

RESUMER 1ER PARCIAL

▼ Autor	Juan Pablo Frascino
☑ Reviewed	<input type="checkbox"/>

CABLEADO ESTRUCTURADO

Sistema de cableado de telecomunicaciones generales en un edificio, establecidos por 2 normas conocidas como EIA/TIA 568

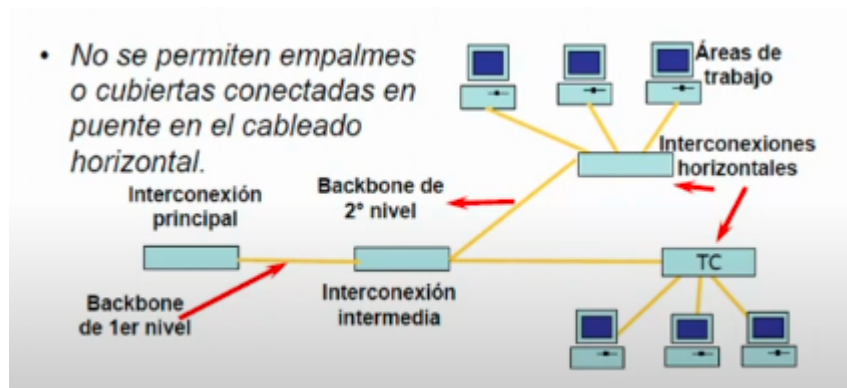
Trata de especificar una "estructura o "sistema" de cableado para empresas o edificaciones que tenga las siguientes CARACTERISTICAS:

- Comun y a la vez independiente de las aplicaciones
- Documentada
- Proyectada a largo plazo(>10 años)
- Administrable
- Adaptable y Escalable
- Confiable

En este cableado se comparten varios servicios, no solo se transmiten datos sino que tambien funcionan por el sistemas de voz/telefonicos, redes de area local, sistemas de video, de seguridad, de control, etc.

TOPOLOGIA

El cableado estructurado se basa en una topologia de estrella extendida, en ella, los diferentes hosts(ej:pc, impresoras, server, etc) se van conectando a un concentrador, al ser extendida tenemos mas de 1 concentrador que lo que nos permite es ir abriendo esa estrella a diferentes niveles horizontales llamados backbone



SUBSISTEMAS DEL CABLEADO ESTRUCTURADO

AREA DE TRABAJO(WA): es el lugar en donde los usuarios interactúan con los equipos terminales de telecomunicaciones se termina en la salida de información mediante Bocas de telecomunicaciones llamados periscopios. Utilizan conectores denominados RJ-45. La distancia máxima es de 3 metros.

CABLEADO HORIZONTAL: Va desde el conector del área de trabajo hasta el armario/gabinete del cuarto de telecomunicaciones(TC), la distancia máxima es de 90 metros y el tendido puede ser por varias formas(aéreo, piso técnico, cable canal, etc).

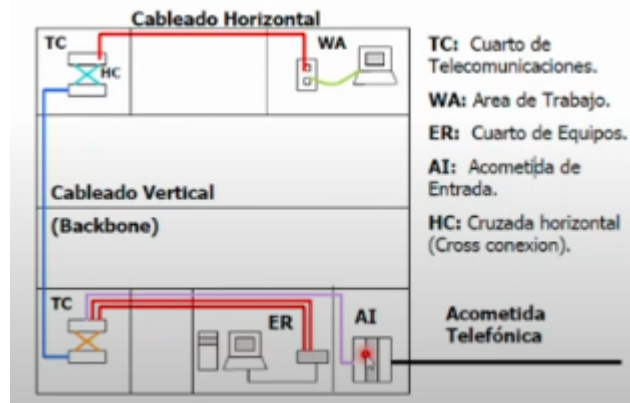
ARMARIO DE TELECOMUNICACIONES(TC): Concentra todas las terminaciones de todo tipo de cable horizontal y las conecta con las terminaciones de los cables de backbone del cableado vertical con el fin de extender el servicio hacia las áreas de trabajo conectadas horizontalmente.

CABLEADO CRUZADO: La interconexión entre el cableado horizontal y el servicio, se realiza de manera cruzada mediante un patch cord en el gabinete del armario de telecomunicaciones. Este tiene de distancia máxima 6 metros.

CABLEADO VERTICAL/BACKBONE: Posibilita la conexión entre los distintos armarios de telecomunicaciones, la sala de equipo y la entrada del edificio.

CUARTO DE EQUIPO/SALA DE EQUIPAMIENTO: La sala de equipamiento o red es el lugar donde se ubican los equipos de comunicaciones (Routers, Central Telefónica), red (Hub o Switchs), servidores, ups, etc. Es el corazón de la red.

ENTRADA DE EDIFICIO: Los cables, elementos y equipos necesarios que conectan las instalaciones externas del proveedor de servicios con el sistema de cableado estructurado de la red local



DISTANCIAS MAXIMAS

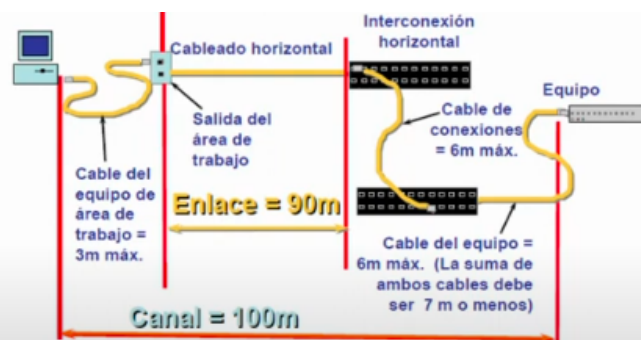
Desde la tarjeta de red hasta la toma: 3 metros

Desde la toma hasta el patch panel: 90 metros

Desde el patch panel hasta el hub: 6 metros

Mínimo dos conectores por puesto de trabajo (voz y datos)

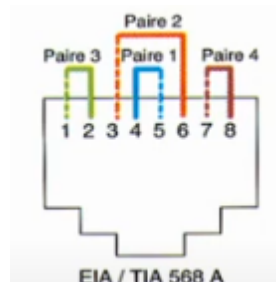
Conector estándar: 4 pares (8 hilos), 100 ohms, UTP

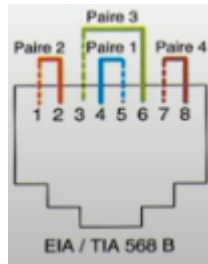


TIPOS DE CABLE

En los cableados horizontales, los latigillos que conectan las computadoras y los patch cord cruzados utilizan CABLES UTP, estos se dividen en categorías dependiendo de su uso y velocidad de transmisión, las mas comunes hoy son la 5 de hasta 100mps y la 6 de hasta 1gbps.

Estos cables siguen 2 normas para su armado mediante fichas rj45:





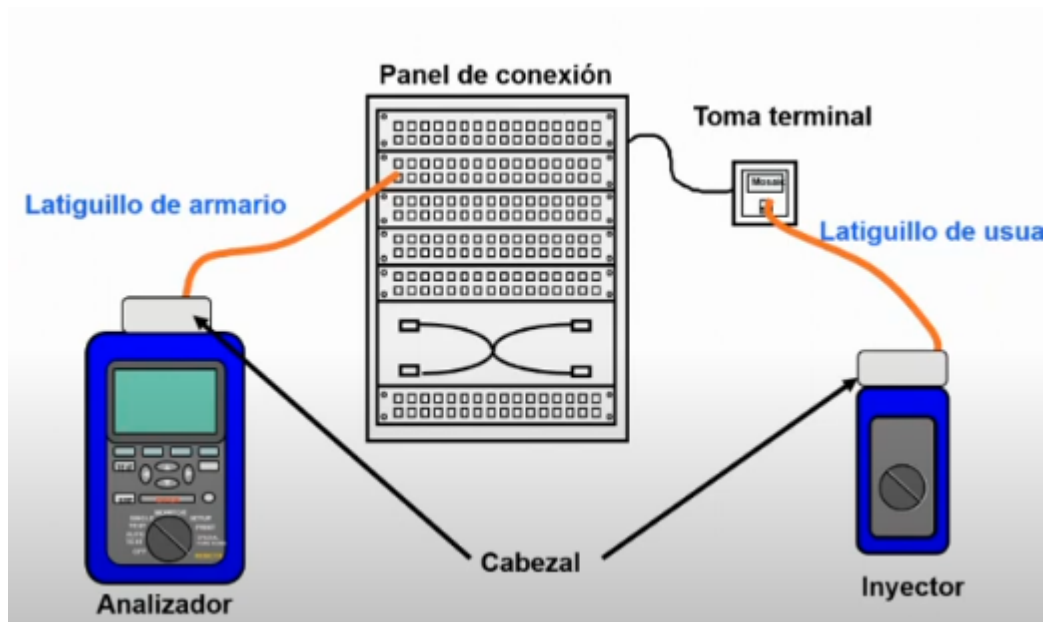
Podemos utilizar cualquiera de las 2 normas pero hay que tener en cuenta los siguientes 2 tipos de cable:

CABLE DERECHO: es aquel que utiliza la misma norma en ambas puntas de cable, utilizado para conectar de un host a un switch, host a un hub, de switch a router (generalmente dispositivos diferentes)

CABLE CRUZADO: es aquel que utiliza una norma distinta de la otra en los extremos del cable, utilizado para conectar de un host a otro host directamente, de un switch a un hub, y de switch a switch, router a router (generalmente dispositivos iguales)

Estos cableados pueden o no estar **CERTIFICADOS**, durante la certificación viene un tercer actor a testear el cableado generando una documentación buscando garantizar la calidad de la instalación siguiendo los estándares de rendimiento, el 100% de operatividad y que se cumpla con la categoría prometida. Además extiende la garantía de los materiales. Se realizan informes donde están las mediciones punto por punto, toma por toma, cable por cable.

ej medición



En la medición se miden parámetros como atenuación(cantidad de db q pierdo en el largo, paradiafonia NEXT/crosstalk(la inducción de un par sobre otro par, si los pares se interfieren entre ellos), retardos de propagación y desfase, impedancia del cable, longitud del cableado, mapa de conexiones.

