Yeison Melo
melocuentamaster@gmail.com
Si encuentras algun error no dudes en hacermelo saber, gracias. Las faltas ortográficas no cuentan ;)

Tipos de redes
Clasificación segun el alcance:

- Wide Area Network, WAN (red de area extendida) : pueden cubrir un area geografica extensa con un numero ilimitado de estaciones. Lo más importante en este tipo de redes es la escalabilidad.
- Local Area Network, LAN (rede de area local): nombre limitado de equipos en un area geografica pequeña, un edifició por ejemplo.

Clasificación segun la extrategia de connexión:

- Switched network (red conmutada): esta formada por una interconnexión de switches/comutadores que tienen como objetivo encaminar la informacón entre los nodes. La ventaja principal es la escalabilidad por este motivo las WANs son siempre redes commutadas.
- Multiaccess network (red de acceso multiple): en este caso el medio de transmisión es compartido y cuando la estación transmisora envia un mensaje lo reciben todos las estaciones conectadas al medio pero solo el destinario se lo queda el resto lo descartan. Suelen ser más baratas de implementar (switches caros) por lo que su uso habitual es en LANs. Se necesita un protocolo de control de acceso al medio (Medium Access Control, MAC).

Arquitectura IEE de una LAN
Estandarización de LANs por parte de IEEE, todos tienen el prefijo 802.x. Separa la capa de enlace datos en dos capas:

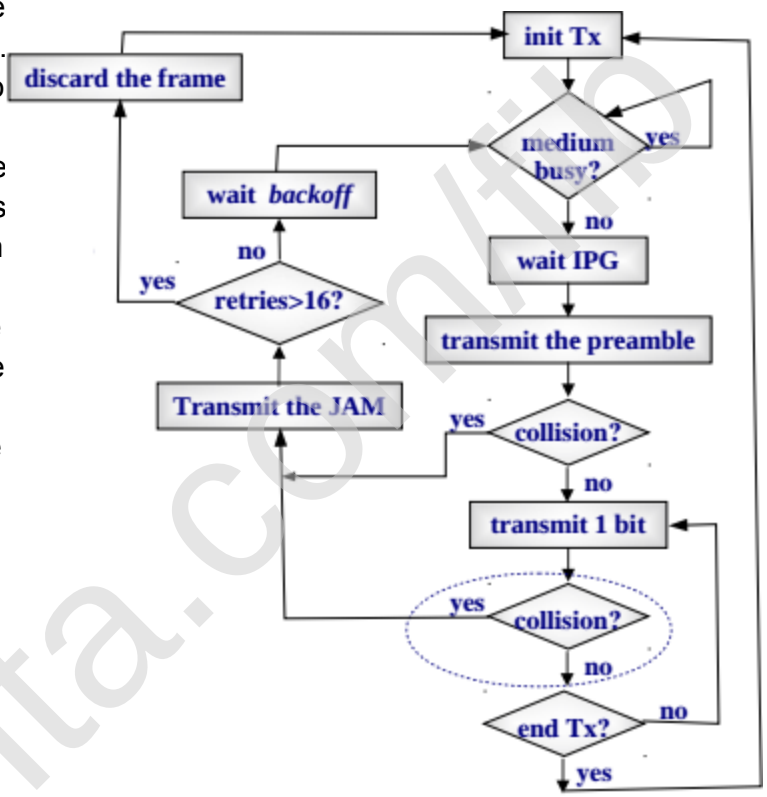
- Logical Link Control (LLC): comun en todos los estandares. Define la interficie con la capa superior, espeficifica 3 tipos de servicios: no orientados a la connexión, orientado a la connexión y confirmados y no orientados a la conexión. Añade cabecera con los campos destination SAP(Service Acces Point, identifica el protoloco de la capara superior), source SAP (información para el protocolo de capara superior) y control (indetifica el tipo de frame).
- Medium Access Control (MAC): diferente para cada tecnología LAN. Se encarga de controlar el acceso al medio. Añade cabecera con los campos MAC destino, Mac origen, Control (información para el funcionamiento del protocolo), Payload(PDU del nivel superior) y CRC (control de errores equivale al checksum de TCP)

