- Control de acceso
- MAC
- Control de Flujo
- Control de Acceso al Medio (MAC)
  - Aloha
  - csma/ca
  - csma/cd
- Colisiones
- Slot Time
- HUBS
- Ethernet Full Duplex
- Control de Flujo Ethernet
- Tipos de Direcciones
  - unicast
  - broadcast
  - multicast
- Bridge vs LAN Switch
- VLAN
  - definición dominio de broadcast
  - definición vlan
  - Trunking
- Conmutadores
  - Gestionables
  - No gestionables
- Ethernet vs Internet
- Cables
  - Tipos
    - U/UTP
    - F/UTP
    - S/UTP

Protocolo ARP(Address Resolution Protocol)

DEFINICIÓN

El protocolo ARP fue creado para obtener la dirección MAC destino, sabiendo la dirección IP que tiene asignada dicha máquina. ARP consta de dos tipos de ARP: request (Interrogación) y reply (respuesta).

Es el encargado de traducir las direcciones IP de 3 bits a las correspondientes direcciones físicas(MAC)

El protocolo ARP está definido en la RFC 826

El proceso de traducir la dirección IP en una dirección de hardware se lo denomina “Resolución de direcciones”

FORMATO DE PETICIÓN ARP

Encabezado				Mensaje ARP
Encabezado MAC		Encabezado IP		
MAC Destino	MAC Origen	IP Destino	IP Origen	¿Cual es tu dirección MAC?
FF:FF:FF:FF:FF:FF	01:00:D1:B5:D4:F1	200.59.4.5	200.59.4.1	

RESPUESTA ARP

Encabezado				Mensaje ARP
Encabezado MAC		Encabezado IP		
MAC Destino	MAC Origen	IP Destino	IP Origen	¿Cual es tu dirección MAC?
01:00:D1:B5:D4:F1	F1:01:E1:B5:F4:14	200.59.4.1	200.59.4.5	

Protocolo RARP(Reverse Address Resolution Protocol)

DEFINICIÓN

El protocolo RARP se utiliza cuando un computador conoce su dirección MAC pero desconoce su dirección IP

El protocolo ARP está definido en la RFC 903

Requiere uno o más hosts de servidores de la red para mantener una base de datos de correspondencias entre direcciones hardware y direcciones de protocolo así que serán capaces de responder a peticiones de hosts de clientes

FORMATO DE PETICIÓN RARP

Encabezado				Mensaje RARP
Encabezado MAC		Encabezado IP		
MAC Destino	MAC Origen	IP Destino	IP Origen	¿Cual es mi dirección IP?
FF:FF:FF:FF:FF:FF	F1:01:E1:B5:F4:14	200.59.4.255		

RESPUESTA RARP

Encabezado				Mensaje RARP
Encabezado MAC		Encabezado IP		
MAC Destino	MAC Origen	IP Destino	IP Origen	¿Cual es tu dirección IP?
F1:01:E1:B5:F4:14	01:00:D3:B5:D3:F1	200.59.4.1	200.59.4.50	

Multidifusión

DEFINICIÓN

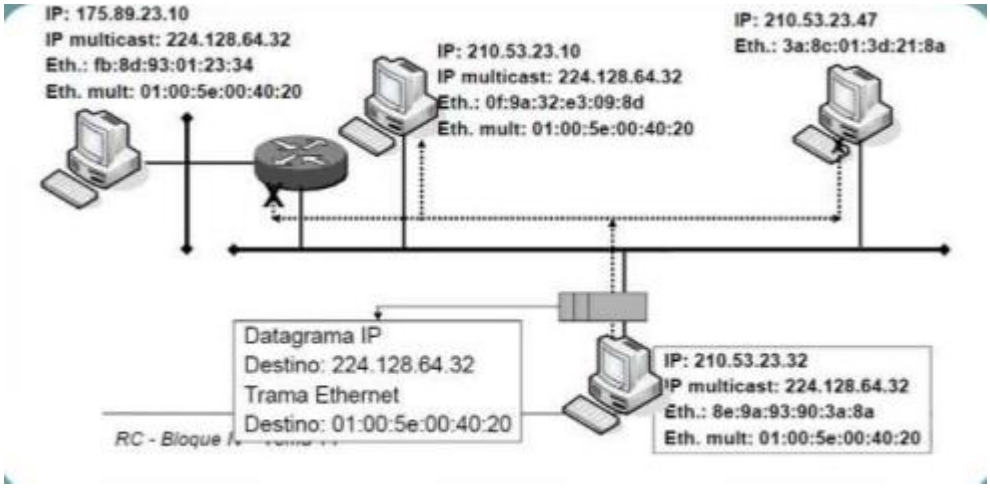
Es el envío de la info en una red de compus a múltiples destinos simultáneamente, usando la estrategia más inteligente para el envío de los mensajes sobre cada enlace de la red solo una vez y creando copias cuando los enlaces en los destinos se dividen
Proporciona:

- Envío de datagramas a destinos múltiples
- Solicitud de servidores por parte de clientes

MULTICAST

Las direcciones Ethernet constan de 48 bits y se denotan como : 0a:53:1f:84:82:0d
El rango 01:00:5e:00:00:00 - 01:00:5e:7f:ff:ff está reservado para las direcciones Ethernet multicast, creando un espacio de direcciones de 23 bits

IGMP (INTERNET GROUP MANAGEMENT PROTOCOL)



Protocolo DHCP(host Dinámico)

DEFINICIÓN

HCP significa Protocolo de configuración de host dinámico . Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma dinámica (es decir, sin intervención particular). Sólo tiene que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo principal es simplificar la administración de la red.

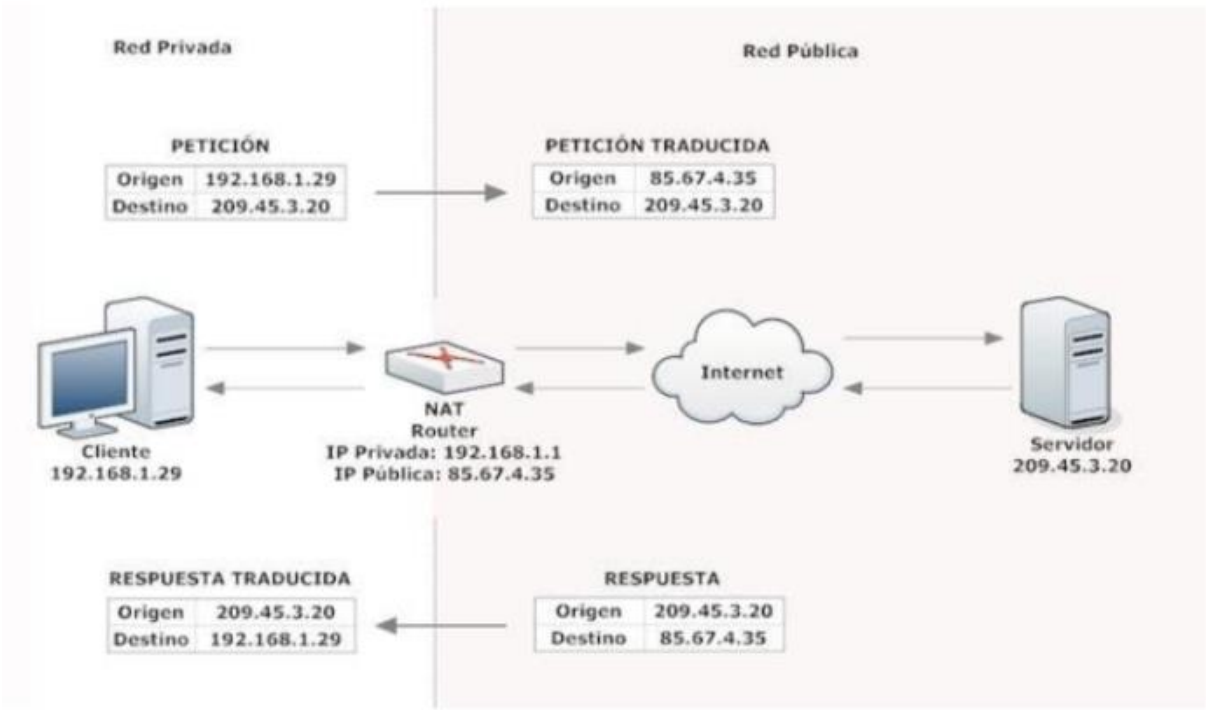
NAT

DEFINICIÓN

La conversión de direcciones de red o NAT se desarrolló para resolver la falta de direcciones IP con el protocolo IPv4

Por lo tanto, el principio de NAT consiste en utilizar una conexión a Internet, que tenga al menos una interfaz de red conectada a la red interna y al menos una interfaz de red conectada a Internet (con una dirección IP enrutable) para poder conectar todos los equipos a la red.

