Redes de Área Local

Redes de área local

Introducción al Curso

Bienvenidos al curso Redes de Área Local.

En este curso pretendemos:

- **Obtener una visión tecnológica y actualizada de las redes de difusión desde el punto de vista de la tecnología predominante en el mercado: Ethernet.**
- **También verás la evolución de estas redes, los elementos de interconexión y sus características diferenciales.**

¡¡ADELANTE!!

1 Introducción a las LAN

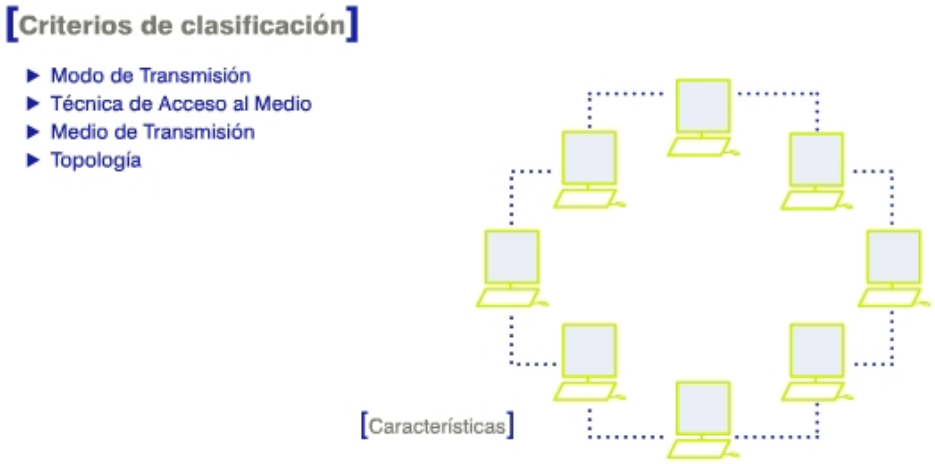
Introducción a la Sección 1

Vas a comenzar el apartado 1:

Introducción a las LAN

Vamos a adentrarnos en el mundo de las redes de área local (LAN). Para ello aclararemos la definición de una LAN, tal y como se concibe actualmente, definiremos las características que diferencian y determinan las tecnologías existentes y las normativas o estándares desarrollados por el IEEE.

Definición



Definición: una LAN (Local Area Network) es una red de DIFUSIÓN de paquetes.

El concepto original parte de la idea de compartir el mismo medio de transmisión por varios dispositivos. En su forma más simple, la transmisión desde una estación es difundida hacia el resto de estaciones.

Según el concepto del Proyecto IEEE 802, una LAN puede describirse por su función y características, en base a lo cual podemos definir:

- **Área moderada**: normalmente una LAN se expande en torno a una distancia de 5 Km.
- **Privada**: pertenencia a una única organización.
- **Canal de comunicación de capacidad media/alta**: Ethernet, tecnología predominante en el mercado, tiene capacidades de transmisión hasta 10Gbps.
- **Baja tasa de errores**.

Modo de transmisión

Se entiende por tal a la manera de aprovechar la capacidad de transmisión del medio físico. Esto es, analógico (banda ancha) o digital (banda base).

Técnica de acceso al medio

Dado que las LAN parten de la base de compartir el medio de transmisión, existen métodos que permiten a los diferentes nodos acceder al medio de forma ordenada y sin conflictos con los demás usuarios.

Medio de transmisión

Define las características del medio físico de interconexión de los elementos conectados a la red.

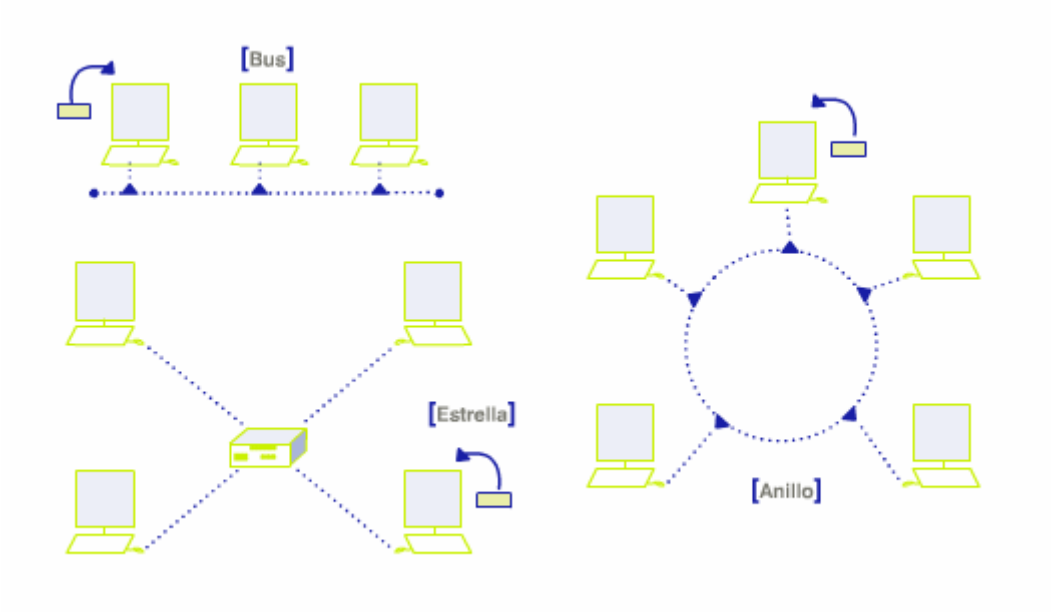
Topología

Define las relaciones de interconexión de los diferentes componentes de la red: bus, anillo, estrella, árbol.

Relación de ideas clave

Una vez que conocemos qué es una LAN, sus principales características y sus criterios de clasificación, veamos ahora cuáles y cómo son las topologías más utilizadas en las LAN.

Topologías LAN



Básicamente, existen 3 topologías: bus, anillo y estrella.

La topología en **árbol** se logra mediante la interconexión de "estrellas".

Topología en bus

En una red en BUS, todos los dispositivos se conectan a un cable de transmisión común, distribuidos a lo largo del mismo. Este cable difunde la información a todas las estaciones.

Topología en anillo

Los nodos conectados están dispuestos de manera que formen una configuración circular sin interrupciones. Los mensajes viajan de un nodo a otro a lo largo del anillo. Los nodos actúan como repetidores activos retransmitiendo los mensajes dirigidos a los demás nodos.

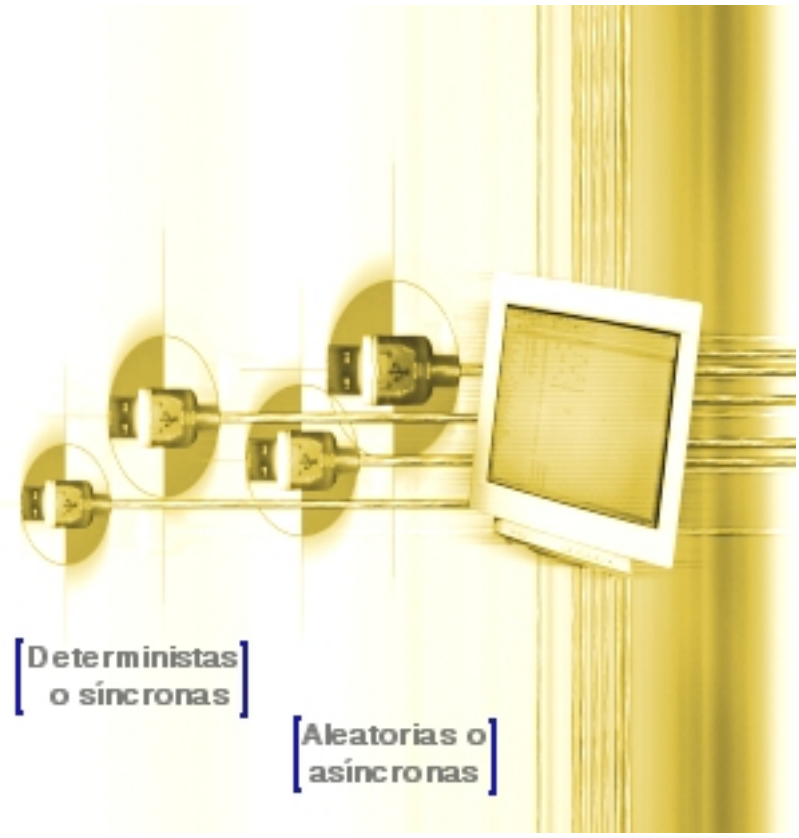
Topología en estrella

Se caracteriza por la existencia de un dispositivo central o conmutador al que se conectan todos los dispositivos por enlaces punto a punto individuales. El nodo central puede ser mas o menos “inteligente” realizando desde una simple función de interconexión hasta otras más complejas como cambio de protocolos, formatos o velocidades.

Relación de ideas clave

Ya que conocemos las topologías, veremos ahora cómo se controla el acceso al medio, es decir, cómo evitar transmisiones simultáneas e identificar a los nodos en la red.

Técnicas de acceso al medio



Son necesarias debido al hecho de que ese medio debe ser compartido por todas las estaciones.

Definen qué dispositivos obtienen el uso del canal o medio de la red, evitan la transmisión simultánea (sólo una estación puede utilizar el canal en un instante dado), controlan el tiempo de uso del canal e identifican y discriminan origen y destino de los mensajes (direcciones físicas de los dispositivos).

Podemos diferenciar dos categorías en las técnicas de acceso al medio.

Deterministas o síncronas

En ellas existe un criterio prefijado de acceso al medio, pudiendo ser este criterio establecido por un elemento central (control centralizado) o conocido por todos los elementos de la red (control distribuido).

Aleatorias o asíncronas

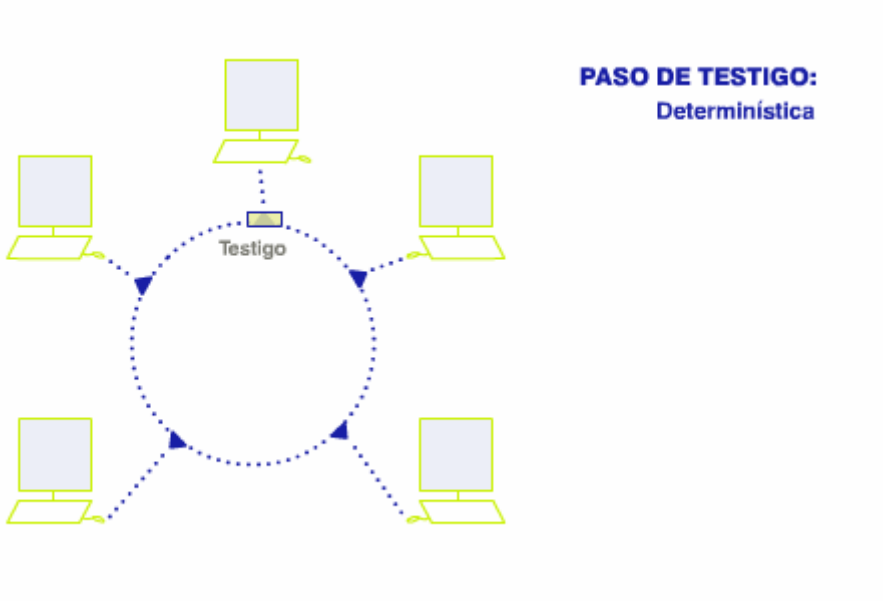
En ellas no existe un criterio fijado de antemano para el acceso al medio, sino que se establece una competencia (contienda) entre todos los elementos de la red para el acceso al medio.

Relación de ideas clave

Veamos ahora las tres técnicas de acceso al medio más utilizadas:

- Token o Paso de testigo.
- Polling o Sondeo.
- CSMA: contienda.

Token o Paso de testigo



Las técnicas de "token" o paso de testigo se basan en la existencia de un mensaje predeterminado conocido como token, que da derecho a transmitir a la estación que lo posee. Es, por tanto, una técnica determinística.

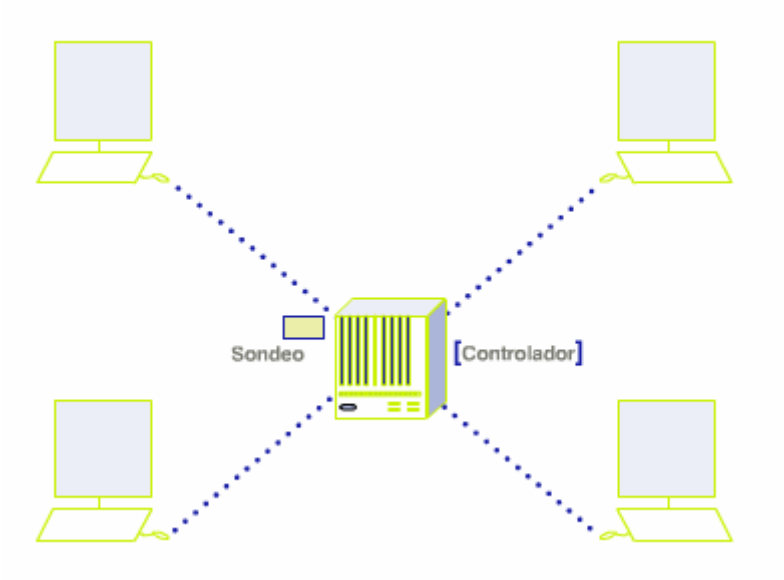
En el caso de topología en anillo, una estación que reciba el testigo y tenga datos que transmitir lo retendrá y pasará a emitir. Una vez terminado el envío de datos pasará a retransmitir el testigo a la siguiente estación en el anillo.

Si una estación recibe el testigo y no tiene información para enviar, se limita a pasar el testigo a la siguiente.

En el método de token no hay un nodo que centralice el control sino que éste va pasando secuencialmente de estación en estación. Sólo es necesaria cierta especialización para el momento del arranque ya que debe haber un nodo específico que ponga en circulación el testigo.

La técnica de paso de testigo, aunque orientada básicamente a anillos (Token Ring), se puede aplicar también a la topología en bus (Token Bus).

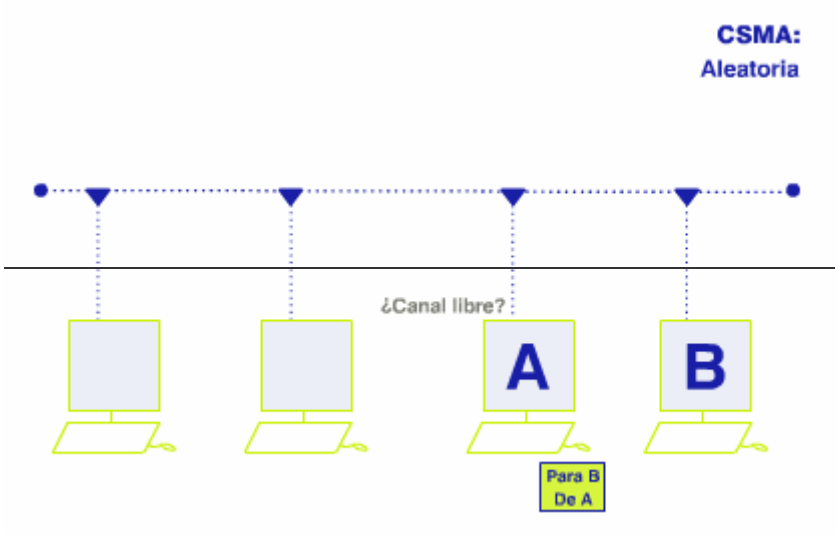
Sondeo

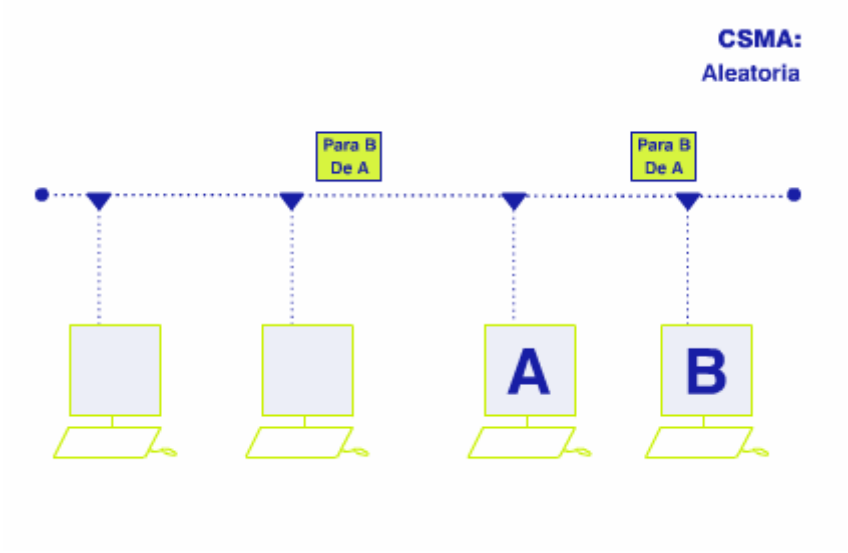


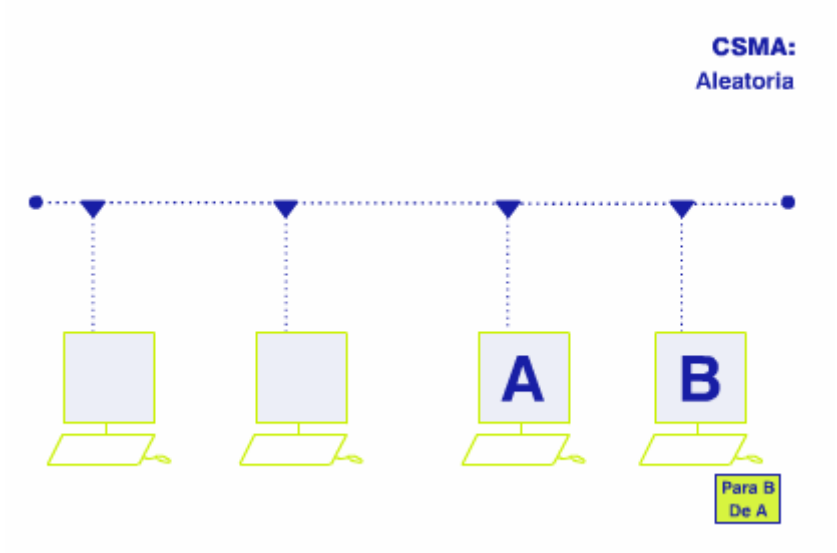
Las técnicas de sondeo, también determinísticas, centralizan el control de acceso al medio en un elemento denominado Controlador o Maestro, el cual pregunta a cada elemento de la red (nodos secundarios), acerca de su necesidad o no de transmisión en un orden predeterminado.