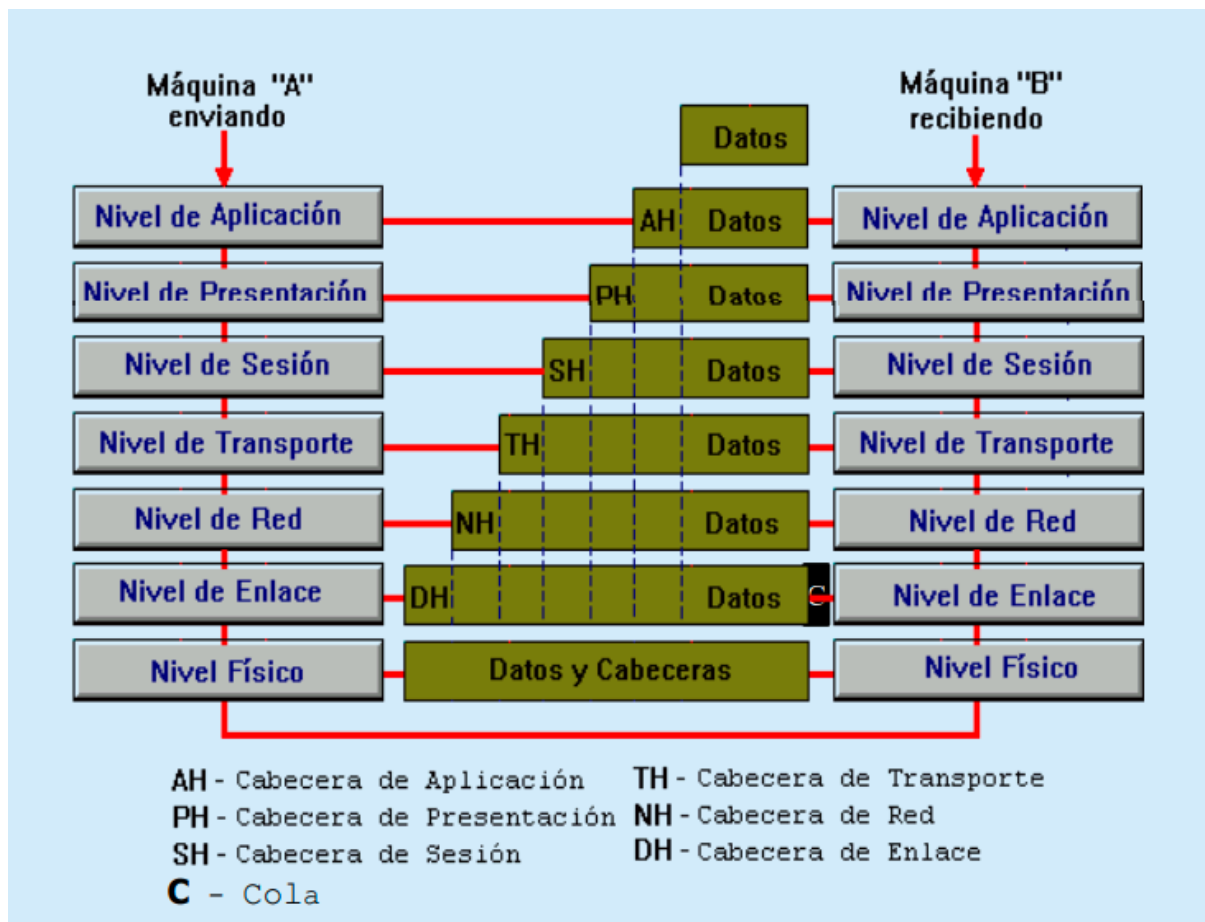
MODELO OSI

El modelo osi(Open System Interconnection), lanzado en 1984, es un conjunto de estándares que garantizan la compatibilidad entre tecnologías de red de distintos fabricantes, este se divide en 7 capas



VENTAJAS DE UN MODELO EN CAPAS:

- Reduce la complejidad
- estandariza las interfaces
- facilita la ingeniería modular
- asegura una tecnología interoperable
- acelera la evolución
- simplifica la enseñanza y el aprendizaje



Cuando una maquina decide enviar informacion por la red va bajando capa por capa desde la capa mas alta(aplicacion) hasta la mas baja(nivel fisico), cada capa le va agreando un encabezado/headear a los datos necesario para la correcta interpretacion y funcionamiento de las capas, la maquina receptara comenzara a recibir la informacion desde el nivel mas bajo e ira subiendo capa por capa hasta el nivel mas alto nuevamente interpretando la informacion con la ayuda de los headers

REDES DE AREA LOCAL-LAN

Las LAN(Local area network) como su nombre lo indica, son redes de area local, a diferencia de otro tipos de redes estas estan restringidas a un area geografica reducida como un edificio de oficina, una casa, nave o campo. Estas redes tambien pueden depender de un canal físico de comunicaciones con una velocidad binaria media/alta y con una tasa de errores reducida.

Razones para instalar una LAN;

- Necesidad de compartir recursos(discos, impresoras, aplicaciones)

- Procesos distribuidos
- sistema de mensajería
- bases de datos
- creación de grupos de trabajo
- gestión centralizada
- seguridad(backup)

Las redes lan además pueden estar construidas con diferentes tipos de medios de transmisión:

- cable coaxial(grueso, fino)
- par trenzado(utp, stp)
- fibra óptica(monomodo, multimodo)

COMPONENTES DE UNA LAN

HARDWARE:

- Servers de infraestructura
- Hosts
- Placas de red
- Cableado
- Conmutadores(switch)/concentradores(hub)

SOFTWARE:

- Sistema operativo de Red
- Protocolos de Comunicaciones

CLASIFICACIONES REDES LAN

puede ser por

MODO DE TRANSMISION:

- BANDA BASE(ej, ethernet)
- BANDA ANCHA(modem)

TOPOLOGIA:

- Anillo
- Bus
- Estrella
- Arbol o estrella extendida/ramificada

METODOS DE ACCESO AL MEDIO

Existen de 2 tipos

PROBABILISTICOS

- CSMA/CD (Carrier Sense Multiple Access / Collision Detection)

DETERMINISTICOS

- token ring
- Polling

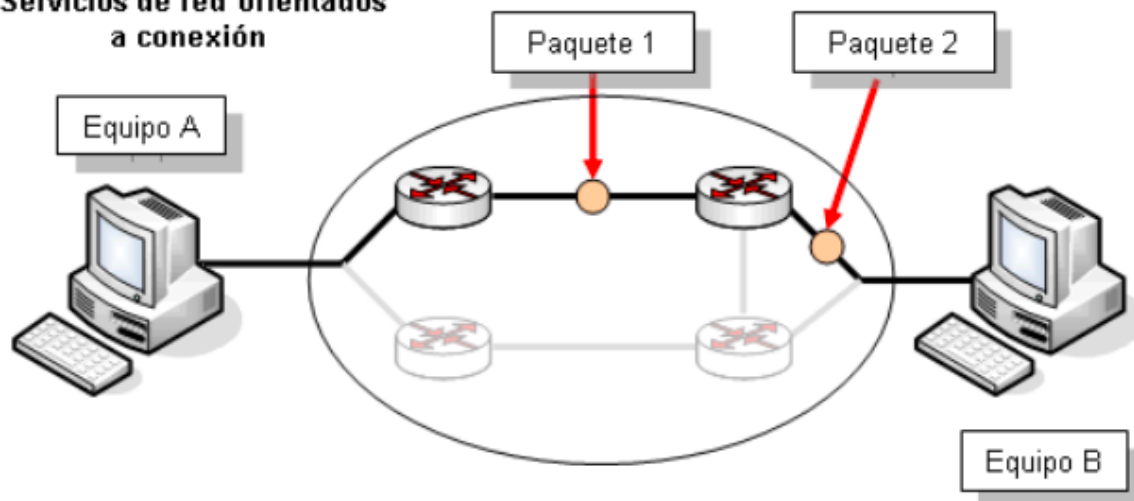
TIPOS DE REDES LAN

Depende en la norma de la IEEE que se basen:

- IEEE 802.3: ETHERNET
- IEEE 802.4: TOKEN BUS
- IEEE 802.5: TOKEN RING

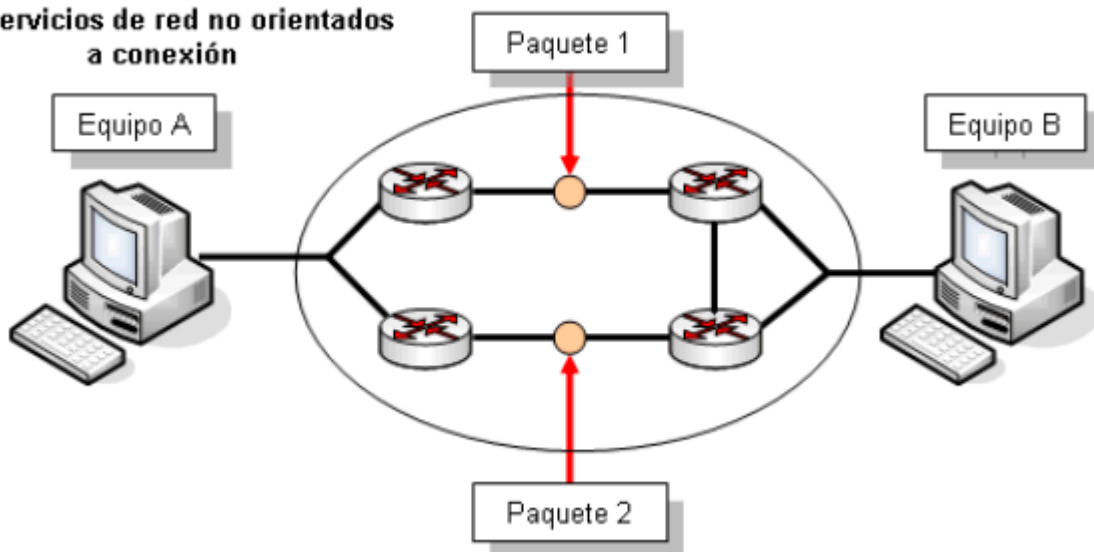
Luego las redes pueden ser tanto orientadas a la conexion, es decir se establece una conexion entre emisor y receptor previamente al envio de datos

Servicios de red orientados a conexión



o no orientadas a la conexión, donde se envían paquetes a través de diferentes rutas atravesando la red y no habiendo contacto entre emisor y receptor antes de que se envíe el paquete.

Servicios de red no orientados a conexión



1. CAPA FÍSICA

Define conexiones físicas.

Aquí opera el HUB

Concentrador-Hub:

- Simula coaxil con cable UTP.
- Señal se replica por todo el cable.
- 1 puerto si escucha, los demás transmiten.
- Dominio de colisiones y de broadcast.
- Mensaje a cada puerto (esté o no conectado).
- Cada Boca = Dominio de colisión. Menos eficiencia, tarda más el mensaje.

