la capa de enlace es el frame o trama, que encapsula un datagrama

Responsabilidad

Transferir datagramas desde un nodo a otro adyacente a través de un link

Contexto

Los datagramas son transferidos por diferentes protocolos de enlace sobre diferentes enlaces (por ejemplo: ethernet, frame relay, 802.11, etc.)

Cada protocolo de enlace brinda diferentes servicios (podría o no proveer rdt: reliable data transfer)

Servicios

- Entramado (framing):
    - Encapsulado del datagrama en la trama, agregando un header y un trailer
- Acceso al enlace:
    - Acceso al canal si es un medio compartido (Medium Access Control)

    - MAC addresses utilizadas en los encabezados de las tramas para identificar el origen y el destino (diferentes de las IP)
- Entrega confiable:
    - Entre nodos adyacentes
    - Rara vez utilizados en enlaces de pocos errores (como la fibra óptica)
    - Usado en enlaces inalámbricos (al tener alta tasa de errores)
    - ¿Por qué confiabilidad a nivel de enlace y end to end?
- Control de flujo:
    - Acuerdo entre los nodos emisor y receptor (acá sí adyacentes)
- Detección de errores:
    - Errores causados por atenuación de la señal, ruido, etc.
    - El receptor detecta presencia de errores y señaliza al emisor para una retransmisión o descarta la trama
- Corrección de errores (FEC: Forward Error Correction):
    - El receptor identifica y corrige los errores en los bits sin necesidad de retransmisión
- Half-duplex y full-duplex:
    - Con half-duplex los nodos pueden transmitir pero no al mismo tiempo

Dónde está implementada

En todos los hosts

En el adaptador de red (NIC: Network Interface Card):

- Tarjetas ethernet, PCMCIA, 802.11
- Implementa las capas de enlace y física (como mínimo)

Incorporadas a los buses del sistema de los hosts

Combinación de hardware, software y firmware

Comunicación de adaptadores

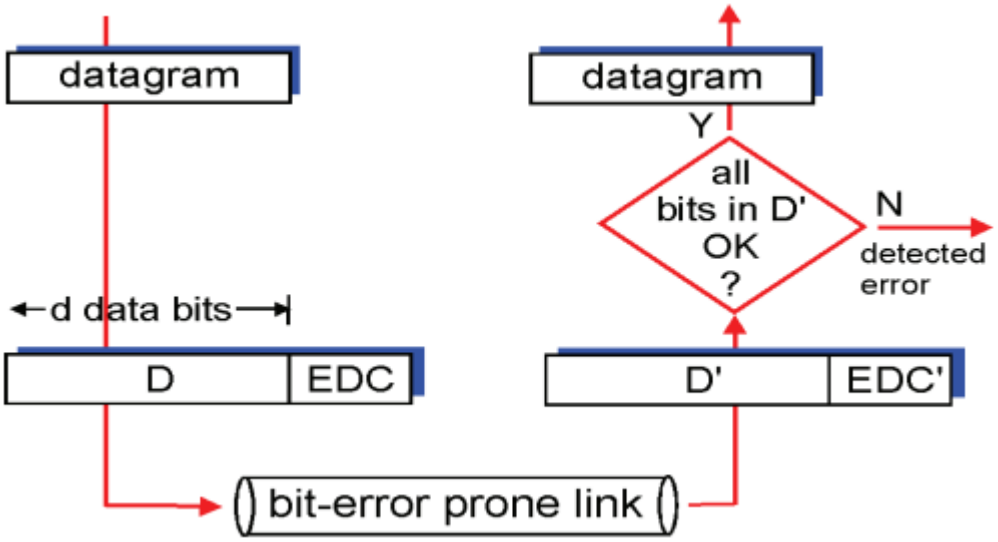
Lado emisor:

- Encapsula el datagrama en una trama
- Agrega bits de chequeo de error, rdt, control de flujo, etc.

Lado receptor:

- Busca por errores, rdt, control de flujo, etc.
- Extra el datagrama y lo pasa a las capas superiores

Detección de errores



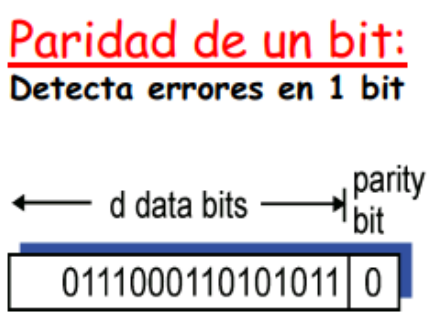
EDC: Error Detection Correction bits (redundancia)

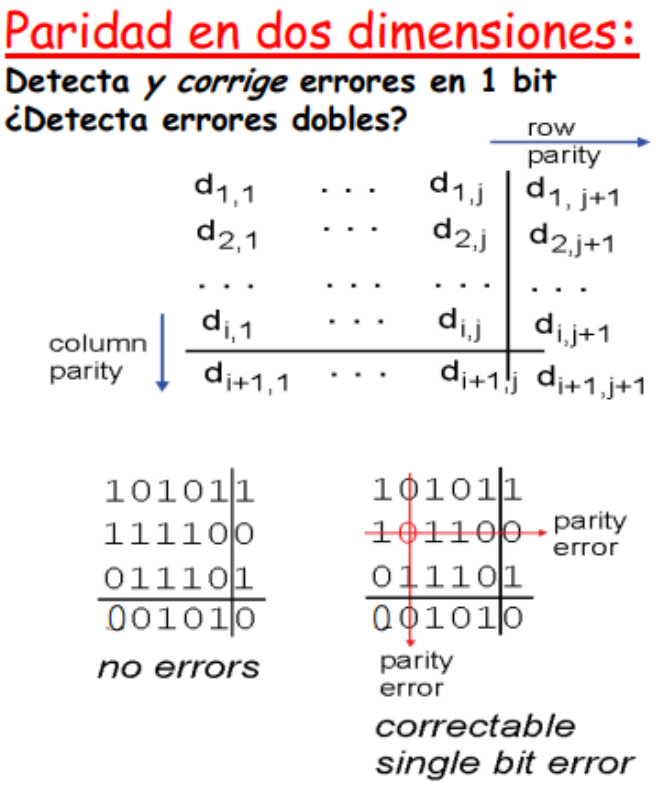
D: Datos protegidos por chequeo de errores. Puede incluir campos del encabezado

La detección no es 100% confiable

Un campo EDC mayor proporciona una mejor detección y corrección pero eso aumenta el tamaño total de la trama (reduciendo la eficiencia de la transmisión) y aumenta el tiempo de procesamiento

Chequeo de paridad





Internet checksum

Objetivo, detectar errores (bits cambiados) en el paquete transmitido (generalmente utilizado en la capa de transporte)

Cyclic Redundancy Check (CRC)