De ser afirmativa la respuesta, la estación trasmite, usualmente a través del propio controlador, en una topología en estrella.

Contienda


CSMA:
Aleatoria
¿Canal libre?
A
B
Para B
De A


CSMA:
Aleatoria
Para B
De A
Para B
De A
A
B


CSMA:
Aleatoria
A
B
Para B
De A

Las siglas CSMA responden a ***Carrier Sense Multiple Access*** **(acceso múltiple con detección de portadora)** y consiste en que cualquier nodo puede enviar un mensaje por el medio común (acceso múltiple) en el momento que lo desee, siempre y cuando no haya otro transmitiendo en ese momento.

Para ello se observa previamente si el canal está ocupado (detección de portadora).

Esto es lo que en lenguaje sencillo se denomina, “escuchar antes de hablar".

Direcciones MAC

Las técnicas de acceso al medio definen, también, que los dispositivos han de estar identificados físicamente en la LAN.

Es lo que conocemos como direcciones MAC.

Los paquetes que se difunden por la red han de llevar identificadores denominados DIRECCIONES MAC o DIRECCIONES FÍSICAS.

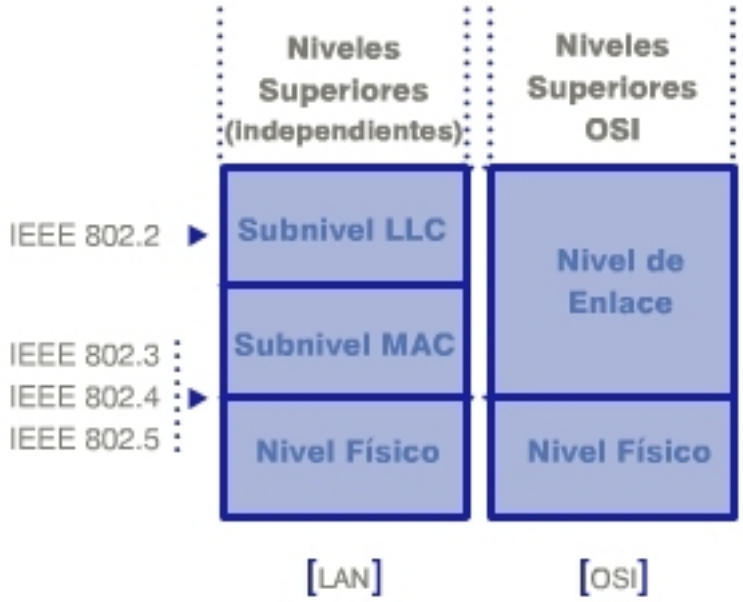
Son números asignados por los fabricantes e introducidos en las interfaces de red (por ejemplo, en el firmware de la tarjeta de red).

Digamos que son como una huella digital: **inmutables y únicas**.

Ahora, conocemos la definición y características de cualquier LAN. Cabe resaltar que la diferenciación real entre una tecnología y otra es la técnica de acceso al medio que cada una utiliza.

Vamos a ver ahora la relación entre las arquitecturas LAN y el modelo OSI.

Normalización LAN



Cuando comenzó el trabajo OSI, se partió de la base de una comunicación punto a punto. En las LANs, donde un único medio físico, sea cual sea su topología, es compartido por numerosos dispositivos, el concepto cambia: se necesitaba una nueva función o servicio para el control de acceso al medio.

Así, el nivel de enlace está dividido en dos subniveles: el **subnivel MAC**, que se encarga de controlar el acceso al medio y define las direcciones físicas de los dispositivos, y el **subnivel LLC** que establece y gobierna el enlace una vez que se ha conseguido (tal y como define OSI).

La función de estandarización de las LAN la ejerce el IEEE **(instituto de ingenieros en electricidad y electrónica)**. En concreto, el comité 802 ha presentado una serie de normas llamadas en su conjunto IEEE 802. Cada tecnología recibe el nombre del subcomité que trabaja en ella.

- **IEEE 802.2**
  Esta norma es aplicable al nivel de enlace del OSI, concretamente al subnivel superior de los dos en que el IEEE divide este nivel, y que se denomina control de enlace lógico (LLC).
- **IEEE 802.3** Define el funcionamiento y protocolos para redes que utilicen control de acceso al medio CSMA/CD (Ethernet).

- **IEEE 802.4** Estándar para redes con topología en bus y técnica de acceso de paso de testigo (Token Bus).
- **IEEE 802.5** Estándar para redes con topología en anillo y técnica de paso de testigo (Token Ring).
- **IEEE 802.11** Define las especificaciones para redes inalámbricas, con acceso mediante CSMA/CA (carry sense multiple access with collision avoidance).

Los niveles inferiores de OSI (1 y 2) se relacionan con las tecnologías de red empleadas (LAN y WAN) y definen, de forma básica, las siguientes funcionalidades:

Nivel 2. Enlace: proporciona el control de sincronización y de errores.

Nivel 1. Físico: provee las características funcionales y de procedimiento para activar, mantener y desactivar la conexión física. Las características eléctricas y mecánicas constituyen la interfaz con el medio de transmisión externo.

Los niveles superiores (3 al 7) se conocen como niveles de usuario y definen, por ejemplo, sistemas operativos de usuario (arquitectura Microsoft, SNA, Novell, etc).

Resumiendo

Hoy por hoy, donde el concepto de compartir el medio de transmisión no es evidente, las redes de área local se diferencian de las tecnologías WAN por su capacidad de difusión ilimitada a todas las estaciones o dispositivos de la red: el BROADCAST, de ahí que se las denomine redes de DIFUSIÓN.

Además, dado que no existía una definición clara en el nivel dos para la implementación del acceso al medio, se definió un subnivel adicional conocido como subnivel MAC, responsable del acceso y direccionamiento dentro de la LAN.

En cualquier tecnología LAN, los paquetes generados por este subnivel y que se entregan a la red contienen, en su cabecera, la dirección MAC destino y origen del mensaje.

Diferentes modos de transmisión, topologías y medios de transmisión pueden ser utilizados en una misma tecnología LAN, incluso varias tecnologías pueden tener características muy similares.

Lo que realmente caracteriza una determinada tecnología es la técnica de acceso al medio empleada.

Por ejemplo, Token Ring es una tecnología que utiliza técnicas de paso de testigo en anillo, Token Bus utiliza paso de testigo con topología en Bus y Ethernet es CSMA/CD, con muy diversas topologías, velocidades, medios y modos de transmisión.

2 Ethernet

Introducción a la Sección 2

Vas a comenzar el apartado 2:

Ethernet

Como habíamos comentado, Ethernet es la tecnología LAN más utilizada en el mundo. El por qué, su evolución y características son el objetivo de este capítulo.

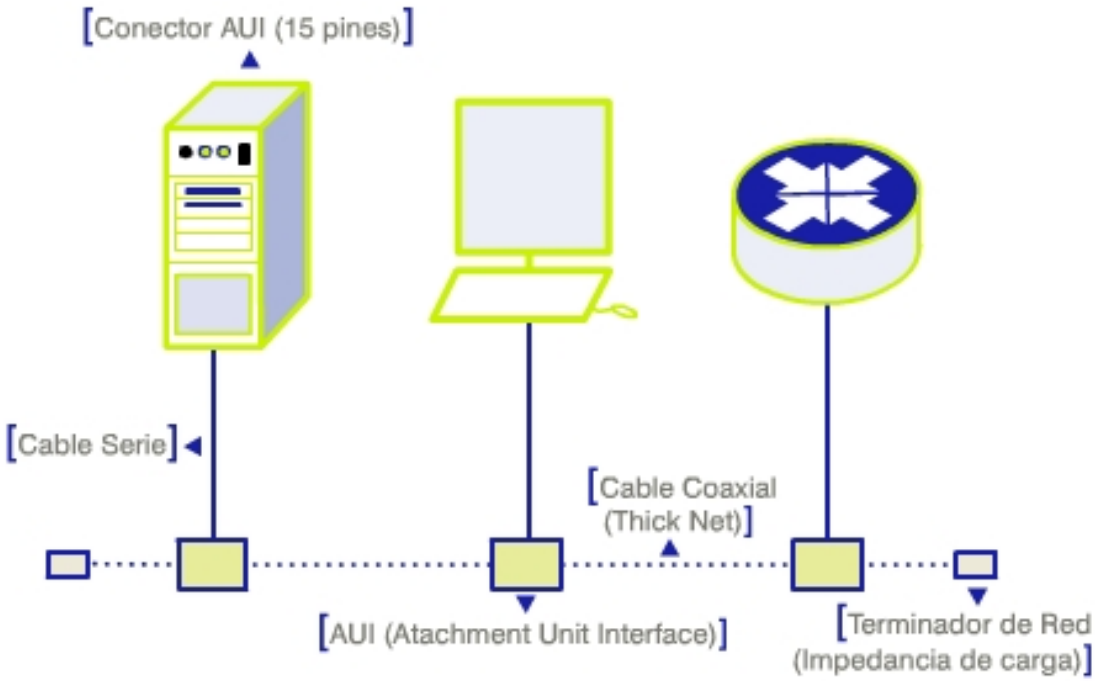
Definición

El término Ethernet se refiere a la familia de productos LAN que abarca el estándar IEEE802.3 y que utiliza como técnica de acceso al medio el CSMA/CD.

Actualmente, cuatro velocidades de operación están definidas:

- **10Mbps** (Ethernet).
- **100Mbps** (Fast Ethernet) .
- **1000Mbps** (gigabit Ethernet) .
- **10000Mbps** (Gigabit Ethernet) .

Antecedentes



Ethernet define una tecnología LAN **desarrollada en los 70s por Xerox**, que opera a 10 Mbps utilizando como técnica de acceso al medio CSMA/CD y como medio de transmisión cable coaxial grueso. En los **80s**, se desarrolla la **especificación IEEE 802.3** basada en esta tecnología, pero con variaciones en las implementaciones a nivel físico de la red (nivel 1). Hoy es la tecnología LAN más utilizada, con más de un 85% de cuota de mercado.

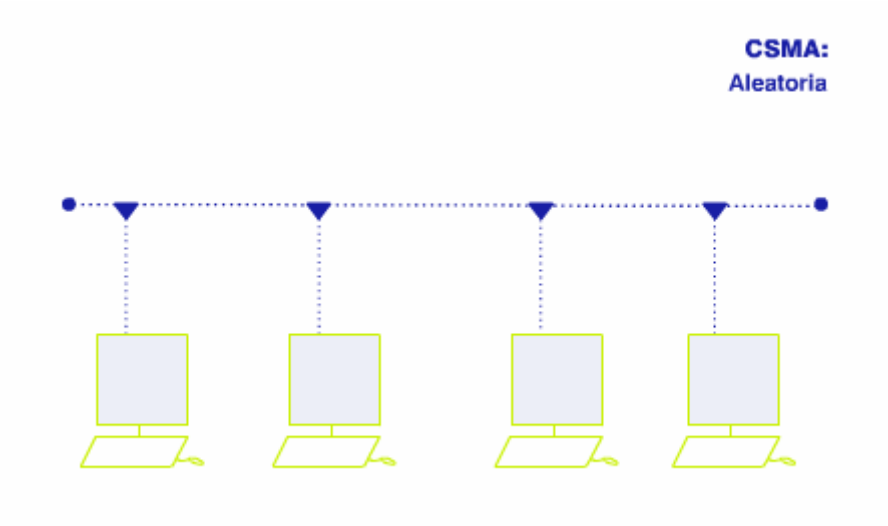
- Es una tecnología sencilla de entender, implementar, administrar y mantener.
- Implementación de bajo coste.
- Flexibilidad y compatibilidad entre las diferentes implementaciones.
- Garantiza la interconexión y operación de cualquier producto de cualquier fabricante.

Relación de ideas clave

En el capítulo anterior mencionamos la técnica de acceso al medio conocida como CSMA.

Veremos ahora que ETHERNET utiliza esta técnica de contienda, con una ligera variante: CD (detección de colisión).

Acceso al medio: CSMA/CD



Las reglas de acceso de CSMA/CD son:

Detección de portadora: cada estación escucha de manera continuada para determinar intervalos donde no ocurran transmisiones.

Acceso múltiple: una estación puede transmitir en cualquier momento en el que no haya tráfico.

Detección de colisión: debido a los retardos de propagación de las señales, la estación sigue "escuchando el canal mientras habla", de modo que si se produce una variación de la señal en la línea respecto a la que está enviando, interpretará que se ha producido una colisión.

En este caso, emite una breve señal de refuerzo de la colisión (jamming) para asegurarse que todos los nodos sean informados del suceso y, así, detengan las transmisiones y temporicen antes de intentar nuevamente transmitir.

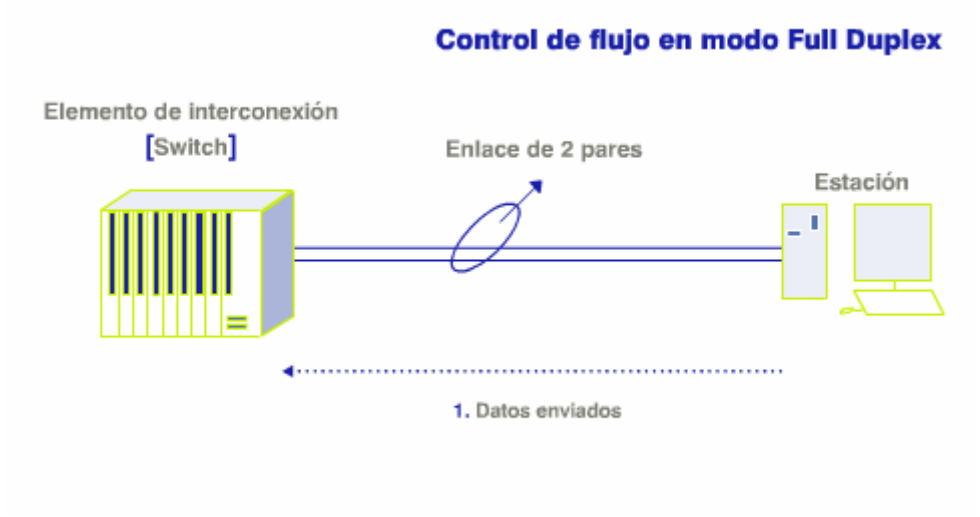
Este tiempo es aleatorio, por lo que normalmente uno de los nodos tomará el canal antes que el resto.

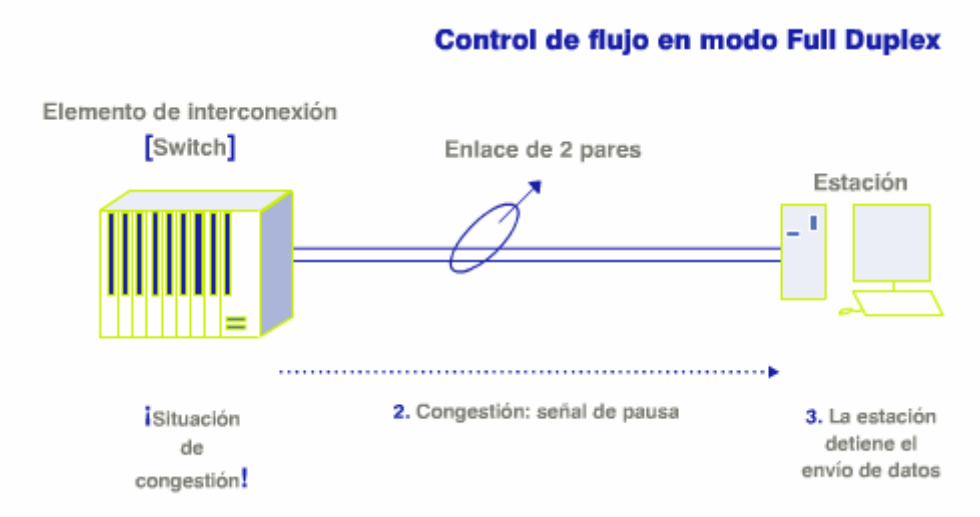
Fíjate que el diámetro máximo del segmento y el tamaño mínimo del paquete Ethernet están íntimamente ligados para que la detección de colisión sea eficaz. Ello define las limitaciones en longitud de segmentos de red y el tamaño mínimo de paquete.

Aunque veremos el formato del paquete posteriormente, esta limitación representa que, para redes de 10 y 100 Mbps, el tamaño mínimo de paquete es de 64 bytes (para redes de 1000 Mbps el tamaño mínimo de paquete ha de ser mayor, 520 bytes).

En un segmento de red, es decir, parte de la red donde no hay discontinuidades del cableado, se define un dominio de colisión como la **zona donde se pueden producir trasmisiones simultáneas y, por tanto, colisiones** (como por ejemplo en la imagen superior).

Transmisión





Ahora que conocemos más en detalle la técnica de acceso al medio utilizada, CSMA/CD, veamos los tipos de transmisión utilizados.

Originalmente, CSMA/CD define transmisión Half Duplex, dado que se utiliza un único conductor, el cable coaxial.

Con la evolución e introducción del par trenzado, aparece la operación en modo Full Duplex, que permite la transmisión/recepción simultáneas sobre enlaces punto a punto (entre estaciones o de la estación al elemento de interconexión).

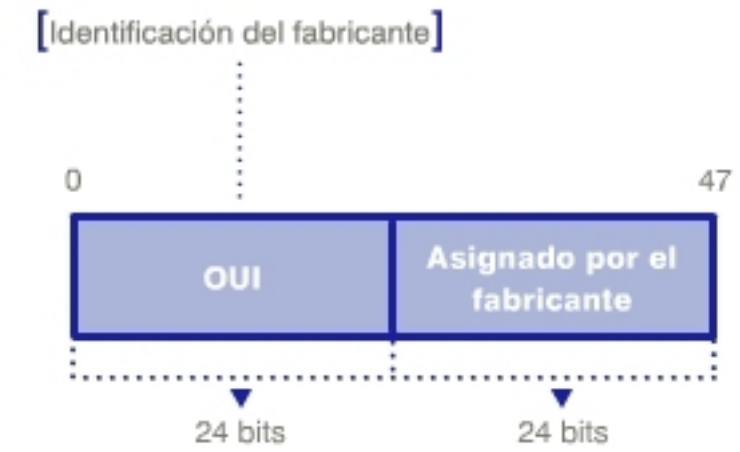
Opcionalmente, también aparece el control de flujo para permitir que, ante congestión en los elementos de interconexión, se pueda informar a la estación que detenga el envío de tramas.

Relación de ideas clave

Como toda implementación de control de acceso al medio (MAC), existen direcciones físicas en ETHERNET.

Veamos cómo son.