2. CAPA DE ENLACE

Tiene como objetivo que:

- La informacion se transmita libre de errores
- Controlar el acceso a la capa fisica
- Direccionar localmente con las direcciones fisicas(MAC address)

Esta utiliza bloques de informacion llamados TRAMAS, y estas tramas difieren dependiendo de que version de la RED LAN ETHERNET(la mas comun de todas, pero hay otras, token ring, wifi, etc) se este utilizando:

Aqui opera el SWITCH

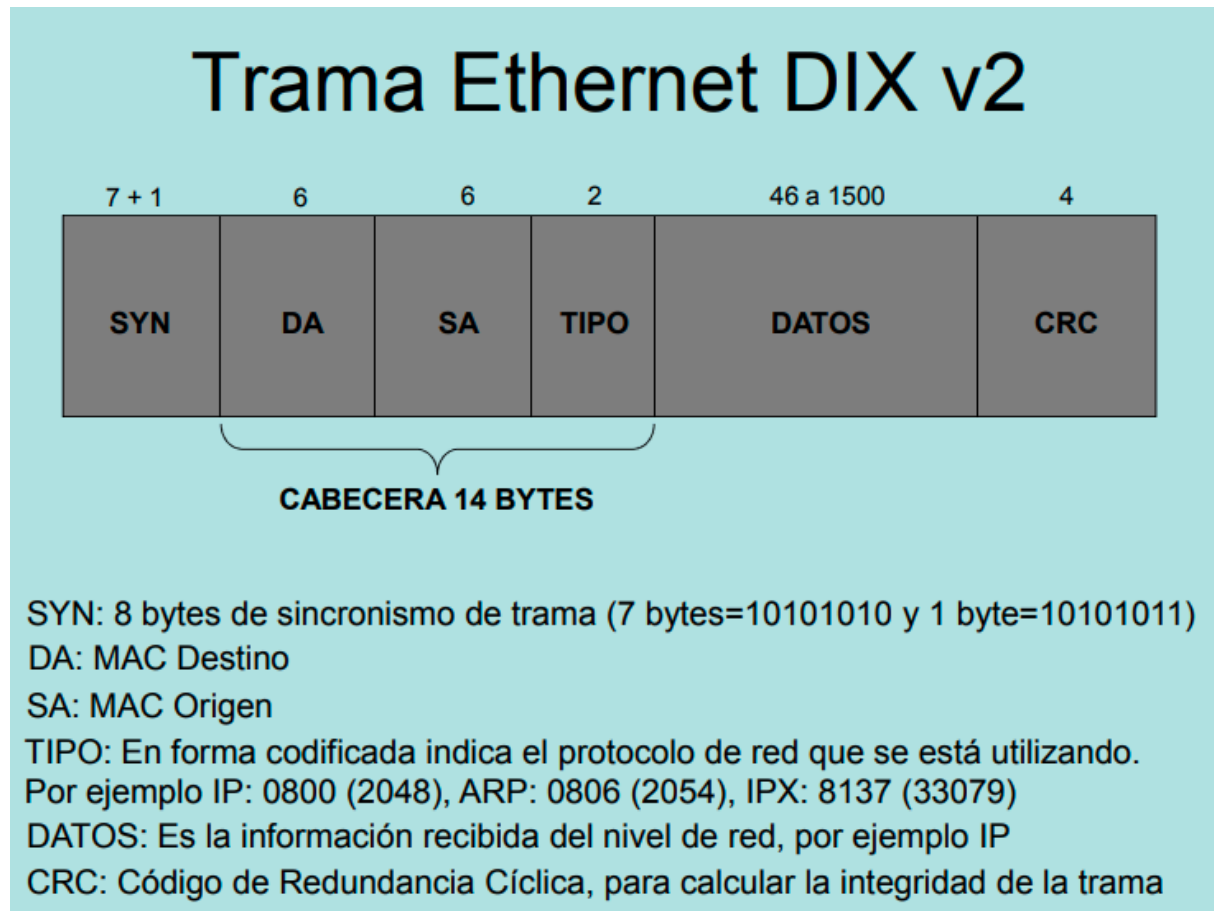
Conmutador-Switch:

- Cada switch es un dominio de colisión.
- Todas las máquinas conectadas son dominio de broadcast (mismo mensaje a todas las conectadas).
- Tablita de cada puerto con su máquina.
- Cualquiera le puede mandar a cualquiera.
- Si más de uno envían a un mismo puerto, gana el que llegó primero.
- Dominio de colisión por puerto
- Dominio de broadcast por switch

PRACTICA APRENDER TRAMAS

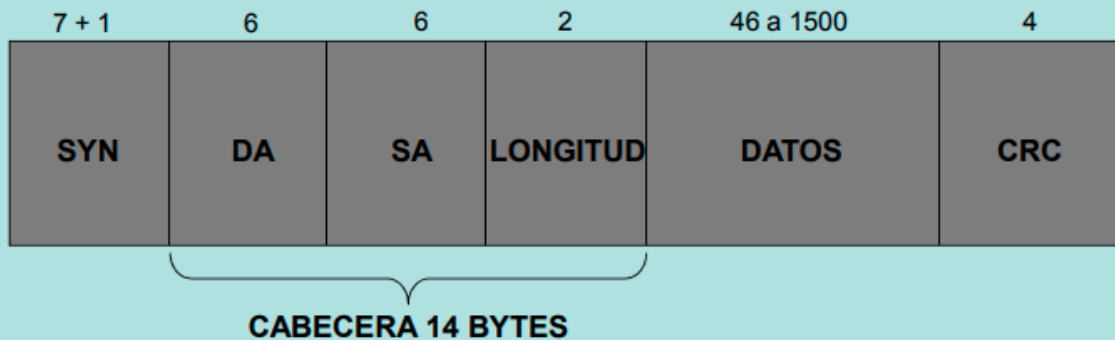
PARA SEPARAR CAMPOS CAPTURA DE RED

DIX V2



IEEE 802.3

Trama 802.3



SYN: 8 bytes de sincronismo de trama (7 bytes=10101010 y 1 byte=10101011)

DA: MAC Destino

SA: MAC Origen

Longitud del Campo de Datos: Indica la cantidad de bytes que tienen los datos

DATOS: Es la información recibida del nivel de red

CRC: Código de Redundancia Cíclica, para calcular la integridad de la trama

COMO IDENTIFICAR CADA UNA

Si el campo Tipo/Longitud(aquel que va luego de los primeros 12 bytes[6 mac destino, 6 mac origen], recordar que los bits de sincronismo no van en las capturas del analizador) es mayor que el hexadecimal 05 DC (decimal1500)(4 hexa=2bytes, 2 ehxa=1 byte), entonces es Ethernet V2, caso contrario es 802.3 y el valor representa la longitud de los datos

MAC ADDRESS

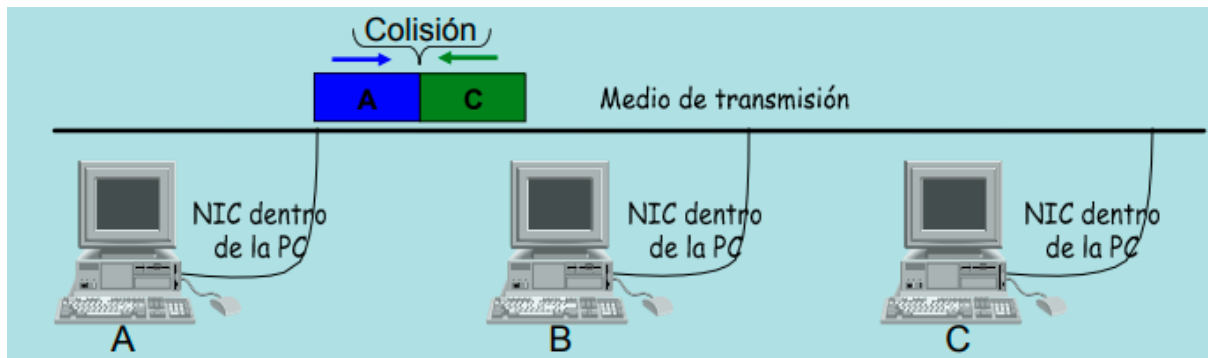
Para ethernet como mencionamos esta compuesta por 6 bytes, los primeros 3 definen al fabricante, y los otros 3 son definidos por el fabricante. Esta direccion esta grabada en las placas de red.

CSMA/CD

La red ETHERNET y sus derivadas funciona con el protocolo CSMA/CD (Carrier Sense Multiple Access/Collision Detect).

Este protocolo simula una conversacion al rededor de una mesa en un cuarto oscuro, antes de hablar cualquier participante escucha por unos segundos para comprobar que nadie este hablando(CARRIER SENSE), cuando esto ocurre, que nadie este hablando, cualquiera tiene oportunidad de tomar el

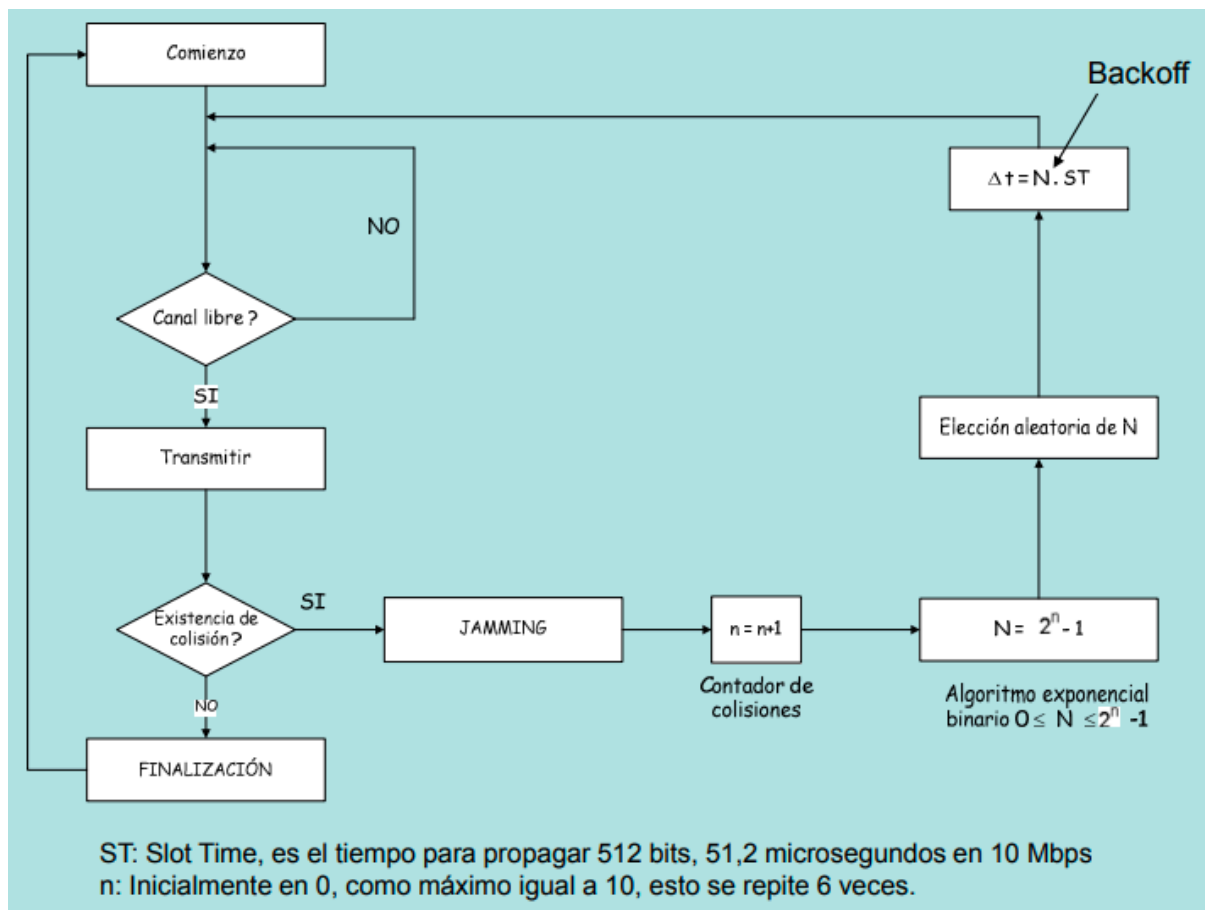
medio(MULTIPLE ACCESS), pero si dos personas comienzan a hablar al mismo tiempo se daran cuenta y dejaran de hablar(COLLISION DETECTION)



Mediante el CS los equipos escuchan el medio y si desean transmitir deben esperar a que se termine para tomar el medio(MA), el tema sucede si dos equipos escuchan silencio y deciden enviar a la vez, en algun punto del medio se genera una colision(CD), por eso inmediatamente despues de transmitir, el equipo transmisor escucha el medio para verificar colisiones. Si ocurre una colision los equipos que la detecten mandaran una señal de interferencia JAM, para detener todas las transmisiones en curso, para evitar la colision nuevamente los equipos realizan un BACKOFF, al esperar un tiempo aleatorio definido por un algoritmo y luego transmitir nuevamente.

