

Redes de computadores

Resúmenes de la Asignatura

Ángel Manuel Gamaza Domínguez

Grado en Ingeniería Informática 2012-2013

Busca tu residencia o piso de estudiantes en Uniplaces



Uniplaces

Este libro se ha realizado utilizando material correspondiente a la bibliografía y transparencias de la asignatura Redes de Computadores del Grado en Ingeniería Informática de la Universidad de Cádiz.

Mi aportación solo consiste en resumir y resolver dicho material para ayudar en la consecución de la asignatura.

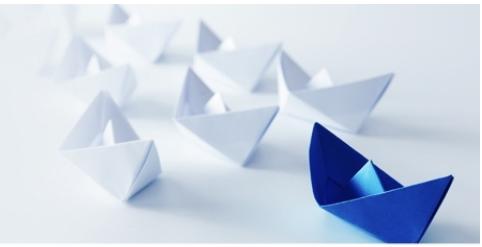
Ángel Manuel Gamaza Domínguez.



INESEM
BUSINESS SCHOOL

Escuela de líderes

Becas | Prácticas | Empleo



Máster en Ciberseguridad



Ángel M. Gamaza

Índice

Resúmenes de teoría	7
Tema 1	7
Tema 2 Parte 1	15
Tema 2 Parte 2	25
Tema 2 Parte 3	35
Tema 3 Parte 1	43
Tema 3 Parte 2	49
Tema 4 Parte 1	55
Tema 4 Parte 2	65
Tema 4 Parte 3	73
Tema 5	81
Tema 6	89
Tabla de direcciones IP	99
Puntos clave prácticas	101
Puntos clave práctica 1	101
Puntos clave práctica 3	102
Puntos clave prácticas 5,6,7,8,9 y 10	103

Tema 1

Arquitectura de Protocolos

Tipos de redes

LAN (Local Area Network)

Extensión limitada a un edificio. Administrada por una sola organización.

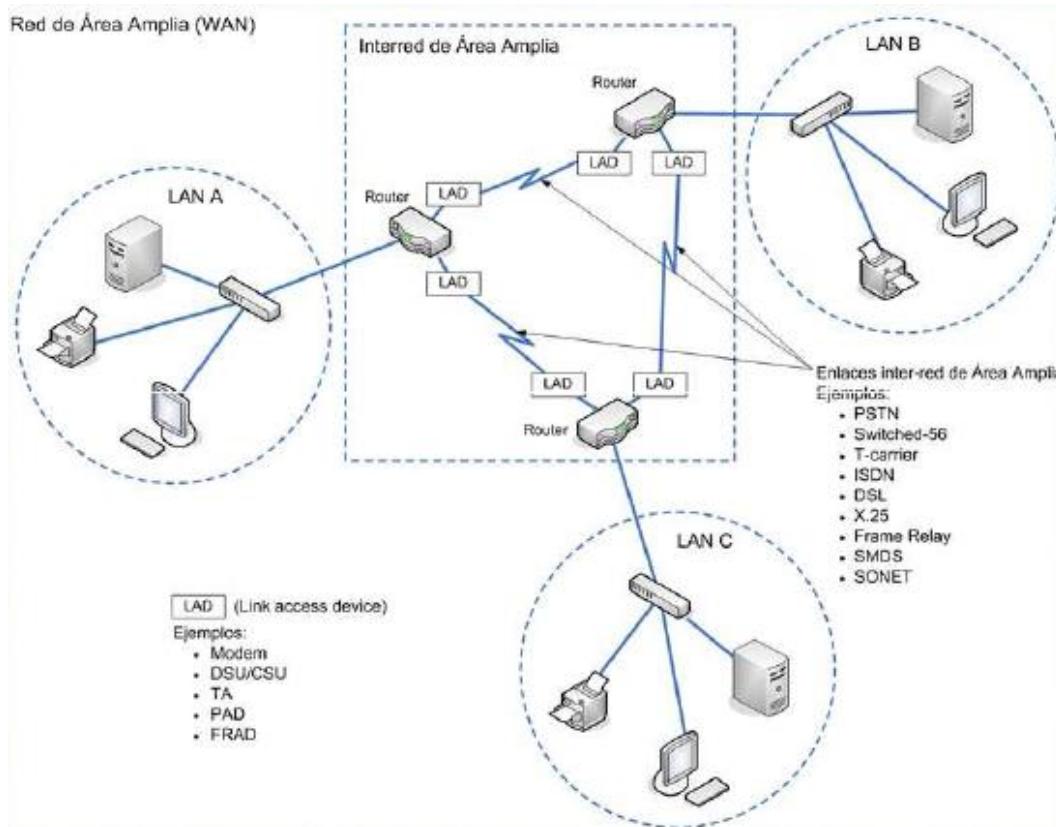
Ejemplo: una casa.

WAN (Wide Area Network)

Área geográfica extensa, como por ejemplo un país. Administrada por Proveedores de Servicio de Telecomunicaciones. Ejemplo: ONO, Telefónica...

MAN (Metropolitan Area Networking)

Un núcleo urbano. Administrada por una sola organización. Ejemplo: Ayuntamiento de Cádiz.





Ángel M. Gamaza

Tipos de dispositivos

Dispositivos finales o hosts

Equipos conectados a la red de comunicaciones que interaccionan con los usuarios: computadoras, impresoras de red, teléfonos VoIP, cámaras de seguridad, dispositivos móviles, etc.

Alojan programas de aplicación: servidor de correo, cliente de correo, etc. Estos programas de aplicación proporcionan servicios o utilizan servicios.

Cada host se identifica con una dirección.

Dispositivos intermediarios o de electrónica de red

Equipos que proporcionan conectividad: hubs, switches, puntos de acceso inalámbricos, routers, módems...

Algunos de estos dispositivos también se identifican con una dirección.

Medio físico

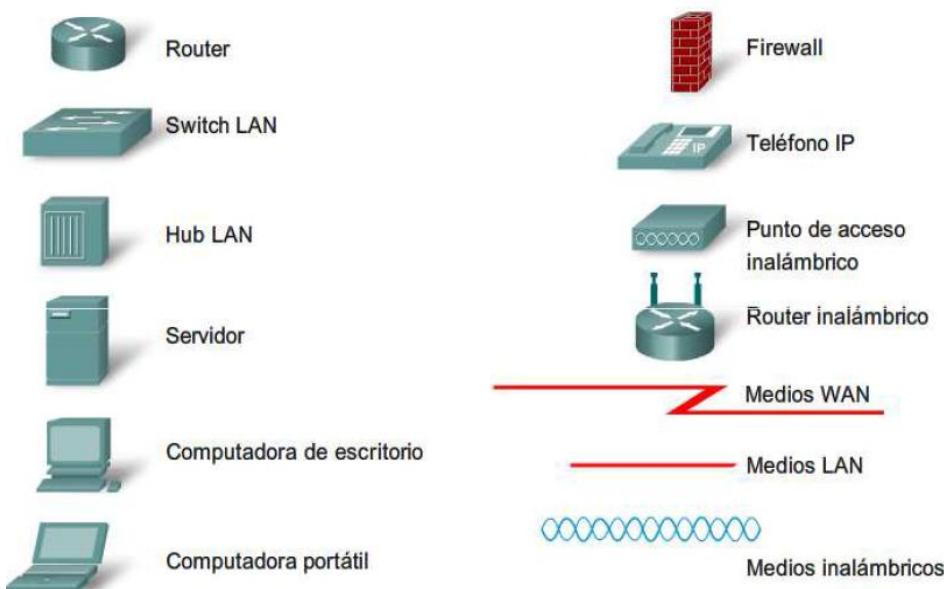
Canal: por el que se transporta información.

Tipos: cable coaxial, fibra óptica...

Cada tipo de medio tiene sus ventajas y desventajas. Factores:

1. Distancia máxima soportada por el medio físico.
2. Ambiente en el cual se instalará el medio físico.
3. Velocidad a la que se deben transmitir los datos.
4. Coste del material y su instalación.

Simbología



Modelo OSI (Open Systems Interconnection)

Diseñado por ISO (International Organization for Standardization) en 1984.

Considerado como una herramienta para enseñar y describir cómo opera una red. Es un modelo teórico.

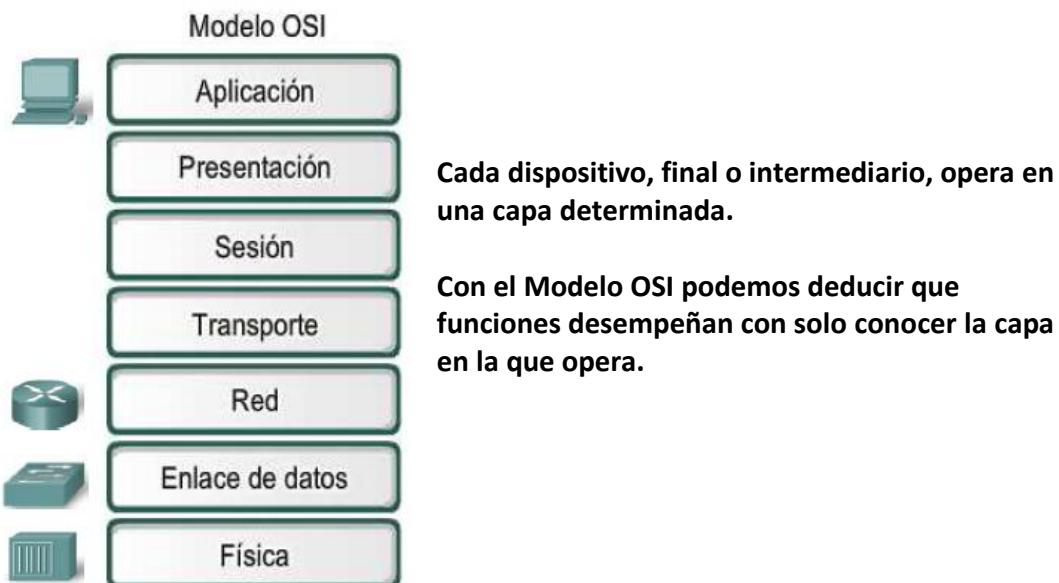
Divide el proceso de comunicación en 7 capas o niveles. Cada capa se encarga de ejecutar una parte del proceso.

Ayuda a entender el complejo funcionamiento de las comunicaciones.

-Describe las funciones que se realizan en cada capa.

-Describe las interacciones entre capas adyacentes.

Proporciona independencia entre capas, es decir, los cambios que se produzcan en una capa NO afectarán a otras capas.



Encapsulación

PDU (Unidad de datos del Protocolo)

La PDU de una capa es la sección de datos más el encabezado (Información de control agregada en cada capa):

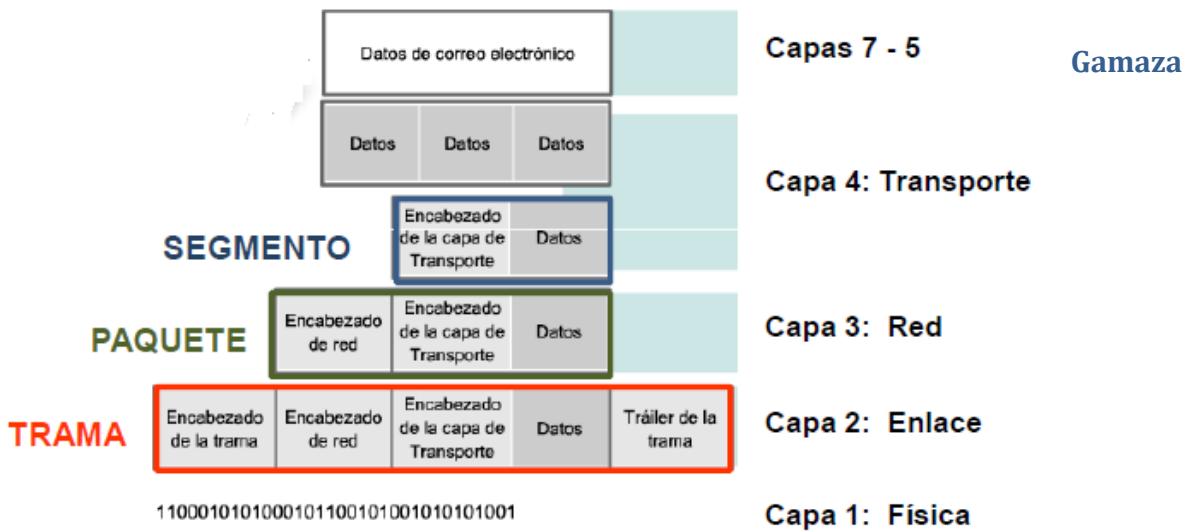
-**Datos**: término general que se utiliza en la capa de aplicación para la PDU.

-**Segmento**: PDU de la capa de transporte.

-**Paquete**: PDU de la capa de red.