Direccionamiento



Ethernet, como cualquier LAN, soporta direccionamiento **unicast** (uno a uno), **multicast** (uno a varios) y **broadcast** (uno a todos).

Una dirección de broadcast son los 48 bits puestos a “1”.

Las direcciones MAC, o direcciones físicas, son direcciones de 48 bits, donde:

- El **OUI**, (Organizationally Unique Identifier), se asigna por la IEEE a una organización (24 bits).
- Los **24 bits menos significativos** son asignados por la organización correspondiente y de forma única a cada adaptador de red (NIC–Network Interface Card).

Relación de ideas clave

Recuerda que el IEEE se encarga de estandarizar las tecnologías LAN.

El subcomité 802.3 es el encargado de Ethernet.

Veamos cómo.

Estandarización

[Ethernet]

CARACTERÍSTICAS	ETHERNET NIVEL FÍSICO
Velocidad (Mbps)	10
Señalización	Banda Base
Longitud Máxima de Segmento (m)	500
Medio de Tx	50-ohm coax (thick)
Topología	Bus

Aunque las especificaciones de Ethernet e IEEE802.3 (nombre que recibe el subnivel MAC en relación al comité del IEEE) son similares en muchos conceptos, existen algunas diferencias.

Veamos.

Ethernet provee servicios correspondientes a los niveles 1 y 2 de modelo OSI.

IEEE 802.3 especifica los servicios asociados al nivel 1 y la porción correspondiente al control de acceso al medio del nivel 2, por lo que no especifica protocolo de control del enlace lógico (la normativa IEEE 802.2 cumple esta función).

Ethernet define una especificación de nivel físico mientras que IEEE 802.3 define diferentes implementaciones a partir de protocolos diferentes de nivel físico, introduciendo el cableado con par trenzado, mediante el uso de HUBs o concentradores de cableado.

Si te fijas, la especificación 10base5 corresponde al Ethernet original.

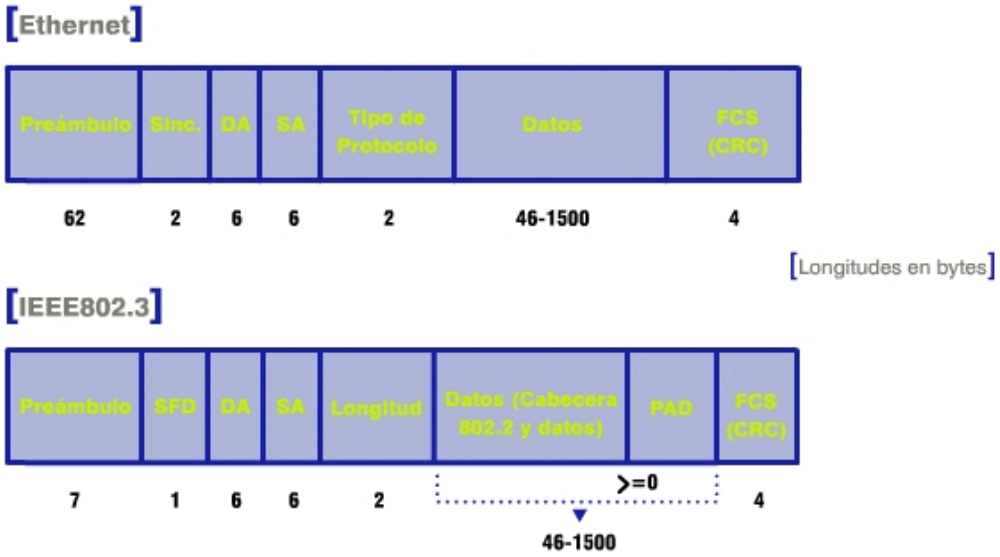
[IEEE 802.3 Nivel Físico]

Especificación	10Base5	10Base2	10BaseT	10BaseFL
Velocidad	10	10	10	10
Modo de transmisión	Banda Base	Banda Base	Banda Base	Banda Base
Longitud máx. segmento	500	185	100	2000
Tipo de medio	50-ohm coax (thick)	50-ohm coax (thin)	Unshield twisted-pair (UTP)	Fibra óptica
Topología	Bus	Bus	Estrella	Punto a Punto

Fíjate que todas las especificaciones de nivel 1 determinan la velocidad, el modo de transmisión (banda base) y el tipo de cable.

Existe una especificación, conocida como 10broad36, que transmite en banda ancha (broadband), pero no se implementa actualmente.

Protocolos



Ahora conocemos el funcionamiento de la técnica de acceso al medio, el direccionamiento y la arquitectura de protocolos ETHERNET e IEEE802.3.

Vamos a analizar el formato de las tramas (paquetes) que se generan. El formato de la trama (paquete) Ethernet (Ethertype) e IEEE802.3 es similar, pero presentan ciertas diferencias.

Preámbulo

Patrón alternativo de ceros y unos que indican la llegada de una trama al receptor. En Ethernet son 62 bits y en 802.3 son 56 bits.

SINC

En Ethernet, es un campo de dos bits, ambos a “1”, que junto con el preámbulo realizan la misma función que en 802.3 el preámbulo y el SFD.

SFD (Start Frame Delimiter)

En IEEE 802.3, este byte termina con dos "unos" consecutivos para sincronizar e indicar el inicio de datos válidos.

DA (Destination Address) y SA (Source Address)

La dirección origen es siempre unicast y la destino puede ser unicast, broadcast o multicast.

Tipo de protocolo (en Ethernet)

Especifica el protocolo de nivel superior transportado en los datos.

En, ***www.cavebear.com/CaveBear/Ethernet/type.html***, puedes consultar los valores asociados a este campo.

Longitud (en IEEE 802.3)

Indica el tamaño del campo de datos. El tamaño máximo es 1500 bytes. Este valor define al software de red si el paquete es ethertype (valor mayor que 1500) o IEEE802.3 (valor menor o igual a 1500).

Datos

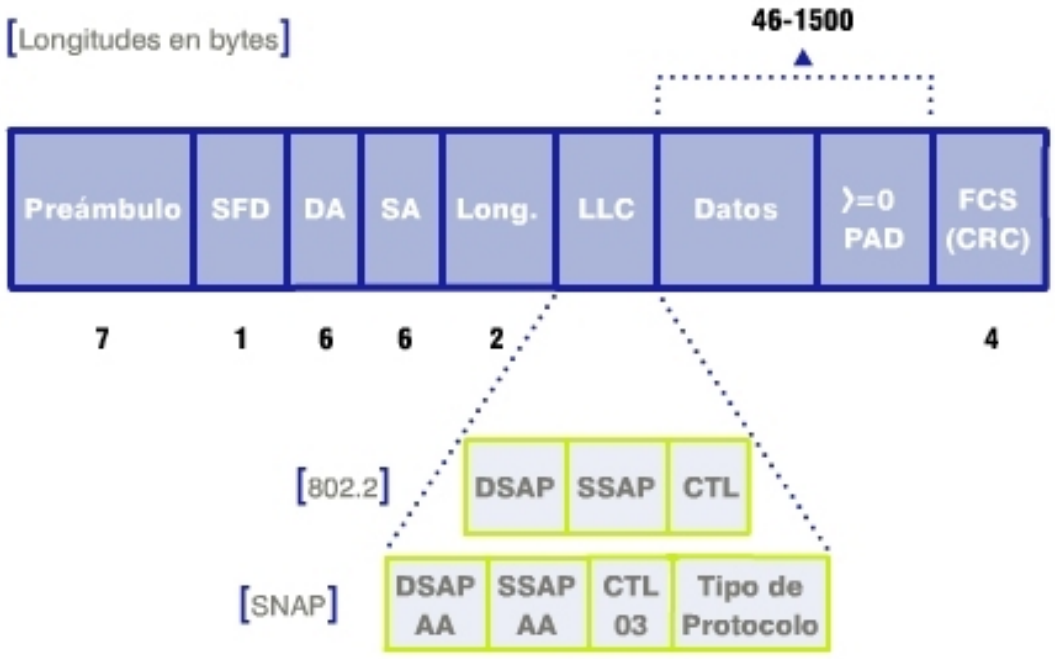
En Ethernet, corresponde a la PDU de nivel 3, mientras que en IEEE802.3 corresponde al protocolo IEEE802.2. Como mínimo son 46 bytes y como máximo 1500 bytes. Si los datos tienen un tamaño inferior a 46 bytes, se completan con el PAD (secuencia de bits de relleno).

FCS

Secuencia de verificación de trama: Código de redundancia cíclica (CRC) de 32 bits para verificar la integridad del paquete.

LLC-IEEE802.2 y MTU en Ethernet

Recordemos que la trama 802.3 no posee mecanismos de identificación del protocolo de nivel superior (red). Por ello, la IEEE define la especificación 802.2 LLC que provee de esta funcionalidad.



LLC es un subconjunto muy simplificado del protocolo HDLC, donde el campo de control (CTL) es siempre 3 (información no numerada) y los campos DSAP (Destination Service Access Point) y SSAP (Source Service Access Point) identifican los procesos o protocolos de nivel superior, origen y destino de los datos transportados.

Existe también el encapsulamiento SNAP, que difiere del anterior en que los campos SSAP y DSAP son siempre AA16 y se incluye un campo adicional de "tipo de protocolo".

Cuando definimos el formato de trama, vimos que el tamaño máximo del área de datos es de 1500 bytes.

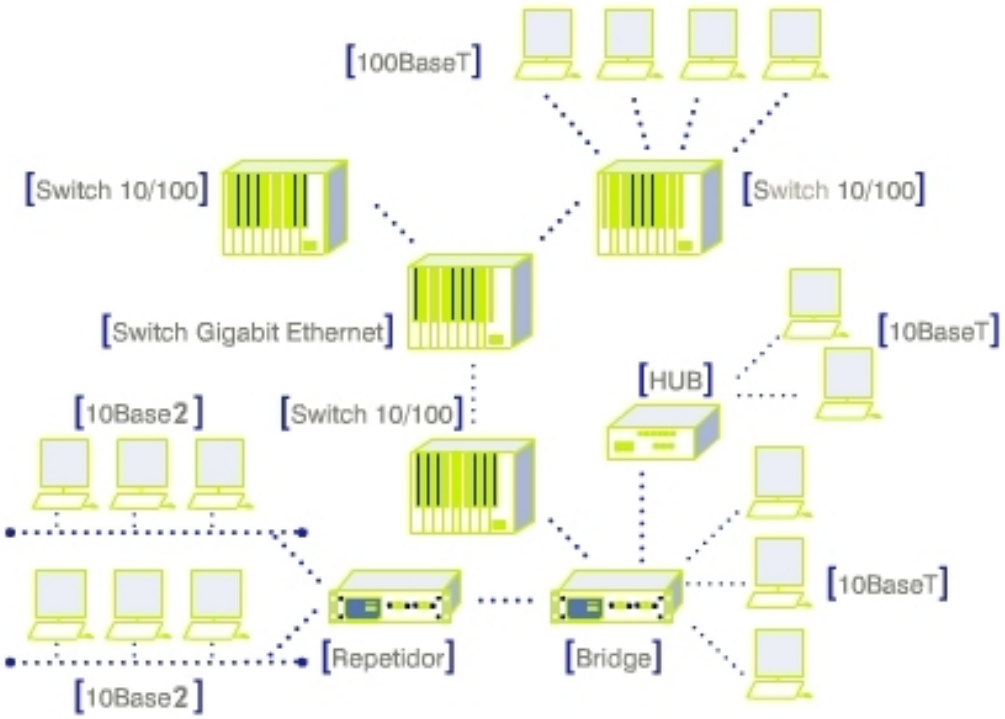
Si a ello añadimos la cabecera y el trailer (CRC) de la trama, tenemos un total de **1518 bytes**.

Esto es lo que se define como la MTU **(Unidad máxima de transferencia)** de una red Ethernet.

Componentes de red

Es hora de ponerlo todo junto.

Veamos cómo se implementa una red Ethernet.



Recuerda que un dispositivo conectado a una red Ethernet puede y debe entender de tramas ethertype y tramas IEEE802.3.

Simplemente verifica el campo tipo de protocolo (longitud) y ya sabe qué hacer.

Actualmente, Ethernet es la tecnología LAN más difundida y desarrollada.

Sus diferentes evoluciones han llegado hasta la implementación a 10 Gbps.

Como puedes observar en la imagen, otro de los factores promotores de Ethernet es la compatibilidad entre todas las especificaciones de nivel físico existentes:

10base2, 10baseT, 100baseT, etc.

Además, se ha requerido la introducción de diferentes elementos de interconexión:

repetidores, HUBs, puentes y switches.

Los veremos en detalle en el siguiente capítulo.

Fast Ethernet (I)

Evolutivamente, **Ethernet ha pasado de** 10Mbp **a velocidades de** 100Mbps **y** 1000Mbps.

Veamos.

Fast Ethernet define la especificación del IEEE para la implementación de 100Mbps. Conserva el formato de la trama 802.3 y la técnica de acceso al medio.

Además, permite velocidades de 10 y 100 Mbps.

Sin embargo, cambia los mecanismos de codificación y la implementación de nivel físico, para lograr el incremento de velocidad.

Fast Ethernet (II)

Especificación	Ratio de transmisión por símbolo	Técnica de Codificación	Cableado	Transmisión full duplex
10baseT	10 Mbaudios	Manchester	2 pares UTP cat. 3 o superior	Soportada
100baseTX	125 Mbaudios	4B/5B	2 pares UTP cat. 5 o STP tipo 1	Soportada
100baseT4	33 Mbaudios	8B/6T	4 pares UTP cat. 3 o superior	No soportada
100baseT2	25 Mbaudios	PAM5x5	2 pares UTP cat. 3 o superior	Soportada

La tabla de la imagen compara las diferentes implementaciones de Fast Ethernet con la especificación 10baseT.

100baseX

Abarca 100baseTX y 100baseFX. Se diseñó para soportar transmisiones sobre dos pares de cobre categoría 5 (TX) o dos fibras ópticas (FX). Utiliza codificación 4B/5B y es full duplex.

Es la especificación más utilizada comercialmente.

100baseT4

Se diseñó para permitir la utilización de los cables UTP categoría 3 utilizados en la implementación de 10Mbps. Se requieren 4 pares, 3 de los cuales se utilizan para las funciones de transmisión/recepción y el cuarto para la detección de portadora.

No soporta transmisión full duplex.

100baseT2

Implementa una mejor alternativa para el uso de cable categoría 3.

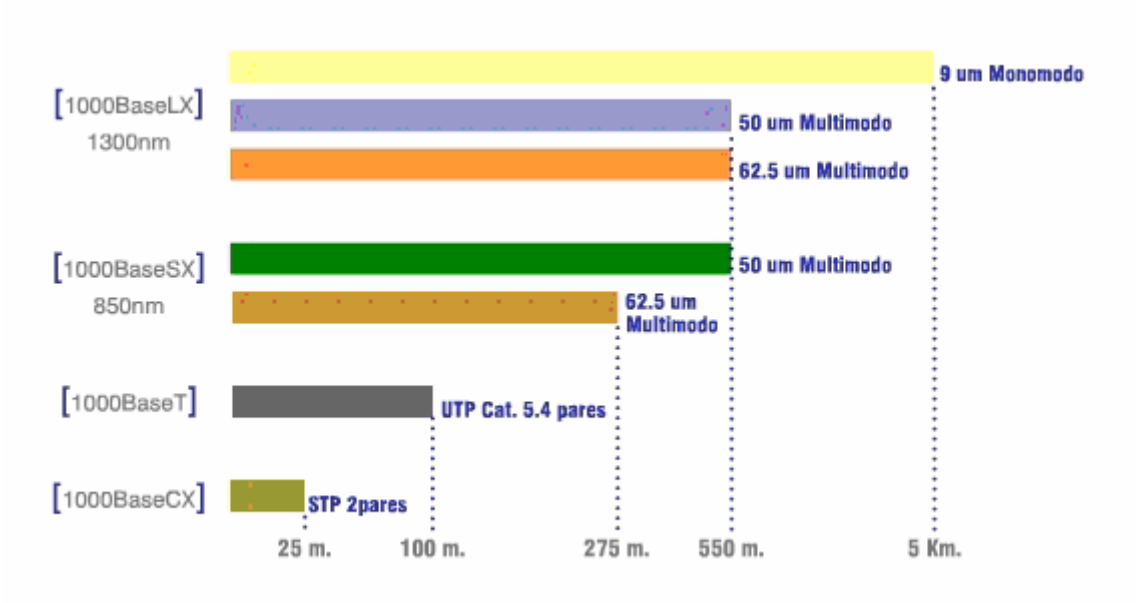
Únicamente usa dos pares, y soporta transmisión full duplex y half duplex.

Gigabit Ethernet (I)

Gigabit Ethernet cubre dos especificaciones: 1000baseT, para cable UTP y 1000baseX para cable STP y fibra óptica multimodo.

Todas las especificaciones funcionan en modo full duplex.

Gigabit Ethernet (II)



La tabla de la imagen compara las diferentes implementaciones de Gigabit Ethernet.

1000BaseLX

Utiliza láser de onda larga sobre fibras monomodo y multimodo.

Los tipos de fibras multimodo que soporta Gigabit Ethernet son fibras de 50 um y 62,5 um de diámetro.

1000BaseSX

Utiliza láser de onda corta sobre fibras multimodo de 62,5 y 50 um de diámetro.

Las principales diferencias entre utilizar láser de onda corta o de onda larga se encuentran en el coste y en la distancia.

1000BaseT

Utiliza 4 pares UTP categoría 5 (o superior), y es la especificación desarrollada por el comité IEEE 802.3ab

1000BaseCX

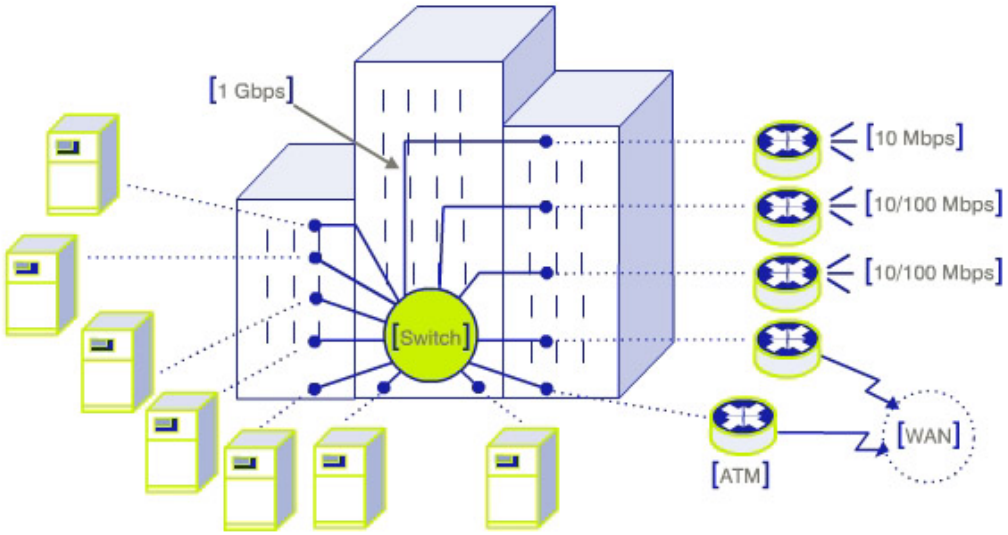
Para distancias muy cortas (25 m o menos), Gigabit Ethernet puede ser transmitido mediante un cable balanceado especial de 150 ohmios.