Importante: La trama debe ser lo suficientemente larga como para permitir la detección de la colisión antes de que finalice la transmisión.

El algoritmo utilizado para esperar un tiempo aleatorio entre colisiones es el llamado ALGORITMO EXPONENCIAL BINARIO:



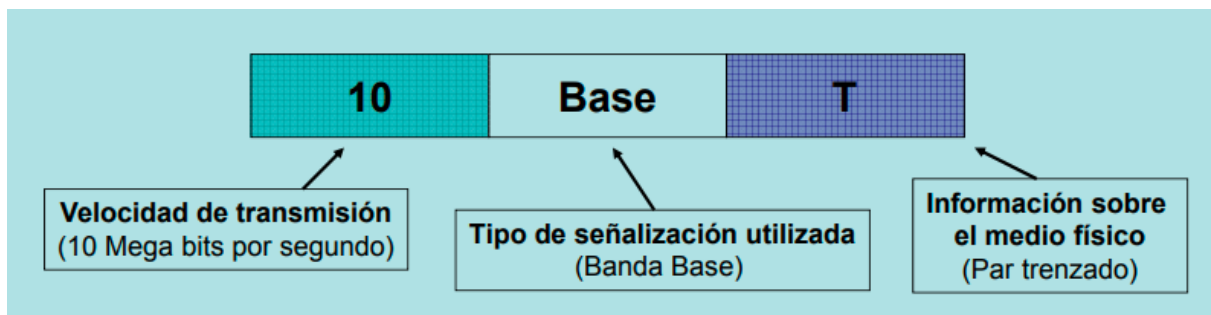
Basicamente se elije un numero aleatorio entre 0 y $2^n - 1$, donde n es el numero de colisiones seguidas, por lo tanto mientras mas colisiones ocurran secuencialmente, mayor sera el posible tiempo de espera, bajando las posibilidades de una proxima colision consecutivamente.

Las direcciones MAC pueden ser de 3 tipos:

- UNICAST: identifican a una sola estacion/equipo, en esta siempre el primer byte es un numero PAR
- MULTICAST: permite que un solo frame Ethernet sea recibido por varias estaciones en forma simultanea(conjunto predefinido de direcciones), en esta siempre el primer byte es un numero IMPAR
- BROADCAST: permite que un solo frame Ethernet sea recibido por todas las estaciones que vean el frame, tiene los 48 bits en 1(ff:ff:ff:ff:ff:ff), esta es un caso especial de las multicast

IDENTIFICADORES IEEE

Se utilizan para identificar los diferentes tipos de medios que puede utilizar ethernet, consta de 3 partes:



Los medios que arrancan con _

- 10 son ethernet
- 100 fast-ethernet
- 1000 giga-ethernet

Los medios que terminan con:

- 5 es coaxil grueso
- 2 es coaxil fino
- T es "twisted" de cables de par trenzado(utp)
- F es fibra optica y define 3 subconjuntos, FB sistemas backbone(escasos), FP conectan estaciones a hubs(no existen practicamente), FL es el MAS UTILIZADO

Variaciones de T y F en diferentes categorias

- 100Base-TX es utp categoria 5 o mas
- 100Base-FX es fibra optica multimodo
- 1000Base-SX (short), fibra optica onda corta
- 1000Base-LX (long), fibra optica onda larga
- 1000Base-CX (cooper), cable de cobre estandar de fibra maximo 25m

Problema

Calcular el tiempo mínimo y máximo de transmisión de las tramas de menor y mayor tamaño para 10Mbps y 100 Mbps.

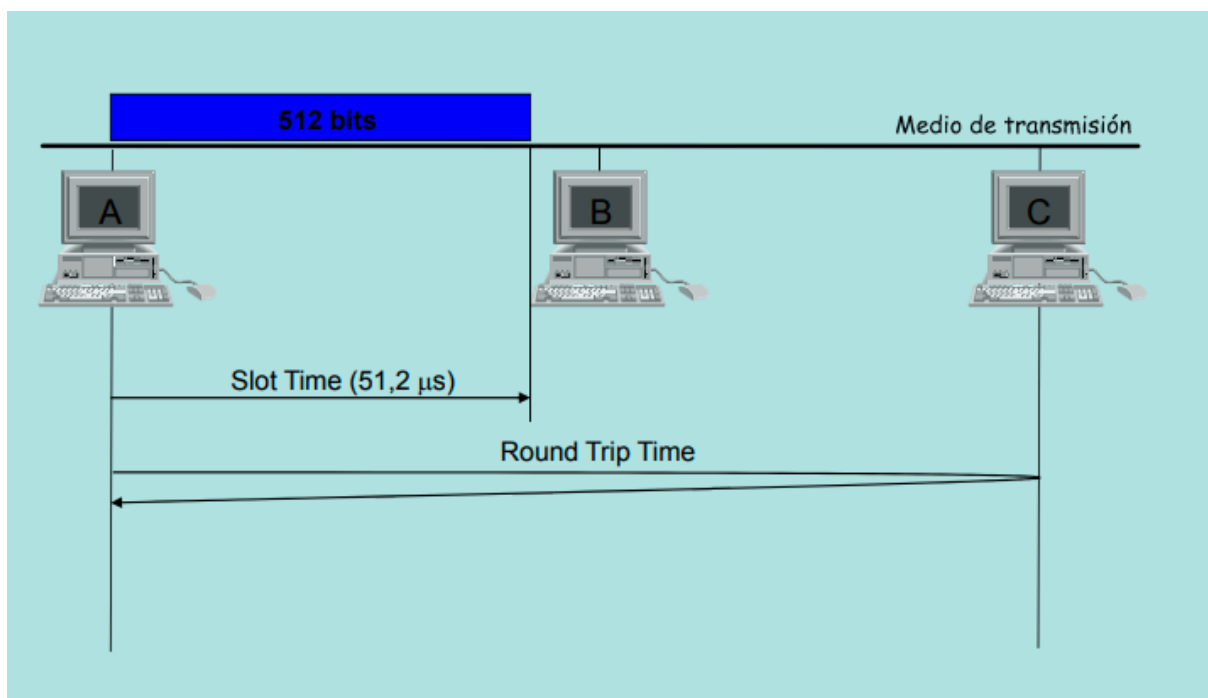
- Se asume que el tiempo de acceso es de 12 bytes.

	10	100
Tiempo de bit (μs)	0,1	0,01
Trama Corta (bytes) $[46 + 14 + 4]$	64	64
Trama Larga (bytes) $[1500 + 14 + 4]$	1518	1518
Duración Trama Corta (μs) $[64 * 8 * 0,1]$	51,2	5,12
Duración Trama Larga (μs)	1214	121,4
Tiempo de acceso (μs) $[12 * 8 * 0,1]$	9,6	0,96
Sincronismo (bytes)	8	8
Duración Sincronismo (μs) $[8 * 8 * 0,1]$	6,4	0,64
Tiempo Total Trama Corta (μs)	67,2	6,72
Tiempo Total Trama Larga (μs)	1230	123

$$51,2 + 9,6 + 6,4$$

Slot Time: Tiempo en transmitir 512 bits (trama corta).

Round Trip Time: Tiempo de ida y vuelta que demora una señal desde los dispositivos ubicados en los extremos de la red



DOMINIOS

Dominio de Colisiones

Área de la red en la cual se pueden producir colisiones.

Red comparte ancho de banda

Colisiones:

Ocurren cuando dos o más dispositivos intentan transmitir datos simultáneamente a través del mismo medio, causando interferencia y pérdida de datos.

Dominio de Broadcast

Conjunto de todos los dispositivos que recibirán frames de broadcast de cualquier dispositivo del conjunto dicho.

Todos los dispositivos reciben misma trama

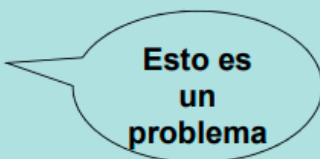
Cada switch es un dominio de broadcast(mismo para todos sus puertos), pero cada puerto del switch es un dominio de colision(uno para cada puerto).

El router corta el dominio de broadcast de una red a otra.

En cambio los hubs no diferencian dominio de host ni de broadcast, todos los dispositivos conectados a un concentrador comparten un único dominio de colisión y un único dominio de difusión.

Longitudes de las Redes (sin considerar repetidores)

- ETHERNET: Aproximadamente 5000 metros
 $(200 * 50) = 10000 / 2 = 5000$
- FAST ETHERNET: Aproximadamente 500 metros
 $(200 * 5) = 1000 / 2 = 500$
- GIGA ETHERNET: Aproximadamente 50 metros
 $(200 * 0,5) = 100 / 2 = 50$



Esto es
un
problema

Importante: Si se aumenta la velocidad:

- Hay que disminuir la distancia
- *Aumentar el tamaño de la trama*

GIGA ETHERNET

Anunciada por la IEEE en 1992, por estandar debe ser compatible con ethernet y fast-ethernet por lo que continua con las características de:

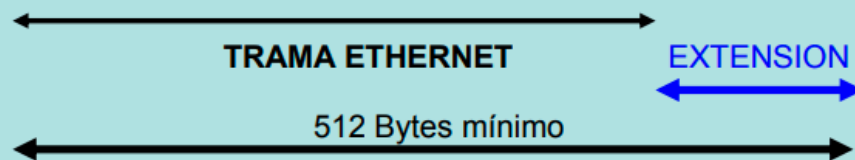
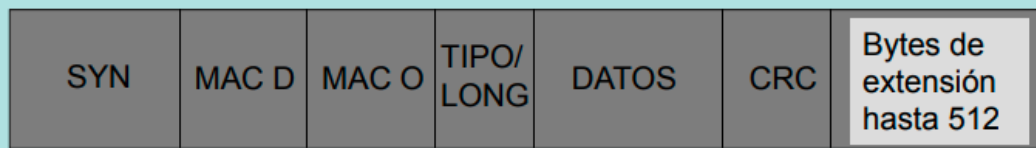
- Método de acceso al medio CSMA/CD
- Soportar half y full duplex
- Utilizar cables UTP, STP y Fibra Óptica

Se decidió aumentar el tamaño de la trama a 512 Bytes

- Se mantuvo el tamaño mínimo de la trama (64 Bytes) para no perder compatibilidad con ethernet y fast-ethernet

Pero si la trama es más corta que 512 bytes se agregan símbolos especiales hasta llegar a 512, a esto se lo denomina "Carrier Extension"