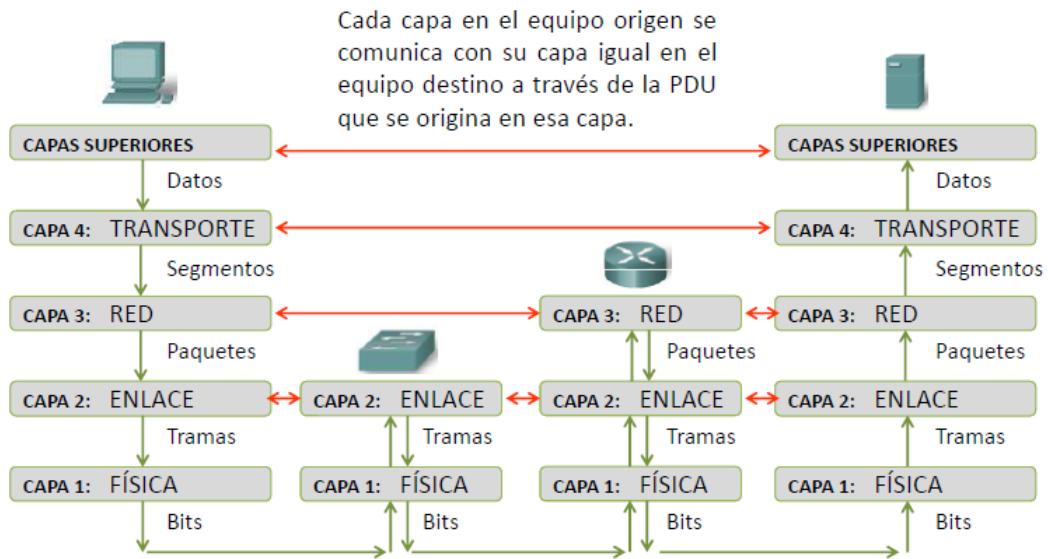
-**Trama**: PDU de la capa de enlace.

-**Bits**: PDU de la capa física.



Proceso de encapsulación

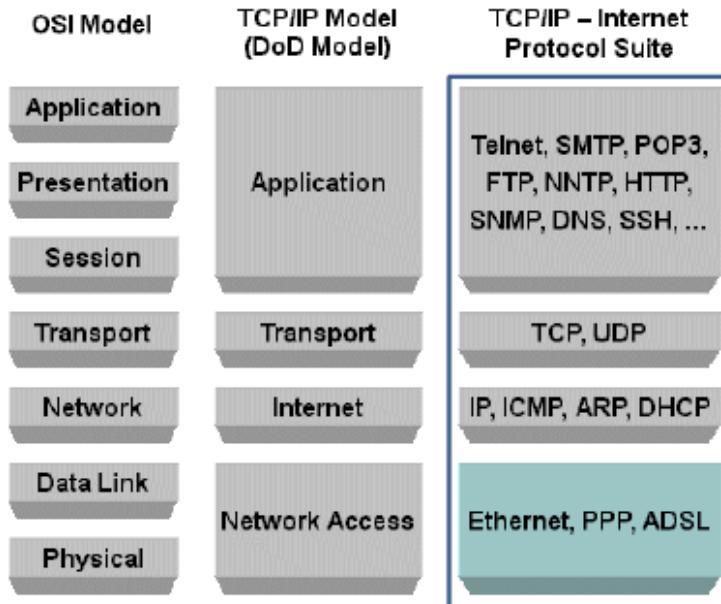
1. El mensaje se crea en la capa de aplicación del host origen.
2. La capa de aplicación entrega el mensaje a la capa de transporte.
3. En la capa de transporte (capa 4) el mensaje se divide en fragmentos. A cada fragmento se le añade un encabezado de capa 4 (**Encapsulación**). El fragmento más el encabezado de capa 4 constituye el **SEGMENTO** que es la PDU de esta capa.
4. La capa de transporte envía los segmentos a la capa de red.
5. La capa de red (capa 3) añade a cada segmento un encabezado de capa 3. El segmento más el encabezado de capa 3 constituye el **PAQUETE** que es la PDU de esta capa.
6. La capa de red envía los paquetes a la capa de enlace.
7. La capa de enlace (capa 2) añade a cada paquete un encabezado de capa 2 y una cola, también llamada tráiler. El paquete más el encabezado de capa 2 más la cola constituye la **TRAMA** que es la PDU de esta capa.
8. La capa de enlace envía las tramas a la capa física.
9. La capa física envía los bits de las tramas al medio físico. Hay que tener en cuenta que las tramas en el medio pueden pasar por **equipos intermedios** (administran los datos para poder llevarlos del origen al destino a través de la dirección IP destino del host y otros procesos que permiten seleccionar la mejor ruta para generar la comunicación)
10. Cuando los datos llegan al host destino se realiza el proceso inverso: se recorren las capas en orden ascendente y se desencapsulan las PDUs.
11. Finalmente, en la capa de transporte se unen los diferentes segmentos para componer el mensaje original y entregarlo a la capa de aplicación.



Modelo TCP/IP o Modelo de Internet

Nació a principio de los 70.

Conjunto o pila de protocolos que sigue un modelo en capas, aunque no se adapta exactamente al modelo OSI.





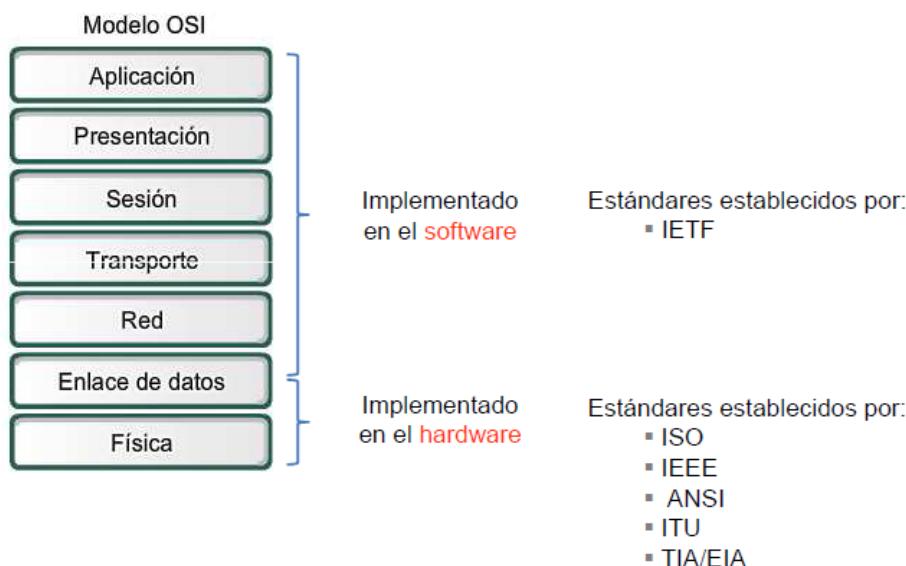
Ángel M. Gamaza

- No es un modelo teórico como el modelo OSI, es un modelo práctico. Hoy en día la mayoría de las máquinas utilizan este modelo.
- En cada una de las capas TCP/IP trabajan distintos protocolos. TCP e IP son dos de los protocolos más conocidos del modelo.
- Las definiciones de estos protocolos se recogen en un conjunto de documentos disponibles al público. Estos documentos se denominan Solicitudes de Comentarios (RFC).

Estandarización

Protocolo: descripción formal de un conjunto de reglas y convenciones que rigen parte del proceso de comunicación.

Estándar: es un protocolo que ha sido avalado por la industria de networking y ratificado por una organización de estándares, como IEEE (Institute of Electrical and Electronics Engineers). El uso de estándares en el desarrollo e implementación de protocolos asegura que los productos de diferentes fabricantes puedan funcionar conjuntamente.



Direccionamiento

Existen varios tipos de identificadores que deben incluirse en los encabezados de las PDUs para que el mensaje llegue satisfactoriamente al host destino.

- CAPA 4: TRANSPORTE** → Incluye en el encabezado del segmento los **puertos** de origen y destino
- CAPA 3: RED** → Incluye en el encabezado del paquete las **direcciones lógicas** de origen y destino
- CAPA 2: ENLACE** → Incluye en el encabezado de la trama las **direcciones físicas** de origen y destino

Direccionamiento físico

La dirección física opera en la capa 2 del modelo OSI. Cada dispositivo de capa 2 tiene una dirección física única que lo identifica. En la tecnología de red Ethernet la dirección física se denomina dirección de Control de Acceso al Medio (MAC).

Características de la MAC:

- Tiene 48 bits: A3-47-1C-30-F1-49
- Los 24 bits más significativos son asignados por IEEE e identifican el fabricante.
- Los 24 bits menos significativos identifican el dispositivo dentro del fabricante.
- Se graba en el hardware del dispositivo durante su fabricación.
- IEEE espera que el espacio MAC-48 no se acabe antes del año 2100.

Direccionamiento lógico

La dirección lógica opera en la capa 3 del modelo OSI. Las direcciones lógicas se han diseñado principalmente para enviar datos a equipos que están en otras redes. Es fundamental cuando la información traspasa los límites de la red local.

Si el protocolo que se utiliza en la capa 3 es IP entonces la dirección lógica se denomina dirección IP.

La dirección IP tiene 32 bits distribuidos en 4 números de 8 bits:

192.168.1.6
11000000.0101000.00000001.00000110

La dirección IP tiene dos partes:

- NET ID:** identifica la red en la que está ubicado el host.
- HOST ID:** identifica el host dentro de esa red.

Si en la red se han definido subredes entonces se puede considerar que la dirección IP tiene tres partes:

- NET ID**: identifica la red en la que está ubicado el host.
- SUBNET ID**: identifica la subred en la que está ubicado el host.
- HOST ID**: identifica el host dentro de esa subred.

Como se observa la dirección IP tiene una estructura jerárquica.

Para distinguir qué parte de la IP identifica la red-subred y qué parte identifica el host se utiliza la máscara.

La máscara es similar a una IP: tiene 32 bits distribuidos en 4 números de 8 bits.

La diferencia es que una máscara tiene que seguir esta estructura: los '1' tienen que estar juntos y situados en la parte más significativa, los '0' tienen que estar juntos y situados en la parte menos significativa.

Algunos ejemplos:

255.255.0.0
11111111.11111111.00000000.00000000
255.192.0.0
11111111.11000000.00000000.00000000

Puertos

Los hosts, ya sean clientes o servidores, pueden ejecutar múltiples aplicaciones de red simultáneamente, cada cual, constituye un proceso.

Es necesario identificar cada proceso de red con un número. A este número se le llama puerto y tiene 16 bits (por tanto hay 65535 puertos).

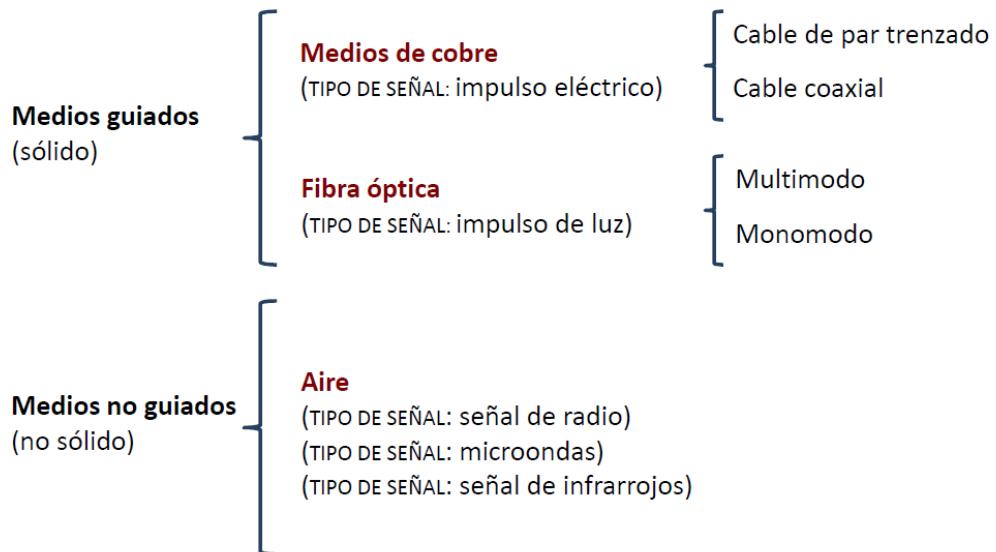
Cuando los datos se reciben en el host destino, se examina el número de puerto para determinar qué aplicación o proceso es el destino correcto de los datos.

Clasificación creada por IANA:

- Puertos bien conocidos**: son los puertos inferiores al 1024. Están reservados para los "protocolos bien conocidos" como por ejemplo HTTP (servidor Web), POP3/SMTP (servidor de correo) y Telnet.
- Puertos registrados**: los comprendidos entre 1024 y 49151. Pueden ser usados por cualquier aplicación.
- Puertos dinámicos o privados**: los comprendidos entre los números 49152 y 65535. Normalmente se asignan de forma dinámica a las aplicaciones clientes.

Tema 2

Capa Física 1ª Parte: Tipos de medios



Medios de cobre

Cable de par trenzado:

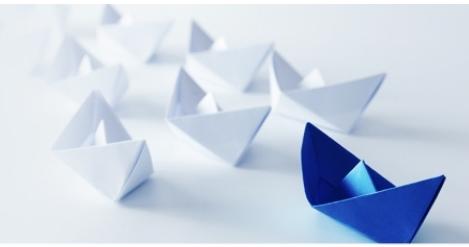
-Cable UTP: 4 pares de hilos de cobre recubiertos por plástico. Conector RJ-45. Distancia máxima 100 m.

-Cable S/FTP: 4 pares de hilos de cobre y un cable de drenaje (masa). Recubrimiento general de cobre y recubrimiento particular de aluminio. Conectores GG45 y TERA. El cable de drenaje debe estar correctamente conectado a tierra, sino podría actuar como antena en vez de como blindaje.

-Cable SF/UTP: Recubrimiento general tanto de cobre como de aluminio. No existe recubrimiento particular. Conectores GG45 y Tera.

La norma EIA/TIA-568A clasifica los cables de par trenzado en categorías, basándose en la frecuencia máxima soportada.