Se trata de un tipo especial de cable STP, en el que los equipos transmisores y receptores comparten tierra común, para minimizar la distorsión y el ruido. Se utiliza un conector DB-9.

Backbone Gigabit Ethernet

Una de las principales implicaciones de Gigabit Ethernet es la creación de Backbones de interconexión de muy alta velocidad en entornos de empresas o campus.

Veamos su implementación.



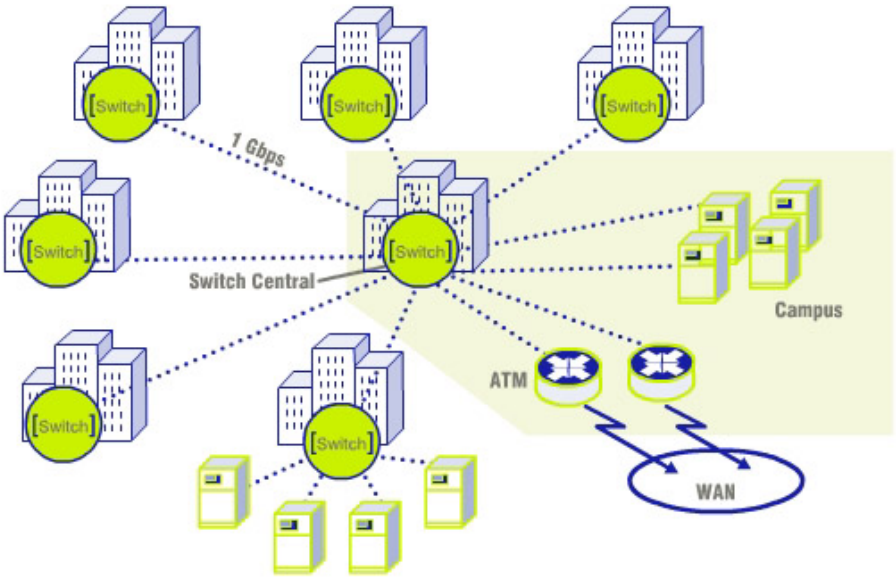
La figura de la imagen representa un backbone de empresa.

Los enlaces del switch gigabit ethernet trabajan a 1 Gbps. A ellos han de conectarse los servidores o los segmentos de red de 100 Mbps.

Incluso, los elementos de interconexión utilizados, como routers o conmutadores ATM.

Fíjate en esta otra imagen, es la configuración de un Backbone tipo campus.

Pasemos al siguiente capítulo para ver la necesidad de interconexión.


Switch
Switch
Switch
1 Gbps
Switch
Switch
Switch Central
Campus
Switch
Switch
ATM
WAN

3 Necesidad de interconexión

Introducción a la Sección 3

Vas a comenzar el apartado 3:

Necesidad de interconexión

En el capítulo anterior vimos que los diferentes medios de transmisión y las características del CSMA/CD introducen limitaciones en el número de dispositivos conectados a la red y las longitudes de la misma. El objetivo de este capítulo es profundizar en estos detalles y la forma de solventarlos.

Introducción

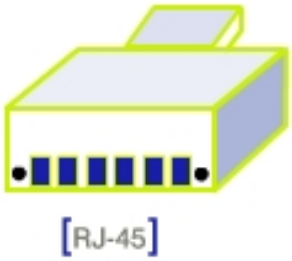
A partir de ahora, ya familiarizados con Ethernet, empezaremos a hablar de interconexión: por qué y cómo.

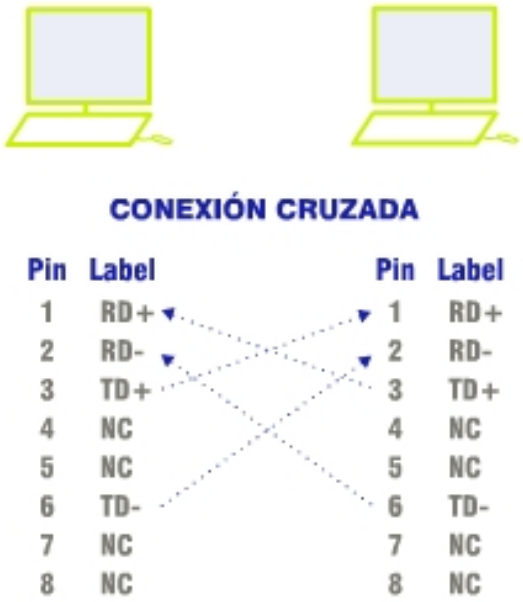
Especificación	Tipo de cable	Long. segmento	nº dispositivos por segmento
10Base2	Tninnet (Coax. 50 ohm)	185 m	30
10Base5	Thicknet (Coax. 50 ohm)	500 m	100
10BaseT	UTP Cat. 3, 4 y 5	100 m	1
100BaseTX	UTP Cat. 5, 6 y 7	100 m	1
100BaseFX	Fibra multimodo de 62.5 o 125 micrones	400 m	2
1000BaseCX	STP	25 m	1
1000BaseT	UTP Cat. 5 (4 pares)	100 m	1
1000BaseSX	Fibra multimodo de 62.5 o 50 micrones. Láser de 780 nanómetros	260 m	1
1000BaseLX	Fibra monomodo de 9 micrones. Láser de 1.300 nanómetros	3-10 Km.	1

En primer lugar, recordemos las limitaciones de las diferentes implementaciones físicas en Ethernet.

Al analizar la tabla se observa que la longitud del segmento y número de dispositivos por segmento son los principales factores limitantes (fíjate en las limitaciones a 10 Mbps).

En segundo lugar, como puedes observar en la figura, el uso de par trenzado requiere que se conecten apropiadamente los pares de transmisión y recepción, es decir, hay que “cruzar” los cables.

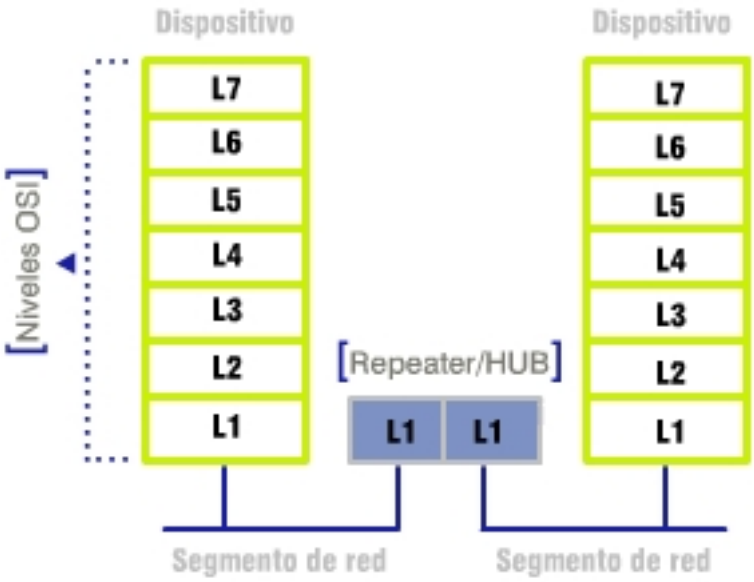




Para un enlace entre dos dispositivos la solución es inmediata.

Sin embargo, para conectar múltiples equipos en red, resulta evidente la necesidad de algún dispositivo que interconecte a los otros entre sí.

Interconexión de nivel 1



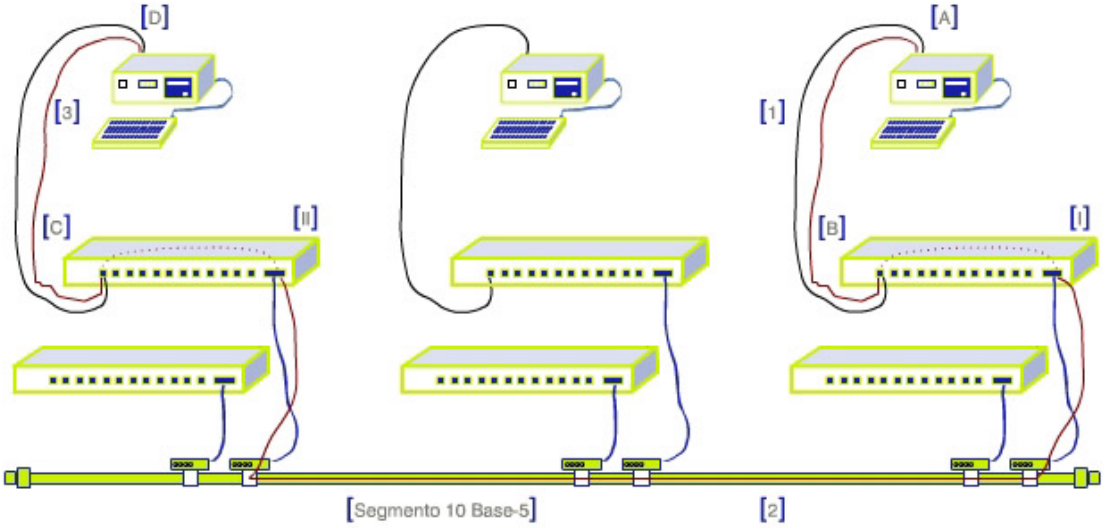
Vamos a definir y analizar los dispositivos considerados como de Nivel 1, que solucionan los problemas anteriormente mencionados.

En el siguiente capítulo analizaremos los de Nivel 2 y las prestaciones que añaden.

Para solucionar el problema de la limitación en la longitud del segmento y el número de dispositivos en la red, aparecen los repetidores.

Los HUBs o concentradores de cableado solucionan la problemática de uso de par trenzado. Ambos son dispositivos que trabajan a nivel físico (1) según el modelo OSI.

Los repetidores

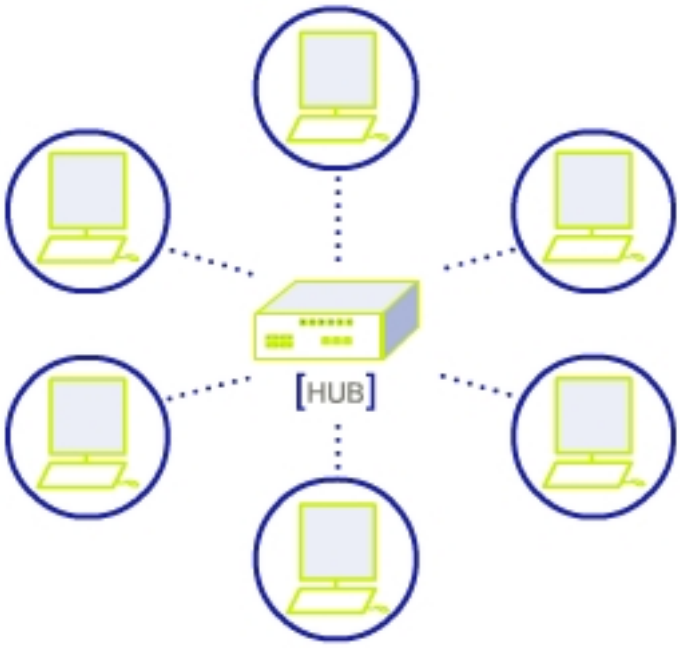


Alargan los segmentos, para solventar las limitaciones de longitud y número de dispositivos conectados. Como tal, es lo que se denomina un dispositivo de Nivel 1 (Físico). Aparece con la especificación 10Base5. **Aislan puertos donde se detectan muchas colisiones**, para evitar que se propague el problema. **Permiten, también utilizar diversos tipos de cableado**, según los puertos que posean.

El uso de repetidores se haya limitado por la norma “543”: entre dos equipos de la red no deberá haber más de 4 repetidores y 5 segmentos de cable.

Igualmente, sólo 3 segmentos pueden tener conectados dispositivos que no sean los propios repetidores, es decir, 2 de los 5 segmentos sólo pueden ser empleados para la interconexión entre repetidores.

Hubs



El otro dispositivo de interconexión considerado como de nivel 1 es el HUB o concentrador de cableado.

En su forma más simple es un repetidor que permite la interconexión de dispositivos mediante par trenzado (especificación 10baseT).

Aunque la topología asociada es una estrella, lógicamente, la red puede considerarse como un “bus”, ya que basta con que una estación ponga una trama en la red para que, automáticamente, todas las otras la vean.

El uso de Hubs también viene limitado por la norma “543”.

Resumen

Los repetidores y los Hubs permiten interconectar segmentos y, por tanto, alargar la red.

Son dispositivos de Nivel 1 aunque algunos de ellos incorporan servicios que permiten monitorizar el estado de los puertos y las colisiones que se presentan.

Incluso, se habla de HUBs de tercera generación, que son dispositivos con funcionalidades adicionales.

Hoy por hoy, la evolución de las LAN ha llevado a la casi desaparición de estos dispositivos en la mayoría de las implementaciones existentes, debido a la aparición de los dispositivos de Nivel 2: **puentes y conmutadores**, que veremos a continuación.

4 Nivel 2: puentes y conmutadores

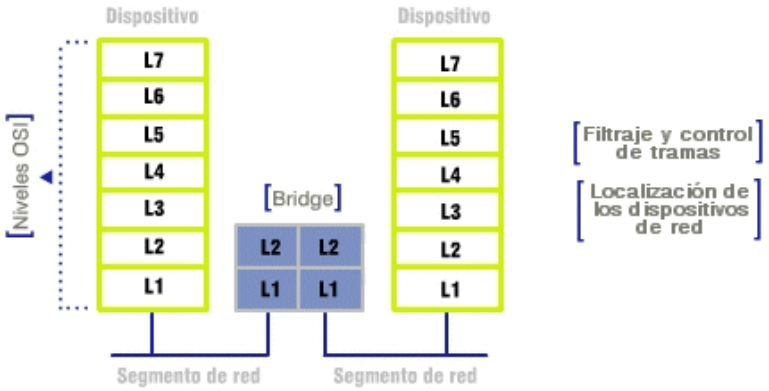
Introducción a la Sección 4

Vas a comenzar el apartado 4:

Nivel 2: puentes y conmutadores

Los dispositivos de Nivel 1 nos permiten solventar esas limitaciones que habíamos visto. ¿Y si ahora les damos un poco más de “inteligencia”? El objetivo de este capítulo es analizar en qué consiste esa “inteligencia” y qué funcionalidades aporta.

Introducción



Los Puentes o Bridges **son dispositivos de interconexión que trabajan a nivel 2 según el modelo OSI**. Su función es recibir las tramas provenientes de los dispositivos conectados a sus puertos, analizarlas a nivel 2 (MAC) y reenviarlas por algún puerto o descartarlas. Los Puentes controlan el flujo de datos, detectan errores de transmisión y controlan el acceso al medio físico para multitud de tecnologías LAN.

Filtraje y control de tramas

También pueden proveer filtraje y control de tramas basados en la información de la cabecera MAC (direcciones y campo de tipo de protocolo), mediante la creación de listas de acceso.

Localización de los dispositivos de red

Los Puentes auto-aprenden la localización de los dispositivos de la red y crean tablas que asocian las direcciones MAC de los equipos con los puertos a los que están conectados al puente. Las tramas entrantes son analizadas y entregadas por el puerto apropiado de acuerdo a esta información.

Beneficios del uso de Puentes (I)

Hemos definido brevemente la función de un Puente.

Veamos **qué beneficios aporta** el uso de los mismos.

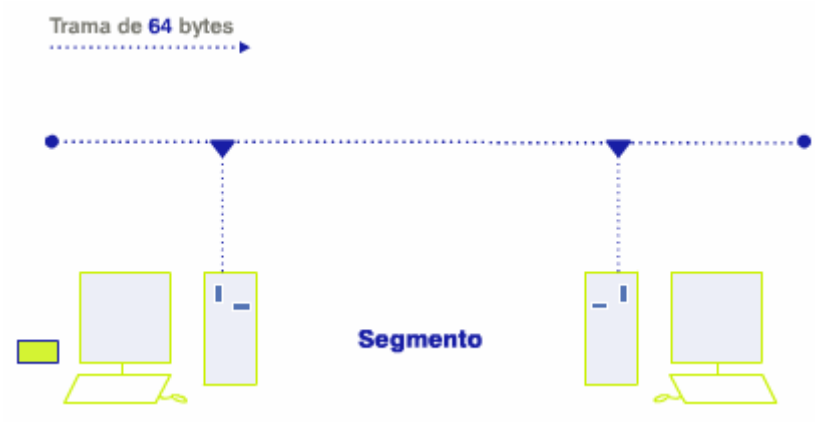
Los Puentes optimizan el tráfico en la red: únicamente entregan tramas por los segmentos que les corresponden.

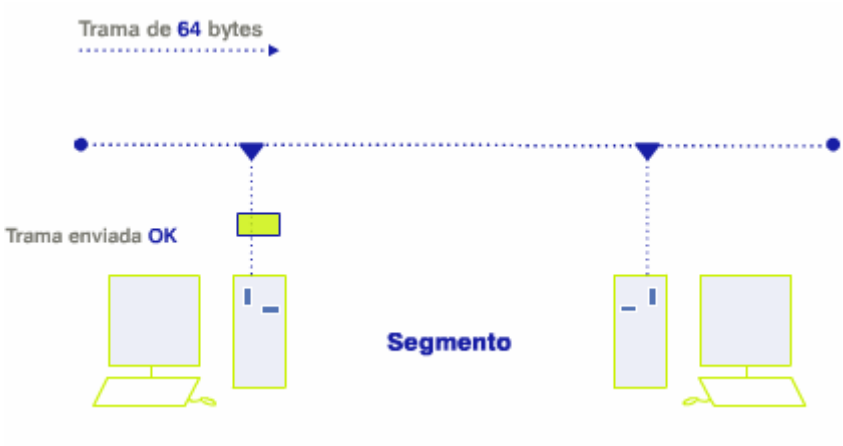
Esto representa una **reducción** en la posibilidad de **colisiones** y menor **contención en el acceso de los dispositivos**.