Ampliamente utilizado

Ver a los bits de datos (D) como los coeficientes de un polinomio. Por ejemplo: 110001 es x^5+x^4+1

Toda la aritmética que se utiliza es módulo 2 sin carry

Elegimos un patrón de r+1 bits (polinomio generador), G, de grado r, que conocen el transmisor y el receptor

El objetivo es determinar r CRC bits, R, tal que <D, R> (concatenado) es divisible exactamente por G

El receptor divide <D, R> entre G. Si el resto es distinto de cero hay error

2^r es desplazar a la izquierda r bits y agregando ceros

Ejemplo

- El emisor busca R, tal que exista Q que cumpla:

$D \cdot 2^r \text{ XOR } R = Q \cdot G$

Que G divida a $D \cdot 2^r - R$ sin resto

$D \cdot 2^r \text{ XOR } R = Q \cdot G$
$D \cdot 2^r \text{ XOR } R \text{ XOR } R = Q \cdot G \text{ XOR } R$
$D \cdot 2^r = nG + R$

$D \cdot 2^r$: dividendo, G: divisor, Q: cociente, R: resto

- si dividimos $D \cdot 2^r$ por G, buscamos el resto R

$$R = \text{resto}\ \left[\frac{D \cdot 2^r}{G}\right]$$

```
          101011
      ------------
1001 ) 101110000
       1001
       ----
        101
        000
        ---
        1010
        1001
        ----
         110
         000
         ---
         1100
         1001
         ----
          1010
          1001
          ----
           011
```

G ← 1001 ; D → 101110000 ; R ← 011

Int. Redes de Computadores - Capa de Enlace 5-16

Protocolos y enlaces de acceso múltiple

Tipos de enlace:

- Punto a punto:
  - PPP para acceso discado
  - Enlace punto a punto entre switch ethernet y host

- Broadcast (cable o medio compartido):
    - Ethernet “legacy”
    - HFC: Hybrid Fiber Cable
    - 802.11: LAN inalámbrica

Único canal broadcast compartido
Dos o más transmisiones simultáneas producen interferencia
Colisión:

- Si un nodo recibe dos o más señales al mismo tiempo
- Simultaneidad en tiempo y frecuencia de dos o más tramas en el mismo medio físico

Un protocolo de acceso múltiple es un algoritmo distribuido que determina cómo los nodos comparten el canal, y determina cuándo el nodo puede transmitir
La comunicación acerca de compartir el canal debe utilizar el mismo canal

Protocolo de acceso múltiple ideal

Canal broadcast con velocidad R bps:

1. Cuando un nodo quiera transmitir lo hará a una velocidad R
2. Cuando M nodos quieren transmitir, cada uno enviará a una velocidad promedio de R/M
3. Completamente descentralizado:
    a. No hay un nodo especial para coordinar las transmisiones
    b. No hay sincronización de relojes o slots

Simple

Protocolos MAC

Particionado de canal

Protocolos de arbitraje
Divide al canal en pequeñas piezas (ranuras de tiempo, frecuencia, código)
Asigna una pieza a un nodo para su uso exclusivo
Estrategia estática

Equitativo

Ineficiente a baja carga: retardo en el acceso al canal, ancho de banda 1/N asignado aún si hay un sólo nodo activo

TDMA

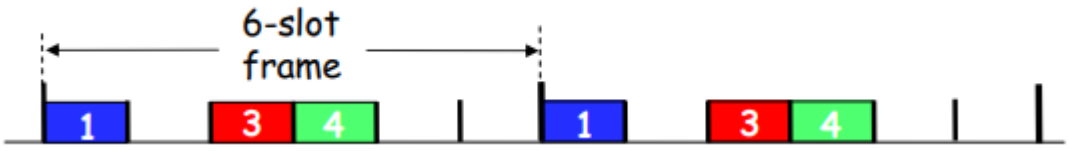
Time Division Multiple Access

Acceso al canal rotativo

Cada estación tiene un slot de longitud fija (longitud = tiempo de transmisión de la trama) en cada vuelta

Los slots sin usar quedan libres

Ejemplo: LAN con 6 estaciones. 1, 3 y 4 tienen trama. Las bandas de frecuencia 2, 5 y 6 están libres



FDMA

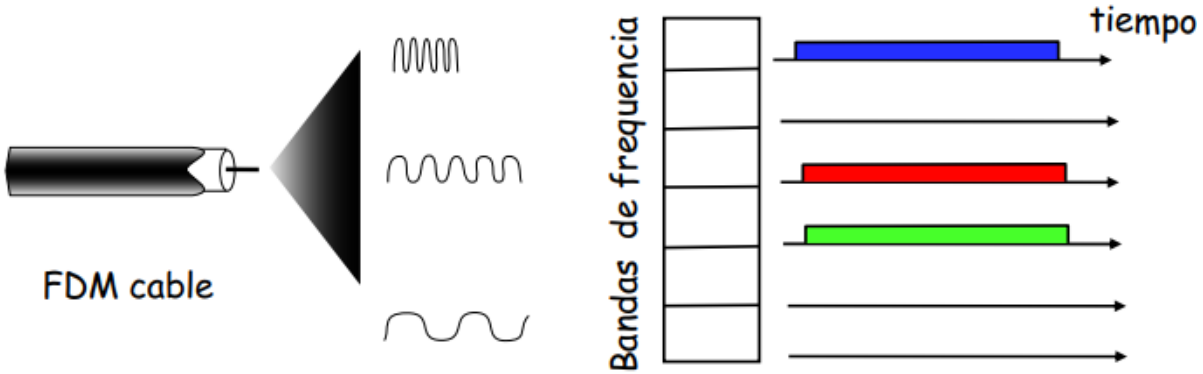
Frequency Division Multiple Access

El espectro del canal se divide en bandas de frecuencia

A cada estación se le asigna una banda frecuencia fija

El tiempo de transmisión no utilizado en las bandas de frecuencia queda libre

Ejemplo: LAN con 6 estaciones. 1, 3 y 4 tienen trama. Las bandas de frecuencia 2, 5 y 6 están libres



Acceso random

El canal no se divide, permite colisiones
“Recuperación” de colisiones
Estrategia dinámica
Alta carga: overhead por colisión

Cuando un nodo tiene una paquete para enviar:

- Transmite a la velocidad total del canal, R
- No existe a priori coordinación entre nodos

Dos o más nodos transmitiendo → colisión

Los protocolos MAC de acceso random especifican:

- Cómo detectar colisiones (directa o indirecta)
- Cómo recuperarse de las colisiones (por ejemplo usando retransmisiones retrasadas)

Ejemplos

- ALOHA ranurado, ALOHA
- CSMA, CSMA/CD, CSMA/CA
- También se los conoce como sistemas de contención o sistemas de contienda

CSMA

Carrier Sense Multiple Access
Escuchar antes de transmitir
Si el canal está libre: transmitir la trama entera
Si el canal está ocupado diferir la transmisión:

- Volver a escuchar después de un tiempo
- Seguir escuchando hasta que quede libre y transmitir
- Seguir escuchando hasta que quede libre y transmitir con probabilidad p

CSMA/CD

Carrier Sense Multiple Access / Collision Detection

Si hay presencia de portadora, se difiere la transmisión (como en CSMA)

Las transmisiones que colisionan son abortadas, reduciendo el desperdicio del canal

Detección de colisión:

- Relativamente fácil en LANs cableadas
- Difícil en LANs inalámbricas

“Toma de turnos”

Los nodos toman turnos, pero los nodos con más tramas para enviar podrían tomar turnos más largos

Estrategia dinámica

Estrategias de reserva o centralizada

Busca lo mejor de particionamiento del canal y acceso random

Polling:

- El nodo master “invita” a los nodos slave a transmitir en turnos
- Típicamente utilizado en dispositivos slave “tontos”
- Sin colisiones
- Determinístico
- Involucra:
  - Overhead por polling
  - Latencia
  - Único punto de falla (master)
- Ejemplo:
  - Bluetooth
  - Un modo de operación de 802.11

MAC

Dirección MAC (LAN/física/hardware/del adaptador/ethernet)

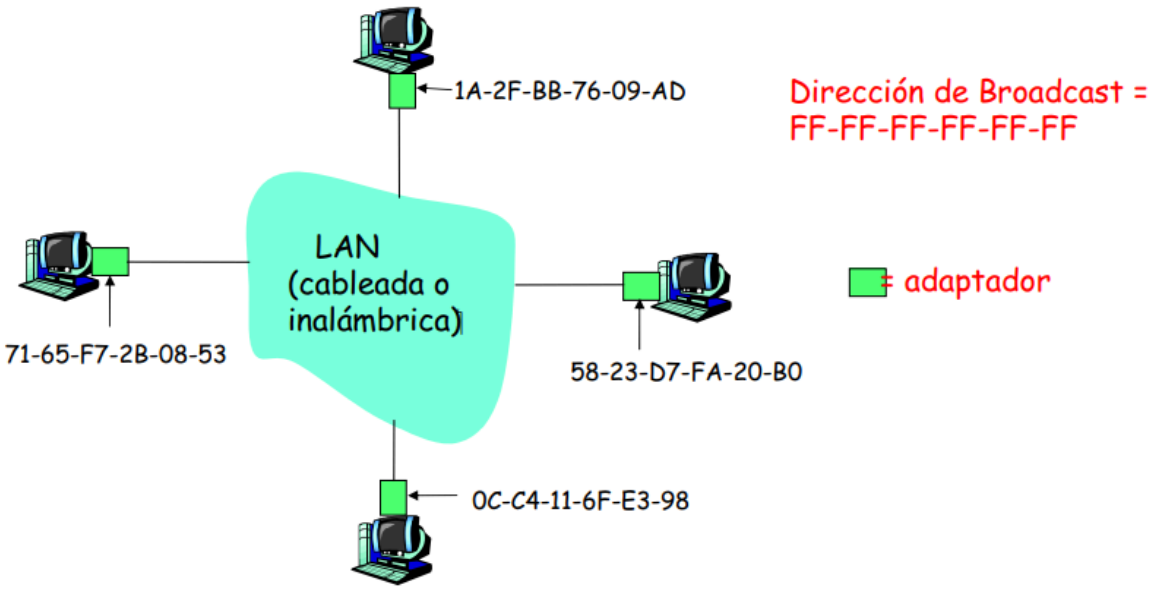
Su función es llevar la trama desde una interfaz a otra interfaz físicamente conectada

Direcciones MAC de 48 bits (en la mayoría de las redes LAN)

Grabada en la ROM de la NIC

Cada vez más se puede configurar por software

Es portable. Puedo mover la NIC de una LAN a otra



ARP

Address Resolution Protocol

¿Cómo determino la dirección MAC de X conociendo su dirección IP?

Cada nodo IP tiene una tabla ARP

Tabla ARP:

- Mapeo de direcciones IP/MAC para algunos nodos de la LAN
- Sus entradas son de la forma: dirección IP - dirección MAC - TTL

Ethernet

Tecnología LAN cableada dominante

Creada en los 70s

NICs baratas y switches baratos

Primera tecnología LAN ampliamente usada

Más simple y barata que token LANs y ATM

Velocidades entre 10Mb/s y 10Gb/s

Es un servicio no orientado a conexión: no hay handshaking entre las NICs emisor y receptor

Es un servicio no confiable:

- La NIC que recibe no envía ACKs o NAKs a la NIC emisora
- El flujo de datagramas pasados a la capa de red puede tener huecos
- Los huecos serán llenados si la app usa TCP, sino se verán los huecos en capa de aplicación

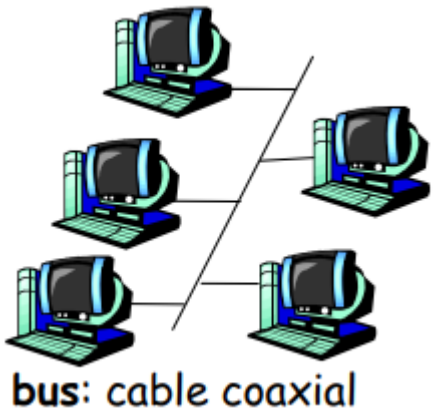
Usa el protocolo MAC CSMA/CD

La detección de colisiones es un servicio de capa física

Topologías

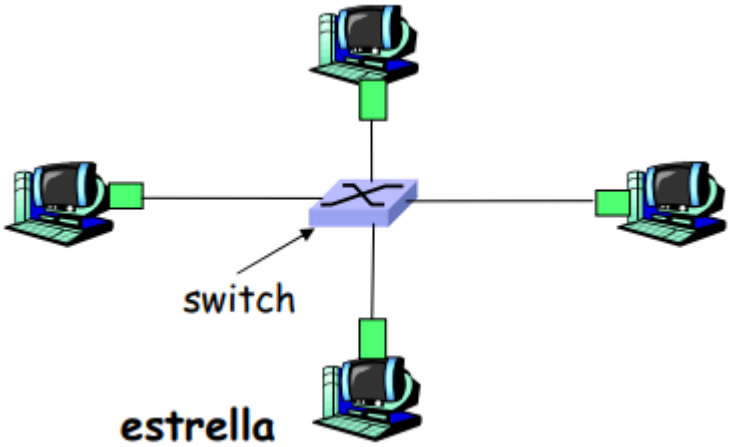
La topología en bus fue popular hasta mediados de los 90:

- Todos los nodos están en el mismo dominio de colisión (pueden colisionar con cualquiera de los otros)