Mayor frecuencia → Mayor velocidad de transmisión



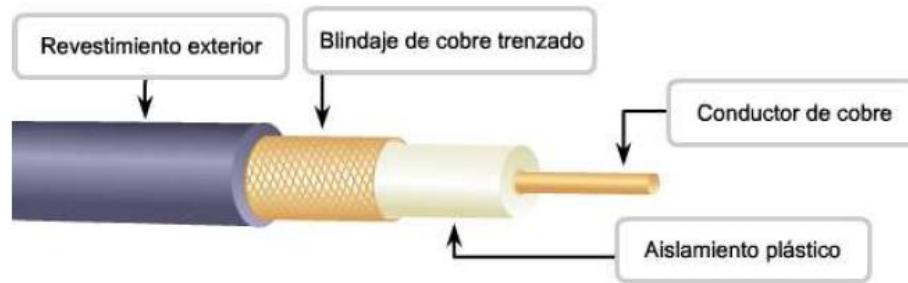
Ángel M. Gamaza

Tipos de cables según terminaciones

Tipo de cable	Terminaciones	Aplicación
Directo	Ambos extremos 568A o ambos extremos 568B	Conectar dos equipos de distinto tipo p.e. PC - Switch
Cruzado	Un extremo 568A y el otro extremo 568B	Conectar dos equipos de igual tipo p.e. Switch - Switch
Transpuesto	Un extremo p.e. 568A y el otro extremo orden de hilos inverso (patentado por Cisco)	Conectar PC al puerto de consola de un switch o router

Excepción: Una conexión PC-Router utiliza cable cruzado

Cable coaxial



El aislamiento es flexible, y el blindaje actúa como conductor interno.

Conectores:



Antiguas conexiones a internet.



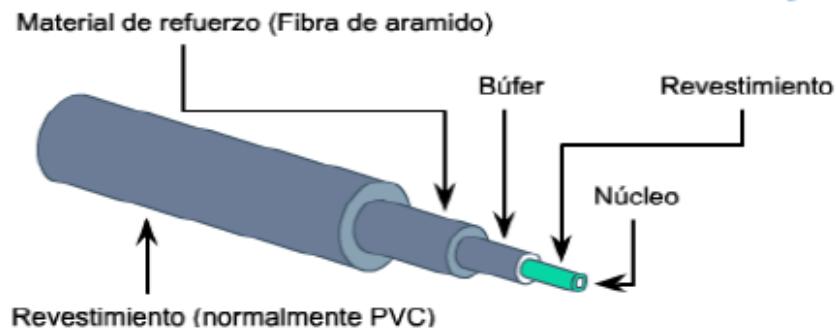
Televisión por cable.

Distancia máxima 500 m.

Utilizado para transportar señales de radiofrecuencia elevadas mediante cableado, especialmente señales de televisión por cable (CATV). La conexión final hacia la ubicación del cliente y el cableado dentro de sus instalaciones aún sigue siendo cable coaxial (HFC -Híbrida de Fibra y Coaxial-).

Fibra óptica

El núcleo es de fibra de vidrio de sílice. El primer revestimiento se encarga de evitar la pérdida de luz. Las demás capas son de refuerzo. La fibra óptica se basa en la reflexión total de la luz.



Conectores ST, SC y LC.

Su fuente de emisión es un láser o LED y su detector es un fotodiodo, que transforma impulsos de luz en voltajes.

Los cables se designan con 2 números separados por una barra, el primero indica el diámetro del núcleo y el segundo el del revestimiento (En μm).

Se requieren dos fibras para realizar una operación full dúplex ya que la luz sólo puede viajar en una dirección a través de un hilo de fibra óptica.

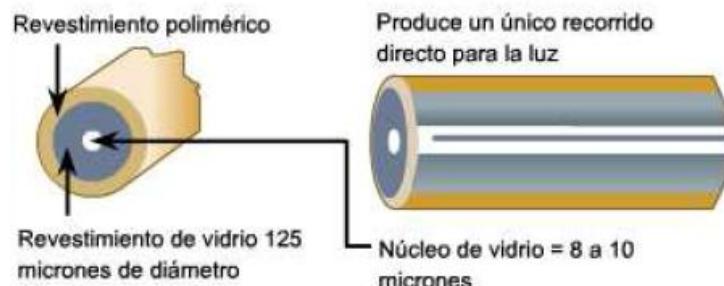
Para que un cable de fibra óptica no tenga pérdidas, se debe cumplir:

- El ángulo de incidencia del haz de luz debe ser mayor que el ángulo crítico.
- El índice de refracción (densidad óptica) del núcleo debe ser mayor que el del revestimiento.

Al curvar demasiado un cable se podrían provocar pérdidas, debido a que el ángulo podría cambiar.

Tipos de fibra óptica

-Monomodo: Un único haz unidireccional, la luz circula por un único camino. Núcleo muy pequeño. Permite largas distancias de transmisión. Fuente de luz: láser.





Conejor Suscriptor (SC)

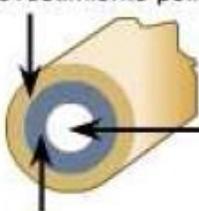


Conejor Lucent (LC)

a

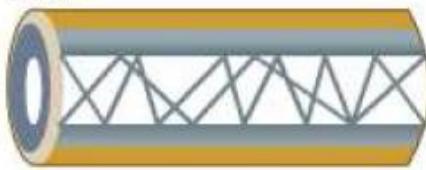
-**Multimodo:** Varios haces de luz, multidireccional. El núcleo tiene muchos caminos (modos) por donde circulan los haces de luz y es mayor que el monomodo. Fuente de luz: LED (Su luz no es unidireccional). Usado en cortas distancias debido a la dispersión modal (Los haces tienen distintos ángulos de incidencia por lo que no llegarán a la vez al receptor).

Revestimiento polimérico



Revestimiento de vidrio 125
micrones de diámetro

Permite recorridos múltiples para
la luz



Núcleo de vidrio = 50/62.5 10
micrones



Conejor ST

El conector de punta recta (ST) es ampliamente
usado con la fibra multimodo



Conejor Lucent (LC)



Conejor Lucent (LC) duplex

Identificación monomodo/multimodo:

El color de la cubierta exterior suele utilizarse para identificar el tipo de cable. El estándar TIA-598C sugiere que la cubierta exterior sea **amarilla** para la fibra **monomodo**, y **naranja** para la fibra **multimodo**. El método más fiable es leer las especificaciones del cable impresas en la cubierta.

-Monomodo es más caro, por lo que no conviene para largas distancias.

-Multimodo es más barato, por lo que se suele usar en distancias cortas.

Cableado Submarino

Los cables submarinos de fibra óptica han posibilitado la transmisión de señales digitales portadoras de voz, datos, televisión, etc... con velocidades de transmisión de hasta 2,5 Gbit/s.

Aunque los satélites de comunicaciones cubren una parte de la demanda de transmisión, especialmente para televisión e Internet, los cables submarinos de fibra óptica siguen siendo la base de la red mundial de telecomunicaciones.

Movistar ha realizado una instalación reciente de fibra óptica que conecta la Península con Canarias, donde Conil es el punto clave.

Medios Inhalámbricos

Bandas de transmisión inalámbrica

Según el rango de frecuencias de trabajo, las transmisiones no guiadas se pueden clasificar en tres tipos:

-Ondas de radio(RF): 3 KHz – 1 GHz

- Omnidireccionales (propagación en todas direcciones).
- Telefonía móvil, radio, televisión.

-Microondas (RF): más de 1 GHz – 300 GHz

- Direccionales (propagación en una cierta dirección, emisor y receptor deben estar alineados).
- Wi-Fi, Bluetooth, Wimax, transmisiones satélite, telefonía fija inalámbrica.

-Infrarrojos: más de 300 GHz – 20 THz

- Extremadamente Direccionales (emisor y receptor deben estar perfectamente alineados).
- Escasa utilización debido al punto anterior. Desplazada por tecnologías como Wi-Fi y Bluetooth.

Las bandas de radiofrecuencias (RF) están autorizadas por las agencias gubernamentales. Para difundir por estas frecuencias hay que tener una licencia y pagar una cuota. Hay tres bandas que no requieren licencia:

- 900 MHz → telefonía móvil (GSM, GPRS)
- 2,4 GHz → Wi-Fi, Bluetooth
- 5 GHz → Wi-Fi

Ejemplos de bandas que sí requieren licencia:

- 2,3 – 5,8 GHz → Wimax
- 1800 MHz, 1900 MHz (según región del planeta) → telefonía móvil (GSM, GPRS)

-Mayor frecuencia → Mayor velocidad de transmisión

-A igual potencia de señal, Mayor frecuencia → Menor alcance de la señal.



Ángel M. Gamaza

Antenas

- Conductor eléctrico utilizado para captar o radiar energía electromagnética.
- Usado tanto para emitir como para recibir.



Wi-Fi



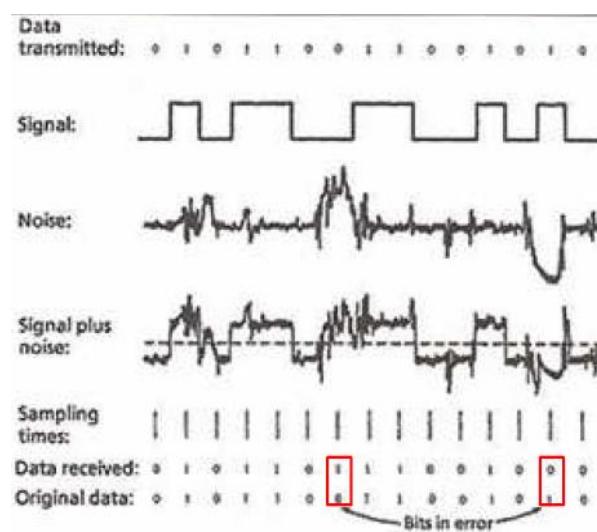
Wimax

Perturbaciones en medios de cobre

Las perturbaciones son efectos nocivos que modifican la forma de la señal durante la transmisión. Tipos:

Ruido

- El ruido es una señal no deseada que se suma a la señal que se está transmitiendo, alterándola y distorsionándola.
- Una gran distorsión de la señal por el ruido puede llegar a originar errores de transmisión.
- Es necesario conocer las fuentes que lo originan para minimizar su efecto en los sistemas de comunicaciones.



Interferencia electromagnética (EMI) o ruido eléctrico

Originada por dispositivos que utilicen o generen tensiones variables. Estas tensiones generan una energía electromagnética que es irradiada como señal de radio. El cable de cobre de la red de comunicaciones actúa como antena y capta esta señal, la cual se sumará a la original.

Ejemplo: rayos, iluminación fluorescente, motores eléctricos, ascensores...

Interferencia de radiofrecuencia (RFI)

RFI constituye un subconjunto de EMI.

RFI va desde 150 KHz hasta 100 MHz, mientras que EMI se expande hasta varios GHz.

La fuente de interferencia puede ser cualquier equipo que genere señales de radio frecuencia (RF), por ejemplo, transmisores de radio y televisión.

Diafonía (crosstalk)

Interferencia entre pares de un mismo cable.

Cuando cambia el voltaje en un par de hilos, se genera energía electromagnética, la cual es irradiada como señal de radio. Los pares adyacentes funcionan como antenas y pueden captar esta señal, la cual interferirá en la transmisión de esos hilos.

Esta interferencia se propaga por todo el par, llegando a ambos extremos.

-La interferencia recibida en el mismo extremo del cable respecto al que se introdujo la señal original se denomina NEXT (diafonía de extremo cercano).

-La interferencia recibida en el extremo opuesto del cable respecto al que se introdujo la señal original se denomina FEXT (diafonía de extremo lejano).

-Se expresa en decibelios (dB) y utilizando números negativos:

-10 dB es más diafonía (más ruido) que -30dB

Medidas Paliativas

El cable coaxial es menos susceptible al ruido EMI/RFI porque la malla conductiva que está conectada a masa desvía a tierra cualquier señal de ruido, evitando que llegue al conductor interior.

Medida paliativa	EMI/RFI	Diafonía
Blindaje en cada par		<input checked="" type="checkbox"/>
Separador de pares		<input checked="" type="checkbox"/>
Trenzado	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Terminación de conectores adecuada	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Señales diferenciales	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Blindaje global	<input checked="" type="checkbox"/>	
Cuidar el diseño de la instalación de cableado	<input checked="" type="checkbox"/>	

Señales diferenciales

Las señales que se transmiten por un cable de par trenzado son diferenciales.

Una señal diferencial se transmite por los dos conductores del par, en lugar de hacerlo por uno sólo.

Por cada conductor se transmite una señal de igual voltaje pero de polaridad opuesta (señales simétricas), llamadas $V(+)$ y $V(-)$.

Cada uno de los hilos envía una copia de los datos, siendo las dos copias imágenes espejo.

El receptor medirá la diferencia entre las dos señales $V(+)$ - $V(-)$.

Las señales diferenciales son más robustas ante las interferencias: el ruido se suma por igual en ambos conductores y al calcular $V(+)$ - $V(-)$ se cancela.

Trenzado de los hilos

Contribuye a la cancelación del ruido

Si los dos cables están trenzados entre sí en intervalos regulares, cada cable está cerca de la fuente del ruido durante la mitad del tiempo y lejos durante la otra mitad. Por tanto, con el trenzado, el efecto acumulativo de la interferencia es igual en ambos cables.

Evita la emisión de ruido

Cuando un hilo está transportando corriente, ésta crea un campo magnético alrededor, el cual puede interferir en hilos cercanos. Para combatirlo, los pares de hilos transportan señales en direcciones opuestas, de modo que los dos campos magnéticos también se generan en direcciones opuestas y se neutralizan.

Al trenzar los pares, se mantienen juntos los dos hilos garantizándose una cancelación de los campos efectiva.

Cuanto más alta es la categoría de un cable de par trenzado, mayor es el paso de trenzado (número de vueltas por unidad de longitud).

Atenuación

La atenuación es la pérdida progresiva de amplitud (intensidad o potencia) en la señal cuando ésta se propaga a través del medio de cobre. Se debe a la resistencia que ofrece el cable.

La pérdida de amplitud provoca que el receptor no sea capaz de distinguir entre un bit 1 o un bit 0.