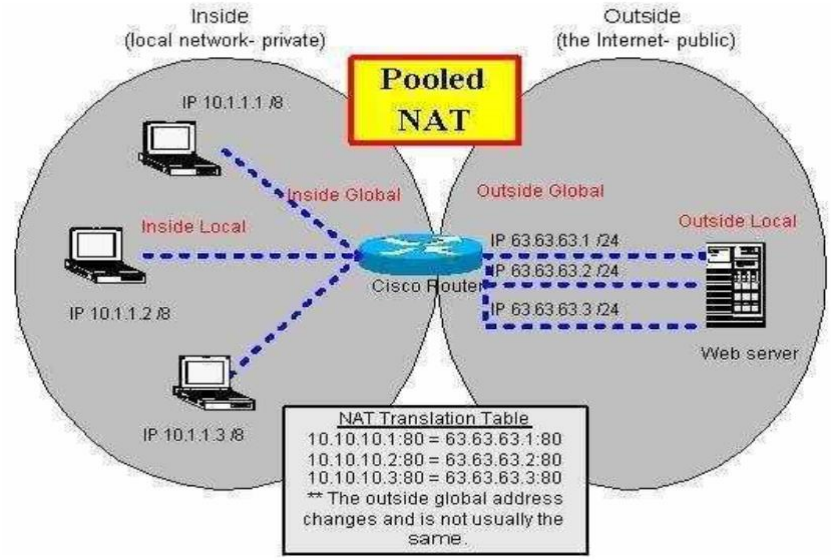
Sale una sola dirección IP



PAT

DEFINICIÓN

El principal inconveniente de NAT, es que por cada host que requiere acceso a Internet en forma concurrente, se necesita una dirección global Salen múltiples direcciones ip.



DNS

DEFINICIÓN

Son las iniciales de Domain Name System (sistema de nombres de dominio) y es una tecnología basada en una base de datos que sirve para resolver nombres en las redes, es decir, para conocer la dirección IP de la máquina donde está alojado el dominio al que queremos acceder. Por lo tanto, el DNS es un sistema que sirve para traducir los nombres en la red, y está compuesto por tres partes con funciones bien diferenciadas.

Cliente DNS: está instalado en el cliente (es decir, nosotros) y realiza peticiones de resolución de nombres a los servidores DNS.
Servidor DNS: son los que contestan las peticiones y resuelven los nombres mediante un sistema estructurado en árbol. Las direcciones DNS que ponemos en la configuración de la conexión, son las direcciones de los Servidores DNS.
Zonas de autoridad (TLD): son servidores o grupos de ellos que tienen asignados resolver un conjunto de dominios determinado (como los .es o los .org)

HTTP

DEFINICIÓN

HTTP son las siglas en inglés de HiperText Transfer Protocol (en español, protocolo de transferencia de hipertexto). Es un protocolo de red (un protocolo se puede definir como un conjunto de reglas a seguir) para publicar páginas de web o HTML.

UPS

Fijarse en el material :D

Clases

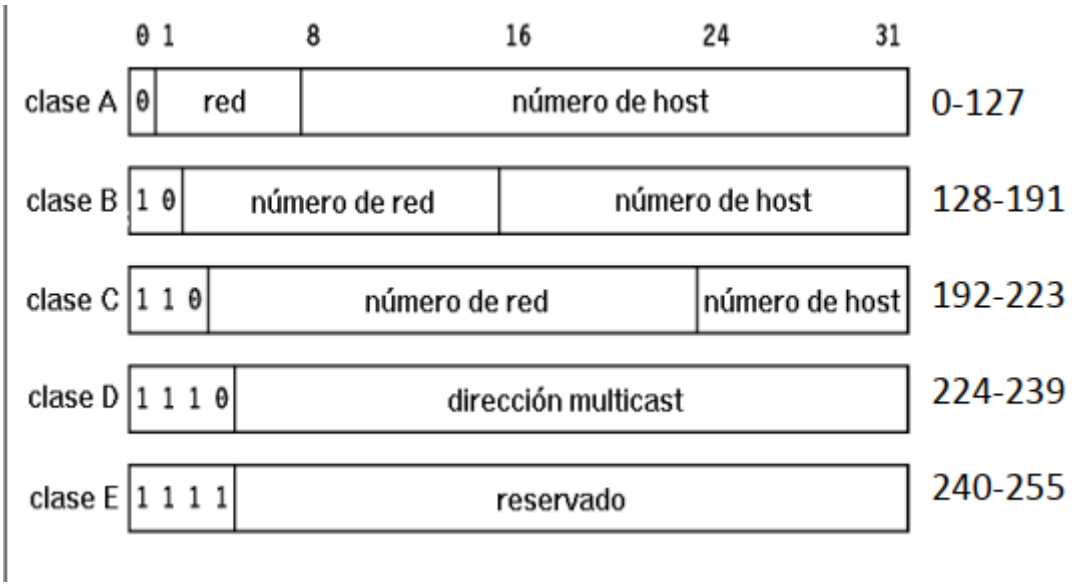
Clase A	Red	Host		
Octet	1	2	3	4

Clase B	Red		Host	
Octet	1	2	3	4

Clase C	Red			Host
Octet	1	2	3	4

Clase D	Host			
Octet	1	2	3	4

Las direcciones Clase D se utilizan para grupos de multicast. No hay necesidad de asignar octetos o bits a las distintas direcciones de red o de host. Las direcciones Clase E se reservan para fines de investigación solamente.