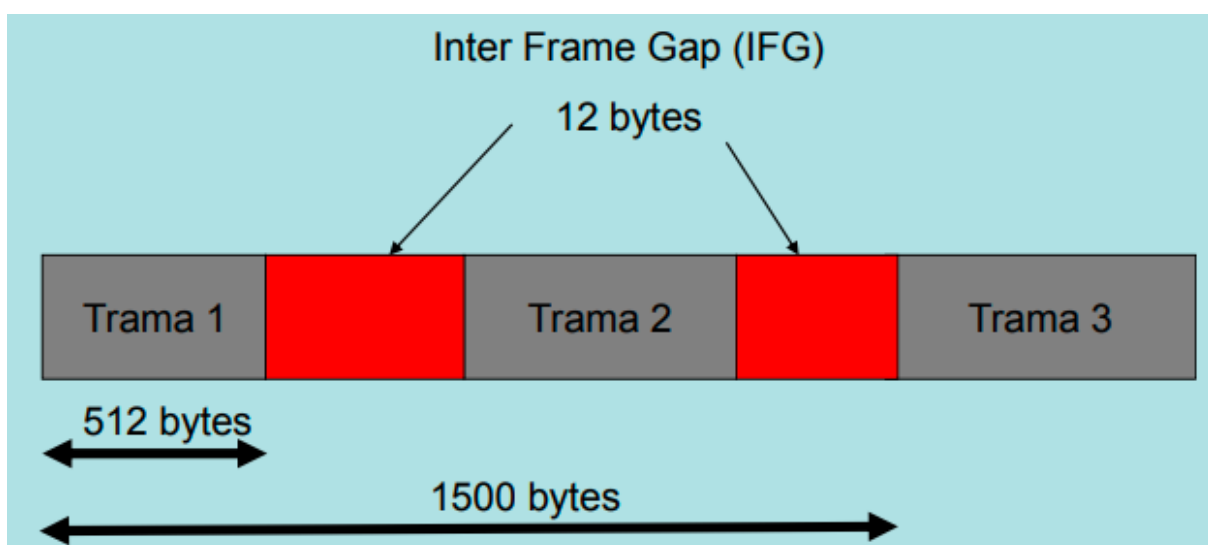
Trama Giga Ethernet



1 bit = 0,001 microsegundos, $512 \times 8 = 4096$ bits,
Duración Trama = 4,096 microsegundos

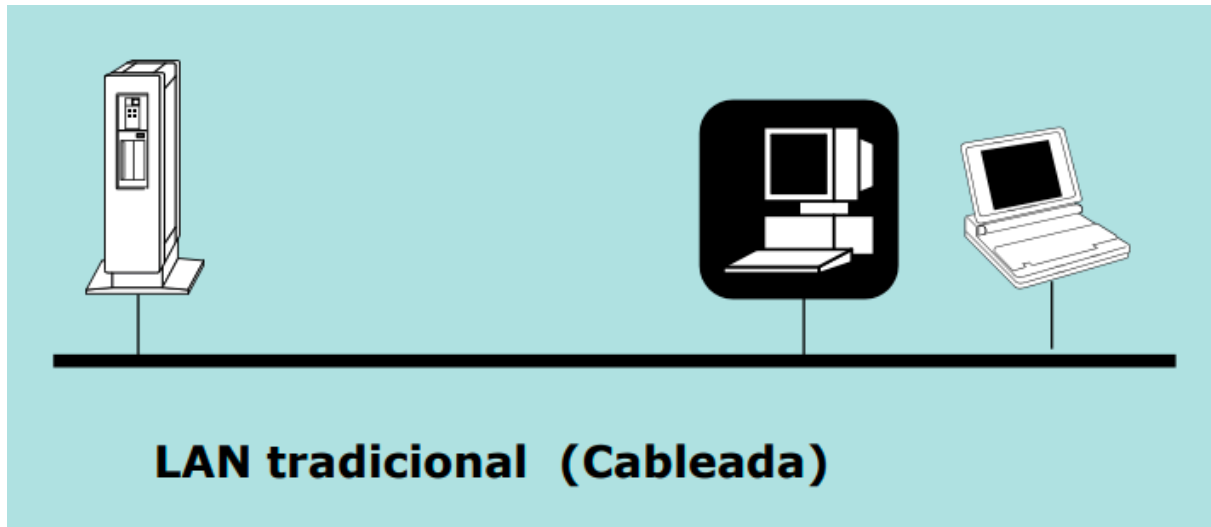
Importante: El problema se presenta en transmisiones de tramas cortas 64 bytes, ya que se necesitan 448 bytes de relleno (12,5 % de rendimiento).

Para solucionar este problema de perder rendimiento al mandar muchas tramas cortas, se utiliza una tecnica llamada PACKET BURSTING donde se agrupan varias tramas cortas de 512 bytes hasta llenar 1500 bytes, el objetivo es enviar mas de un frame durante el tiempo de transmision de equipo



REDES INALAMBRICAS

En una LAN tradicional(cableada) los clientes y el servidor tienen una ubicación fija



pero con el tiempo fue incrementando en el número de usuarios que tienden a la movilidad y que requieren acceso a la red sin importar donde se encuentren, por lo que el uso del cable se volvió poco práctico o incluso imposible de implementar en estos casos.

Es por eso que nacen las redes wireless, estas redes tienen múltiples aplicaciones como facilitar la ampliación de las redes LAN, interconectar edificios, permitir el acceso a viajeros o conexiones Ad Hoc(dispositivo a dispositivo).

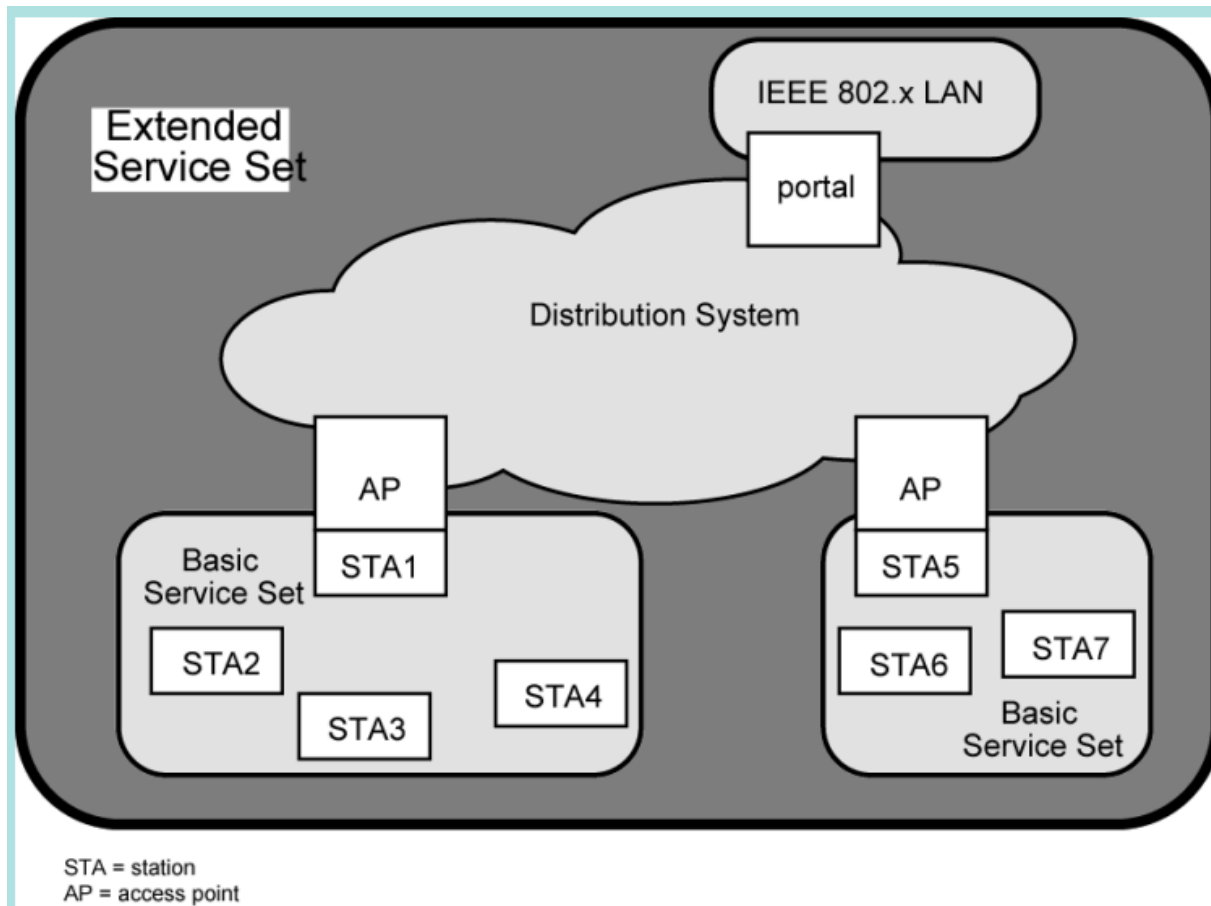
Cuales son los requisitos que debe cumplir una red wireless?

- buen rendimiento
- buena cantidad de nodos
- debe estar conectada a la LAN troncal
- buena área de cobertura
- bajo consumo de energía
- seguridad
- licencia
- itinerancia

- configuracion dinamica

IEEE 802.11

Debido al rapido crecimiento de las redes lan wireless, la ieee decide desarrollar un protocolo el control de la capa de acceso al medio y la capa fisica con la denominacion 802.11



STATION(STA): Son las maquinas o hosts, las estaciones dentro del ESS pueden

comunicarse o moverse entre BSS's de manera transparente

ACCESS POINT(AP): Es un puente entre la red inalámbrica y la red cableada. Se encarga de realizar las conversiones de tramas

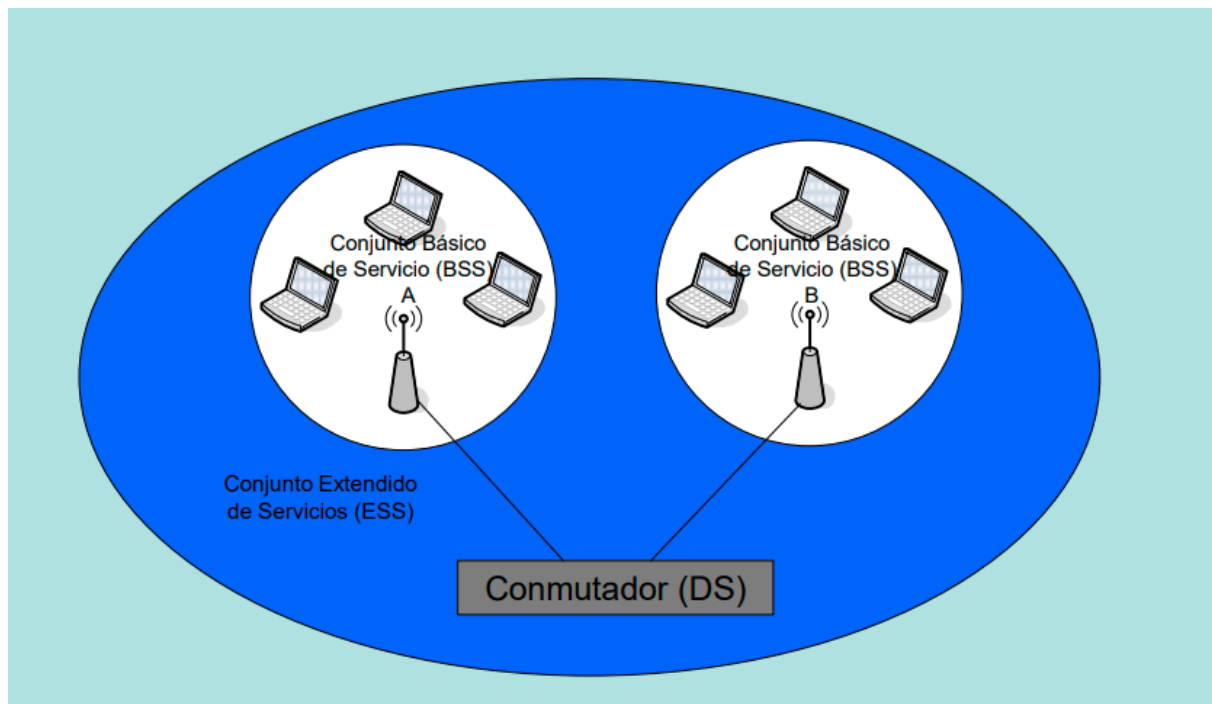
BASIC SERVICE SET (BSS): Bloque mínimo de una red inalámbrica, puede estar en