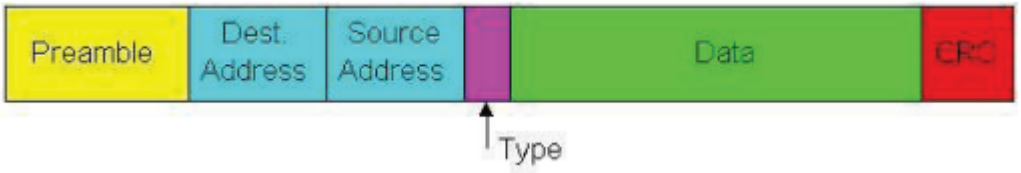
La topología estrella es la que se usa hoy:

- Switch activo en el centro
- Cada “spoke” corre el protocolo ethernet (los nodos no pueden colisionar con el resto)



Estructura de la trama

El adaptador del emisor encapsula el datagrama IP (u otro paquete de protocolo de capa de red) en una trama ethernet



Preamble

7 bytes con el patrón 10101010 seguido por un byte con el patrón 10101011

Utilizado para despertar al receptor y sincronizar relojes entre el emisor y el receptor

Direcciones

6 bytes cada una

Si el adaptador recibe una trama con su dirección (o la de broadcast) como dirección destino, pasa los datos en la trama al protocolo de capa de red

En otro caso, el adaptador descarta la trama

Type

2 bytes

Multiplexación

Indica el protocolo de la capa superior (casi siempre IP pero podría ser IPX, AppleTalk, etc.)

Data

De 46 a 1500 bytes

CRC

4 bytes

CRC-32

Chequeado en el receptor. Si se detecta un error se descarta la trama

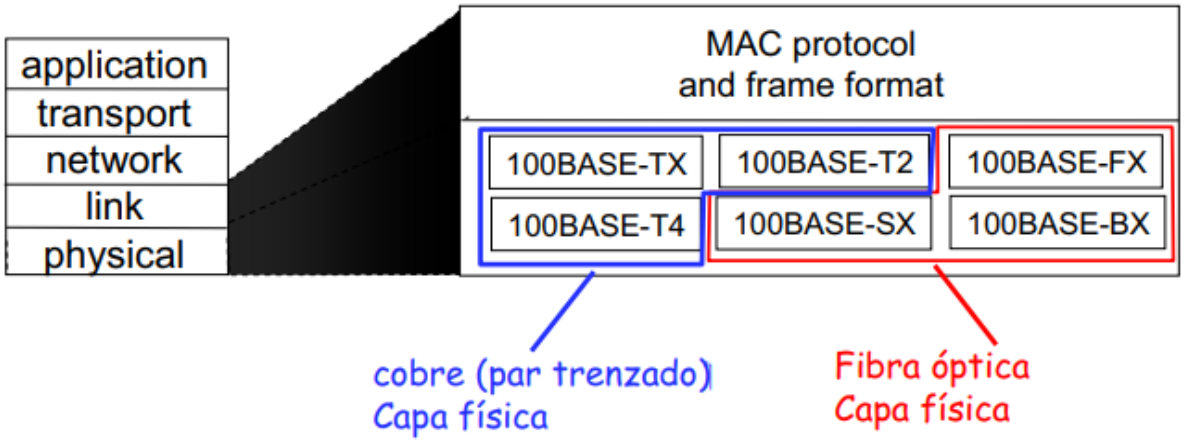
Para calcularlo se usa todo menos el preamble

Estándares

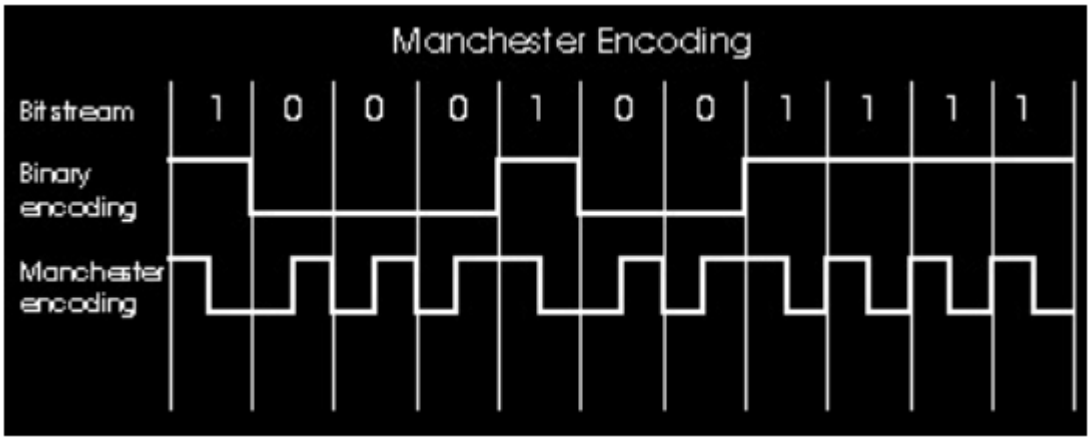
Protocolo de MAC y formato de trama único

Diferentes velocidades de transmisión

Diferentes medios físicos: cable, fibra óptica



Codificación Manchester



Utilizado en 100BASE-T

Cada bit tiene una transición

Permite que los relojes de los nodos emisores y receptores siempre estén sincronizados entre sí: no se requiere un reloj centralizado o global

Hub

Repetidor de capa física (“tonto”)

Los bits que llegan en un link salen por todos los otros links a la misma velocidad

Todos los nodos conectados al hub pueden colisionar con los otros

No existe buffering de tramas

No hay CSMA/CD en el hub: la NIC del host detecta las colisiones

Switch

Dispositivo de capa de enlace más inteligente que los hubs

Tienen un rol activo:

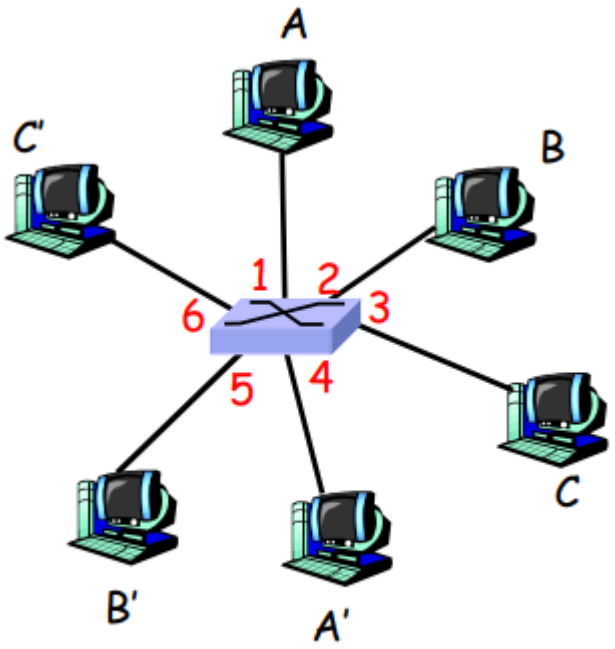
- Almacena y envía tramas ethernet
- Examina la dirección MAC destino de la trama entrante, realiza un envío selectivo de la trama a uno o más links de salida. Cuando la trama sea enviada en un segmento utiliza CSMA/CD para acceder al segmento