Máscara de subnet

Direcciones privadas, reservadas y públicas

CLASE	RANGO	REDES	Hosts por red
A	10.0.0.0 a 10.255.255.255	1	16.777.214
B	172.16.0.0 a 172.31.255.255	16	65534
C	192.168.0.0 a 192.168.255.255	256	254

Direcciones Loopback

El dispositivo de red loopback es una interfaz de red virtual. Las direcciones del rango '127.0.0.0/8' son direcciones de loopback, de la cual la que se utiliza de forma mayoritaria es la 127.0.0.1, por ser la primera de dicho rango.
Es una dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos. La dirección de loopback crea un método de acceso directo para las aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí. Al utilizar la dirección de loopback en lugar de la dirección host IPv4 asignada, dos servicios en el mismo host pueden desviar las capas inferiores del stack de TCP/IP. También es posible hacer ping a la dirección de loopback para probar la configuración de TCP/IP en el host local

Direcciones de Red

Las direcciones de Red son útiles para tomar decisiones de ruteo. No son válidas para asignar a hosts. Se obtienen con ciertas combinaciones de dirección y máscara de subred. Una dirección de red trivial termina con bits en cero en la parte que identifica a los hosts (10.0.0.0), sin embargo, es posible utilizar una dirección no terminada en ceros.

Direcciones de Broadcast

Una dirección de broadcast es útil para enviar mensajes a todas las estaciones que pertenecen a la misma red o subred. Cada red o subred tiene su propia dirección de broadcast y análogamente a las direcciones de red, existen direcciones de broadcast que terminan en 1s en la parte que identifica hosts (10.255.255.255).
Una vez más es posible combinar una dirección IP con ina máscara adecuada para convertirla en una dirección de broadcast aunque no termine en 1s.

Framing

Significa definir la estructura de los campos de los frames o tramas.
Todos los dispositivos que participan en una red deben conocer el formato de los frames para poder enviar o recibir información

Control de acceso

Es la lógica que permite compartir un medio de transmisión. De esta forma, múltiples dispositivos pueden acceder a un bus compartido , o al mismo canal de transmisión/recepción de datos.
La topología lógica de la red es determinada por el mecanismo de control de acceso al medio (media access control).
Ethernet >> BUS
FDDI >> Anillo

MAC

La dirección MAC (siglas en inglés de media access control; en español “control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, es única para cada dispositivo. Está determinada y configurada por el IEEE y el fabricante (los primeros 24 bits) utilizando el organizationally unique identifier. La mayoría de los protocolos que trabajan en la capa 2 del modelo OSI usan una de las tres numeraciones manejadas por el IEEE: MAC-48, EUI-48, y EUI-64, las cuales han sido diseñadas para ser identificadores globalmente únicos.

Control de Flujo

Los mecanismos de control de flujo permiten administrar la velocidad de transmisión de estaciones remotas. No todas las estaciones tienen las mismas características de performance y utilización por lo que es necesario contar con un mecanismo de control de flujo.
La IEEE ha subdividido la capa de enlace en dos subcapas:
LLC (Logical Link Control)
MAC (Media Access Control)
LLC: Permite múltiple comunicaciones por un mismo medio (IEEE 802.2)
MAC: administra los protocolos de acceso al medio
Los protocolos que utilizan MAC son :
Ethernet

Token Ring
FDDI

Control de Acceso al Medio (MAC)

ALOHA

Cuando el emisor quiere transmitir una trama, simplemente la emite. No se preocupa por si el canal está libre. Una vez transmitido se pone a la escucha esperando recibir confirmación de que la información ha sido recibida correctamente por el destinatario (CRC). Si la confirmación no llega en un tiempo razonable preestablecido, el emisor supone que ha ocurrido un error y retransmite.

CSMA/CA

Carrier sense multiple access/ Collision Avoidance, se basa en evitar las colisiones en lugar de detectarlas, generando una señal de reserva de canal. Si la reserva es exitosa , se asume que la portadora está disponible. Este es el mecanismo de acceso principal de las redes LAN Wireless (IEEE802.11). Es half duplex

CSMA/CD

Las estaciones antes de transmitir, deberían detectar si el canal ya estaba en uso (es decir si había portadora), en cuyo caso esperarían a que la estación activa cesara de transmitir. Además cada estación, mientras transmitiera, estaría continuamente monitoreando el medio físico por si producía alguna colisión, en cuyo caso pararía y transmitiría más tarde. CSMA/CD es un mecanismo de acceso al medio de tipo probabilístico. Esto significa que, bajo condiciones aprobadas, existe una probabilidad muy alta de que una estación determinada pueda transmitir, sin embargo , físicamente es posible utilizar una configuración estrella , como se observa en la actualidad con el protocolo Ethernet. Es half duplex

Colisiones

La colisión se detecta al comparar lo que se transmite con lo que se recibe, cuando no coinciden ambas señales .
Al detectar la colisión ambos dispositivos cesan de transmitir, enviando una señal llamada jamming, que sirve para indicar a los demás que no interpreten lo transmitido como datos válidos. Y que esperen un tiempo aleatorio antes de volver a transmitir.
La primera vez intentarán volver a transmitir aleatoriamente dentro de un intervalo de tiempo. Si al volver a intentarlo una colisión ocurre nuevamente, entonces repiten el mismo proceso, pero el tiempo aleatorio que esperarán será el doble que el anterior.