Tipos de MACS

- Token passing (paso de testimonio): acceso regulado por un testimonio/toke, el dispositivo que lo tiene es el unico que puede transmirtir y el resto permanece en silencio. Normalmente, desues de transmitir una la estación pasa el token.
- Acceso al medio aleatorio: no hay token, las estaciones intentan transmirtir en el momento decesado, si coincide con otra transmisición tendremos una colisición y las estaciones esperaran un tiempo aleatoreo (backoff) para volver a intentarlo. Probabilidad no nula de colisión.

- Carrier Sense Multiple Acces/Collision detection (CSMA/CD): en este caso particular de acceso aleatoreo, la estación “escucha” el medio antes de transmitir. Es el protocolo utilizado por las **LANs Ethernet**.

- Después de detectar que el medio esta libre se espera un tiempo IPG (96bits) para transmitir. Después de este transmitira aunque el medio este ocupado.
- Al detectar una colisición se emite el señal de jam/congestión (32bits) asegurando que todas las estaciones detectan la colisición y descarten la trama.
- La transmisción del preambulo nos e interrumpe aunque haya colisición se comprobara al final.
- Si se ha intentado transmitir un mismo frame mas de 16 veces con colisición se descarta.



Transmissión y recepción
Full duplex: enviar y recibir a la vez por lo tanto se desactiva el mecanismo CSMA/CD, no pueden corrurir colisiones. Las targetas de red estan coenctadas, punto a punto, utilizan un mecanimos que poseen de

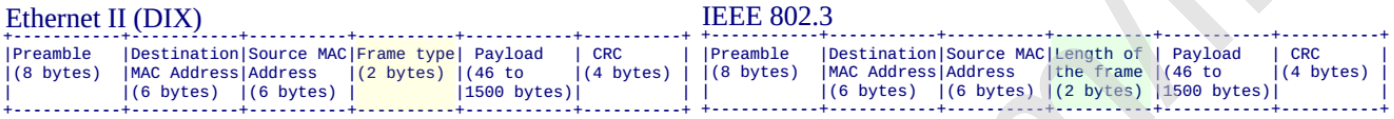
auto-negociación para detectar si ambas pueden utilizar este modo. Dado que se necesitan lineas separadas para enviar y recibir no todos los estandares soportan este modo. Si uno de las dos NICs no lo soporta se trabajara en Half Duplex.

Half duplex: en este caso solo se puede enviar or recibir por lo tanto se necesita un CSMA/CD para intentar evitar colisiones.

Ethernet

Formatos de trama

En la prática se utilizan dos formatos de trama



Preambulo: sirve pra sincronizar las targetas en la recepción de la trama.
Tipo: identifica el protocolo de la capa superior → trama DIX no utiliza la capa intermedia LLC
Payload: campo de información tamaño entre 46 y 1500. Si el tamaño es inferior a 46 bytes se añaden de relleno al final. Ya que con tramas menores a 46bytes es posible que no se detecte una colisión al ser tan pequeñas que antes de que se detecte ya se haya dado por enviada completamente sin problemas.
CRC: detección de errores.

La unica diferencia es el campo tipo en la trama IEEE es el tamaño del Payload así podemos saber cuantos bytes extras se han añadido para llegar al tamaño minimo ya que el campo Lenght no lo tiene en cuenta. En Ethernet por lo tanto hace falta un mecanismo adicional. Por otro lado el tamaño del campo Type de la trama DIX es siempre major a 1500 por lo tanto si es igual o menor se identifica como una trama 802.3.