Los switches tienen las siguientes características:

- Transparentes: los hosts no se enteran de la presencia de switches
- Plug and play y self learning: no necesitan ser configurados para su operación básica

Permite múltiples transmisiones simultáneas:

- Los hosts tienen conexiones dedicadas directas al switch
- Los switches hacen buffer de las tramas
- El protocolo ethernet es usado en cada link entrante, pero no hay colisiones: full-duplex (cada link es su propio dominio de colisión)
- Switching: A-to-A' and B-to-B' simultáneamente sin colisiones (no sería posible con un hub)



switch con seis interfaces (1,2,3,4,5,6)

Self-learning

El switch aprende qué hosts pueden ser alcanzados a través de qué interfaces:

- Cuando una trama es recibida, el switch aprende la ubicación del emisor: el segmento LAN de entrada
- Registra el par emisor/ubicación en la tabla del switch

Dir. MAC	interfaz	TTL
A	1	60

Tabla del switch (inicialmente vacía)

Filtering/forwarding de tramas

Cuando una trama es recibida:

1. Registra el link asociado con el host que envía
2. Busca en la switch table utilizando la MAC de destino
3. Si encuentra una entrada para el destino
    a. Si el destino está en el segmento de dónde llegó la trama la descarta
    b. Sino, hace forward de la trama en la interfaz indicada
4. Si no encuentra una entrada para el destino
    a. Flood: forward en todas las interfaces menos desde la que llegó

Técnicas de conmutación de tramas

Técnicas usadas por los switches para pasar la trama desde el puerto de entrada hasta el de salida

Se decide en función de la DA (Destination Address)

Dos grandes familias:

- Cut-through:
    - Solo espera la DA
    - No realiza FCS (Frame Check Sequence)
- Store and forward:
    - Espera toda la trama
    - Realiza FCS

Switches versus routers

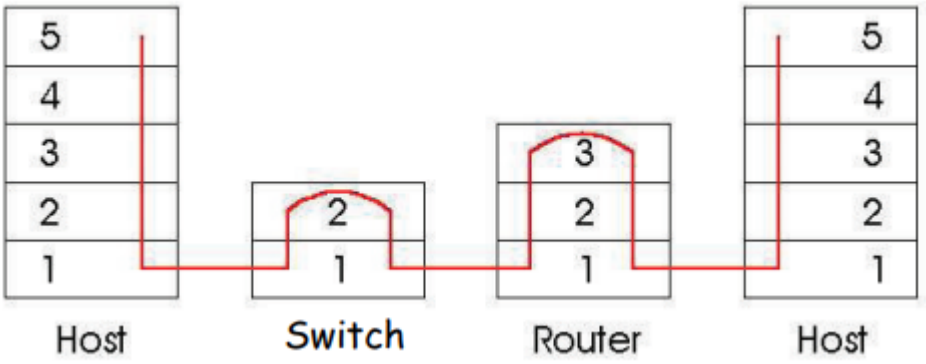
Ambos dispositivos son store and forward

Los routers son dispositivos de capa de red (examinan los encabezados de la capa de red)

Los switches son dispositivos de capa de enlace

Los routers mantienen tablas de routing e implementan algoritmos de routing

Los switches mantienen tablas de switch, implementan filtrado y algoritmos de aprendizaje



Segmentado de redes LAN

Teoría de Darwin de las redes LAN:

- La evolución del hub al switch
- Existió un dispositivo intermedio que vivió poco

Hub:

- Capa física
- 1 dominio de colisión y 1 dominio de broadcast

Bridge:

- Capa de enlace
- 1 dominio de colisión en cada puerta y 1 dominio de broadcast

Switch:

- Capa de enlace
- 1 dominio de colisión en cada puerta y 1 dominio de broadcast
- Pero además:
    - Mayor cantidad de puertas que un bridge
    - Mayor capacidad de conmutación de tramas que un bridge

Red switcheada

Redundancia:

- Confiabilidad, disponibilidad
- Costos
- Pero quizás también inestabilidad:
    - Por ejemplo, un simple ARP request puede generar una tormenta de broadcast y afectar la performance de los switches de toda la red
    - Algo similar puede ocasionar un unicast
    - Precisamos de una solución que evite los loops pero sin perder las bondades de la redundancia
- En la capa de enlace no existe el concepto TTL

Spanning Tree Protocol (STP)

Protocolo de gestión de capa de enlace que pone a disposición la redundancia de caminos pero previene posibles loops en la red de switches (posible origen de duplicación de mensajes)

El objetivo es que en cada instante exista solo un camino activo entre dos switches → que existan loops físicos pero no lógicos

Se define un árbol a través del cual se alcanza a todos los switches, pero el árbol se poda de tal forma que algunos puertos quedan bloqueados a la espera de algún cambio topológico y los restantes puertos están en estado de forwarding

Es un protocolo transparente para los usuarios

VLAN

Virtual LAN

Ejemplo

Empresa con k departamentos

1 red LAN por departamento:

- Agrupar lógicamente usuarios de la red y recursos conectados a puertos definidos administrativamente

En los 90s, k redes LAN independientes significaba instalar k hubs (como mínimo)

Luego se incorporaron los switches, ahora k redes LAN técnicamente puede significar simplemente instalar 1 switch

Una VLAN permite crear switches virtuales en uno o más switches y de esa forma separar dominios de broadcast (más pequeños)

Se debe definir:

- Cantidad
- Nombre de cada una (“color”)
- Miembros de cada una

En cada puerto del switch, una sóla VLAN posible, salvo en los trunks

Enlace de datos punto a punto

Un emisor, un receptor, un enlace. Más fácil que un enlace broadcast:

- No se requiere Medium Access Control
- No se necesita direccionamiento MAC explícito

Protocolos point to point más populares:

- PPP: Point-to-Point Protocol
- HDLC: High Level Data Link Control

PPP

Requerimientos de diseño:

- Simple
- Entramado de paquete: encapsulado del datagrama de capa de red en una trama de capa de enlace

- Transparencia: debe poder llevar cualquier patrón de bit en el campo de datos (incluso los vinculados al framing)
- Multiplexación: porta datos de capa de red de cualquier protocolo (no solo IP) al mismo tiempo
- Detección de errores (no corrección)
- Estado de la conexión: detectar y señalizar a la capa de red sobre fallas en el link
- Negociación de la dirección de la capa de red: un endpoint puede configurar la dirección de red del otro
- Posibilidad de negociación de opciones
- Posibilidad de negociación de datos