Minimizando la posibilidad de que ambas estaciones vuelvan a colisionar. Si volviera a ocurrir una colisión, el intervalo volverá a duplicarse.
El proceso se puede repetir hasta 16 veces como máximo. Si un dispositivo agota las 16 posibilidades, el protocolo especifica que se debe desistir y reportar a las capas superiores q

Slot Time

Speed	Slot time[3]	Time Interval	Distancia Recorrida (aprox)
10 Mbit/s	512 bit times	51.2 microseconds	15400 metros
100 Mbit/s	512 bit times	5.12 microseconds	1540 metros
1 Gbit/s[4]	4096 bit times	4.096 microseconds	1200 metros

HUBS

Los Hubs permiten tener varios puertos Ethernet y “expandir” Ethernet
Hay dos tipos de hubs
– Hubs Repetidores
– Hubs de conmutación de paquetes (switches)
Todos los repetidores y los segmentos en una LAN Ethernet deben cumplir con las restricciones de Round Trip Timing
Cada puerto de un switch opera como una LAN Ethernet diferente (las restricciones de Round Trip Timing se terminan en el puerto del switch)
Los repetidores permiten tener una LAN Ethernet con varias docenas de estaciones. Los switches permiten enlazar un amplio número de la LAN’s Ethernet siendo capaz de soportar miles de estaciones.

Ethernet Full Duplex

• En full duplex el dispositivo puede envíar y recibir datos simultáneamente (en teoría ofrece el doble de ancho de banda).
• En full duplex:
– No se comparte el segmento físico: sólo se interconectan dos dispositivos.
– Las dos estaciones deben ser capaces y estar configuradas para trabajar en full duplex.
– El medio debe tener trayectorias independientes para transmitir y recibir datos que operen de manera simultánea (no se utiliza CSMA/CD, aunque se respeta el IFG)
• 10BaseT, 10Base-FL, 100BaseTX, 100BaseFX, 1000Base-SX, 1000Base-LX, 1000Base-CX y 1000Base-T pueden usar full duplex
• En fibra óptica, los enlaces full duplex pueden ser más largos que en half duplex.

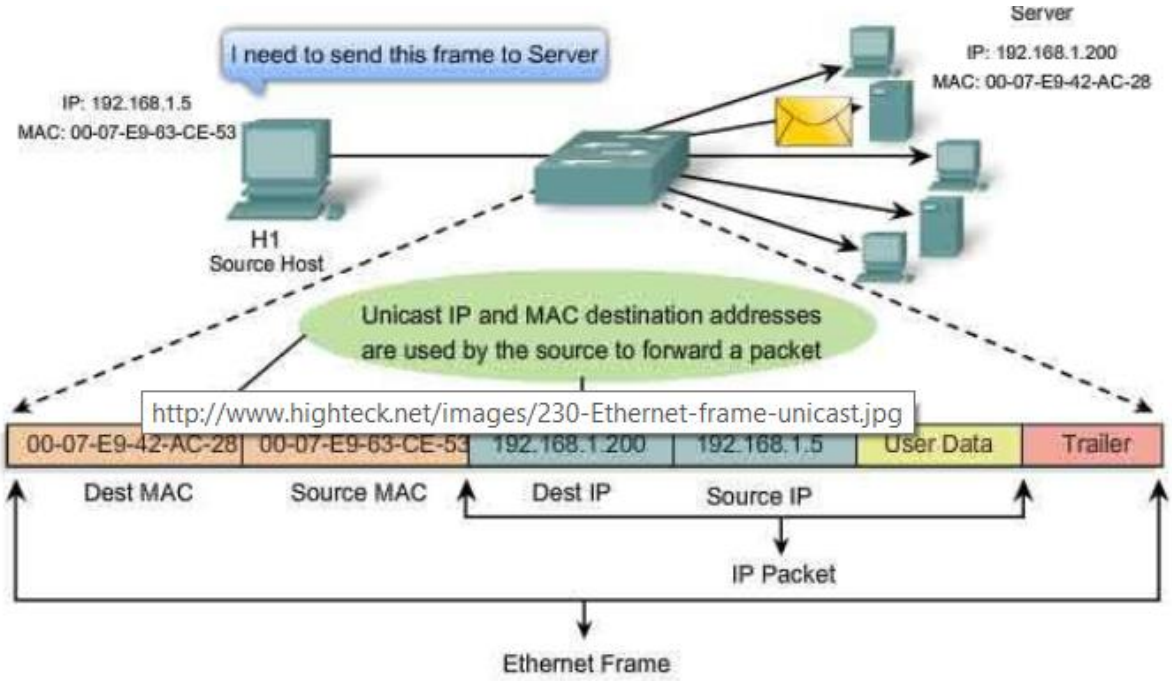
• ¡No existen repetidores full duplex!
• Full duplex se utiliza para enlaces entre switches o entre switch y servidor. Se puede utilizar también en un enlace a un equipo de un usuario.
• Debe asegurarse que las dos estaciones estén configuradas para full duplex. Si una estación está full duplex y la otra half duplex se pueden presentar problemas de colisiones tardias.
• Cuando un segmento físico utiliza full duplex, el protocolo CSMA/CD queda deshabilitado y las restricciones de RTT desaparecen permitiendo utilizar mayores longitudes en los cables de F.O. Por ejemplo en 100Base-FX, que está limitado a 412 m en half duplex puede llegar hasta 2 Km en full duplex. En fibra monomodo puede llegar a los 20 Km.
• El aumento de longitud del cable en full duplex NO aplica para cable de cobre