Se expresa en decibelios (dB) y utilizando números negativos.

-10 dB es una atenuación menor que -30 dB

Factores que contribuyen a incrementar la atenuación:

- La longitud del cable.
- Las señales de alta frecuencia.
- Cuanto mayor es la frecuencia de la señal que circula por el cable, mayor es la atenuación.

Medidas paliativas:

- No exceder las distancias máximas permitidas.
- Si hubiera que exceder esas distancias, utilizar dispositivos que regeneren la señal (hub, switch, etc).

Perturbaciones en otros medios

Como la fibra de vidrio no es un conductor eléctrico:

- La fibra óptica es inmune a EMI y RFI.
- En la fibra óptica no existe diafonía.

Problemas de la fibra óptica

- El coste de instalación es elevado.
- Fragilidad de las fibras.
- Disponibilidad limitada de conectores.
- Dificultad de reparar un cable de fibras roto en el campo.
- La fibra óptica no transmite energía eléctrica, esto limita su aplicación donde el terminal de recepción debe ser energizado desde una línea eléctrica. La energía debe proveerse por conductores separados.



Ángel M. Gamaza

Interferencias y atenuaciones en medios inalámbricos

Los obstáculos que causan interferencia pueden ser de tres tipos:

- 1 - Los que retienen la señal y que son inherentes a toda casa (paredes, suelo, muebles, etc.). Cuando menor es la cantidad de obstáculos que deba atravesar la señal mayor es la cobertura.**
- 2 - Los obstáculos que modifican la señal y que son en su mayor número objetos metálicos (tal como es sabido por todos, los aparatos metálicos reflejan las ondas y las llenan de ruido). Cuanto más alejados de ellos mejor será el alcance.**
- 3 - Los que vampirizan las ondas y que son los aparatos que compiten por la señal (aquí englobamos a todos los aparatos inalámbricos que utilicen la misma frecuencia del router). Lo ideal es adquirir dispositivos inalámbricos que utilicen una frecuencia distinta a 2.4 Ghz.**

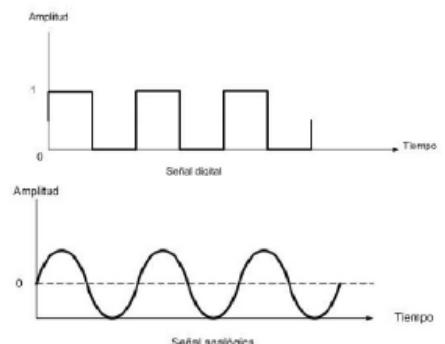
Tema 2

Capa Física 2ª Parte: Señales. Estándares de la capa física

Tipos de señales:

Señal digital: Es una señal discreta, sólo puede tomar un conjunto finito de valores (Ej: {5V, 0V}). La transición entre los valores es repentina, como una luz que se enciende y apaga.

Señal analógica: Es una señal continua, puede tomar infinitos valores. La onda cambia suavemente en el tiempo.



Los datos a transmitir por un host son digitales. Sin embargo, la transmisión por un medio de comunicación puede ser:

-**Digital:** Los datos digitales hay que convertirlos en una señal digital (proceso de codificación en línea).

-**Analógica:** Despues de convertir los datos digitales en señal digital, hay que transformar esta señal en analógica (proceso de modulación).

Componentes de una señal: Armónicos

Una señal está compuesta por varias, incluso infinitas, señales sinusoidales simples llamadas armónicos, cada cual, tiene una frecuencia y amplitud determinada.

Ancho de banda

El espectro de una señal es la colección de todos los armónicos de ésta. Para visualizar el espectro se utiliza un gráfico en el dominio de la frecuencia.

El ancho de banda es el ancho del espectro de la señal. Para calcular el ancho de banda hay que restar a la frecuencia más alta del espectro la frecuencia más baja. Se mide en Hz.

El ancho de banda del medio es el rango de frecuencias que soporta el medio físico y está limitado por las propiedades físicas del canal.

Una señal digital generalmente requiere más ancho de banda que una analógica, ya que si no se enviaría solo el espectro significativo de ésta (Subconjunto de armónicos de amplitud más significativa)

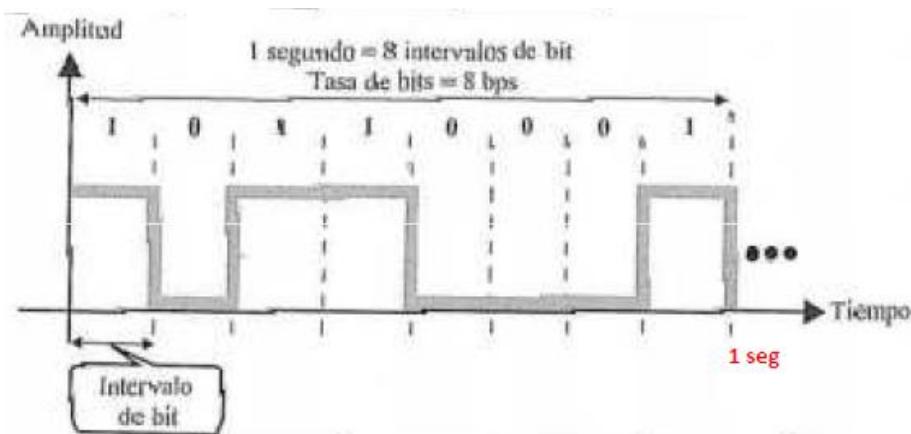
Tasa de transferencia

La mayoría de las señales digitales son aperiódicas, con lo que los términos con los que las describiremos serán:

-Intervalo de bit: Tiempo necesario para enviar un único bit.

-Tasa de bits (o tasa de transferencia o velocidad de transferencia): Número de bits enviados en un segundo. Expresado en bits por segundo (bps). Depende en gran medida del tipo de codificación utilizado.

NO CONFUNDIR: Tasa de Transferencia y Ancho de Banda.



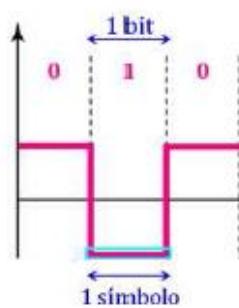
Tasa de señalización

Número de símbolos de señal (también llamados estados de señal) transmitidos en un segundo o número de veces que puede cambiar la señal en un segundo. Se mide en baudios

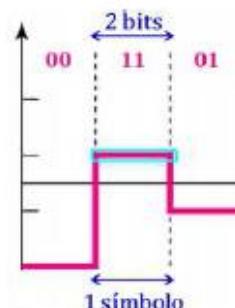
Un símbolo de señal puede representar varios bits (como veremos esto lo determina el método de codificación utilizado).

bps y baudios no son sinónimos.

Tasa señalización = Tasa transferencia



Tasa señalización < Tasa transferencia



Tipos de transmisión

Banda base

La señal es transmitida en su banda de frecuencias original, no sufre ningún proceso de modulación. Sólo se transmite una señal por el medio físico.

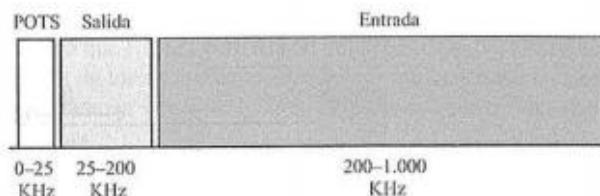
Ejemplo: Ethernet

Banda ancha

Se pueden transmitir varias señales por el medio físico. El ancho de banda del medio es dividido en canales (bandas), cada cual, es capaz de transferir una señal de datos de forma independiente. La división de canales se realiza mediante multiplexación por división de frecuencias (FDM).

La señal debe ser modulada para trasladarla a su canal.

Ejemplos: ADSL. Esta tecnología de red divide el ancho de banda del medio en tres bandas. La primera banda se utiliza para el servicio telefónico, la segunda se usa para enviar datos y la tercera para recibir datos.



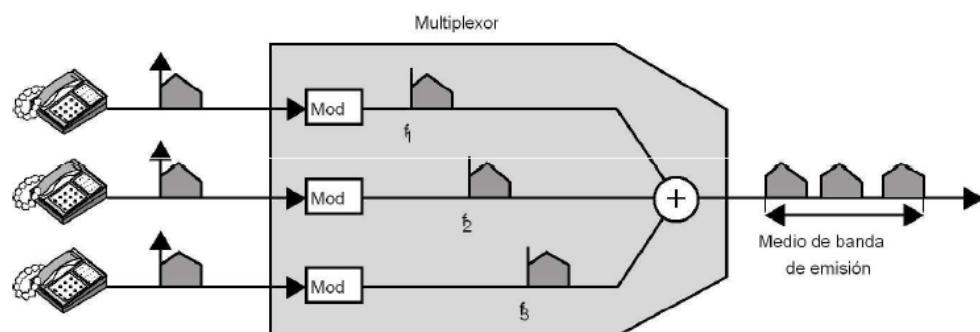
Multiplexación

Transmisión simultánea de varias señales por el mismo canal.

Tipos:

-Multiplexación por División de Frecuencia (FDM).

Emitiendo:



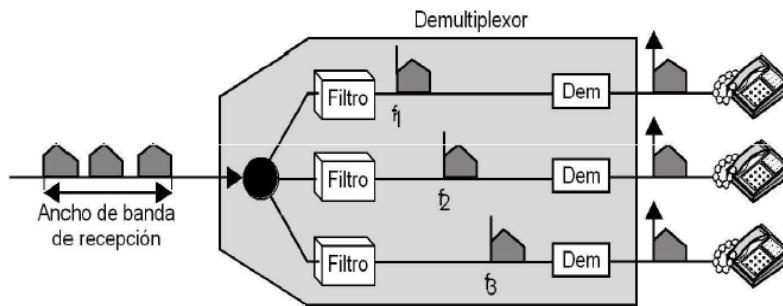


Máster en Ciberseguridad



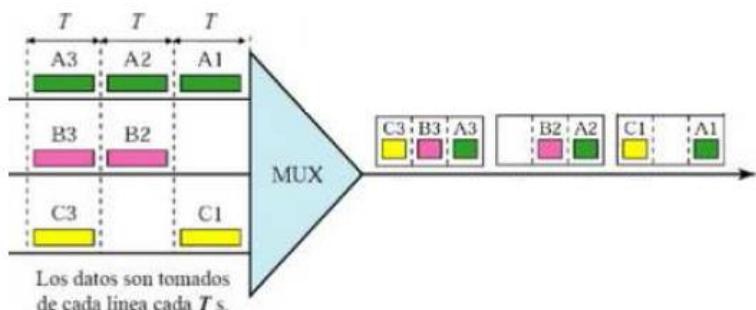
Ángel M. Gamaza

Recibiendo:



-Multiplexación por División de Tiempo (TDM).

El ancho de banda del medio es asignado a cada dispositivo emisor durante fracciones del tiempo (ranuras).

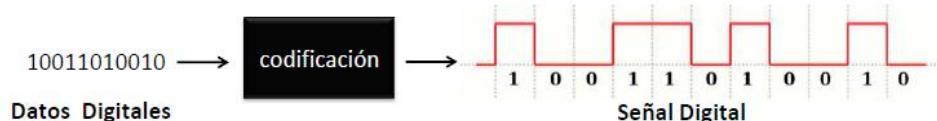


-Multiplexación por División de Longitud de Onda (WDM).

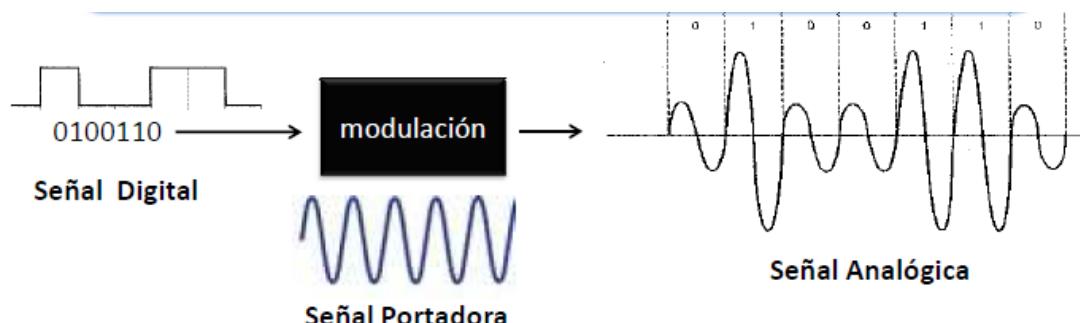
Codificación en línea

Es el proceso que convierte los datos digitales en señales digitales.

Los 1 y 0 se traducen en pulsos de tensión o en pulsos de luz (señales electromagnéticas), según el medio físico.



En el proceso de modulación la señal digital* se convierte en analógica. Se realiza variando una o varias características (amplitud, frecuencia, fase) de una señal analógica llamada portadora. Esta variación se rige por los cambios que marca la señal de entrada (en nuestro caso, la señal digital). Algunos tipos de modulación: ASK, FSK, PSK.



Sincronización

Tanto el emisor como el receptor tienen un reloj. Éstos deben estar sincronizados para detectar correctamente cuándo comienza un bit y cuando termina. La falta de sincronización entre estos relojes provoca errores en la decodificación de la señal.

Soluciones:

- **Transmitir dos señales en paralelo:** la señal de datos y una señal de reloj. Esta señal de reloj permitirá al dispositivo receptor sincronizar su temporizador. Para ello hay que doblar el número de líneas y se incrementa el coste.

- **El receptor puede utilizar las transiciones de la señal para sincronizar su temporizador.** Esto será posible si se utilizan esquemas de codificación que eliminan la componente continua.