No requerimientos:

- Corrección/recuperación de errores
- Control de flujo
- Entrega de tramas en orden (secuenciamiento)
- No hay necesidad de soporte de enlaces multipunto

Recuperación de errores, control de flujo y secuenciamiento son relegados a las capas superiores

Clase 2 - Bridging y switching

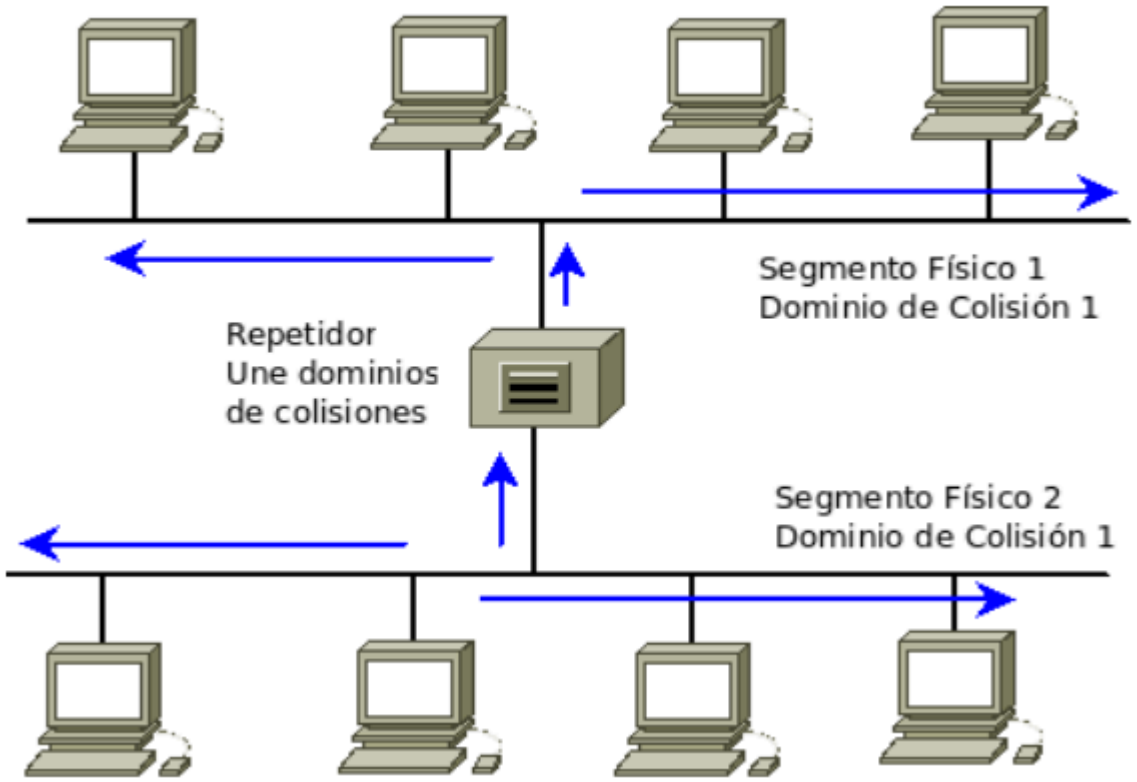
Dominio de colisión

- Hasta donde pueden extenderse las colisiones
- Hasta donde llega la señal de una trama unicast
- Todas las estaciones en el mismo dominio de colisiones ven los datos transmitidos de cada una
- Un repetidor o un hub extienden un dominio de colisión

Repetidor

Amplificador digital, dos puertos

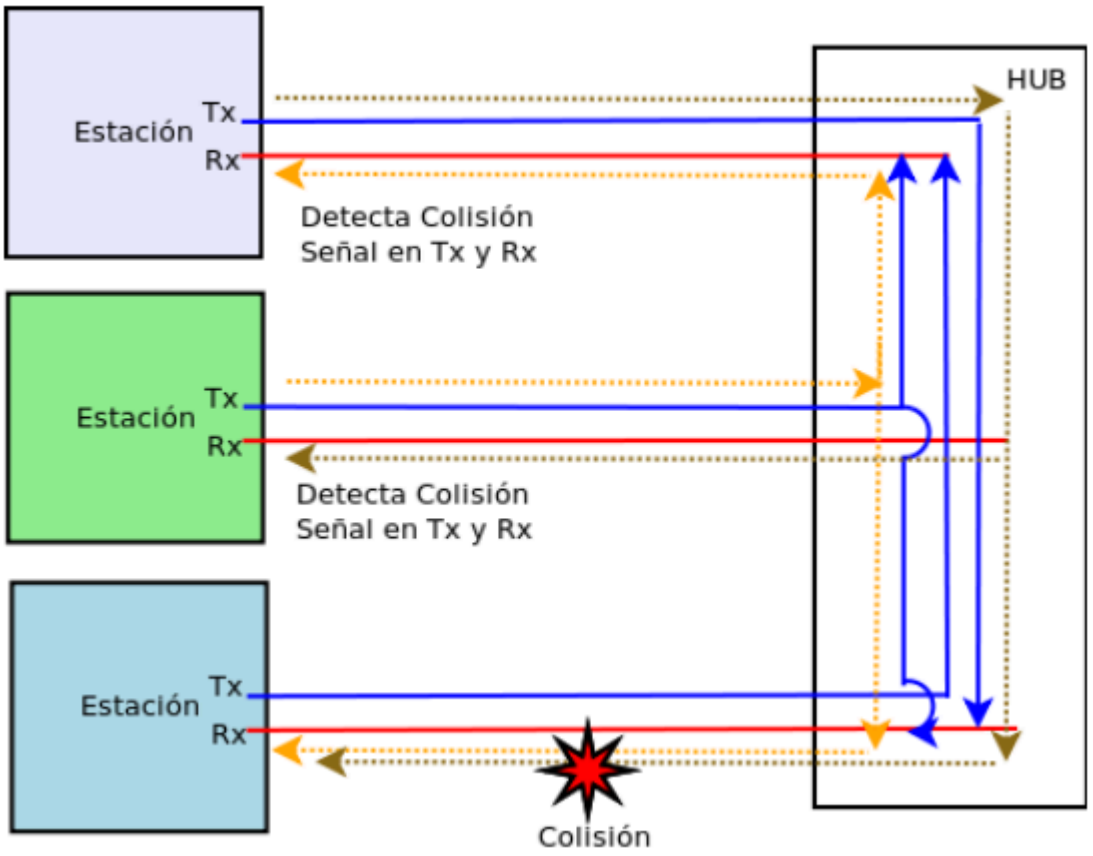
Regenera la señal une dominios de colisión generando un único, permite extensión