Control de Flujo Ethernet

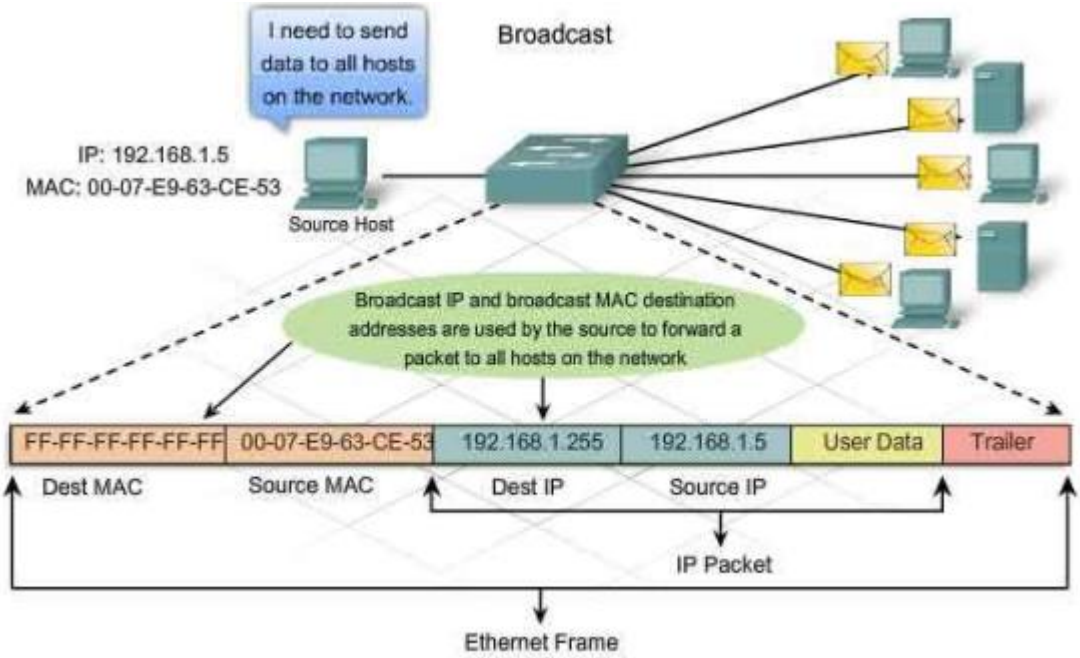
• Full duplex exige un mecanismo de control de flujo entre las estaciones (una estación puede enviar una mayor cantidad de datos que lo que la otra puede guardar en el buffer de su interface de red)
• El suplemento 802.3x (ethernet full duplex), de marzo de 1997, incluye una especificación de un mecanismo de control de acceso al medio (MAC) opcional que permite, entre otras cosas, enviar un mensaje para control del flujo llamado PAUSE.
• Los frames de control MAC se identifican porque el valor de tipo es 0x8808.
• Estos frames tienen códigos de operación (opcodes) en el campo de datos. El tamaño de estos frames se fija al mínimo establecido en el estándar (es decir 46 bytes de carga útil).
• El opcode está en los dos primeros bytes del campo de datos.