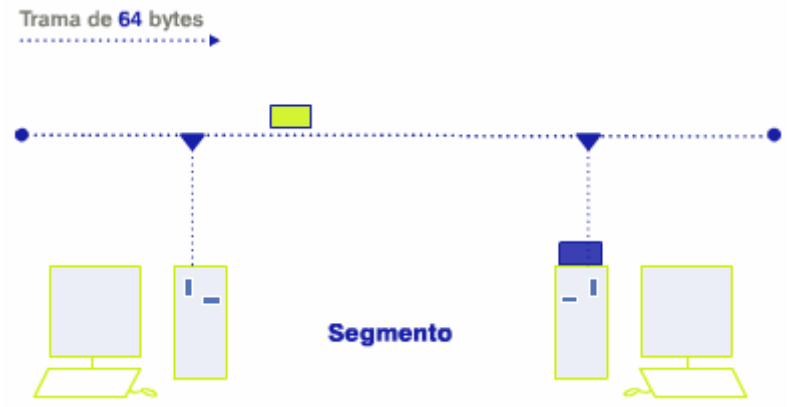
Por otro lado, nos permiten "salvar" las limitaciones impuestas por las longitudes máximas de segmentos, dado que los puentes reciben, almacenan y reenvían los paquetes.

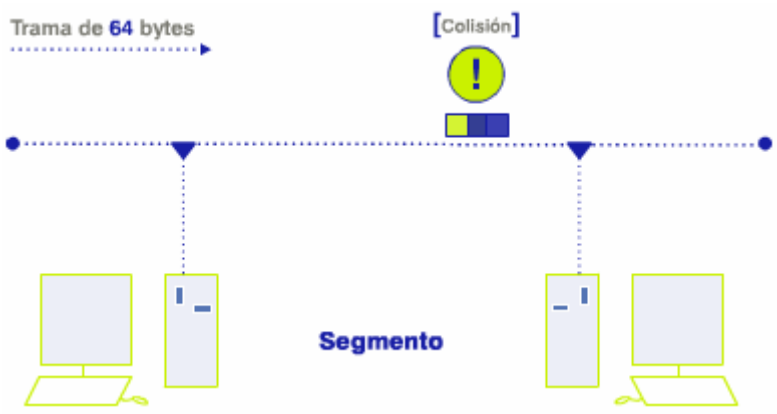
Veámoslo.

Beneficios del uso de Puentes (II)







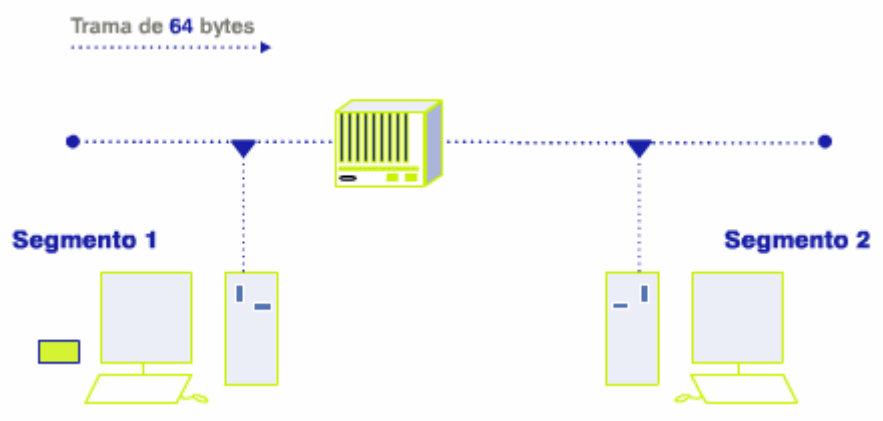


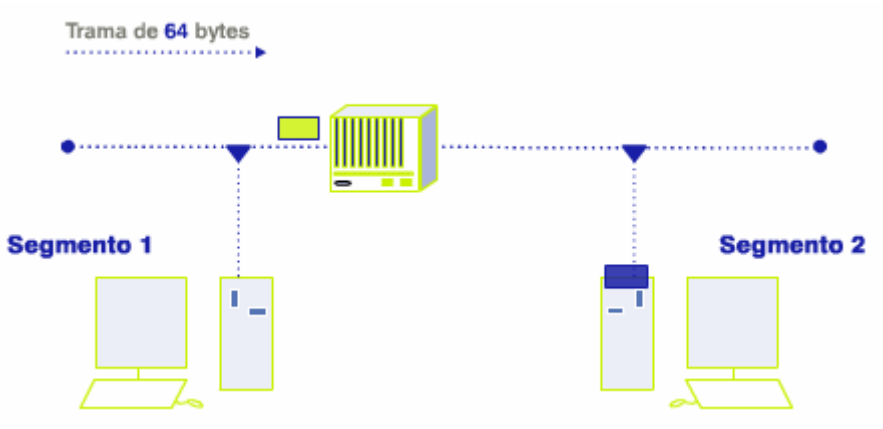
En un segmento de longitud superior a la permitida, si la estación A transmite una trama de longitud mínima (64 bytes), estará a la escucha hasta terminar de transmitir.

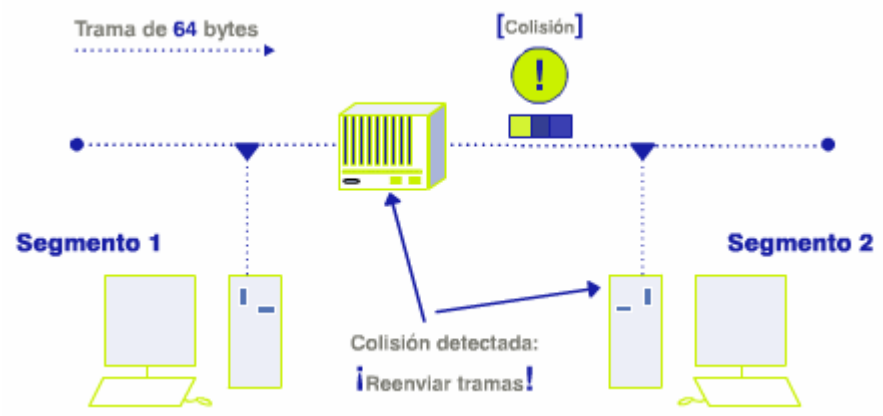
Una vez finalizada la transmisión, presupone que la trama llegó correctamente. Sin embargo, como el segmento es más largo de lo debido, la trama continua propagándose.

Otra estación, que detecta el medio libre, inicia la transmisión y se produce una colisión, no detectada por la estación origen.

Beneficios del uso de Puentes (III)







Si introducimos un Puente y dividimos la red en dos segmentos, la trama transmitida por la estación A será recibida por el Puente. El Puente retransmite la trama y la estación B comienza a transmitir.

Al ocurrir la colisión, tanto el Puente como la estación B retransmitirán siguiendo el proceso de detección de colisiones.

Funcionamiento de los Puentes

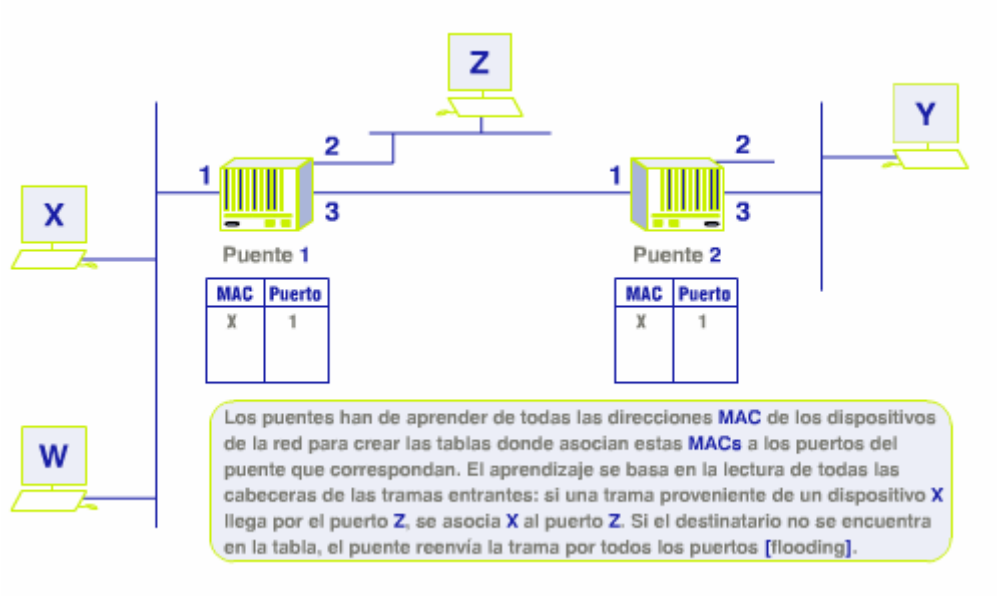
Los Puentes, genéricamente, funcionan bajo el concepto de "transparent Bridging", interconectando diferentes segmentos de red y realizando una serie de funciones.

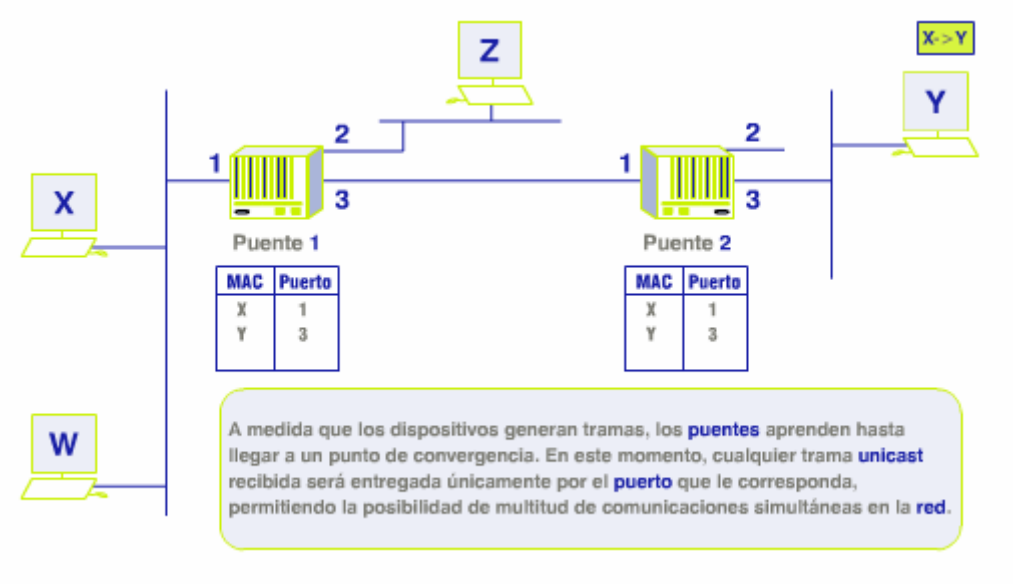
Funciones

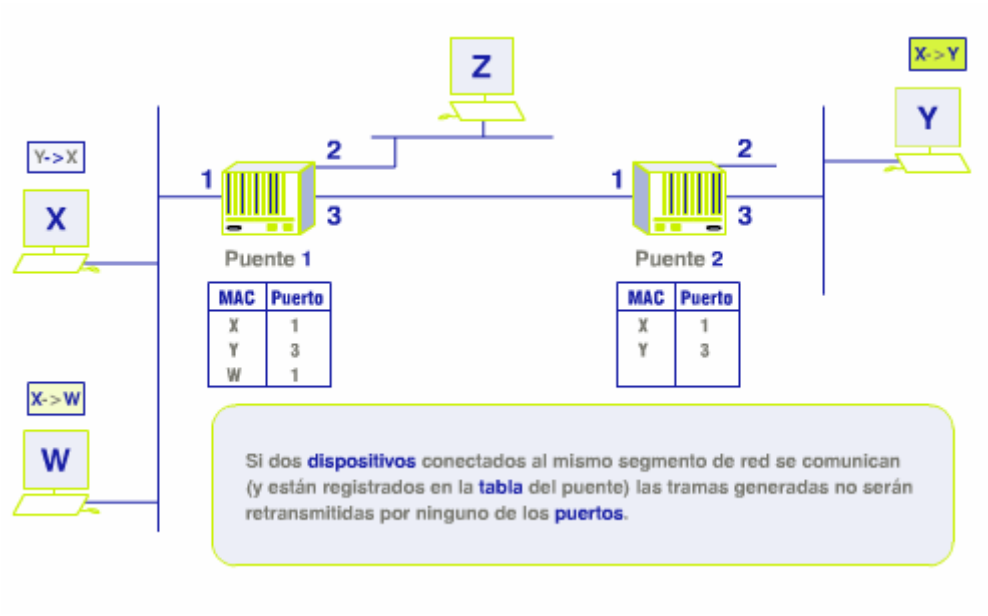
- Aprendizaje.
- Reenvío de tramas.
- Filtrado de tramas.
- Eliminación de bucles.

A continuación veremos estos mecanismos.

Mecanismos


Z
Y
X
W
1
2
3
1
2
3
Puente 1
Puente 2
MAC
Puerto
X
1
MAC
Puerto
X
1
Los puentes han de aprender de todas las direcciones MAC de los dispositivos de la red para crear las tablas donde asocian estas MACs a los puertos del puente que correspondan. El aprendizaje se basa en la lectura de todas las cabeceras de las tramas entrantes: si una trama proveniente de un dispositivo X llega por el puerto Z, se asocia X al puerto Z. Si el destinatario no se encuentra en la tabla, el puente reenvía la trama por todos los puertos [flooding].


X->Y
Z
Y
X
W
1
2
3
1
2
3
Puente 1
Puente 2
MAC
Puerto
X
Y
1
3
MAC
Puerto
X
Y
1
3
A medida que los dispositivos generan tramas, los puentes aprenden hasta llegar a un punto de convergencia. En este momento, cualquier trama unicast recibida será entregada únicamente por el puerto que le corresponda, permitiendo la posibilidad de multitud de comunicaciones simultáneas en la red.



Fíjate en la animación superior para conocer los mecanismos de los Puentes.

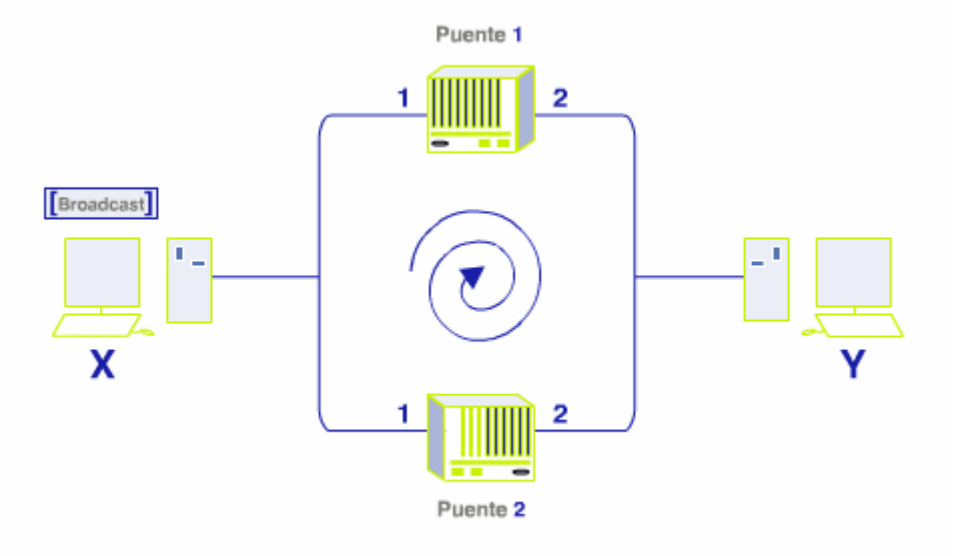
Los bucles

El funcionamiento de los Puentes, como habrás observado, es relativamente sencillo.

Sin embargo, existe la posibilidad de que nuestra red contenga bucles entre los Puentes.

Veamos.

El problema de los bucles



Cuando existe más de un trayecto posible entre dos Puentes de una LAN, se puede producir un bucle (loop).

Por ejemplo, en la imagen puedes observar que si se genera una trama de broadcast (difusión ilimitada), al ser recibida por el Puente 1, éste debe reenviarla por todos los Puertos.

Cuando el Puente 2 la recibe, realiza el mismo proceso, y el puente 1 recibe nuevamente la trama y repite el proceso: se ha creado un bucle.

El protocolo STP

Este problema ha de ser solventado.

Para ello se desarrolló lo que se conoce como el protocolo STP.

El Spanning Tree **(árbol de expansión)** es un protocolo Puente a Puente diseñado para detectar y remover los bucles en la red.

Desarrollado originalmente por DEC, fue estandarizado bajo la normativa IEEE802.1d

Consiste, básicamente, en que los Puentes se comunican unos con otros utilizando mensajes denominados BPDUs ***(Bridge Protocol Data Units)***.

Estos mensajes permiten determinar el que será el Puente Raiz (root) y el coste del trayecto hacia este Puente, para seleccionar los trayectos de menor coste y bloquear los restantes.

Si un Puente falla, se recalculan los trayectos. El algoritmo utilizado para todos estos cálculos se denomina STA (Spanning Tree Algorithm).

Si algún Bridge de la red no soporta STA, puede utilizarse, pero es responsabilidad del usuario, el evitar la creación de bucles.

Veamos el formato de los mensajes BPDUs, para luego poder entender el funcionamiento del STP mediante un ejemplo.

Bridge Protocol Data Units (BPDUs)

Las BPDUs son mensajes de configuración y mensajes de cambio de topología. Los **primeros** se envían **para establecer la topología de la red** y los **segundos cuando se ha detectado un cambio**. El formato del paquete es siempre el mismo.

Identificador de protocolo

Valor cero.

Versión

Valor cero.

Tipo de mensaje

Cero (configuración) y 128 (cambio).

Apuntador

1 byte. Sólo se utilizan los dos primeros bits. El bit TC (cambio de topología), señala un cambio de topología. El bit TCA (confirmación de cambio) se activa para confirmar la recepción de un mensaje de configuración.

ID Raiz

Identifica el Puente Raiz listando su prioridad (2 bytes) y su ID (6 bytes).

Coste de Trayectoria Raiz

Contiene el costo de trayectoria del Bridge que envía el mensaje de configuración hacia el Puente Raiz.

ID del Bridge

Cada uno de los Puentes posee un identificador compuesto por 8 bytes. Los dos primeros, conocidos como la prioridad, los determina el administrador. Por defecto, este valor es 32768. Los 6 bytes restantes es la dirección MAC de uno de los puertos del puente (la menor).

ID del Puerto

Identifica el puerto del cual se envió el mensaje de configuración.

Edad del mensaje

Especifica el tiempo que ha transcurrido desde que la raiz envió el mensaje de configuración en el que se basa el mensaje actual.