Componente continua (DC)

Si se transmiten de forma consecutiva una secuencia larga de 1 ó una secuencia larga de 0, no hay transiciones de voltaje en la señal ("la señal es una línea", se dice que se ha creado una componente de corriente continua).

Cuando una señal no varía, el receptor no puede determinar el principio y el final de cada bit.



Un esquema de codificación debe procurar:

- **Proporcionar sincronización entre emisor y receptor a través de las transiciones de los pulsos recibidos.**

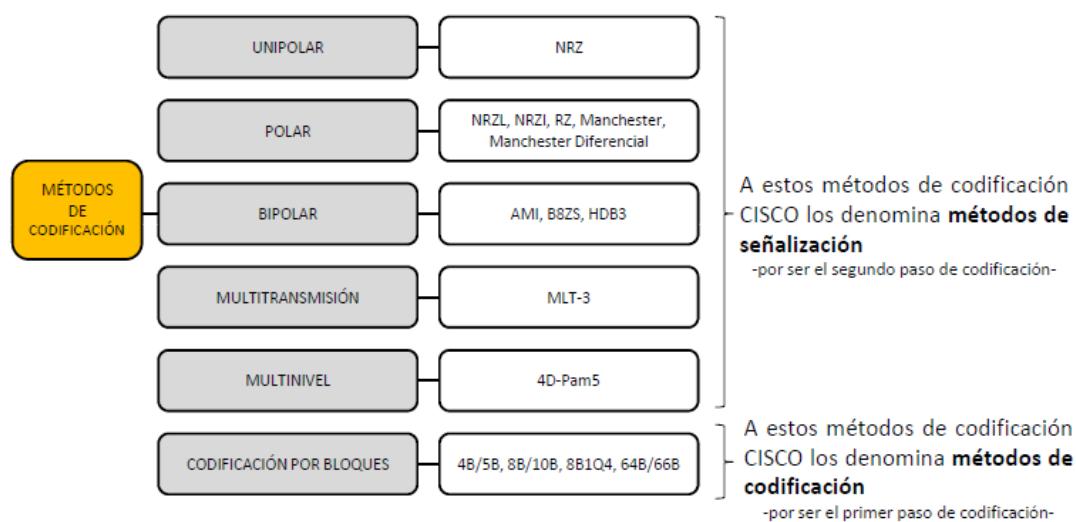
- **Minimizar la componente continua (DC).**

En todos los estándares Ethernet se utilizan dos pasos de codificación por separado para mejorar la integridad de la señal. Cada estándar designa qué método de codificación se debe utilizar.

Los dispositivos transmisor y receptor deben pertenecer al mismo Estándar, así sabrán como representar los 1 y los 0. Si se utilizan diferentes estándares en cada extremo de la transmisión, no se podrá llevar a cabo la comunicación a través del medio físico.

En el dispositivo receptor:

- 1. Las señales se vuelven a convertir en bits (decodificación).**
- 2. Se examinan los bits para determinar la trama. Para ello, el dispositivo localiza los patrones de bits del comienzo y el final de la trama.**
- 3. La capa Física envía la trama a la capa de Enlace de datos.**



Estándar 802.3 (Ethernet)

Es una especificación para Redes de Área Local (LAN).

100BaseTx (Fast Ethernet)

Medio: UTP categoría 5 o superior

Velocidad: 100 Mbps

Longitud máx. segmento: 100 m

Codificación en línea: 4B/5B + MLT-3

Tx/Rx:

- Un par para transmitir:
 - pin 1: TD+
 - pin 2: TD-
- Un par para recibir:
 - pin 3: RD+
 - pin 6: RD-

Cable UTP directo para conexión PC-Router y cruzado para conexión PC-PC.

100BaseFX (Fast Ethernet)

Medio: Fibra óptica multimodo

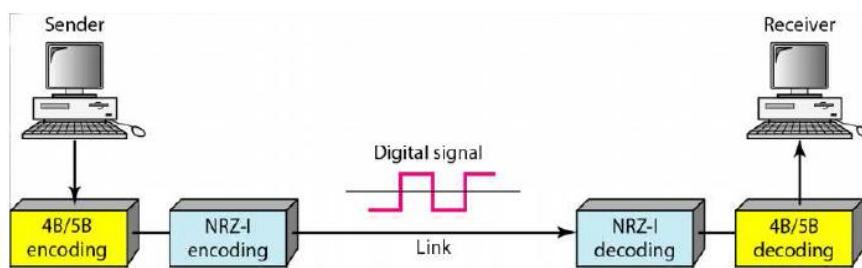
Velocidad: 100 Mbps

Longitud máx. segmento: 2 km

Codificación en línea: 4B/5B + NRZI

Tx/Rx:

- Un hilo de fibra para transmitir
- Otro hilo de fibra para recibir



Codificación 4B/5B

Es un tipo de codificación mB/nB: a cada m bits le corresponde un código de n bits, en este caso.

-**Códigos de Datos:** A cada una de los 16 combinaciones posibles de cuatro bits se le asigna un código de 5 bits para representarla.

-**Códigos de Control:** Los códigos que no se han asignado para representar datos se usan para control, por ejemplo, para delimitar el comienzo y el final de trama (PDU de capa 2).

Codificación NRZI

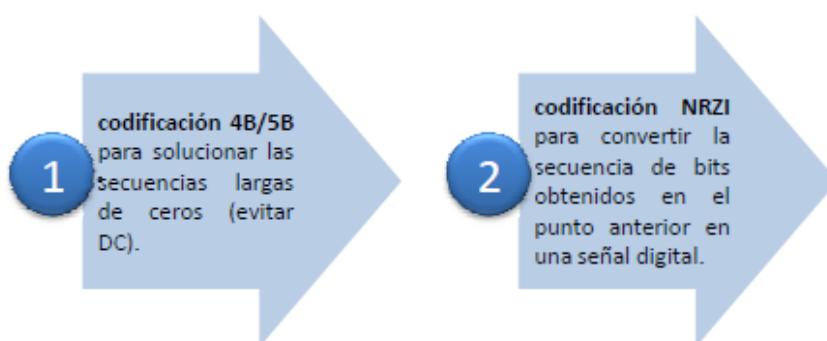
Se definen dos niveles de intensidad para los pulsos de luz (o dos niveles de voltaje si la transmisión tuviera lugar en un medio de cobre): un nivel de intensidad bajo y un nivel de intensidad alto.

Un 1 se representa con un cambio de intensidad en el pulso de luz: del nivel alto al bajo o del nivel bajo al alto, según corresponda.

Un 0 se representa con un NO cambio de intensidad en el pulso de luz.

Debido al tiempo necesario para activar y desactivar el transmisor de luz, en fibra óptica la luz es pulsada siempre usando potencia baja y otra alta.

¿Por qué se utilizan dos pasos de codificación?





Ángel M. Gamaza

1000BaseT (Gigabit Ethernet)

Medio: UTP categoría 5e o superior

Velocidad: 1 Gbps

Distancia máxima: 100 m

Codificación en línea: 8B1Q4 + 4D-PAM5

Tx/Rx: Los cuatro pares de hilos transmiten y reciben simultáneamente

Sofisticados circuitos híbridos en los dispositivos que acceden al medio pueden actuar a la vez como Tx y Rx en los mismos hilos.

1000BASE-T permite la transmisión y recepción de datos en ambas direcciones (en los cuatro pares al mismo tiempo). Este flujo de tráfico crea colisiones permanentes en los pares de cables que generan patrones de voltaje complejos.

Los circuitos híbridos que detectan las señales utilizan técnicas sofisticadas como cancelación de eco, corrección automática de errores de capa 1 (FEC) y una prudente selección de los niveles de voltaje.

Codificación 4D/PAM5

En el segundo paso de codificación de 1000BaseT se utilizan los cuatro pares del cable para enviar la información (100BaseTx que utiliza solo uno).

Por cada par se envían dos bits de datos utilizando un código de 4 bits (4D).

Se utilizan cinco niveles de tensión (PAM5): -2, -1, 0, +1, +2 V.

1000BaseSX (Gigabit Ethernet)

Medio: Fibra óptica multimodo

Velocidad: 1 Gbps

Longitud máx. segmento: 220 m - 550 m (según tipo de fibra)

Codificación en línea: 8B/10B + NRZ

Tx/Rx: Un hilo de fibra para transmitir
Otro hilo de fibra para recibir

NOTA: La S proviene de Short, esto quiere decir que la señal que se transmite es de onda corta. La fuente que genera la señal es un laser de bajo coste o un diodo LED.

1000BaseLX (Gigabit Ethernet)

Medio: Fibra óptica monomodo o multimodo

Velocidad: 1 Gbps

Longitud máx. segmento: 550 m - 10 km (según tipo de fibra)

Codificación en línea: 8B/10B + NRZ

Tx/Rx: Un hilo de fibra para transmitir
Otro hilo de fibra para recibir

NOTA: La L proviene de Long, esto quiere decir que la señal que se transmite es de onda larga. La fuente que genera la señal es un laser.

10-Gigabit Ethernet

Estándares : Existen muchos estándares 10 Gigabit

Medio: Monomodo, multimodo, par trenzado de alta categoría

Velocidad: 10 Gbps

Distancia máxima: 100m - 80 km (según el medio)

Codificación en línea: 64B/66B + 2D-PAM16 (entre otras)

Estándar 802.5 (Token Ring)

Es otra especificación para Redes de Área Local (LAN).

Topología: tiene topología física estrella y topología lógica en anillo.

Cable especial apantallado: aunque el cableado también puede ser par trenzado.

Longitud máxima de la red: no más de 366 metros.

La distancia entre una computadora y el MAU: no puede ser mayor que 100 metros.

A cada MAU (Unidad de Acceso a Múltiples Estaciones) se pueden conectar ocho computadoras.

Velocidad máxima de transmisión: entre los 4 y los 16 Mbps.

El High Speed Token Ring (HSTR): elevó la velocidad a 110 Mbps pero la mayoría de redes no la soportan.

En desuso por la popularización de Ethernet, actualmente no es empleada en diseños de redes.

Estándar 802.11 (Wi-Fi)

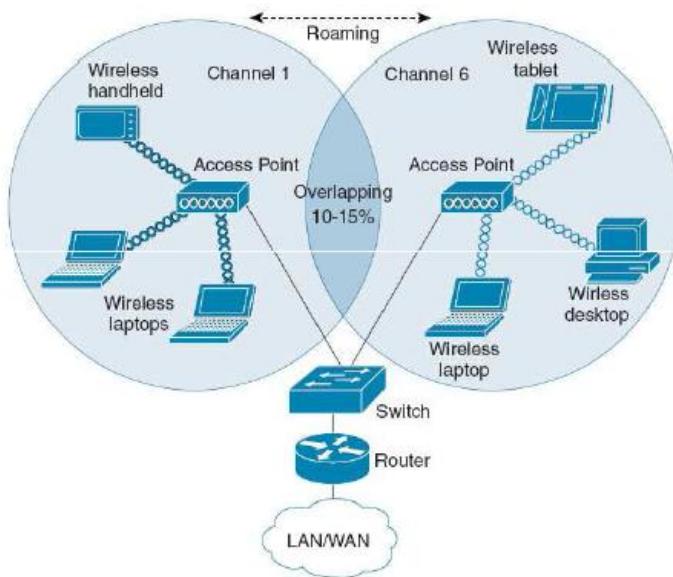
Es una especificación para Redes Inalámbricas de Área Local (WLAN).

	Estándar	Frecuencia	Tasa de transferencia (teórica)	Compatibilidad
■	802.11b	2,4GHz	11 Mbps	
■	802.11a	5GHz	54 Mbps	
■	802.11g	2,4GHz	54 Mbps	■
■	802.11n	2,4GHz y 5GHz	600 Mbps	■ ■ ■
■	802.11ac	menor de 6GHz	1Gbps	■ ■ ■ ■

A igual potencia, una señal de 2,4GHz tiene más alcance y pueden penetrar mejor en los muros que una señal de 5GHz.

Hablar de alcance involucra muchos factores: potencia de la antena, frecuencia de la señal, obstáculos, condiciones atmosféricas, etc.

Esquema de una red conectada por Wi-Fi



Estándar 802.15.1 (Bluetooth)

Es una especificación para Redes Inalámbricas de Área Personal (WPAN).

Medio: Posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda de los 2,4 GHz.

Velocidad:

Versión	Tasa de transferencia
1.2	1 Mbps
2.0 +EDR	3 Mbps
3.0 + HS	24 Mbps
4.0	24 Mbps

Alcance: Diseñado especialmente para dispositivos de bajo consumo, que requieren corto alcance de emisión.

Clase	Potencia	Alcance (aprox.)
1	100 mW	100 m
2	2.5 mW	10 m
3	1 mW	1 m

Tema 2

Capa Física 3^a Parte: Cableado estructurado. Topología física

Cableado estructurado

Es el sistema organizado de cables y elementos de conexión que constituye la red de telecomunicaciones (voz y datos) de un edificio (o conjunto de edificios).

Elementos que intervienen en la instalación:

Cables, canalizaciones, rosetas, paneles de conexión, armarios, etiquetas, etc.

Siempre se debe seguir la normativa. Así se garantiza una instalación correcta, un rendimiento adecuado, las medidas de seguridad necesarias, etc.

Una red que es capaz de adaptarse a un crecimiento posterior se denomina **red escalable** (la cantidad de cables instalados debe satisfacer necesidades futuras).

Una red debe ser escalable.

Normativa

Existen distintos tipos de normativas, entre ellas tenemos:

- Aenor (Normativa de ámbito español).
- CENELEC (Normativa de ámbito europeo).
- ISO/IEC (Normativa de ámbito mundial).
- TIA/EIA (Normativa de ámbito de la industria).
- IEEE (Normativa de ámbito de la industria).