Denominación XBaseY

las X hace referencia a la velocidad de transmissión en Mbps. Base hace referencia a que la codificación es en banda base. Finalmente la Y puede tener diferentes significados si es un numero se refiere a la distancia máxima del segmento en centenares de metros, sino hace referencia al medio de transmisión T:UTP, F: fibra optica, TX: full duplex….

Dispostivos:

Hubs: todo lo que reciben por un puerto lo transmiten por resto de puertos. Puede ser ineficiente dado a que propagarán las colisiones (señales de jam). Todos los dispotivos conectados a un hub forman un unico dominio de colisión.

Bridges: tiene un numero reducido de puertos 2 por ejemplo. Trabaja en la capa 2 (enlace de datos modelo osi), en cada puerto tiene una NIC que trabaja en modo “promiscuo” (captura todo el trafico que circula) . Dispone de una tabla MAC con las tuplas {MAC,puerto}. Es decir tiene las direcciones MACs que cuelgan de cada puerto. El bridge construye dicha tabla cada vez que le llega una trama añade el puerto y la MAC

origen a en su tabla. Despúes mira la dirección MAC destino y encuentra en que puerto se encuentra mirando la tabla para enviarlo por este, sino no tiene dicha dirección en su tabla o si es una MAC de broadcast, enviará la trama por todos los puertos menos por el que lo ha recibido. Si detecta que el destino esta conectado al mismo puerto por el que ha recibido la trama la descarta. De aquí se desprende que cada puerto de un bridge es un dominio de colision diferente y por lo tanto los segmentan. Las entradas en la tabla tienen un time-out que se refresca cada vez que una entrada se utiliza, si salta el time-out la entrada se borra, de esta forma se mantienen las tablas pequeñas y actualizadas.

Switch: tiene la misma funcionalidad que un bridge pero con más puertos y mayor capacidad de conmutación de trama entre los puertos (dos o más pares de puertos pueden estar transmitiendo información a la vez). Cada puerto de un switch es un dominio de colisión. Los puertos pueden transmitir a diferentes velocidades y en full o half duplex. Seguridad → las estaciones solo pueden capturar el trafico de sus dominios de colisión.

Router: tienen el mismo funcionamiento que los switch pero con una importante diferencia segmentan los dominios de broadcast (direcciones MAC utilizadas por protocolos, para hacer llegar la trama a todos las estaciones de la red, como puede ser ARP. Es decir cuando un router recibe una trama de broadcast (FF:FF:FF:FF:FF) la descarta a diferencia del switch o bridges. De aqui se desprende que: todos los equipos conectados a un mismo switch o bridge forma un mismo dominio de broadcast y que cada puertod e un rputer es un domino de broadcast diferente. De aquí que el protocolo ARP visto en temas anteriores no pueda resolver @IPs que esten fuera de su dominio de broadcast ya que para abandonar este necesitan un router.

Switches - Control de flujo

Antes hemos visto que los puertos transmiten de forma independiente entre ellos y que por lo tanto a diferentes velocidades. Si en un extremo de un puerto tenemos una estacion que transmite a una velocidad más elevada que la estación receptora, la cola del puerto al que esta conectado la estación receptora se llenara rapidamente y empezaremos a peder tramas. Cuando esto pasa se activa el control de flujo para conseguir adaptar la velocidad del puerto más rápido a la del más lento. El switch frena la transmisión de datos del puerto que envia datos hacia el puerto congestionado, hay dos técnicas:

- Señal Jabber (half duplex): el switch envia una señal por el puerto por lo tanto las estacones conectadas que estarán utilizando CSMA/CD dejarán de transmitir al ver el medio ocupado.
- Frames de Pause (full duplex): el switch envia una trama especial con un entero (2bytes) indicado el numero de “slot times” que la estación debe estar en silencio.

Visto el funcionamiento del flujo de control podemos deducir que puede introducir ineficiencias ya que aunque tengamos un equipo que transmita a una determinada velocidad si lo hace hacia un equipo menos potente deberá adaptarse a este al realizar la conexión mediante un switch.