Edad máxima

Indica cuándo debe eliminarse el mensaje de configuración actual.

Tiempo de saludo

Periodo entre los mensajes de configuración del Puente Raiz.

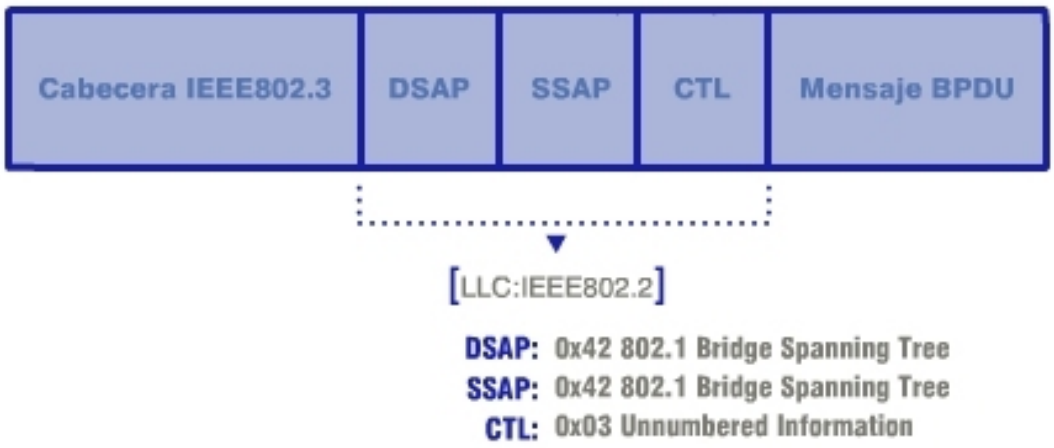
Pausa de envío

Tiempo de espera antes de la transición a un nuevo estado después de un cambio de topología.

Encapsulamiento de BPDUs

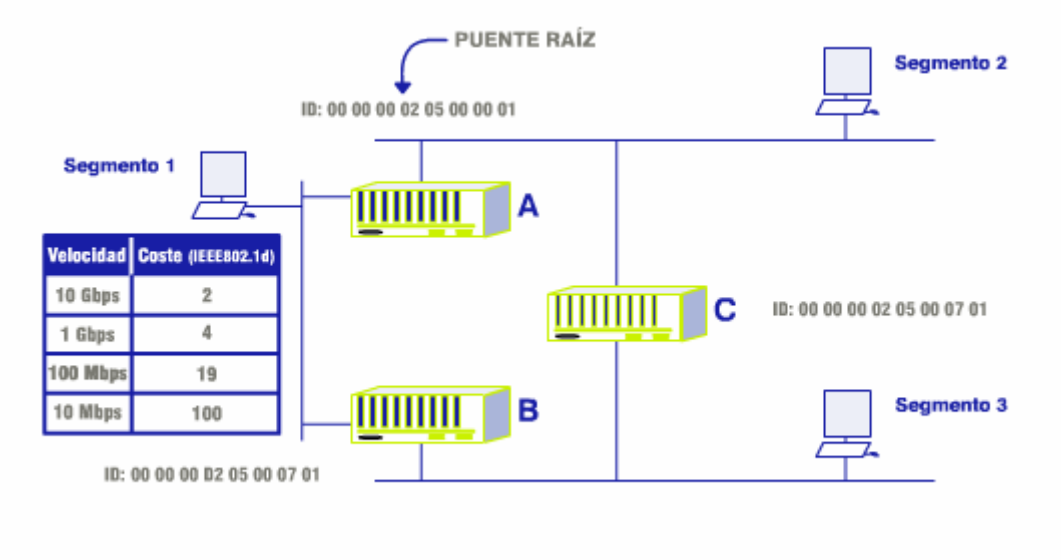
Los mensajes BPDU se encapsulan en tramas tipo IEEE802.3, lo que determina que el procesamiento de la información es a

nivel 2.



Las direcciones MAC destino son **direcciones de Multicast reservadas para el funcionamiento de este protocolo**, las cuales sólo reconocen los Puentes.

Funcionamiento del STP (I)



Veamos un ejemplo de **operación del STP en una red con bucles**.

Selección del Puente Raiz

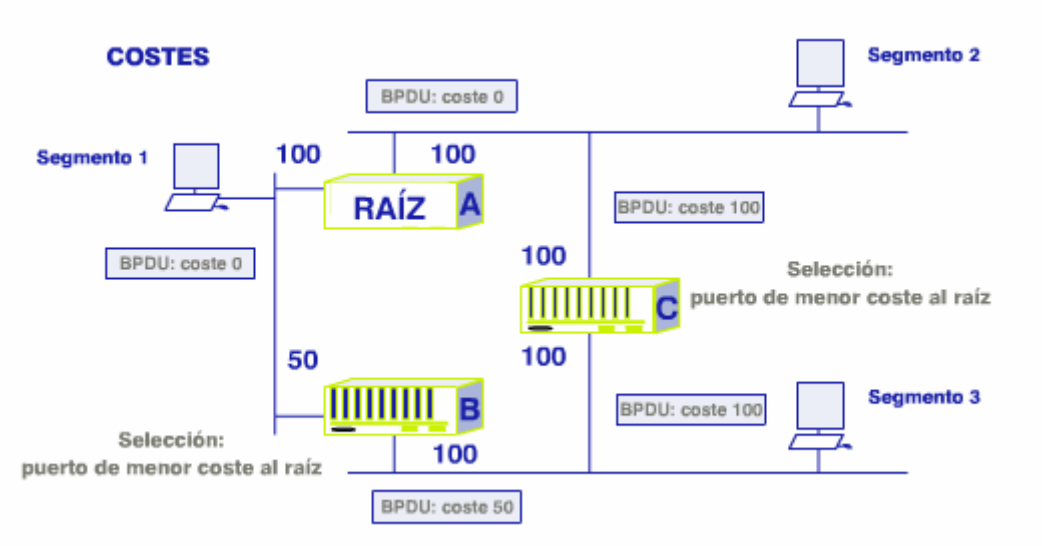
Lo primero que han de seleccionar los puentes de una estructura de red es el Puente Raiz. Para determinar el Puente Raiz de la topología de la red se utiliza el ID (identificador) del Puente. Recuerda que está constituido por la prioridad y la dirección MAC de menor valor.

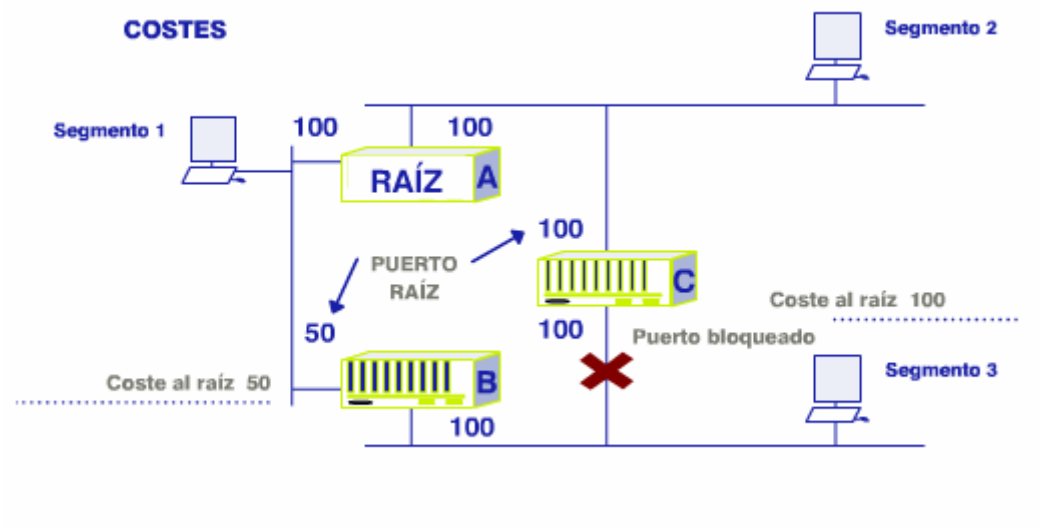
Costes de los puertos

Todos los puertos de los Puentes tienen asignado lo que se denomina el coste, es decir, un **valor que viene por defecto relacionado con la velocidad del segmento al que está conectado**.

Sin embargo, este valor puede ser modificado por el administrador.

Funcionamiento del STP (II)





Selección del Puerto Raíz

Cada Puente de la red calcula el coste total asociado al trayecto por cada una de las posibles rutas hacia el Puente Raiz. Para este cálculo el Puente Raiz envía BPDUs con coste 0 (ya que es el raiz) que son retransmitidas por los demás Puentes con los costes apropiados. Si se reciben mensajes por más de un Puerto se deduce la existencia de un bucle. Finalmente, **mediante el algoritmo STA cada Puente determina el Puerto de menor coste al raíz y lo define como Puerto Raiz**.

Selección del Puente Designado

El Puente designado es aquel que **proporciona el mínimo costo de trayecto a la raiz**, y es el único al que se le **permite enviar tramas hacia y desde el segmento del cual es Puente Designado**.

Para definirlo, los Puentes calculan el coste para llegar al Puente raíz a través del Puerto Raiz. Los demás Puentes bloquean los Puertos conectados al mismo segmento.

Convergencia

De acuerdo a lo que hemos visto, se ha de determinar apropiadamente qué puertos han de estar bloqueados y cuáles pueden reenviar tramas.

Esto llevará un tiempo denominado tiempo de Convergencia que, de acuerdo a los tiempos predefinidos en el protocolo STP, oscilará alrededor de 50 segundos.

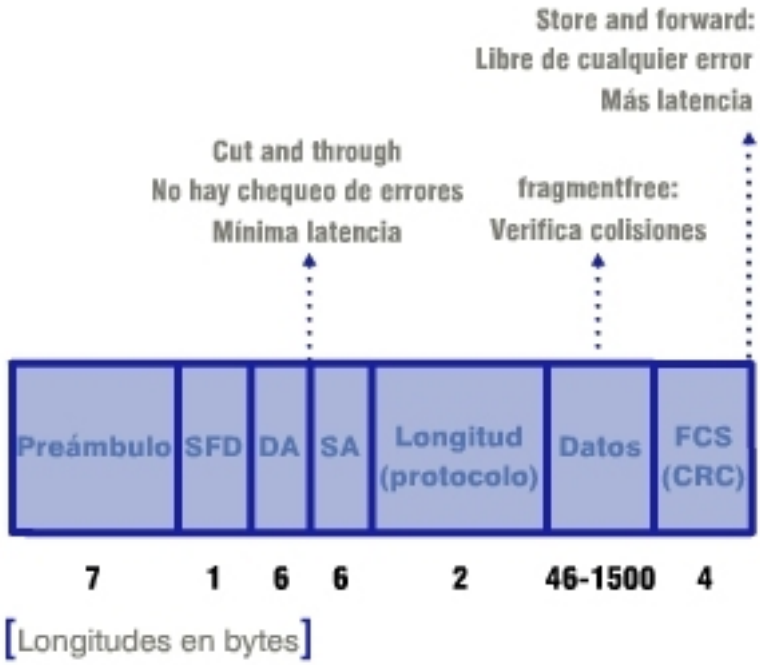
RECAPITULEMOS…

Hemos visto qué son los Puentes, sus ventajas y funcionamiento. Sin embargo, también existen otros dispositivos de nivel 2 en las LAN conocidos como Conmutadores o Switches.

Podemos pensar en ellos como en Puentes con muchos más Puertos, ya que ambos funcionan basándose en el autoaprendizaje y creación de tablas que relacionan las direcciones MAC de los dispositivos con los Puertos a los que se hayan conectados para, así, realizar labores de conmutación de las tramas por los Puertos apropiados.

Sin embargo, existen ciertas diferencias entre ellos, veámoslas.

Conmutadores Vs Puentes



La principal diferencia entre los puentes y los conmutadores es la velocidad de procesamiento: los **puentes** trabajan por mecanismos **software**, en el modo conocido como store and forware (almacenamiento y reenvío): recibe la trama, verifica el CRC (si hay errores descarta la trama) y, analizando la dirección MAC destino, reenvía el paquete por el puerto adecuado.

Los **conmutadores** realizan el proceso de conmutación por **hardware** utilizando procesadores ASICs (Application-Specific Integrated Circuits) que permiten mayor velocidad en el proceso de conmutación.

Además, los **puentes no soportan más de 16 puertos**, mientras que los **conmutadores pueden llegar a tener cientos de puertos**. Todo lo demás, el aprendizaje, reenvío de tramas, filtraje y protocolo STP, es igual en ambos.

Podemos decir, que puentes y conmutadores realizan las mismas funciones, pero los conmutadores son más eficientes y versátiles.

Existen tres diferentes modos de operación de los conmutadores.

Store-and-forward

Tal y como procesa las tramas un puente: almacena trama, verifica el CRC y reenvía según la tabla de conmutación.

Cut-through

En este modo, el conmutador espera únicamente a recibir la dirección MAC destino y automáticamente analiza la tabla y conmuta. No hay verificación del CRC, ni posibilidad de detectar colisiones en el segmento.

FragmentFree (cut-through modificado)

El conmutador recibe los primeros 64 bytes de la trama (tamaño mínimo en ethernet) y luego conmuta. De esta forma se asegura de la ausencia de colisiones.

Conclusión

Es en el nivel 2 donde se generan las tramas Ethernet (o en su defecto de la tecnología LAN correspondiente).

Si un dispositivo de interconexión es capaz de analizar la información del protocolo del subnivel MAC, puede realizar funciones de filtrado y reenvío basándose en las direcciones MAC destino de las tramas: esto es lo que hacen los Puentes y los Conmutadores al crear las tablas de conmutación, que relacionan sus Puertos con las direcciones MAC de los dispositivos conectados a ellos.

Los Conmutadores poseen capacidad para mayor número de Puertos y pueden operar en tres modos, de los cuales el “Cut-through” es el que introduce menor latencia en la red.

Los Puentes únicamente trabajan en el modo “store and forward”.

5 Redes de área local virtuales (VLAN)

Introducción a la Sección 5

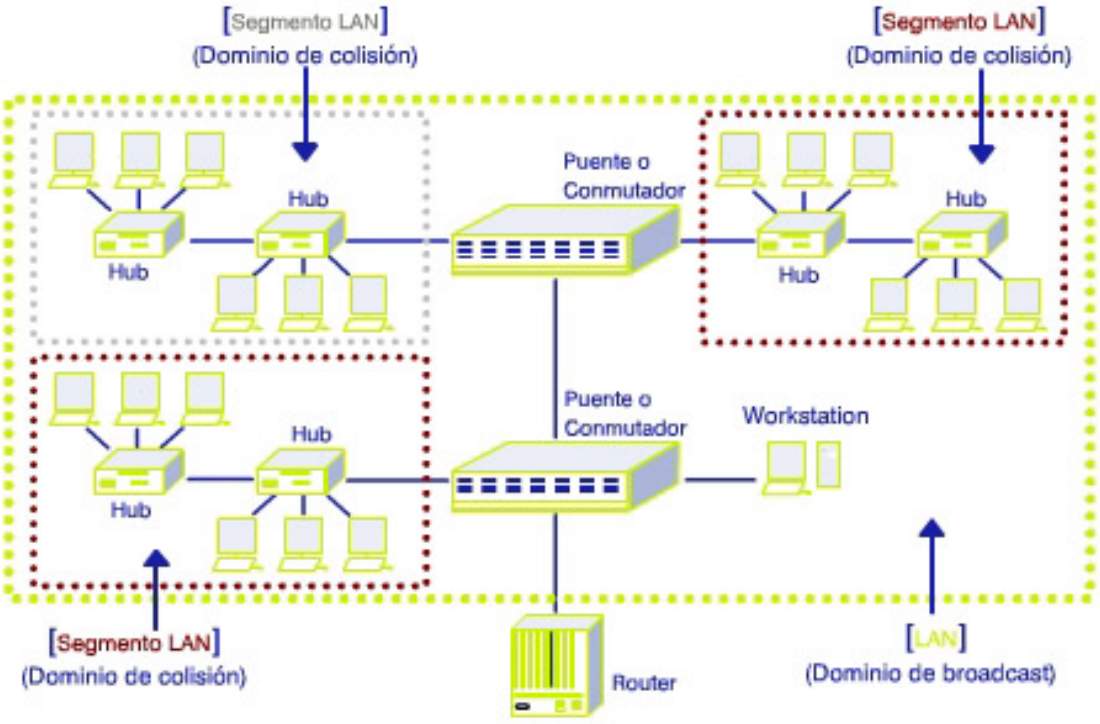
Vas a comenzar el apartado 5:

Redes de área local virtuales (VLAN)

El objetivo de este último capítulo es comprender, definir y analizar el funcionamiento de lo que se conoce como Redes de Área Local Virtuales (VLAN).

Introducción

Recordemos que, originalmente, las redes de área local se definieron como una red de ordenadores situados en la misma zona o área.



Hoy día, las Redes de Área Local se definen como dominios de difusión o *broadcast*; es decir, si un usuario difunde información sobre su LAN, dicha información será recibida por todo el resto de usuarios de dicha LAN.

Sin embargo, esto implica que todo el tráfico de broadcast puede ser "leído" por cualquier dispositivo de la LAN.

Recuerda también que los puentes y conmutadores son elementos de contención de colisiones por naturaleza.

Eso define la existencia de dominios de colisión dentro de un dominio de difusión.

Los Routers, es decir, dispositivos de interconexión de nivel 3, permiten aislar los equipos introduciendo direccionamiento lógico.

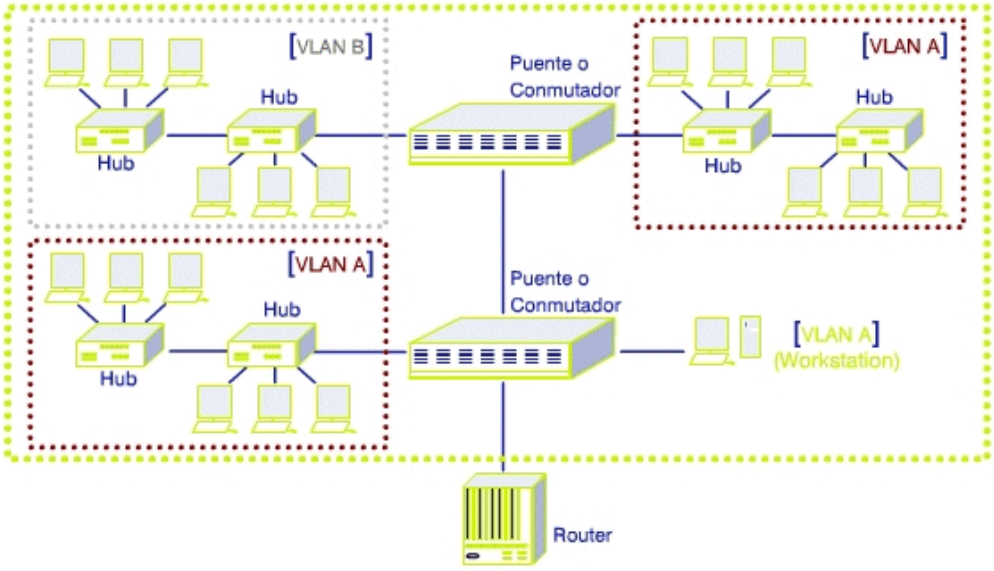
Además, contienen el tráfico de broadcast y facilitan la gestión de zonas dentro de la LAN creando una red IP.