Distribuidores

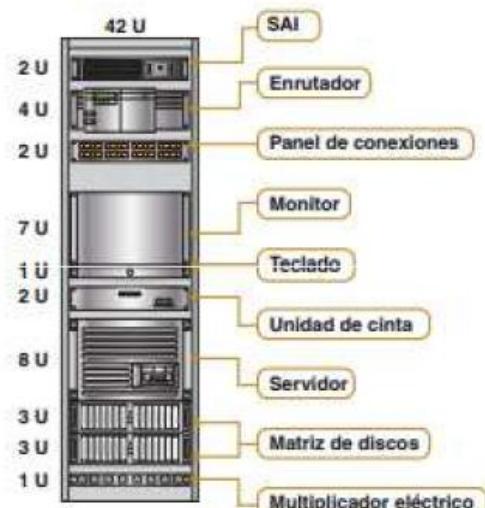
Otras denominaciones:

- Armario de comunicaciones.
- Bastidor.
- Rack.

Utilizado para albergar principalmente:

- Equipos de electrónica de red.
- Paneles de conexión.

Están ubicados en salas debidamente acondicionadas.





Máster en Ciberseguridad

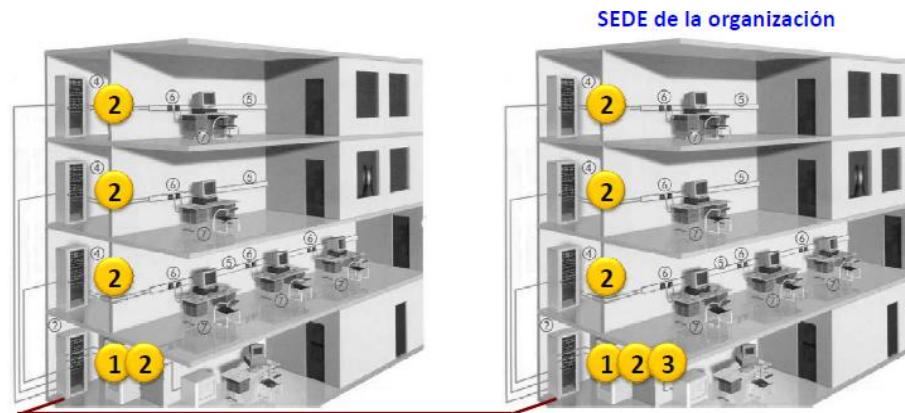
Ángel M. Gamaza

Dimensiones estandarizadas:

- Ancho:** 19 pulgadas.
- Altura:** Se mide en U (rack Unit).
- 1U = 1,75 pulgadas = 3 orificios de atornillaje.**



Los fabricantes de dispositivos dimensionan sus equipos para que se puedan instalar en los distribuidores, ocupando 1, 2 ó más U.



1. Distribuidor de planta (ubicado en la sala de telecomunicaciones -TR-).
2. Distribuidor de edificio (ubicado en la sala de equipamiento -ER-).
3. Distribuidor de campus (ubicado en la sala de equipamiento -ER-).

La sala de equipamiento (ER) es la sala de telecomunicaciones principal del edificio, es el centro de la red de voz y datos.

Por lo general, en esta sala podemos encontrar:

- Distribuidor de edificio.**
- Centralita telefónica (PBX).**
- Punto de demarcación (Demarc, PoP): dispositivo que establece la frontera entre la red del usuario y la red del proveedor de telecomunicaciones.**
Identifica dónde termina la responsabilidad del proveedor y dónde comienza la responsabilidad del cliente.
- Servidores.**
- Acometida:** Entrada de servicios de telecomunicaciones al edificio.

La sala de telecomunicaciones (TR) es una sala pequeña que sólo da cabida al distribuidor de planta. Suele haber una por planta. En algunos casos, como se verá posteriormente, es necesario más de una TR por planta.

Distribuidor de planta:

-Mínimo uno por planta. Que haya más de uno depende de la extensión de la planta.

Distribuidor de edificio (también denominado distribuidor principal):

-Sólo uno por edificio.

-Suele estar en la planta baja, por estar allí el punto de demarcación, ó en uno de los pisos centrales.

-El distribuidor de edificio puede ser también distribuidor de planta.

Distribuidor del campus:

-Sólo hay uno en el campus.

-El distribuidor del campus puede ser también distribuidor de planta y de edificio.

Subsistemas de cableado

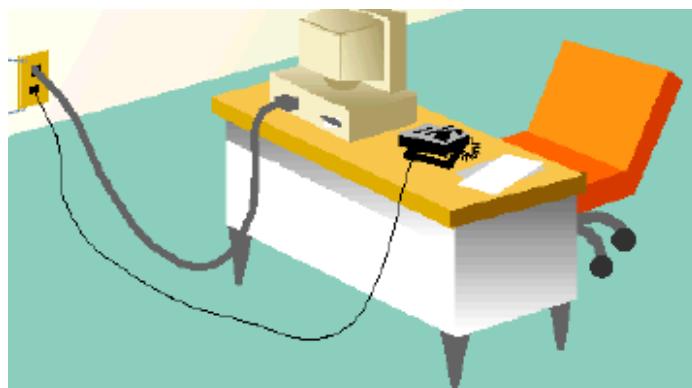
El cableado estructurado divide el cableado de un edificio en cuatro subsistemas:

-**Subsistema de cableado del área de trabajo.**

Cableado que conecta los equipos del puesto de trabajo (ordenador, teléfono, fax, impresora de red, etc) a las rosetas.

Cable datos: cable de par trenzado (UTP, S/FUTP, etc) y conector RJ45. Según normativa no debe exceder de 5 m.

Cable de voz: formado por 2 o 4 hilos sin trenzar.



Roseta: dispositivo pasivo. Cada toma debe estar etiquetada.

Otras denominaciones:

-Jack.

-TAT (Toma de Acceso de Telecomunicaciones).



Cada puesto de trabajo debe tener por lo menos dos tomas, una para datos y otra para voz.

-Subsistema de cableado horizontal.

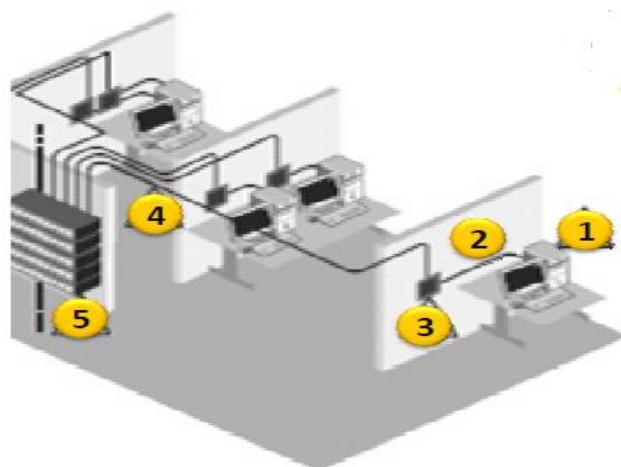
Cableado que conecta las rosetas con el distribuidor de planta, concretamente con las tomas del panel/es de conexión del distribuidor. Se suele utilizar cable de par trenzado.

El tendido de cableado puede discurrir por:

-Canaletas.

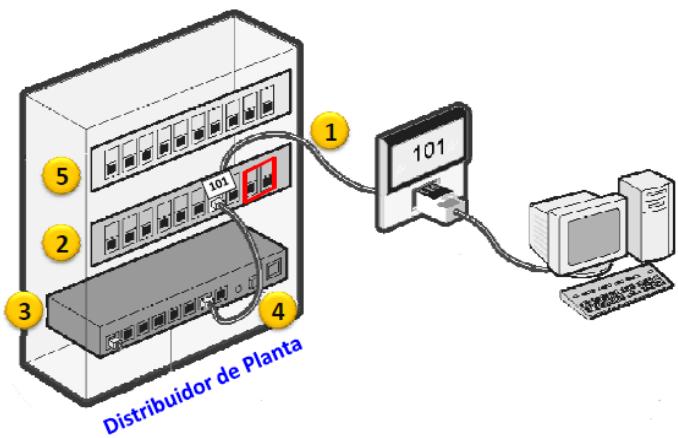
-Techo técnico (falso techo).

-Suelo técnico (falso suelo).



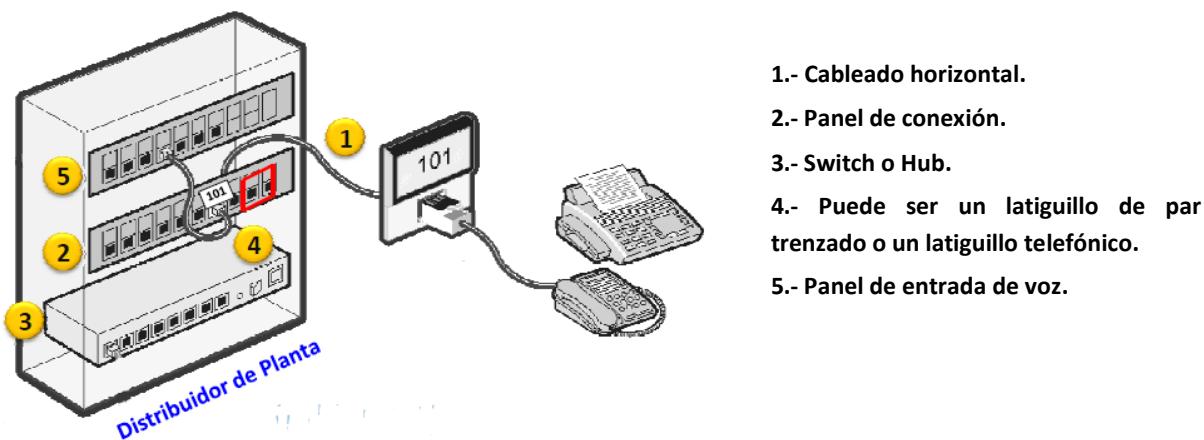
- 1.- Equipo de puesto de trabajo
- 2.- Cableado del área de trabajo
- 3.- Roseta
- 4.- Cableado horizontal
- 5.- Distribuidor de planta

-Panel de conexión (o Patch Panel): dispositivo pasivo. Cada toma debe estar etiquetada y en correspondencia con su roseta.



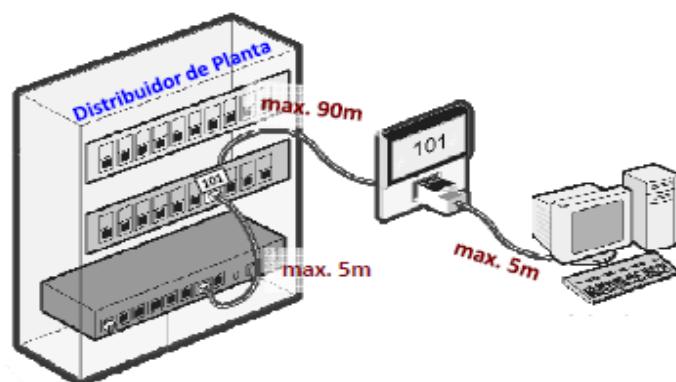
1. Cableado horizontal (según normativa no debe exceder de 90 m.).
2. Panel de conexión.
3. Switch o Hub.
4. Latiguillo (patch cord) de par trenzado (según normativa no debe exceder de 5 m.).
5. Panel de entrada de voz.

-Panel de entrada de voz: dispositivo pasivo. Utilizado para la conexión vertical de voz.



Por razones de atenuación, la distancia máxima que permite el cableado de par trenzado es 100 metros. La normativa establece:

- Longitud máxima del cable horizontal es 90 m.**
- Longitud máxima del latiguillo en el área de trabajo es 5 m.**
- Longitud máxima del latiguillo que conecta panel de conexión y equipo activo en el distribuidor de planta es 5 m.**



Un distribuidor de planta da cobertura a un determinado radio, el cual aparentemente podría ser 90 m. pero hay factores que disminuyen este valor.

Debido a que el recorrido del cable no sigue normalmente una línea recta entre roseta y distribuidor, ya sea por el plus de la altura del falso techo o los rodeos por ventilación, iluminación, etc. Se determina que el radio del área de cobertura de un distribuidor de planta sea **50 m.**

Si la planta del edificio es muy extensa será necesario disponer de más de un distribuidor por planta.