Hub

Repetidor multipuerto

Usado en 10BaseT y 100BaseT

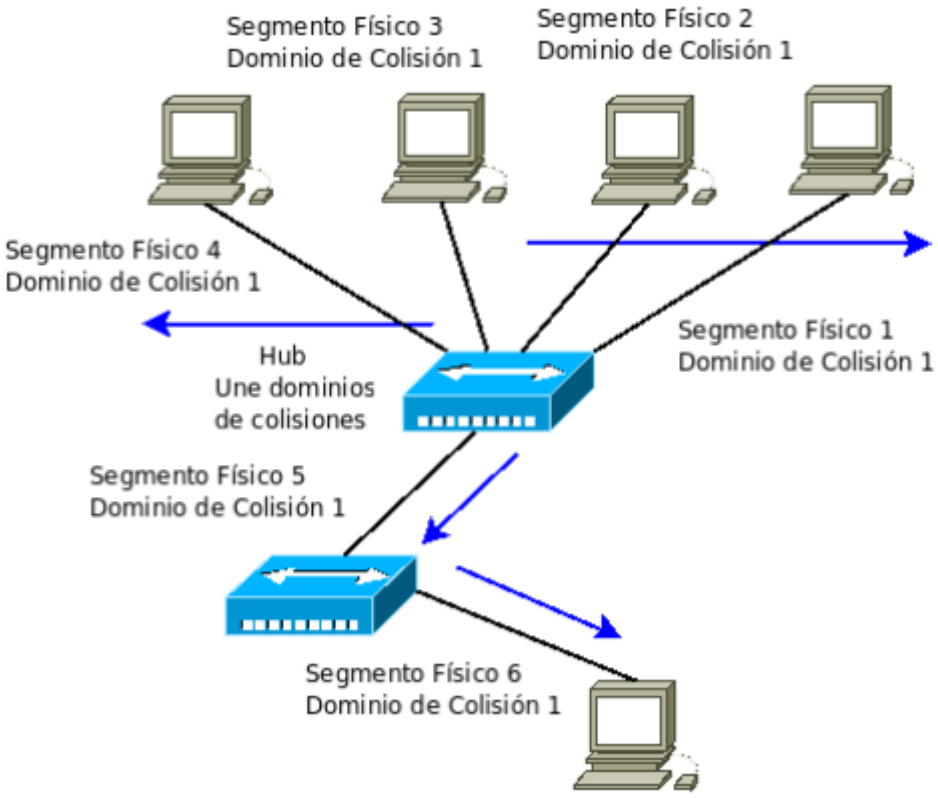


Tipos de Hubs

- Hubs pasivos: solo envían la señal por todos los puertos restantes
- Hubs activos: regeneran la señal, mayor alcance
- Hubs inteligentes: pueden poseen administración, permiten detectar problemas. Los hubs pueden detectar colisiones y generar JAMs

Cascadas/Uplinks

Permitir interconectar concentradores y repetidores para extender la red



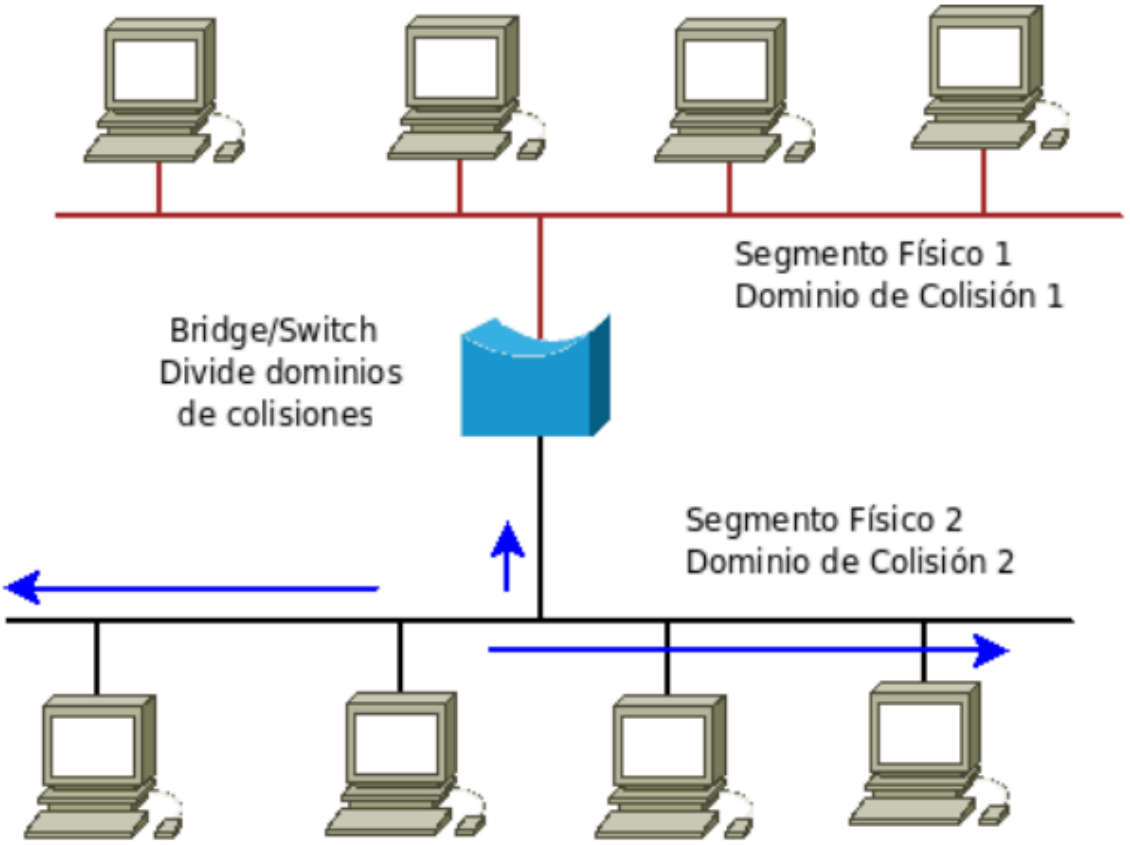
Bridge

Permite:

- Adaptar entre dos protocolos de nivel de enlace o físico, pueden ser diferentes
- Dividir dominio de colisión

Características:

- Permite escalabilidad
- Implementado por software
- Dos puertos en general
- Bridge Ethernet podría adaptar dos tecnologías de nivel físicas, e.g.: 10Base2 y 10BaseT



Switch

Un bridge multipuerto que trabaja con la misma tecnología de enlace y física en c/u
Trabaja en hardware, ASIC, múltiples puertos
Puertos trabajan en FDX, micro-segmentación

Razones para usarlos

- Dividen la red en partes más pequeñas (dominios de colisiones, micro-segmentación)
- Seguridad: VLANs, admin
- Mejoran el rendimiento de la red. FDX vs. HDX
- No hay colisiones
- Los switches tienen menor delay
- Actualidad Switches multilayers o L3/capa3