Sin embargo, existe una alternativa al uso de routers para dividir la LAN: la creación de redes de área local virtuales (VLAN).

Relación de ideas clave

Ahora que conocemos que las VLAN son una alternativa al uso de routers para contener el broadcast, veamos una definición más amplia.

Definición de VLAN



Las VLANs pueden verse como un grupo de estaciones finales, situadas quizás en múltiples segmentos de LAN, que no están constreñidas por su localización física y que pueden comunicarse entre ellas como si estuviesen en la misma LAN. Una VLAN puede ser un subconjunto de puertos en un conmutador y/o diversos puertos en conmutadores diferentes.

En la figura puedes observar cómo diferentes elementos de nuestra LAN original ahora pertenecen a dos VLAN diferentes (A y B). Esto quiere decir que sólo los dispositivos correspondientes a la misma VLAN pueden comunicarse entre ellos y recibir tráfico de difusión proveniente de alguno de ellos.

Los elementos de la otra VLAN no “verán” este tráfico.

Tipos de VLAN

Existen diversas formas de configurar los puentes o conmutadores para la creación de VLANs.

Se pueden dividir las soluciones para la creación de VLANs en varios tipos generales.

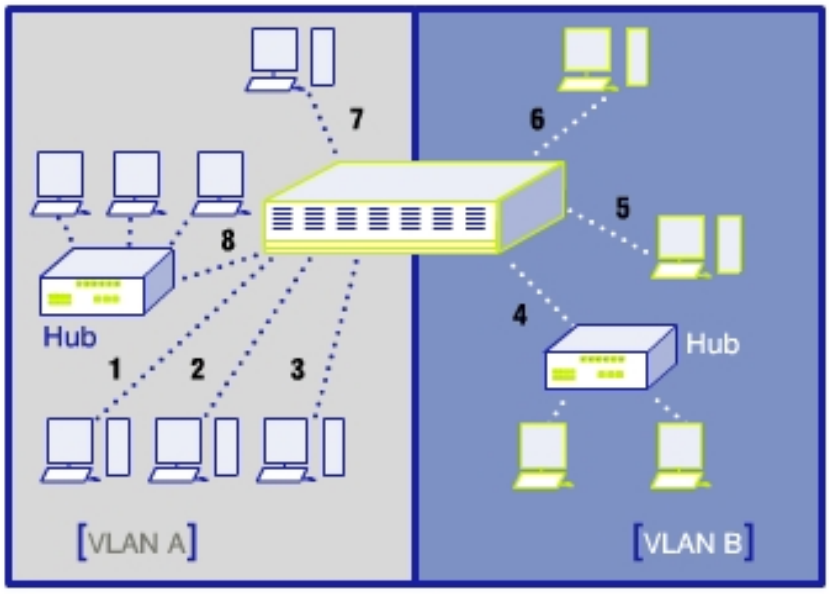
Tipos de VLAN

- Agrupación por puertos.
- Agrupación de nivel MAC (por direcciones MAC).
- Agrupación según el nivel 3 (por protocolo o por dirección de protocolo).

Vamos a analizar cada una de ellos.

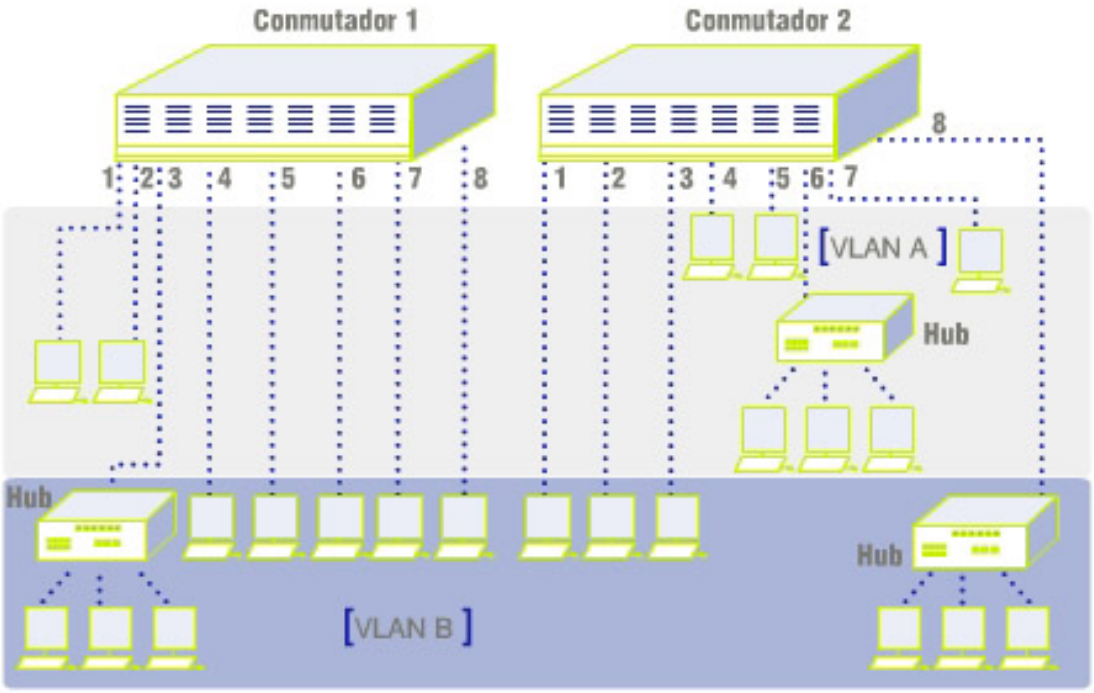
VLAN por agrupación de puertos

Muchas de las implementaciones iniciales de VLAN definían la pertenencia a una VLAN por grupos de puertos de conmutación (por ejemplo, los puertos 1, 2, 3, 7 y 8 de un conmutador pertenecen a la VLAN A, mientras que los puertos 4, 5 y 6 pertenecen a la VLAN B).

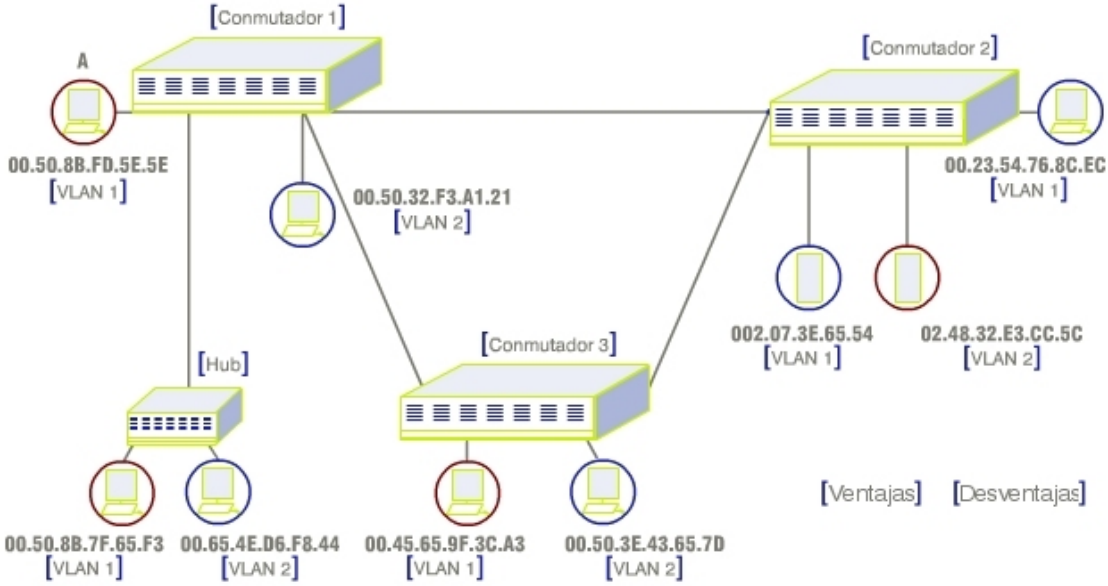


Por lo tanto, en muchas de estas implementaciones iniciales, las VLAN sólo eran soportadas en un único conmutador.

La segunda generación de implementaciones soportan VLANs que se extienden por múltiples conmutadores (por ejemplo, puertos 1 y 2 del conmutador 1 y puertos 4, 5, 6 y 7 del conmutador 2 forman la VLAN A, mientras que los puertos 3, 4, 5, 6, 7 y 8 del conmutador 1 junto con los puertos 1, 2, 3 y 8 del conmutador 2 forman la VLAN B).


Conmutador 1
Conmutador 2
1 2 3 4 5 6 7 8
1 2 3 4 5 6 7
8
[VLAN A]
Hub
Hub
Hub
[VLAN B]

Pertenencia a VLAN por dirección MAC



Este tipo de VLAN **se configura asociando a una VLAN determinada las direcciones MAC de un grupo de dispositivos, no importa dónde estén situados**.

En el ejemplo de la figura, si el dispositivo “A” tratase de enviar una trama a cualquier dispositivo de la VLAN2, el conmutador no entregaría el paquete. Más aún, cuando “A” genere una trama de broadcast, ésta llegará únicamente a los segmentos donde estén definidos miembros de la VLAN1.

VENTAJAS

Debido a que las direcciones MAC están programadas en el hardware del interfaz de red de la estación, las VLANs basadas en direcciones MAC permiten mover una estación de posición física en la red, mientras que se mantiene la pertenencia de dicha estación a su VLAN.

En este caso, podemos pensar en las VLAN definidas por direcciones MAC como *VLANs basadas en el usuario*.

DESVENTAJAS

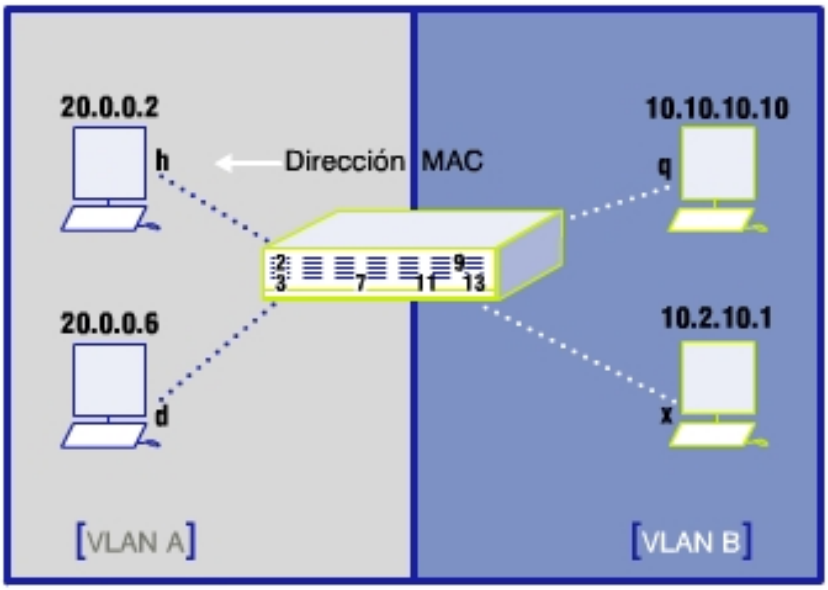
Todos los usuarios deben ser configurados inicialmente en, al menos, una VLAN, lo que se vuelve un gran inconveniente cuando manejamos redes grandes en las que hay que configurar miles de usuarios.

El comportamiento de la VLAN se degrada en cuanto varios miembros de diferentes VLANs coexisten en un mismo puerto del conmutador (mediante un hub, por ejemplo).

El método de comunicación de información de pertenencia a una VLAN entre conmutadores también sufre un alto grado de degradación en implementaciones a gran escala.

Pertenencia a VLAN por información de nivel 3

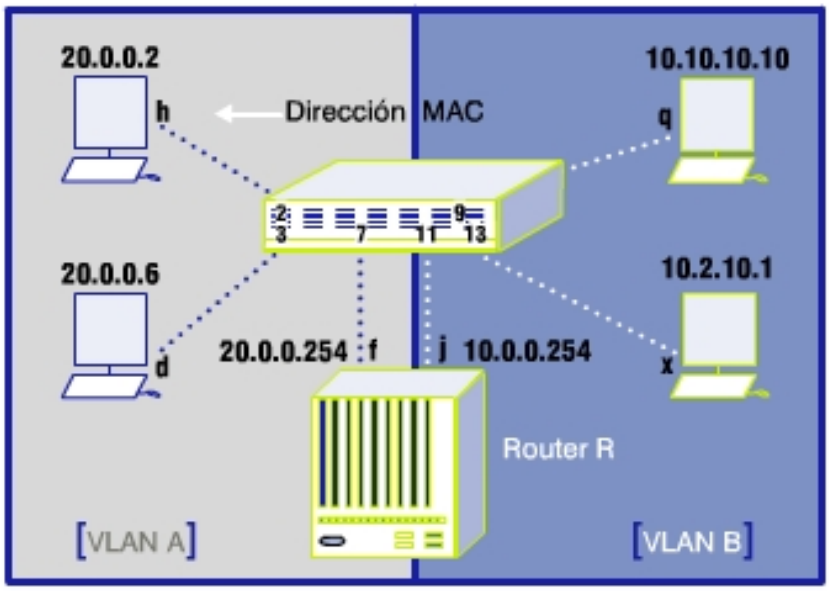
Por último, veamos la creación de VLANs por agrupación según nivel 3.



Las VLANs basadas en información de nivel 3 tienen en cuenta el tipo de protocolo de nivel 3 o el tipo de dirección de nivel 3 (por ejemplo, direcciones IP).

En la figura, configuramos la VLAN A asociada a la red 20.0.0.0 y la VLAN B a la red 10.0.0.0.

Aunque un conmutador inspeccione las direcciones IP de los paquetes para determinar la pertenencia a una VLAN, no se realiza ningún proceso de encaminamiento, y a las tramas que atraviesan el conmutador se le aplican procedimientos de conmutación, de acuerdo con la implementación del protocolo STP.



Si se requiere de encaminamiento, habrá de utilizarse un router.

VENTAJAS

Este tipo de VLAN permite independizar la VLAN de la ubicación física de los dispositivos e incluso de su interfaz de red.

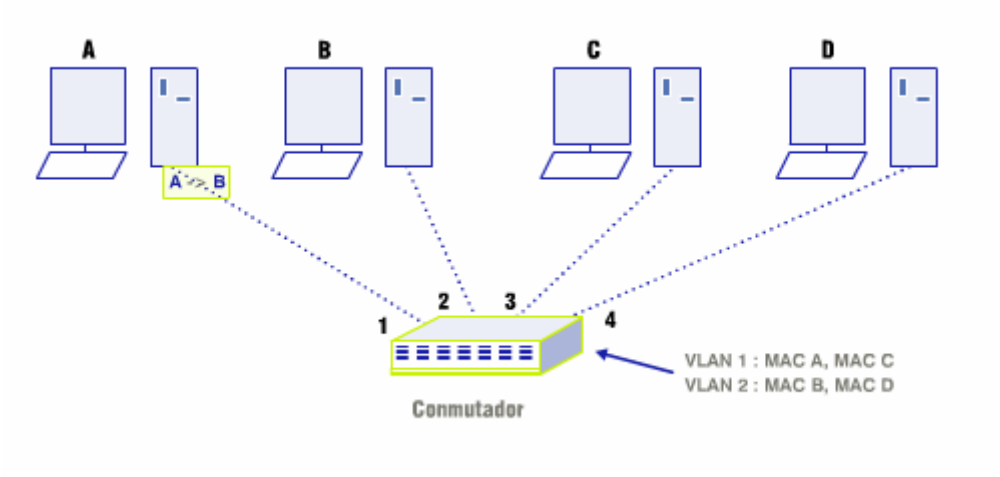
Los conmutadores que se ocupan del nivel 3 (layer 3 aware) disponen, a menudo, de la funcionalidad de envío de paquetes (packet forwarding), que forma parte del proceso de encaminamiento implementada con ASICs, **mejorando así las prestaciones sobre los routers basados completamente en software.**

Etiquetado de Tramas

Ahora, hemos de plantearnos cómo un conmutador con elementos de varias VLAN puede conocer la existencia de elementos de esas VLANs conectados a otros conmutadores, para realizar el proceso de reenvío apropiadamente.

Veamos el Etiquetado.

Etiquetado implícito



Cuando un conmutador basa su decisión de pertenencia de una trama a una determinada VLAN en función del puerto, la dirección MAC o la información de nivel 3, se dice que es etiquetado implícito.

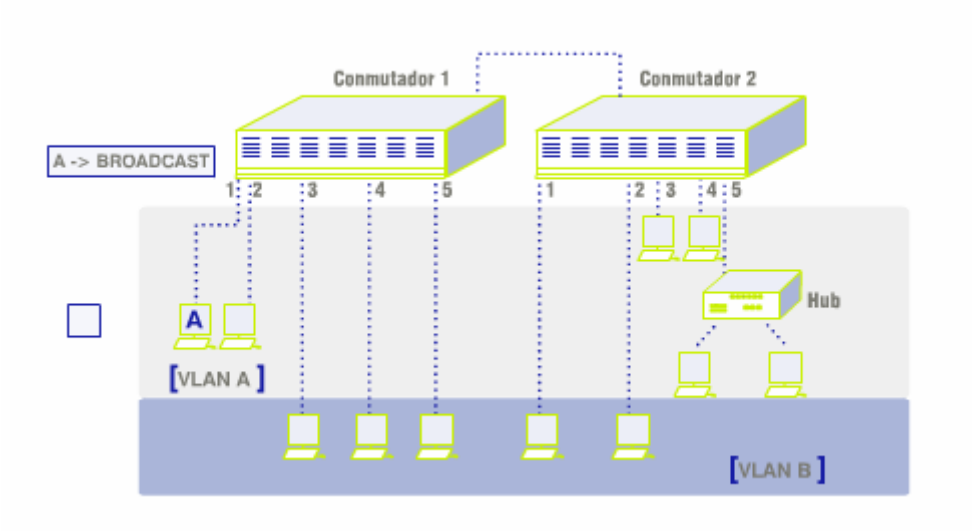
Este tipo de etiquetado limita el funcionamiento del conmutador a la información registrada y conocida por él.