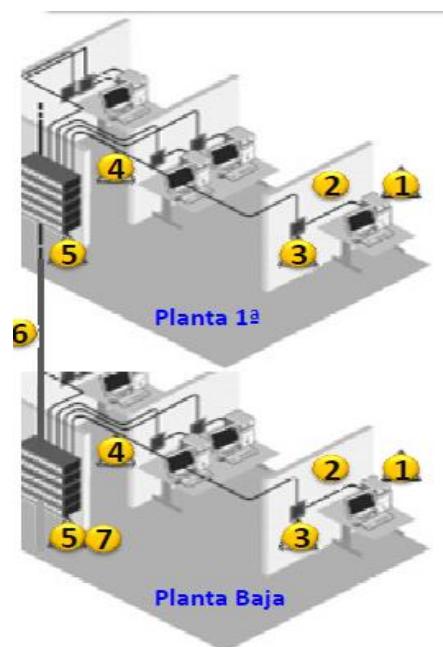


Ángel M. Gamaza

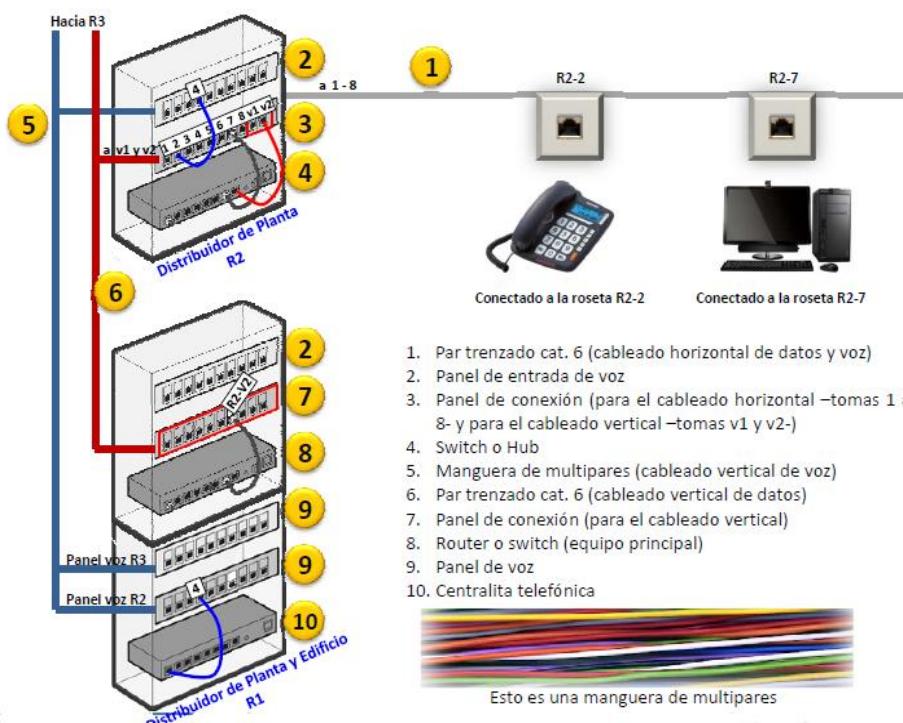
-Subsistema de cableado vertical (También llamado cableado troncal o Backbone).

Cableado que conecta cada distribuidor de planta con el distribuidor de edificio (generalmente es fibra óptica aunque también puede ser par trenzado).

El tendido de cableado discurre por: **Conducto vertical entre pisos.**



- 1.- Equipo de puesto de trabajo
- 2.- Cableado del área de trabajo
- 3.- Roseta
- 4.- Cableado horizontal
- 5.- Distribuidor de planta
- 6.- Cableado vertical
- 7.- Distribuidor de edificio



1. Par trenzado cat. 6 (cableado horizontal de datos y voz)
2. Panel de entrada de voz
3. Panel de conexión (para el cableado horizontal –tomas 1 a 8- y para el cableado vertical –tomas v1 y v2–)
4. Switch o Hub
5. Manguera de multipares (cableado vertical de voz)
6. Par trenzado cat. 6 (cableado vertical de datos)
7. Panel de conexión (para el cableado vertical)
8. Router o switch (equipo principal)
9. Panel de voz
10. Centralita telefónica



Esto es una manguera de multipares

-Subsistema de cableado troncal del campus.

Sólo existe en las redes de área local que tengan más de un edificio. Conecta cada distribuidor de edificio con el distribuidor de campus. Se suele utilizar fibra óptica.

Etiquetado

Los elementos que hay que etiquetar (rotular) para que queden perfectamente identificados son:

- Cables** (excepto latiguillos): Los cables deben estar claramente rotulados en ambos extremos para evitar confusión.
- Rosetas**.
- Cada toma de los paneles de conexión**.
- Racks**.

Certificación de la red

Una vez que concluimos la instalación de la red, llega el momento de verificar la funcionalidad y rendimiento del cableado mediante el proceso de certificación.

En este proceso, se estudia cada segmento de cable:

- Horizontal**.
- Vertical**.
- Troncal de campus**.

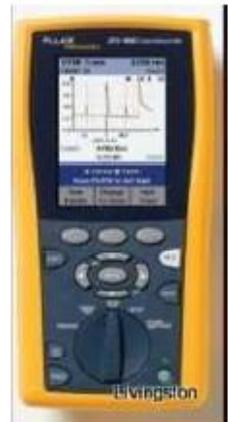
Cada segmento de cable debe superar un test.

Los parámetros a verificar son:

- Mapa de cableado** (son las terminaciones).
- Longitud del segmento de cable** (no debe superar los máximos establecidos).
- Atenuación**.
- Diáfonía**.
- etc.**

Los valores de referencia son establecidos por la normativa.

Una instalación queda certificada cuando todos los segmentos de cable que la componen pasan el test.



Dispositivo Certificador

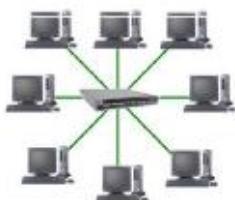
Topología física

Describe la disposición física de los cables y dispositivos.



Bus

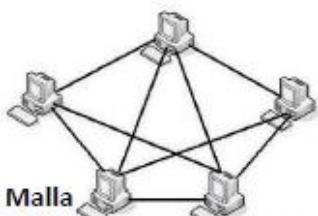
Todas las estaciones se conectan a un único cable.



Estrella

Las estaciones se conectan a un nodo central.

Si falla el nodo central se cae toda la red.



Malla

Conecta cada estación con todas las demás para conseguir redundancia y tolerancia a fallos.



Anillo

Las estaciones se conectan formando un anillo, cada estación está conectada a la siguiente y la última está conectada a la primera.

La comunicación se da por el paso de un token (símil: cartero que pasa recogiendo y entregando paquetes de información).

Si falla alguna estación se cae toda la red.



Estrella extendida

Redes en estrella conectadas.

Si falla uno de los nodos centrales se cae parte de la red.

Tema 3

Capa de Enlace 1ª Parte: Funciones de la capa de enlace

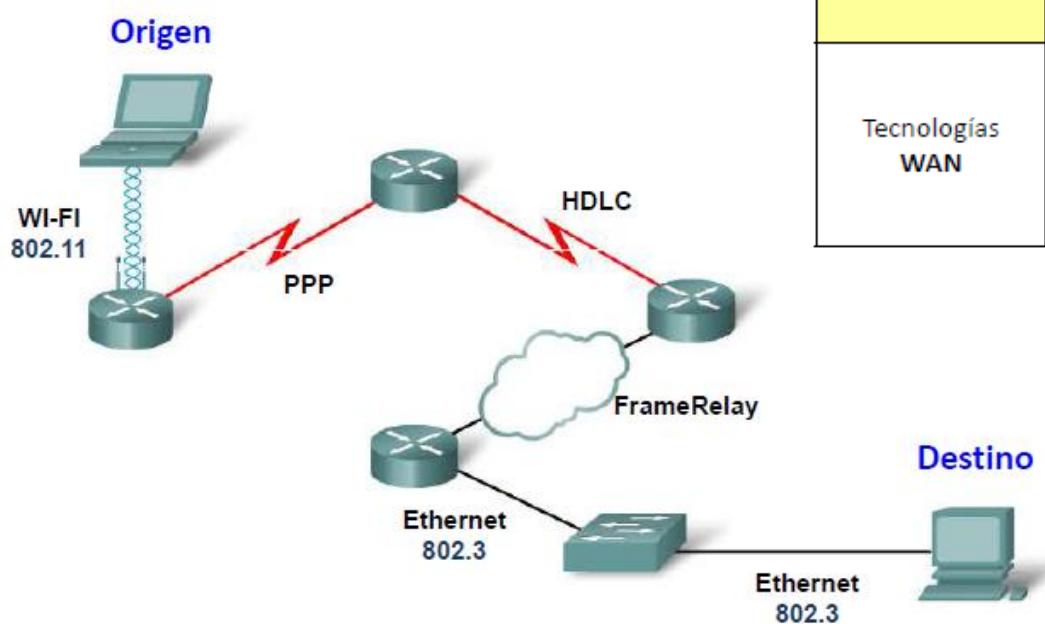
Dispositivos de capa 2

- Switch.
- Punto de acceso.
- Tarjeta de interfaz de red (Network Interface Card – NIC –).

Tecnologías de red

Cuando hablamos de **tecnología de red** nos referimos siempre a las capas 1 y 2 del modelo OSI.

Las **tramas**, durante su recorrido, pueden pasar por diferentes tecnologías de red.



Funciones de la capa de enlace

- Direccionamiento físico. A3-56-2C-78-F1-49
- Encapsular los paquetes en tramas.
- Arbitrar el acceso al medio físico.
- Detectar errores en los datos recibidos (y corrección en algunos casos).





Ángel M. Gamaza

-Proporcionar una entrega confiable (esta función sólo la tienen algunas tecnologías como Wi-Fi).

-Controlar el flujo de datos para adaptarse a la capacidad del medio.

-Aislar las capas superiores de la tecnología de red utilizada.

Muchos servicios proporcionados por la capa de enlace (CAPA 2) tienen un fuerte paralelismo con los servicios proporcionados por la capa de transporte (CAPA 4).

-Las dos capas pueden proporcionar entrega confiable.

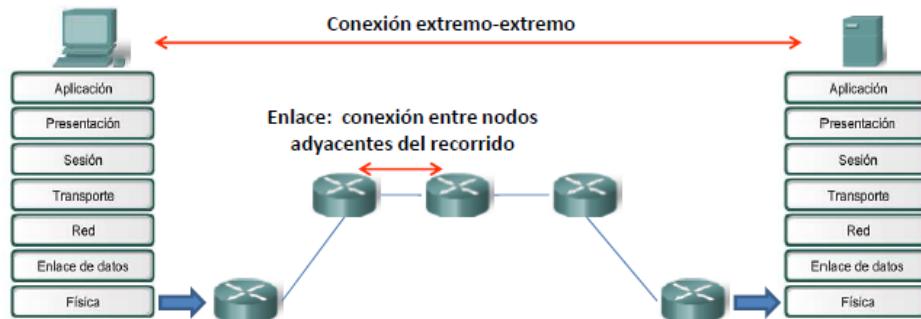
-Las dos capas pueden proporcionar detección de errores.

-Las dos capas pueden proporcionar control de flujo.

DIFERENCIA:

-La capa de transporte (capa 4) proporciona estos servicios a nivel de conexión extremo-extremo.

-La capa de enlace (capa 2) proporciona estos servicios a nivel de enlace.

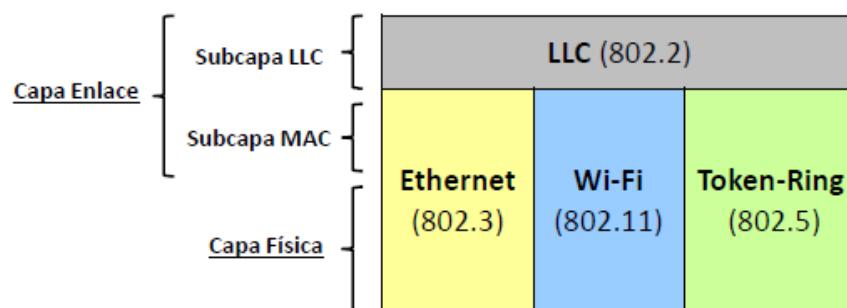


Subcapas de la capa de enlace

La capa de enlace se divide en dos subcapas:

-**Subcapa LLC (IEEE 802.2)**: Se encarga principalmente de aislar las capas superiores de la tecnología de red utilizada.

-**Subcapa MAC (IEEE 802.3, 802.11, 802.5, etc.)**: Se encarga prácticamente de las demás funciones de la capa de enlace.



Direccionamiento físico

Cada dispositivo de capa 2 tiene una dirección física única que lo identifica.

En las tecnologías LAN, como Ethernet, Wi-Fi y Token-Ring, la dirección física se denomina dirección de Control de Acceso al Medio (dirección MAC).

Características de la MAC:

- Tiene 48 bits: A3-47-1C-30-F1-49

- Los 24 bits más significativos son asignados por IEEE e identifican el fabricante (este identificador es el OUI -organizationally unique identifier-).

- Los 24 bits menos significativos identifican el dispositivo dentro del fabricante.

- Se graba en el hardware del dispositivo durante su fabricación.

- Tienen una estructura plana (no son jerárquicas como las IPs).

Un switch posee una dirección MAC.

Cuando un dispositivo quiere comunicarse con todos los dispositivos de la subred (o red si no hay subredes), la dirección MAC destino debe ser FF-FF-FF-FF-FF-FF (dirección MAC de difusión).

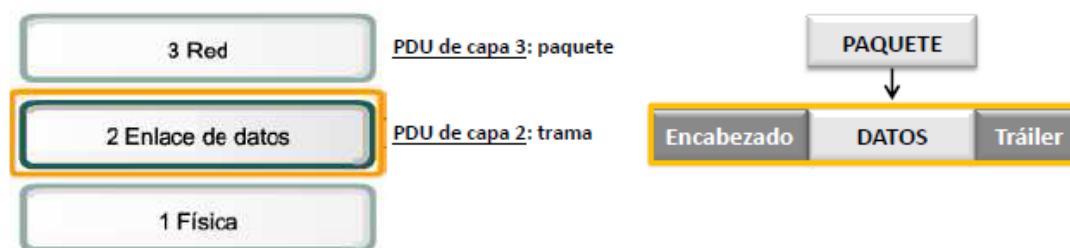
Formato de la Trama

La trama tiene tres partes:

- Encabezado.

- Datos: es la PDU de capa 3 (paquete).

- Tráiler.



Los campos del encabezado, del tráiler y la longitud de la trama varían de una tecnología a otra.

Tecnología <u>Ethernet</u>	Preámbulo	MAC destino	MAC origen	Tipo	Datos	FCS			
	8 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes			
Tecnología <u>Wi-Fi</u>	Control	Duración	MAC destino	MAC origen	RA	TA	Secuencia	Datos	FCS
	2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	6 bytes	2 bytes	0-2312 bytes	4 bytes
Tecnología <u>PPP</u>	Señalización		Dirección	Control	Protocolo	Datos	FCS		
	1 byte	1 byte	1 byte	2 bytes	variable	2 ó 4 bytes			

Cuando en la ruta hay que saltar de una tecnología de red a otra, el dispositivo intermediario, generalmente un router, transforma las tramas de un formato a otro.