Tipos de Direcciones

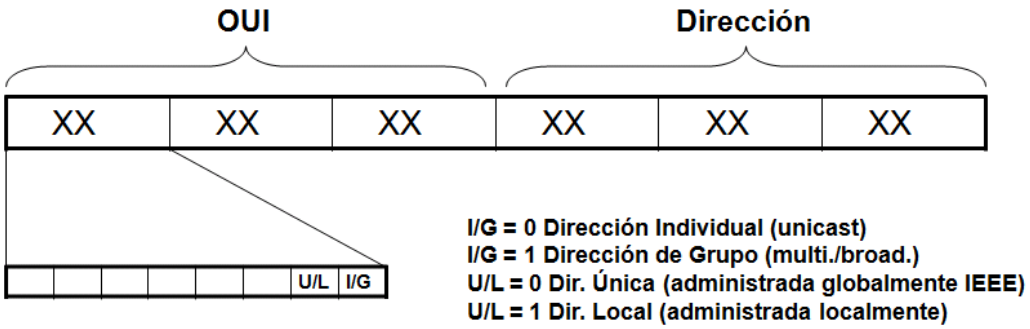
UNICAST



BROADCAST



Direcciones multicast en Ethernet:

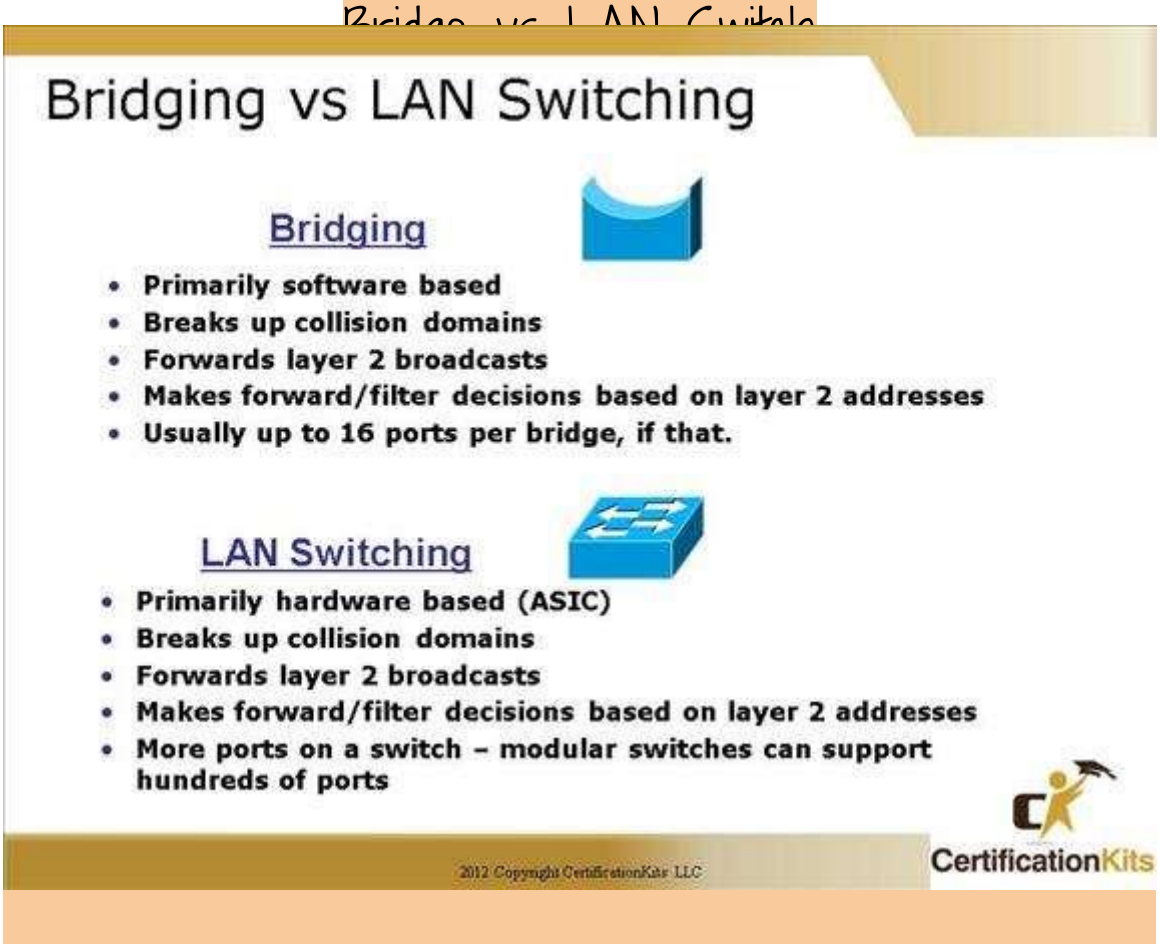


- En Ethernet los bits dentro de cada byte se representan en orden inverso. Por tanto el bit I/G es el último del primer byte.
- Regla:

  En Ethernet una dirección es multicast si y solo si el segundo dígito hexadecimal es impar.