Switches - Spining tree protocol

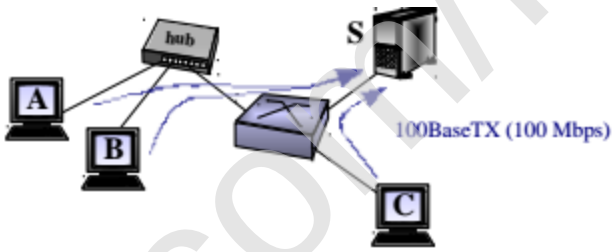
En una red no podemos tener un bucle formado por switches, si una estación envia una trama de broadcast esta se transmitiria de forma indefinida en la red ya que cada switch la enviaría por todos sus

puertos, después el rebote de otro switches de los que forma el bucle, probocando lo que se conoce como una tormenta de brodcast.

Pero pese a esto puede que tenegamos bucles de switches en nuestra red sea por error humano o para tener mas de un camino en caso de fallo de alguna linea. Para resolver este problema tenemos el STP básicamente los switches intercambia una serie de mensajes para obtener una red en forma arborea, para que esto suceda el STP puede bloquear puertos de algunos switches. Los puertos que estan en este estado descartan todas las tramas que reciben y solo procesan los mensajes STP de forma que pueden volver a estar activos si hay algun cambio en la topologia.

Reparticion del medio de transmisión

Hubs: si tenemos un cuello de botella (varias estaciones trasmitiendo a la vez) la velocidad del puerto receptor es repartida de forma igualitaria entre **todos** los puertos activos del hub.



If A, B and C simultaneously transmit to S:
throughput C ≈ 100 Mbps / 2 = 50 Mbps
throughput A = throughput B ≈ (100 Mbps / 2) / 2 = 25 Mbps

Switch: la velocidad transmisión de la estacion receptora es repartida entre los diferentes puertos que envian hacia esta de forma igual.

LAN's virtuales

Motivación: eficiencia y seguridad al tener los equipos separados en dominios de broadcast diferentes. Independencia de licalización de los equipos de una misma VLAN.

Cada VLAN funciona como una red diferente y por lo tanto cada uno tiene asociacda una dirección red diferente. El tipo más conocido es VLAN's por puertos. Cada puerto del switch corresponde una VLAN diferente. Para cada uno el switch tiene una tabla MAC diferente. Si llega una trama de broadcast solo sera enviada por los otros puertos que pertenezcan a la mismaVLAN, de aqui que las VLANs segmenten los dominios de brodcast.

Para no tener que conectar más de un puerto entre dos switches o un router con un switch, para comunicar equipos separados que **pertecen a la misma VLAN** se utilizan los enlaces trunking. Estos enlaces sopartan el trafico de más de una VLAN cuando una trama es enviada se añade un *tag* que identifica la VLAN a la que pertenece y que es eliminado cuando viaja por un enlace que no es trucking.

Cada VLAN tiene una dirección de red diferente. Por lo tanto cuando intento comunicar con un dispositivo de la misma VLAN , aunque este en un lugar totalmente diferente al origen, no hace falta direccionamiento de nivel 3 (ip) y por lo tanto el intercambio de información es entre dispositivos de la capa 2 (tramas - switch/es, de workers en IDF-1 a workers IDF-2 o MDF). Cuando intento comunicarme con un equipo de otra VLAN la dirección de red cambia y por lo tanto si necesito direccionamiento IP que solo lo puede proporcionar el router, por lo tanto el paquete se envia al gate way por defecto pasando antes por el switch (de cualquiera de workers a cualquiera de programmers o direction).

Internamente el switch se encagar de hacer un mapeo para que su funcionamiento sea el usual (antes explicado) pero solo dentro de la VLAN de la trama que ha recibido, sea en el momento de detectar donde esta el destino y hacer llegar la trama a este o de guardar la direccion MAC origen.