- modo infraestructura: las estaciones se comunican a traves del AP
- modo ad hoc: conexion entre 2 estaciones

EXTENDED SERVICE SET (ESS): Conjunto de uno o mas BSS, el identificador es el llamado SSID

DISTRIBUTION SYSTEM(DS): Mecanismo que se utiliza para controlar a que AP se envian las tramas, por ejemplo un conmutador/switch

PORTAL: Puente entre cable e inalambrico, es la integración lógica entre LAN's cableadas y 802.11



MEDIO FISICO

Existen 3 medios fisicos que pueden implementarse para la transmision de inalambrica:

1. INFRAROJO(IR): uso comun en hogares, unica celda
2. RADIO FRECUENCIA ESPECTRO EXPANDIDO: funciona en las bandas ISM(industrial, scientific y medical) no tienen licencias, varias celdas
3. MICROONDAS DE BANDA ESTRECHAS: puede funcionar con o sin licencia

INFRAROJO(IR)

La transmision opera en el espectro de la luz, utilizando la misma señal de frecuencias usada sobre enlaces de fibra optica. Son sistemas relativamente

simples de buena velocidad y de bajo costo, lo que los vuelve muy populares. Detectan solo la amplitud de la señal y por lo tanto reducen en gran parte la interferencia.

2 formas convencionales de configurarlas:

- Transmisión dirigida: En una sola dirección con un rango de dos km, puede ser utilizada al aire libre, ofrece el máximo ancho de banda
- Transmisión omnidireccional: en todas direcciones, esto reduce la cobertura a un área de 2 a 10 metros.

Aun así, el infrarojo presenta ciertas desventajas como interferencias de otras fuentes que pueden afectar sensiblemente a la red, compartir espectro con el sol y otras cosas como luces fluorescentes, y además que necesitan una línea de visión libre ya que no pueden atravesar objetos opacos

RADIO FRECUENCIA ESPECTRO EXPANDIDO(RF)

Emplea 2 tecnologías de espectro disperso:

- Espectro disperso con código de secuencia directa(DSSS)
- Espectro disperso con salto de frecuencia (FHSS)

La mayoría de productos para wireless LAN se desarrollan actualmente con FHSS

MICROONDAS(MW)

Los sistemas de microondas (MW) operan en la banda de los 5.8 GHz y en potencias menores a los 500 miliwatts, por regulaciones de la FCC.

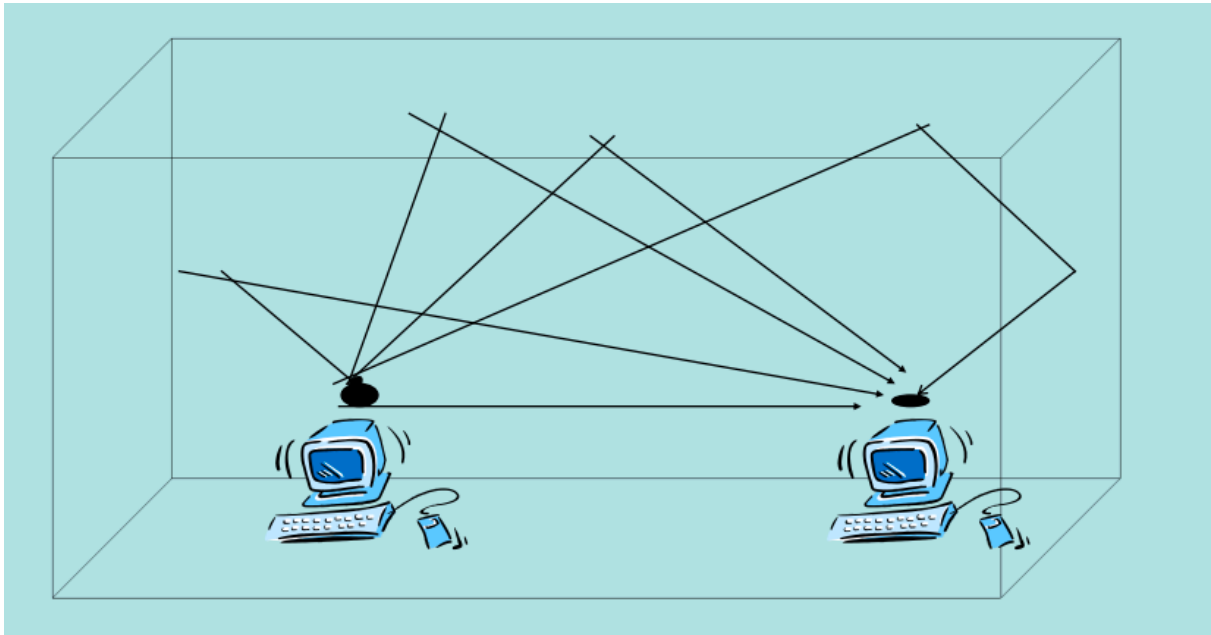
No se utiliza frecuentemente en el mercado. Emplean transmisión de banda angosta.

Su principal ventaja es su alto rendimiento (Throughput) debido a que su transmisión no involucra overhead.

TRAYECTORIA MÚLTIPLE(MULTIPATH)

Es la interferencia causada por el rebote de las señales en paredes y otros elementos que llegan al receptor en diferentes tiempos es llamada INTERFERENCIA POR TRAYECTORIAS MÚLTIPLES

Afecta todos los sistemas(IR, RF, MW), aunque el FHSS de RF lo soluciona inherentemente mediante un simple salto a otras frecuencias.



FRECUENCIAS FISICAS DEL WIRELESS

Capa Física

➤ Infrarrojo

1 y 2 Mbps funcionando con $\lambda = 850$ a 950 nm

➤ Espectro expandido de secuencia directa

1 y 2 Mbps funcionando en la banda de $2,4$ GHz

➤ Espectro expandido con salto en frecuencia

1 y 2 Mbps funcionando en la banda de $2,4$ GHz

➤ IEEE 802.11a

6 a 54 Mbps funcionando en la banda de 5 GHz

➤ IEEE 802.11b

5 ó 11 Mbps funcionando en la banda de $2,5$ GHz

CONTROL DE ACCESO AL MEDIO (IEEE 802.11)

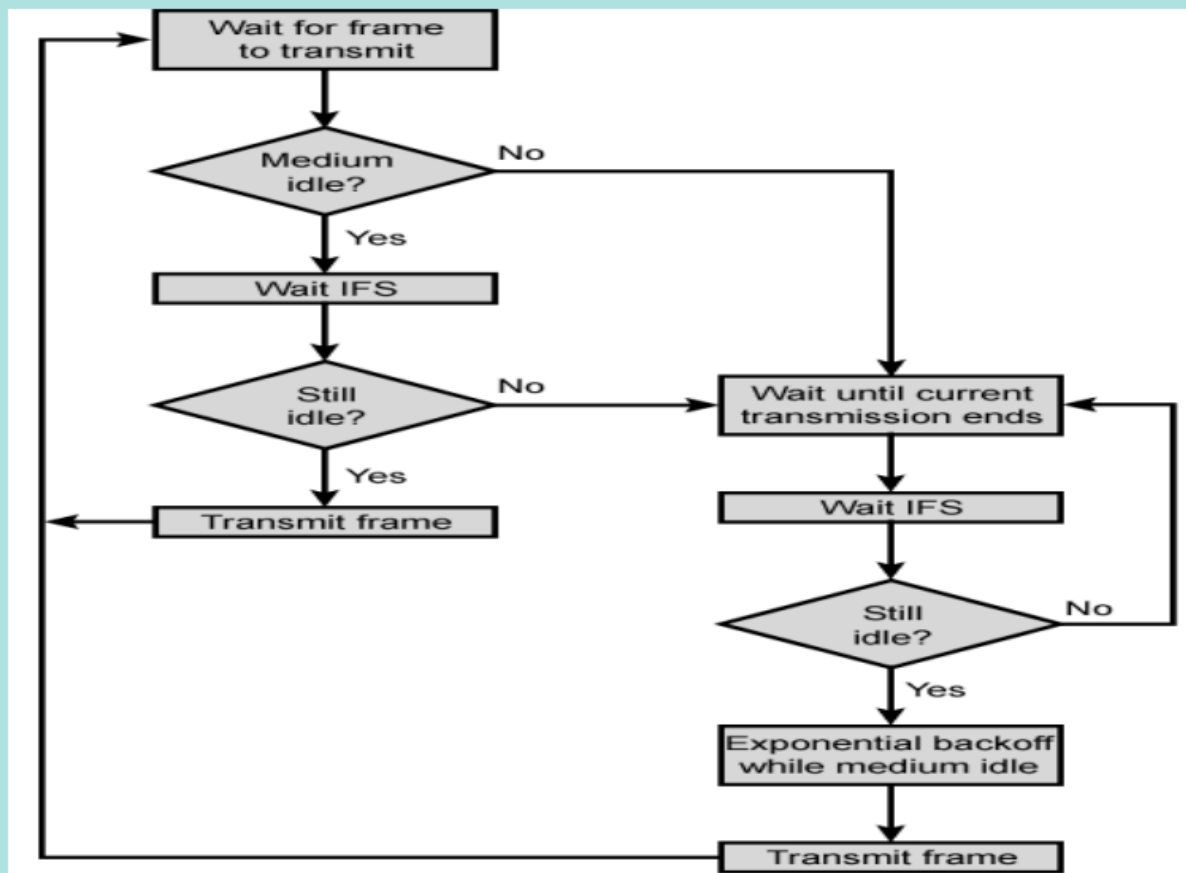
Existen 2 metodos:

Funcion de coordinacion distribuida(DCF): Utiliza el algoritmo CSMA/CA

Funcion de coordinacion puntual(PCF): Funciona en 2 periodos de tiempos, periodos con conflicto(CP) y periodos sin conflictos(CFP), durante el CP se utiliza el CSMA/CA y para los CFP el AP utiliza round robin para determinar que estacion transmite en cada momento.

PROTOCOLO CSMA/CA(CARRIER SENSE MULTIPLE ACCESS COLLISION AVOIDANCE)

Lógica de Control de Acceso al Medio



Antes de transmitir informacion una estacion debe testear el medio/canal inalambrico y verificar si esta libre o ocupado.

Si el medio esta libre se debe esperar un tiempo adicional llamado IFS(espaciado entre tramas)

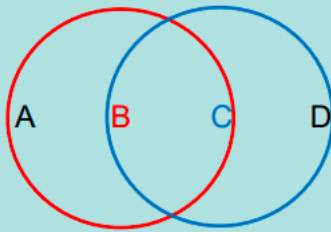
Si durante el IFS o bien desde el inicio el medio esta ocupado, debe esperar a que la transmision actual termine.

Una vez la transmision termina ejecuta el algoritmo BACKOFF dando una nueva espera aleatoria exponencial para reducir la posibilidad de colision

Durante la ejecucion del backoff se continua escuchando por al menos un IFS, cosa que si el medio se ocupa durante el tiempo de un IFS o superior el backoff queda suspendido hasta que termine y se repita la transmision y se repita el ciclo.