Funciones del switch

- Aprender direcciones MAC: el dispositivo guarda las direcciones MAC asociadas a cada puerto en una base de datos
- Reenviar/filtrar paquetes: al recibir una trama, el switch revisa su base de datos MAC para determinar a través de qué puerto puede alcanzar la dirección de destino
- Evitar bucles de capa 2: los switches administran los bucles de redundancia con STP. Bridges sólo una instancia de STP, switches podrían correr varias

Métodos de conmutación de tramas

- Store and Forward (Almacena y Envía):
    - Lee toda la trama y chequea CRC
    - Más seguro
- Fragment Free (Libre de Fragmentos):
    - Lee los primeros 64 bytes
- Cut-through (de corte):
    - Lee hasta la dirección destino
    - Más rápido

VLANs

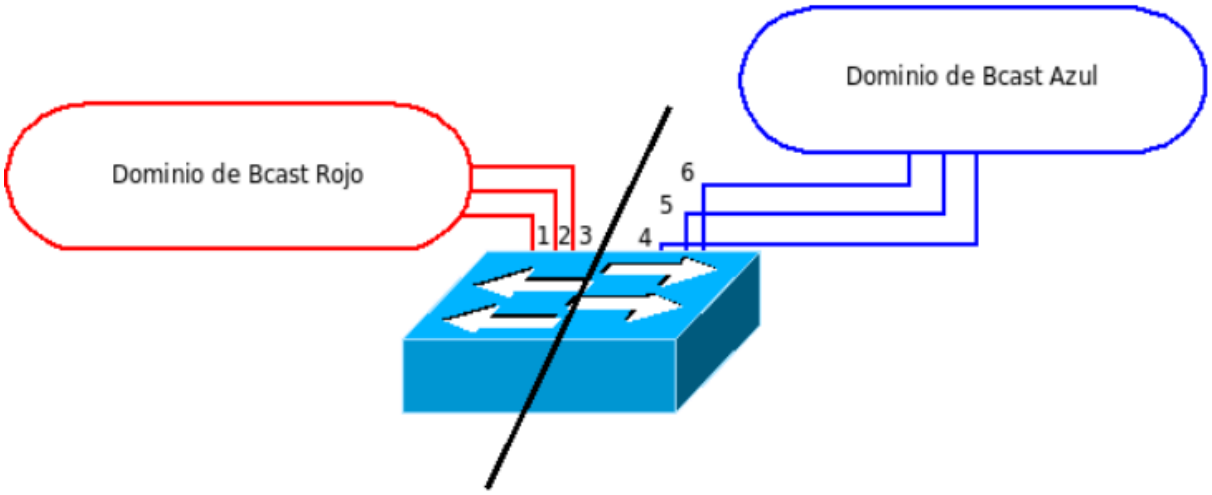
Dividir un switch en switches virtuales cada uno sobre una VLAN (Virtual LAN)

Cada VLAN es un dominio de broadcast independiente

Para lograr conectividad se deben conectar mediante uplinks o routers

Los uplinks compartidos entre VLANs marcan el tráfico con TAGs: 802.1Q tagged ports/trunks

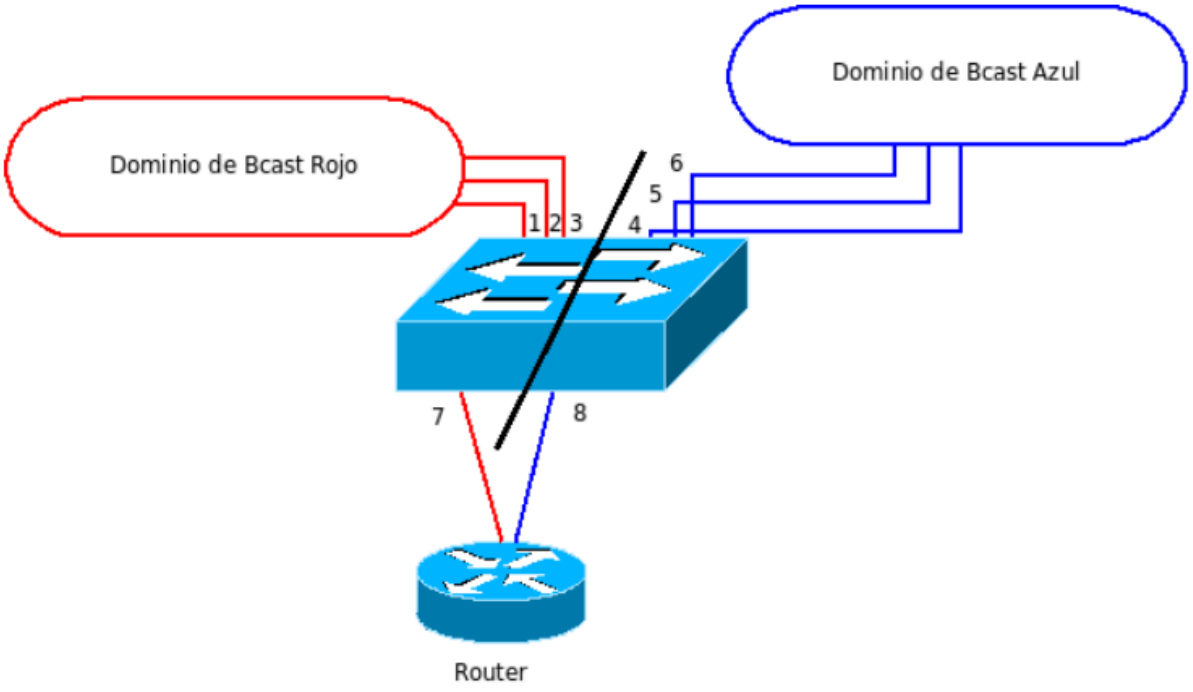
Separadas



Divide dominios de broadcast independientes

Cada puerto en una VLAN (dominio)

Conectadas



Interconectar VLANs mediante dispositivo L3 (router)

Clase 3 - ARP

ARP

Protocolo de L2, a veces considerado L3

Protocolo “Helper” de IP

Mapea Dir. Lógicas (IP) a Dir. Hardware (MAC)

Trabaja conjuntamente con Ethernet (u otros protocolos de L2 multiacceso con broadcast: Token Ring, FDDI, 802.11)

Trabaja de forma dinámica, auto-aprendizaje, sin configuración

Puede configurarse de forma estática

Definido en RFC-826

RARP (Reverse Address Resolution Protocol)

Protocolo de L2, utilizado para mapear direcciones físicas (MAC) a direcciones lógicas (IP)

Utilizado en redes multiacceso como Ethernet

Utilizado por estaciones sin disco para obtener su dirección IP

Hoy es un protocolo en desuso, superado por BOOTP/DHCP

RFC-903