Etiquetado explícito

Otro método de etiquetado recibe el nombre de EXPLÍCITO. En éste, el conmutador añade a la trama una etiqueta que define la pertenencia de esa trama a una VLAN determinada.

De esta forma, otros conmutadores con elementos de esa VLAN podrán reenviar el paquete por el puerto adecuado.

Veamos el Etiquetado explícito

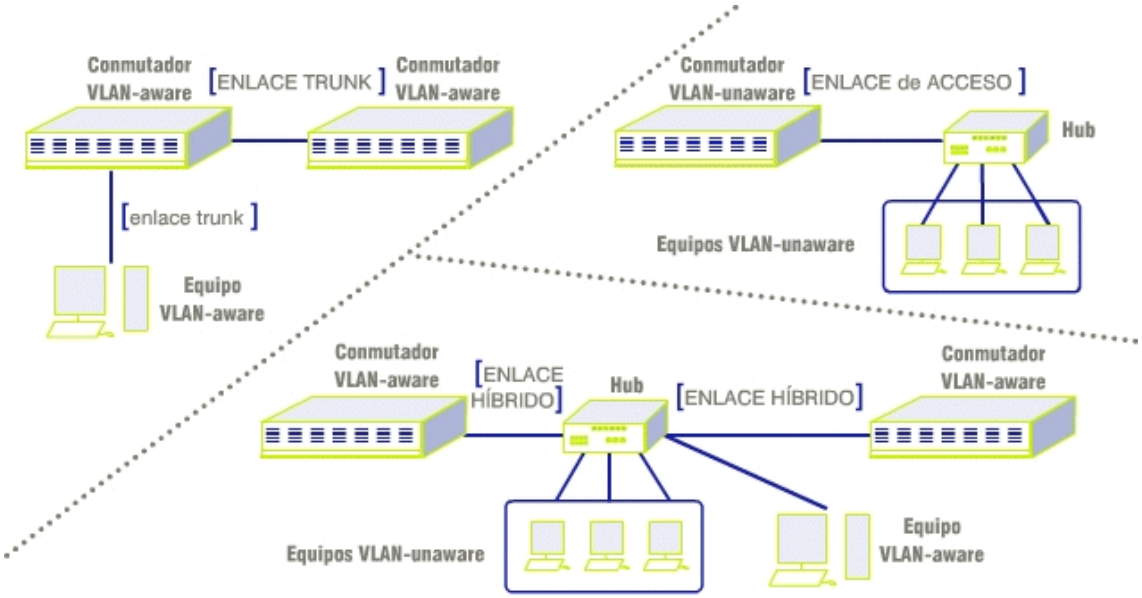


Cuando un conmutador de una VLAN recibe una trama de datos de una estación terminal, determina hacia dónde debe enviar la trama basándose en operaciones normales de LAN (conmutación de nivel 2).

Una vez que el conmutador determina hacia dónde debe encaminar la trama, debe decidir si añade la etiqueta de VLAN a dicha trama y la envía.

Si la trama se envía hacia un dispositivo que tiene conocimiento de la existencia de VLANs (VLAN-aware), se añade la etiqueta de VLAN a la trama. Por el contrario, si el destino es un dispositivo que no entiende de la implementación de VLANs (VLAN unaware), no añade ninguna etiqueta y envía la trama sin el identificador de VLAN.

Tipos de enlaces entre dispositivos VLAN



Como has visto, existen dispositivos que entienden de etiquetado explícito (VLAN aware) y otros que no (VLAN unaware). En función de esto, también existen diferentes tipos de enlaces, en general, tres tipos: Trunk, de acceso e híbrido.

Enlace de Acceso

Un enlace de acceso conecta un dispositivo VLAN-unaware a un puerto de un conmutador VLAN-aware.

Todas las tramas que circulan por los enlaces de acceso deben utilizar el etiquetado implícito. El dispositivo VLAN-unaware puede ser un Hub, un PC, etc.

Trunk

Todos los dispositivos conectados a un enlace trunk, incluyendo las estaciones de trabajo, deben ser VLAN-aware.

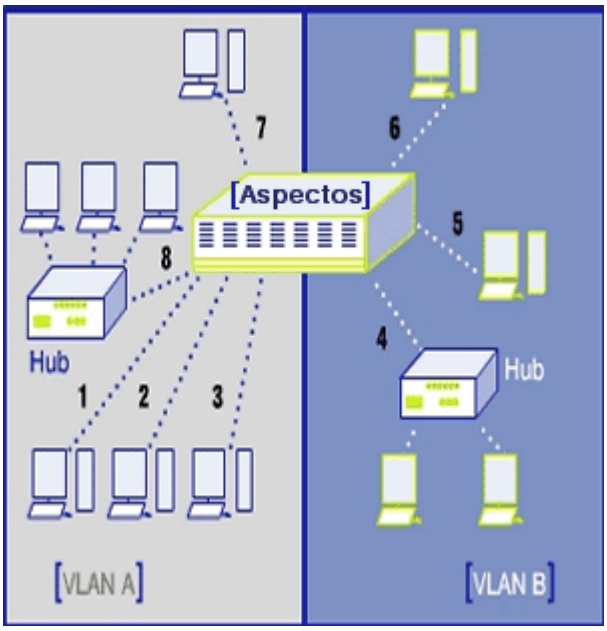
Todas las tramas en un enlace trunk deben tener una cabecera especial asociada a ellas. Estas tramas especiales se denominan tramas etiquetadas (tagged frames).

Enlace Híbrido

Un enlace híbrido es una combinación de los dos tipos de enlace anteriores. Se trata de un enlace al que, tanto dispositivos VLAN-aware como VLAN-unaware, se encuentran asociados.

A través de un enlace híbrido pueden circular tramas etiquetadas y tramas no etiquetadas (etiquetado implícito), pero todas las tramas para una VLAN determinada deben estar o etiquetadas o no etiquetadas.

Estandarización de las VLAN



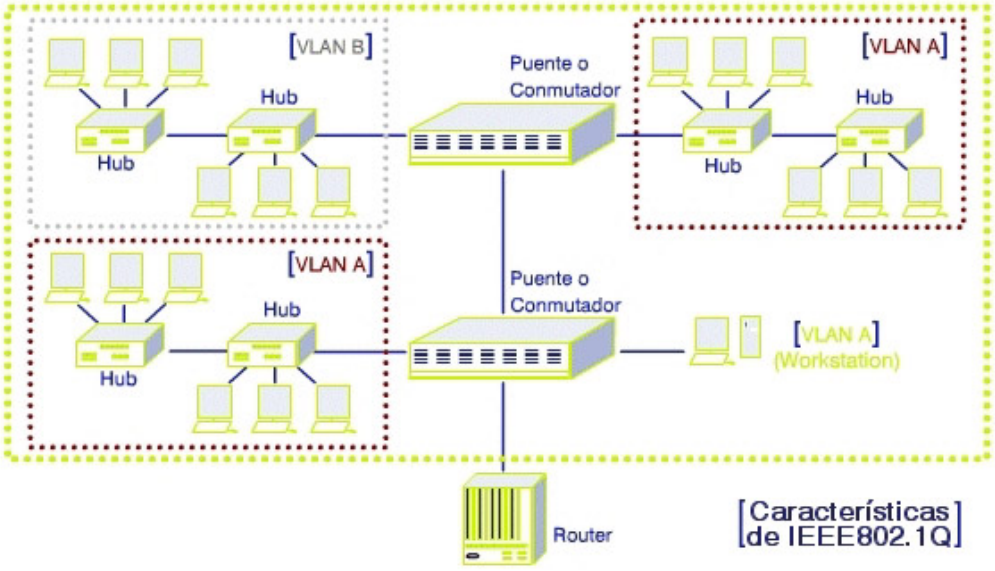
Por último, necesitamos definir el formato de las etiquetas. Veamos las normativas IEEE desarrolladas.

En marzo de 1996, el IEEE 802.1 (Internetworking Subcomettee) completó la fase inicial de investigación para el desarrollo de un estándar para VLAN y propuso ciertas resoluciones concernientes a tres aspectos.

ASPECTOS

- La arquitectura de las VLAN.
- Un formato estandarizado de etiquetado de tramas (frame tagging) para la comunicación de la información de pertenencia a una VLAN a través de múltiples equipos de diferentes fabricantes (normativa IEEE802.1q).
- Las directrices para una futura estandarización de las VLAN.

IEEE802.1Q: etiquetado de tramas



El estándar IEEE802.1Q se ha erigido como solución genérica para el etiquetado explícito de tramas en las VLANs.

El formato de etiquetado de tramas IEEE 802.1Q se erige en 1999 como estándar para la comunicación de información de pertenencia a una VLAN.

Sin embargo, el estándar sólo es aplicable a VLANs definidas en los niveles 1 y 2 (por puertos y por direcciones MAC, respectivamente).

Características de IEE802.1Q

- Define una arquitectura para la utilización de los servicios de VLAN sobre las LANs conmutadas IEEE 802 existentes.
- Define el formato de trama para el transporte de etiquetas de VLAN tanto en tramas Ethernet/IEEE 802.3 como en tramas Token-Ring.
- Define los protocolos y mecanismos mediante los cuales se puede comunicar la información de configuración y de pertenencia a VLANs entre dispositivos VLAN-aware.
- Define los criterios y procedimientos para el envío de tramas en una red con dispositivos VLAN-aware IEEE 802.1Q.
- Asegura la completa interoperabilidad y coexistencia con dispositivos no VLAN-aware.

Relación de ideas clave

Fíjate que una de las principales características de IEEE802.1Q es su compatibilidad con dispositivos VLAN unaware.

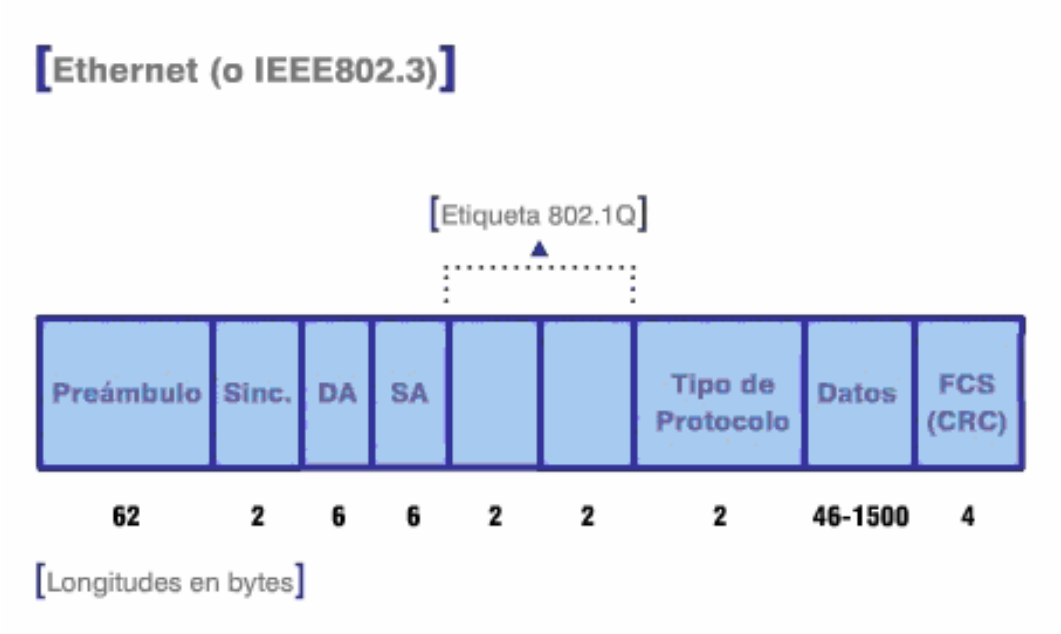
Esto es porque la etiqueta se inserta en medio de la cabecera MAC.

Veamos el caso aplicado a Ethernet.

Formato de Tramas 802.1Q

El formato de la etiqueta en una trama Ethernet se muestra en la figura.

La etiqueta de la cabecera añade cuatro octetos (dos nuevos campos) después del campo dirección MAC origen. Veamos.

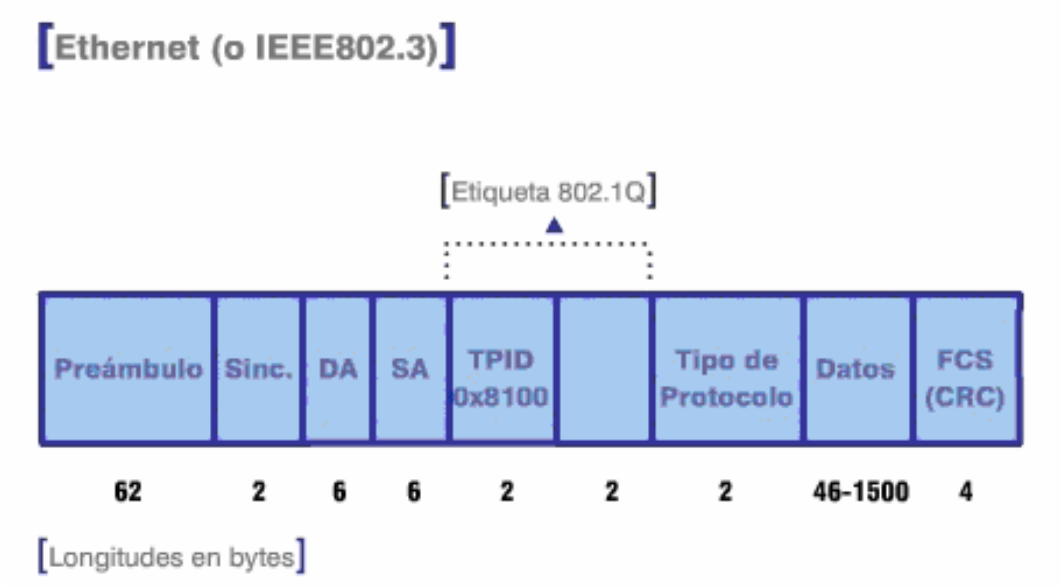


El TPID

Tag Protocol Identifier (TPID).

Es el valor que indica la presencia de una etiqueta VLAN.

Se trata de un valor de tipo Ethernet que identifica a la trama como una trama etiquetada 802.1Q (0x8100).

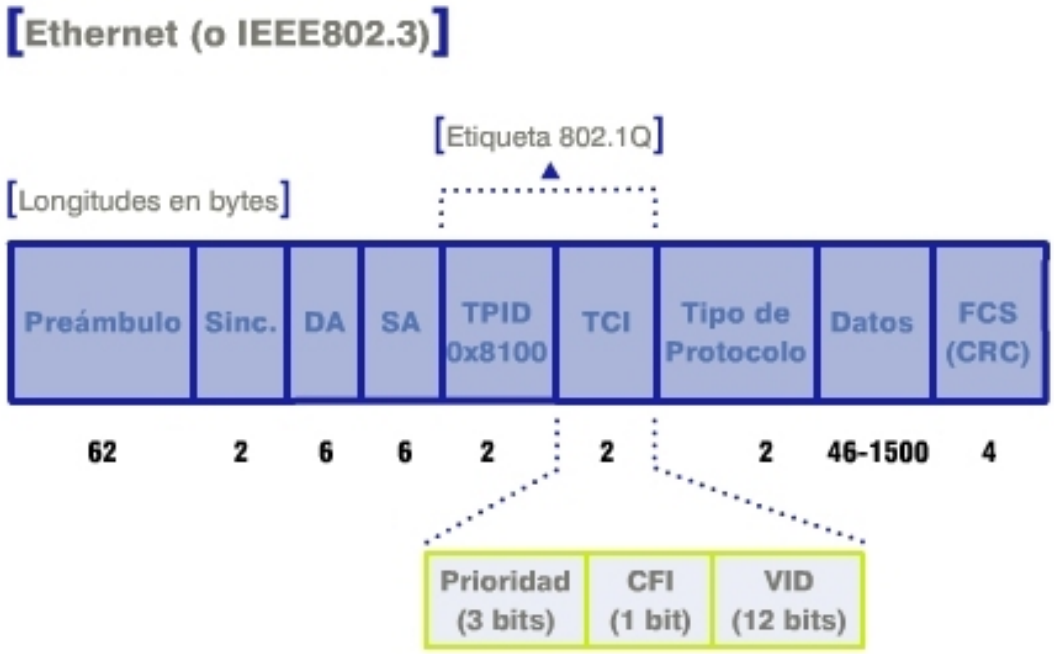


Si un dispositivo VLAN unaware recibe una trama etiquetada, al leer este campo (que correspondería a tipo de protocolo) interpreta que es protocolo 802.1Q y se "salta" los 4 octetos.

El TCI

Tag Control Information (TCI).

Incluye un identificador de VLAN (VID), de 12 bits, que identifica la VLAN a la que pertenece la estación que generó la trama.



Los primeros 3 bits de la etiqueta 802.1Q se utilizan según la especificación 802.1p para establecer la prioridad del paquete.

El bit CFI (Canonical Format Indicator) indica si la información de dirección MAC está o no en formato canónico.

(Se dice que una dirección utiliza el formato canónico cuando el octeto menos significativo de la dirección es el que se escribe más a la izquierda).

Conclusión

Durante todo este módulo hemos hablado de las LAN, hoy por hoy definidas como redes de DIFUSIÓN.

Ethernet, considerada como la tecnología predominante en el mercado, ha sufrido diferentes procesos evolutivos, desde la especificación original desarrollada por Xerox, hasta las implementaciones a 10Gbps, pasando por el proceso de estandarización de la IEEE.

Con su evolución se han introducido elementos adicionales para la interconexión cuya función original era solventar las limitaciones propias de los medios físicos y la técnica de acceso al medio CSMA/CD.

Estos elementos también evolucionan con la aparición de puentes y conmutadores que permiten optimizar el tráfico de la red y, en cierta forma, eliminar los dominios de colisión así como mejorar el rendimiento.

Las necesidades de las redes de difusión de hoy implican el uso de las denominadas VLAN o redes de área local virtuales.

Éstas introducen un nuevo concepto: el etiquetado de las tramas para poder identificar la pertenencia a una VLAN determinada.

El uso de VLANs permite aislar dominios de difusión y dar mayor seguridad a la red.

Concluyendo, el mundo de las redes de difusión evoluciona continuamente, apareciendo elementos con funcionalidades nuevas que proveen de servicios, como

la conmutación de nivel 3 y de nivel 4. Conocer los fundamentos de estas redes, su evolución y situación en el entorno OSI, permiten avanzar y asimilar los conceptos de una tecnología en constante cambio.