Problemas de CSMA/CA

Nodos ocultos: Una estación cree que el canal está libre, pero está ocupado por otra estación que no escucha



$A \rightarrow B$

$C \rightarrow B$

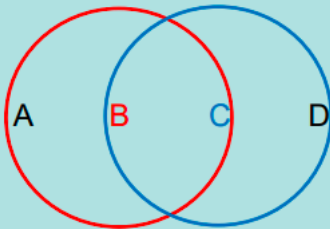
Si A y C desean comunicarse con B envían una trama

A no se da cuenta de lo que hace C

Para C ocurre lo mismo

Se produce colisión, pero a diferencia de ETH no se dan cuenta

Nodos Expuestos: Una estación cree que el canal está ocupado, pero está libre porque el nodo al que escucha no le interferiría para transmitir a otro destino



$B \rightarrow A$

B envía una trama a A

C sabe de esto porque escucha a B

Sería erróneo para C suponer que no puede transmitir ya que escucha a B

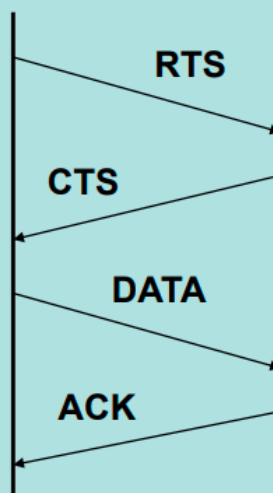
C puede transmitir a D

26

CSMA/CA

➤ Entrega Fiable de Datos

- Falta de fiabilidad por ruido, interferencias, etc.
- Protocolo de intercambio de 4 tramas (RTS, CTS, Datos y ACK). RTS y CTS se pueden deshabilitar



The 4-way Handshake

- El mensaje RTS contiene la dirección destino y la duración de la transmisión
- Las estaciones entonces conocen el tiempo que deben esperar antes de intentar transmitir
- El destino envía un mensaje corto llamado: CTS (Clear to Send)
- El mensaje CTS indica a la fuente que puede enviar la información sin que se presenten colisiones

ESTRUCTURA DE LOS FRAME 802.11

Frame	Duration	Address	Address	Address	Sequence	Address	Frame	FCS
Control	ID	1	2	3	Control	4	Body	
2	2	6	6	6	2	6	0-2312	4

La longitud de los campos es en bytes

dir 1;DESTINO

dir2;ORIGEN

dir3;AP

Cada trama consiste:

Encabezado MAC: El encabezado MAC consiste de 7 campos y es de 30 bytes de longitud, los campos son:

- Control de la Trama: El campo de control de frame es de 2 bytes de longitud y está a su vez formado de 11 sub-campos(LA LONGITUD DE CAMPOS ES EN BITS)

Protocol	Type	Subtype	To	From	More	Retry	Pwr	More	WEP	Order
Version			DS	DS	Frag		Mgt	Data		
2	2	4	1	1	1	1	1	1	1	1

- Duración/ID
- Dirección1, 2, 3
- Control de secuencia
- Dirección 4

Cuerpo del frame

Secuencia de verificación del frame (FCS)

TIPOS DE TRAMAS

Tramas de control, ej RTS, CTS

Tramas de datos, existen 8 tipos pero solo 4 transportan datos de las capas superiores

Tramas de gestion, utilizadas para gestionar las comunicaciones entre las estaciones y los puntos de acceso

SERVICIOS

Dependiendo que valor pongamos en los campos tipo y sub tipo del campo FRAME CONTROL, estamos especificando un tipo de servicio

Tipo / Subtipo	00 - Supervisión (management)	01 - Control	10 - Datos	11 - Extensión
0000	Association Request	reserved	Data	DMG - Beacon
0001	Association Response	reserved	Data +CF-Ack	reserved
0010	Reassociation Request	reserved	Data +CF-Poll	reserved
0011	Reassociation Response	reserved	Data +CF-Ack +CF-Poll	reserved
0100	Probe Request	Beamforming Report Poll	Null (no data)	reserved
0101	Probe Response	VHT NDP Announcement	CF-Ack (no data)	reserved
0110	Timing Advertisement	Control Frame Extension	CF-Poll (no data)	reserved
0111	Reserved	Control Wrapper	CF-Ack +CF-Poll (no data)	reserved
1000	Beacon	Block Ack Request (BlockAckReq)	QoS Data	reserved
1001	ATIM	Block Ack (BlockAck)	QoS Data +CF-Ack	reserved
1010	Disassociation	PS-Poll	QoS Data +CF-Poll	reserved
1011	Authentication	RTS	QoS Data +CF-Ack +CF-Poll	reserved
1100	Deauthentication	CTS	QoS Null (no data)	reserved
1101	Action	Ack	Reserved	reserved
1110	Action No Ack	CF-End	QoS CF-Poll (no data)	reserved
1111	Reserved	CF-End +CF-Ack	QoS CF-Ack +CF-Poll (no data)	reserved

SEGURIDAD

Wired Equivalent Privacy WEP (1999), en 2001 se descubrio vulnerabilidades

Wi-Fi Protected Access WPA, similar al wep pero con generacion de clave temporal, se descubrieron vulnerabilidades

WPA 2 2004, utiliza un algoritmo de encripcion mas robusto llamado AES, dando mas seguridad a la conexion entre cliente y access point.

RESUMEN VELOCIDADES

Protocolo	Frecuencia	Ancho del canal	Máxima tasa de datos
802.11ax	2.4 or 5GHz	20, 40, 80, 160MHz	2.4 Gbps
802.11ac wave2	5 GHz	20, 40, 80, 160MHz	1.73 Gbps
802.11ac wave1	5 GHz	20, 40, 80MHz	866.7 Mbps
802.11n	2.4 or 5 GHz	20, 40MHz	450 Mbps
802.11g	2.4 GHz	20 MHz	54 Mbps
802.11a	5 GHz	20 MHz	54 Mbps
802.11b	2.4 GHz	20 MHz	11 Mbps
Legacy 802.11	2.4 GHz	20 MHz	2 Mbps

3. CAPA DE RED

Encargada de proporcionar conectividad y que los datos lleguen desde el equipo origen hasta el destino

PRACTICA APRENDER DATAGRAMA IP

PARA SEPARAR CAMPOS CAPTURA DE RED

Internet Protocol IP

Es un servicio sin conexión y no confiable dado que la entrega no está garantizada. Los paquetes/datagramas son tratados de forma independiente de los demás, no hay circuitos vitales, estos se pueden perder, duplicar, retrasar, que el IP no informara de esto ni al receptor ni al emisor.

IP

Formato del Datagrama

0	4	8	16	20	24	31
VERS	HLEN	DSF (Ex TOS)	TOTAL LENGHT			
IDENTIFICACION			FLAG	FRAGMENT OFFSET		
TTL		PROTOCOLO	HEADER CHECKSUM			
SOURCE IP						
DESTINATION IP						
OPCIONES						
DATOS (UDP, TCP. ETC.)						

Arriba de los datos se llama HEADER, este esta formado minimamente por 5 palabras de 32 bits/4 bytes/ 8 hexa, este caso se llama cabeza sin opcion y en total son 20 bytes, si se agregan opciones sea agregarian nuevas palabras de 4 bytes hasta llenar las opciones necesarias.

CAMPOS

- **VERS:** Versión del IP. Suele ser 4 o 6 en binario.
- **HLEN:** Longitud del encabezado. Indica cuantas palabras de 32 bits habrá en el encabezado (normalmente hay un 5).
- **DSF (Ex TOS):** Campo de servicio diferenciado (Ex Tipo de servicio).
- **TOTAL LENGTH:** Longitud Total. Cantidad de Bytes (Cabecera + Datos), máxima $2^{16} = 64.000$ bytes.
- **IDENTIFICATION:** Identifica al datagrama IP. Es un número.
- **FLAG:** 3 bits. [x, y, z]
 - **X:** En cero (0)
 - **Y:** Uno mismo lo setea.
 - 1 → No fragmentar.
 - 0 → Se puede fragmentar.

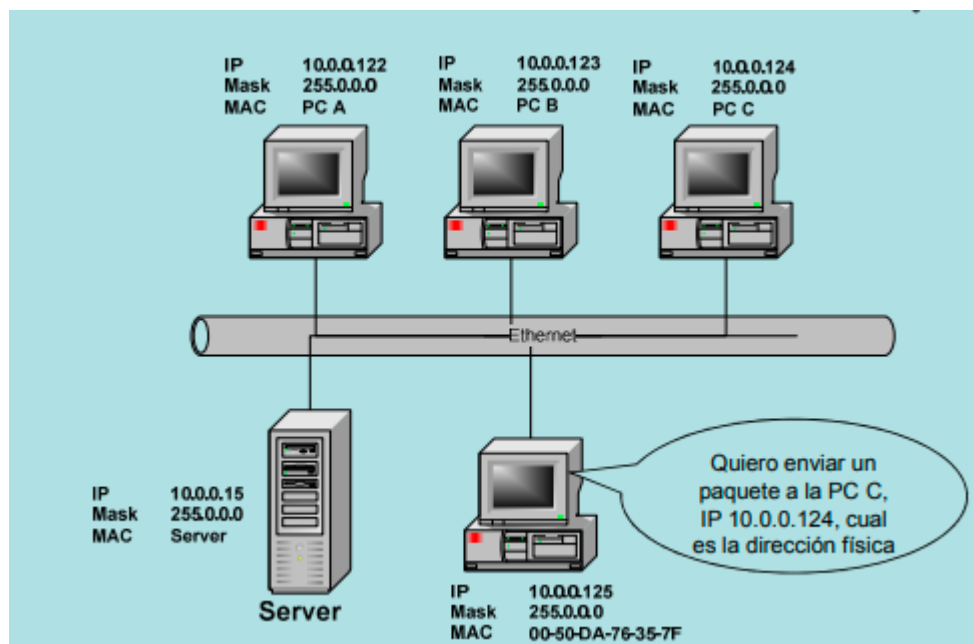
- **Z:** Más fragmentos. Es automático el seteo.
 - 1 → Hay más fragmentos.
 - 0 → Último o no hay más fragmentos
- **FRAGMENT OFFSET (Desplazamiento del Fragmento):**
 - Representa el Total Lenght. Mide palabras de 64 bits (8 bytes).
 - 13 bits.
- **TTL: Time To Live.**
 - 8 bits.
 - Es el tiempo de vida.
 - Paquete cuando está en 0 lo descarta ("muere").
 - Normalmente en 128.
 - Router lo va bajando de a 1.
- **PROTOCOLO:** 8 bits.
- **HEADER CHECKSUM:**
 - 16 bits.
 - Solo para el Header, no a los datos.
 - En cada Router se recalcula.
- **SOURCE IP:**
 - 32 bits.
 - Dirección de origen.
- **DESTINATION IP:**
 - 32 bits
- **OPCIONES:**

PRACTICA MTU CONSULTAR CUADERNO

PROTOCOLO ARP Adress Resolution Protocol

Este protocolo se encarga de relacionar direcciones fisicas(MAC) con logicas(IP)ra

El host busca en su tabla ARP la direccion fisica, si la encuentra construye el paquete, si no la encuentra envia un broadcast a la red local



PAQUETE ARP

0		8		16		24		31	
TIPO DE HARDWARE				TIPO DE PROTOCOLO					
HLEN		PLEN		OPERACION					
SENDER HA (octeto 0 - 3)									
SENDER HA (OCTETO 4 - 5)				SENDER IP (OCTETO 0 - 1)					
SENDER IP (OCTETO 2 - 3)				TARGET HA (OCTETO 0 - 1)					
TARGET HA (octeto 2 - 5)									
TARGET IP (octeto 0 - 3)									

CAMPOS ARP

- Tipo de Hardware: Indica el tipo de interfaz porejemplo, Ethernet el valor es 1.
- Tipo de Protocolo: Indica el protocolo utilizado, por ejemplo IP el valor es

0800 (hex).