  Ej.: la dirección AB-00-03-00-00-00 es multicast.

Bridge vs LAN Switch



VLAN

DEFINICIÓN DOMINIO DE BROADCAST

Es el conjunto de enlaces por los cuales se propagará un broadcast. Estos normalmente terminan en dispositivos de capa 3, definiendo a los routers como frontera de los dominios de broadcast. La comunicación entre estaciones ubicadas en distintos dominios de broadcast es mediante router

DEFINICIÓN VLAN

Una VLAN (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física.
Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, limitaciones de dirección, etc.), ya que se define una segmentación lógica basada en el agrupamiento de equipos según determinados criterios (direcciones MAC, números de puertos, protocolo,

etc.)

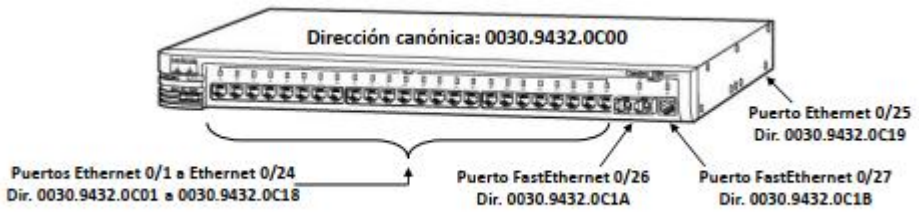
TRUNKING

Un trunk es un puerto que permite la comunicación entre dos dispositivos sin mezclar la información de las Vlans transportadas. Los puertos en modo trunk pueden multiplexar todas las Vlans sobre un solo enlace físico.

Conmutadores

GESTIONABLES

• Los conmutadores gestionables tienen una dirección MAC asociada a cada puerto, más una dirección asociada al equipo en su conjunto que llamamos dirección 'canónica'. Todas ellas son globalmente únicas y normalmente consecutivas.
• Cuando un conmutador quiere asociar el envío de una trama al puerto por el que la manda utiliza la dirección MAC del puerto. Si el envío no se quiere asociar a ningún puerto en particular se utiliza la dirección MAC canónica.
• Las direcciones MAC del conmutador no aparecen nunca en las tramas reenviadas por éste, solo en las propias



NO GESTIONABLES

Ethernet vs Internet

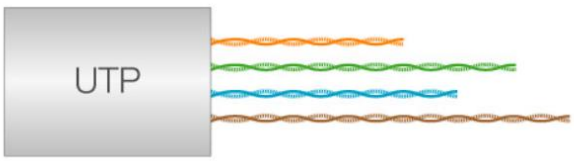
Característica	Ethernet	Wi-Fi
Velocidad	Hasta 1 Gbps	Hasta 870 Mbps en el nuevo estándar
Canal compartido	No	Si
Interferencia	Casi nula	Múltiple
Distancia	Permite abarcar varios kilómetros	Si nos alejamos del punto de acceso perdemos conexión
Half-duplex	Sí	No
Estándar actual	802.3	802.11n
Transferencia	A través de cable UTP cat 5 o 6	A través de señales inalámbricas
Instalación	Compleja	Sencilla

Cables

TIPOS

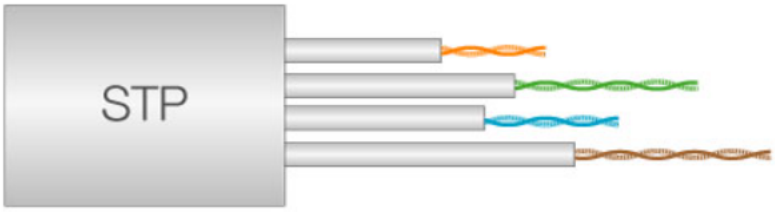
U/UTP

Es un par trenzado no blindado



F/UTP

En este caso, cada par va recubierto por una malla conductora que actúa de pantalla frente a interferencias y ruido eléctrico. Su impedancia es de 150 Ohm. El nivel de protección del STP ante perturbaciones externas es mayor al ofrecido por UTP. Sin embargo es más costoso y requiere más tiempo de instalación. La pantalla del STP para que sea más eficaz requiere una configuración de interconexión con tierra (dotada de continuidad hasta el terminal), con el STP se suele utilizar conectores RJ49. Es utilizado generalmente en las instalaciones de procesos de datos por su capacidad y sus buenas características contra las radiaciones electromagnéticas, pero el inconveniente es que es un cable robusto, caro y difícil de instalar.



S/UTP

Es un par trenzado blindado, que sí posee un recubrimiento aislante para proteger la transmisión de potenciales interferencias. Entre sus usos se cuentan las redes informáticas Ethernet y Token Ring y cabe mencionar que su precio es superior al de los UTP;