- HLen y PLen: Estos campos permiten utilizar el paquete en distintos protocolos.

- Operation: A través de un código especifica las 4 operaciones:

Solicitud ARP=1

Respuesta ARP=2

Solicitud RARP=3

Respuesta RARP=4

- Sender HA: Dirección física (MAC) de la fuente.
- Sender IP: Dirección lógica (IP) de la fuente.
- Target HA: Dirección física (MAC) del destino.
- Target IP: Dirección lógica (IP) del destino.

PROTOCLO RARP Reverse Adress Resolution Protocol

La funcion de este protocolo es asignar direcciones IP a los hosts, por ej a aquellos que no tienen discos rigidos, existen protocolos mas modernos que brindan mas parametros de configuracion.

- BooTP (Bootstrap Protocol)
- DHCP (Dynamic Host Configuration Protocol)

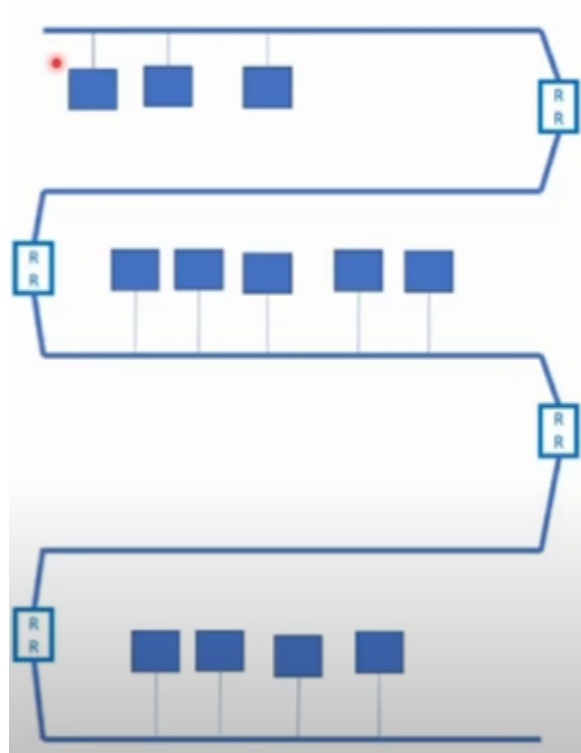
El protocolo DHCP tiene como funcion configurar de forma automatica ciertos tipos de parametros en los hosts como:

- Direccion IP
- Direccion de Default gateway
- Mascara
- IP de los DNS
- Nombre de dominio

Se configura un servidor que asigna direccion ip mediante 4 mensajes:

- DHCP DISCOVERY →
- DHCP OFFER←
- DHCP REQUEST→
- DHCP ACKNOWLEDGE←

TOPOLOGIAS DE 5-4-3



RED DE CABLE COAXIAL

5 cables coaxiales, 4 repetidores regenerativos, 3 segmentos con maquinas(los impares,1,3y5)

DIRECCIONES IPv4

Compuestas por un numero binario de 32 bits sepado en 4 octetos por puntos, la asignacion de direcciones las realiza la ICANN.

Se dividen en clases:

- CLASE A: El primer bit del primer octeto es 0(del 0 al 127) y son /8 pero 7 bits de red porque 1 es para indentificar
- CLASE B: Los primeros bits del primer octeto es 10(del 128 a 191) y son /16 pero 14 bits de red porque 2 son para indentificar
- CLASE C: Los primeros bits del primer octeto es 110(del 192 al 223) y son /24 pero 21 bits de red porque 3 son para indentificar

Las direcciones tambien pueden ser privadas o publicas

PRIVADAS:

10.0.0.0 A 10.255.255.255 /8

172.16.0.0 A 172.31.255.255 /16

192.168.0.0 a 192.168.255.255 /24

El resto fuera de ese rango son PUBLICAS, excepto el rango de las 127.0.0.0 a 127.255.255.255 que son direcciones especiales reservadas para el ambito local.

SUBNETTING

Utilizado para mejorar la distribucion de las direcciones IP, por eso se crearon dos tecnicas para separar las ip tomando prestados bits de los campos de los hosts de las mascara naturales para proporcionar una mayor cantidad de subredes y reducir el numero de hosts de cada una.

- V L S M (Variable Lengh Subnetting Mask) 255.255.255.0 donde en binario los 1 son red y 0 hosts
- C I D R (Classless Inter Domain Rounting) / barritas

N A T (Network Address Traslation)

Es un método que se utiliza para cambiar las direcciones IP de las conexiones Puede ser estático o dinámico

Se utiliza utiliza para ahorrar ahorrar direcciones direcciones IP's públicas

PRACTICA SUBNETTING CONSULTAR CUADERNO Y APRENER RANGOS, PUBLICAS, PRIVADAS

VLAN (VIRTUAL LOCAL AREA NETWORK)

Permite definir redes locales con computadores ubicadas en diferentes redes físicas

Permite la separación de dominios de broadcast

- Usar la regla "1 Vlan/1 subred IP", es decir, usar un enrutador para enrutar paquetes entre diferentes VLANs.

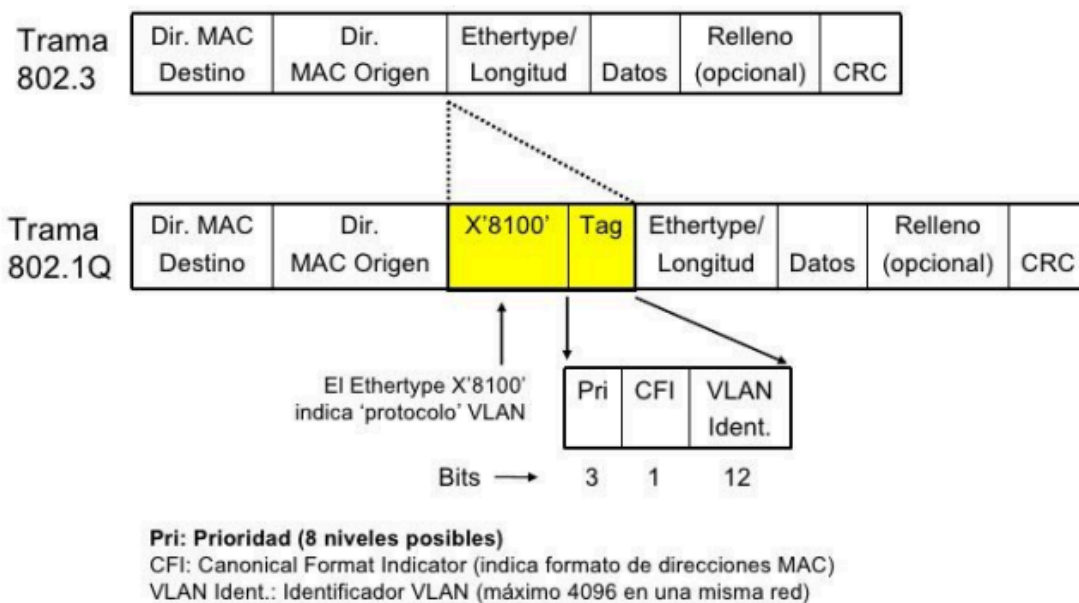
RAZONES PARA USAR VLANS

- Adaptación a diferentes estructuras organizacionales.
- Reducir la contención por el uso de la red.
- Permite balancear la carga de la red.
- Facilita agregar y cambiar de lugar las computadoras, reduciendo costos de administración.
- Ayuda a implantar políticas de seguridad.
- Permite reubicar servidores en lugares físicamente apropiados

Estándar 802.1q

Este protocolo interconecta VLANs entre varios switches, routers y servidores, proporcionando a su vez un mayor nivel de seguridad entre los segmentos de redes internas.

Se agrega una nueva etiqueta a la trama ethernet de 802.3 luego de la dirección MAC origen



802.1Q tag format

16 bits	3 bits	1 bit	12 bits
TPID	TCI		
	PCP	DEI	VID

Esta nueva etiqueta se divide en 2, un primer campo de 16 bits que indica el número 8100 en hexa que indica el protocolo vlan, y luego la etiqueta en sí que está compuesta por 3 bits que indican la prioridad, 1 que indica el formato de las direcciones mac y 12 bits para ID de la VLAN. (Permite 4095 VLANs individuales aunque algunos números ya están reservados)

Para implementar las VLAN debemos configurar los puertos de los switch de una manera específica, existen 2:

Access: La principal utilidad que se le da a este tipo de puertos es para conectar equipos finales, los puertos de acceso solo transportan tráfico de una sola vlan. Este tipo de puerto recibe las tramas ethernet y se encarga de agregar/quitar los encabezados 802.1Q para que la comunicación Host/Switch no tenga modificaciones

Trunk: La principal utilidad que se le da a este tipo de puertos es para realizar la conexión entre

switches, un puerto trunk puede transportar tráfico de múltiples vlans, por lo que, podemos tener múltiples vlans en los switches y solo un enlace para transportar todo el tráfico. Este tipo de puerto no retira los encabezados 802.1Q y es utilizado para comunicarse con el Router (configurado con subinterfaces) o interconectar más Switches .

COMO SE CONFIGURAN LAS VLAN

- 1.Introduzco la vlan a crear en la base de vlan con dos parametros 1.numero
2.nombre
- 2.Configuro en cada puerto el modo access o trunk y a que vlan pertenece

STP(SPANNING TREE PROTOCOL)

El objetivo de este protocolo es generar una topología lógica sin bucle a partir de una topología física con bucle. Esta topología sin bucle recibe el nombre de árbol. Este protocolo se conoce como las IEEE 802.1D

Por cada red se genera un spanning tree que contiene lo siguiente:

- Un switch raíz por red
- Todos los puertos del switch raíz son designados
- Un puerto raíz por switch no raíz
- Un puerto designado por segmento
- Puertos sin utilizar, no designados

Los puertos raíz y los puertos designados se utilizan para enviar (F) tráfico de datos.

Los puertos no designados descartan el tráfico de datos. Estos puertos se denominan puertos de bloqueo (B) o de descarte.

El switch raíz(el que comanda la red) tiene todos sus puertos designados mientras que los switch no raíz tendran puertos raíz para comunicarse con otros switches, puertos designados para comunicarse con hosts, y puertos bloqueados para evitar bucles.

No obstante el spanning tree realiza un scaneo periodico de la red, descubriendo caidas en conexiones, si esto sucede reevalua la red, y en caso de ser necesario abre los puertos bloqueados y vuelve asignar los puertos o switch raices para que no se corte la comunicacion ni haya bucles.

El switch raíz se elige por prioridad, la cual puede ser definida manualmente o sino es el número de mac address más bajo.