Formato de la trama:

-**Tipo** (campo insertado por la subcapa LLC): indica qué protocolo de la capa de red recibirá los datos después de la desencapsulación. Un host puede soportar múltiples protocolos de red: IP, IPX, etc.

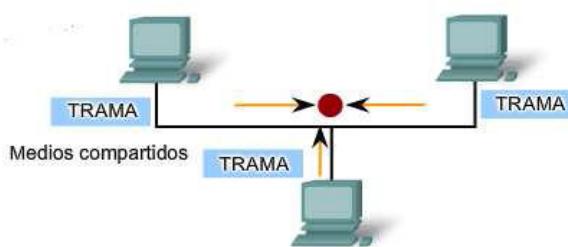
-**Datos**: contiene la PDU de capa 3 (paquete). La unidad de transferencia máxima (MTU) de Ethernet es 1500 bytes. Si el paquete supera los 1500 bytes, se fragmentará en paquetes más pequeños en la capa de red, para que lleguen a la capa de enlace paquetes menores de 1500 bytes. Si el paquete tiene menos de 46 bytes, se incluirán bits de relleno en la trama.

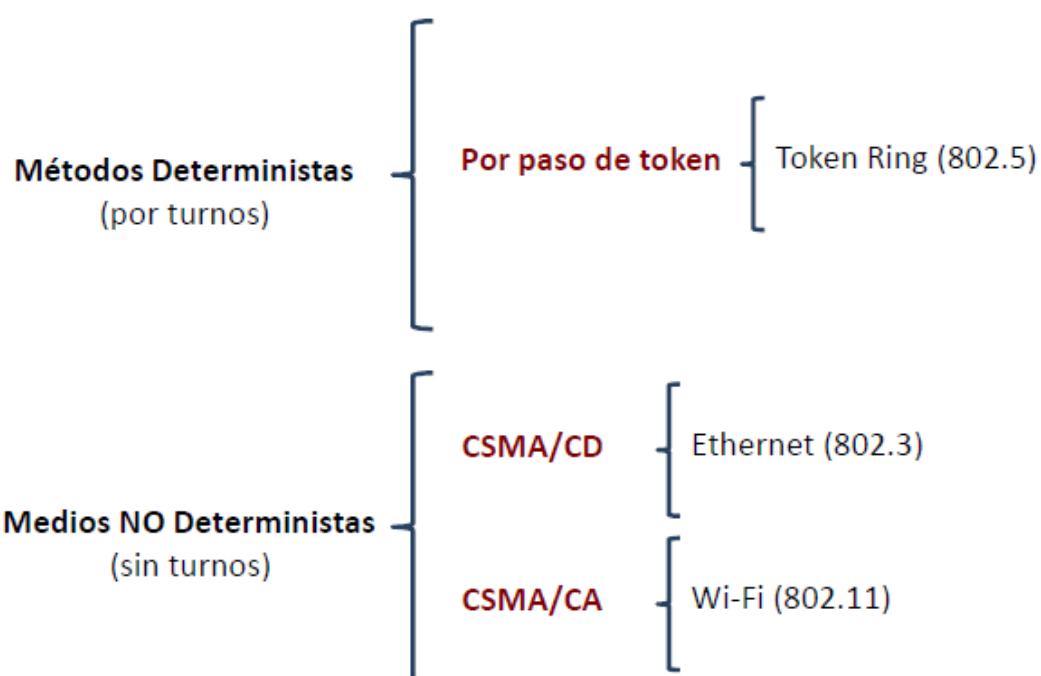
-**FCS** (secuencia de verificación de trama): valor utilizado para detectar errores en la trama.

Control de acceso al medio

Es la regulación para acceder al medio de los dispositivos.

Si no se regula el acceso al medio y varios dispositivos quieren transmitir al mismo tiempo se producirán muchas colisiones (choques de tramas), las cuales ocasionan tramas dañadas que deben volver a enviarse.





Paso por token

Utilizado en la tecnología de red Token-Ring.

-El acceso al medio es por turnos.

-Por la red circula un paquete especial llamado token (testigo), que irá pasando de un dispositivo a otro.

-Cuando un dispositivo recibe el token, significa que es su turno y podrá transmitir. Si no desea transmitir, debe pasar el token al siguiente dispositivo en la red.

Ventajas y desventajas:

-No hay colisiones.

-Puede ser ineficiente porque un dispositivo tiene que esperar su turno antes de poder utilizar el medio.

CSMA/CD

Utilizado en la tecnología de red Ethernet.

-**CS** (detección de portadora): Cuando un dispositivo quiere enviar datos, primero debe comprobar si el medio está ocupado. Si no está ocupado, transmite.

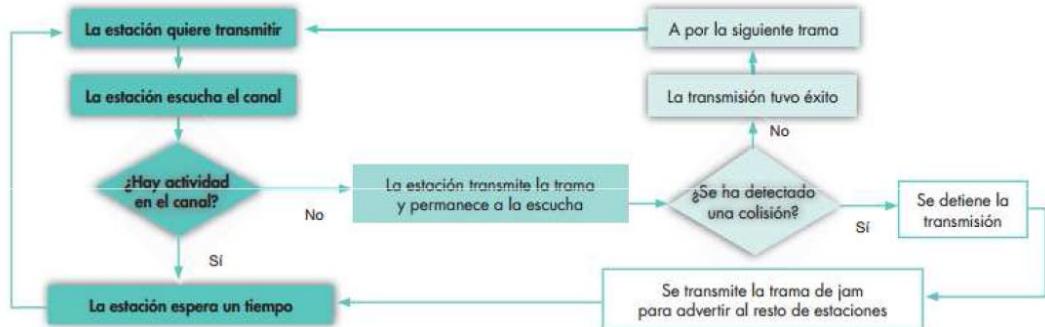
-**CD** (detección de colisión): Durante la transmisión, el dispositivo sigue "escuchando el medio" por si se produce una colisión.

Si se produce una colisión,

1. Se advierte al resto de equipos.

2. Los equipos esperan un tiempo aleatorio para volver a transmitir.

¿Cómo pueden los dispositivos detectar una colisión? Pueden detectarla porque la amplitud de la señal aumenta.



CSMA/CA

Utilizado en la tecnología de red Wi-Fi.

-**CA (anulación de colisión):** En los medios inalámbricos también se pueden producir colisiones, pero no existe ningún método que permita detectarlas. Ante este problema, el receptor está obligado a confirmar las tramas que recibe con acuses de recibo (ACK).

Detección de errores

La técnica utilizada es CRC (código de comprobación de redundancia cíclica), basada en aritmética polinómica y aritmética módulo 2.

1. El dispositivo emisor calcula el valor CRC sobre los bits de la trama y lo introduce en el campo FCS del tráiler.
2. Cuando la trama llega al dispositivo receptor, el nodo receptor calcula su propio CRC de la trama.
3. El nodo receptor compara los dos valores CRC (CRC calculado por él y CRC del tráiler).
 - Si son iguales, no hay error y envía los datos de la trama (paquete) a la capa 3.
 - Si son distintos, hay error y se descarta la trama.

Los errores de bits en la transmisión se producen principalmente por ruido o atenuación de la señal.

Errores no detectados: Existe siempre la pequeña posibilidad de que, aún siendo iguales los dos valores CRC (caso: que los errores en los bits se cancelen entre sí cuando se calcula el CRC), la trama esté realmente dañada. En este caso, serán los protocolos de capas superiores los que solucionen este problema.

Tema 3

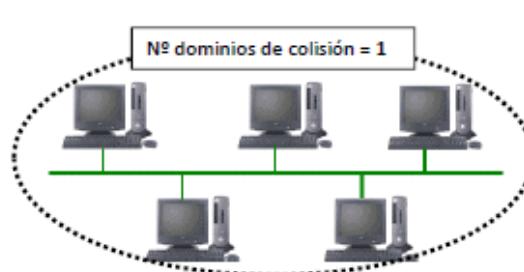
Capa de enlace 2^a Parte: Modo de operación de un Switch

Dominio de colisión

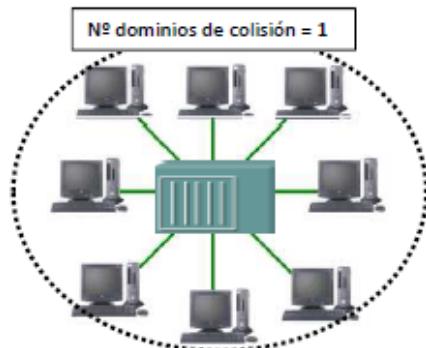
Un dominio de colisión es un segmento (sección) de red donde pueden producirse colisiones.

Las colisiones hacen que la red sea poco eficiente. Cada vez que se produce una colisión, todas las transmisiones se detienen un tiempo aleatorio.

IMPORTANTE: Un administrador de red debe saber identificar los dominios de colisión.



Ethernet topología bus utilizando únicamente un cable coaxial para interconectar los equipos (antiguas Ethernet).



Ethernet topología estrella utilizando como dispositivo de interconexión un hub. Cuando un hub (dispositivo de capa 1) recibe tramas por un puerto, las envía por todos los puertos excepto por el de origen.

Cuantos menos dispositivos tenga un dominio de colisión MEJOR.

- Menor probabilidad de colisionar.
- Menor congestión de la red.
- Mayor posibilidad de encontrar el medio libre para transmitir.

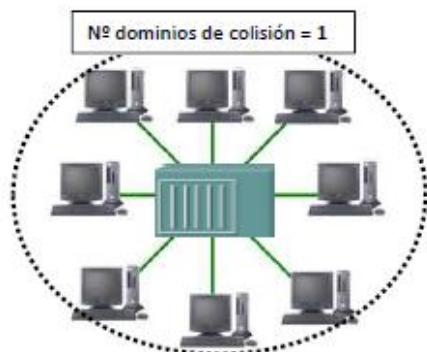
El objetivo es dividir (SEGMENTAR) un dominio de colisión en otros más pequeños.

Para segmentar un dominio de colisión hay que utilizar switches (dispositivos de capa 2) o routers (dispositivos de capa 3).

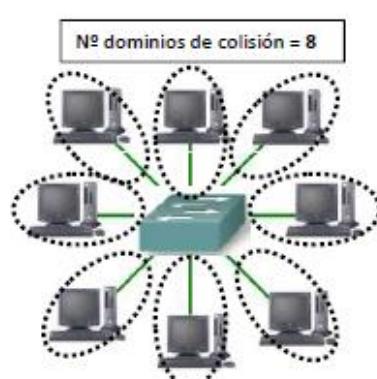
Estos dispositivos son más “inteligentes” que un hub. Antes de enviar la trama, averiguan en qué puerto está el equipo destino. Sólo enviarán la trama por el puerto correcto, reduciendo el tráfico en la red y el número de colisiones.

Los dispositivos de capa 3 (routers) realizan más funciones que la de dividir un dominio de colisión y su modo de operación es diferente a un switch.

Una red conmutada (red que utiliza switches en lugar de hubs) permite varias transmisiones simultáneas sin que colisionen las tramas.



Este esquema no permite transmisiones simultáneas, cuando un dispositivo está transmitiendo todos los demás tienen que esperar.



En este esquema, cuando un dispositivo va a transmitir, se crea una conexión punto a punto con el puerto destino.

Este esquema sí permite transmisiones simultáneas porque en el switch pueden coexistir diferentes conexiones punto a punto.

Modo de operación de un Switch

El switch contiene una tabla llamada **tabla CAM** (Content Addressable Memory) que registra en qué puerto se localiza cada equipo de la subred o red (si no hay subredes).

Dirección física	Puerto
00-00-AA-00-00-88	Fa0/1
00-00-FF-00-00-33	Fa0/1
00-00-FF-00-00-44	Fa0/2
B8-00-FF-AA-00-55	Fa0/3
...	...

Tabla CAM del switch

Modo de operación del Switch

Paso 1

Se enciende el Switch.

Cuando se enciende un switch, la tabla CAM está vacía.

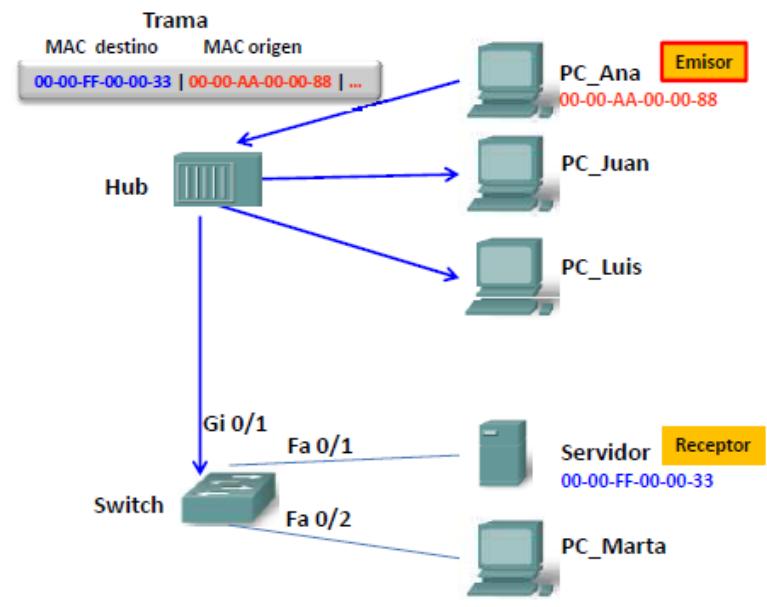
Paso 2

PC_Ana envía una trama al servidor.

Cuando el hub recibe la trama, la envía por todos sus puertos, excepto por el origen.

Tabla CAM del switch

Dirección física	Puerto



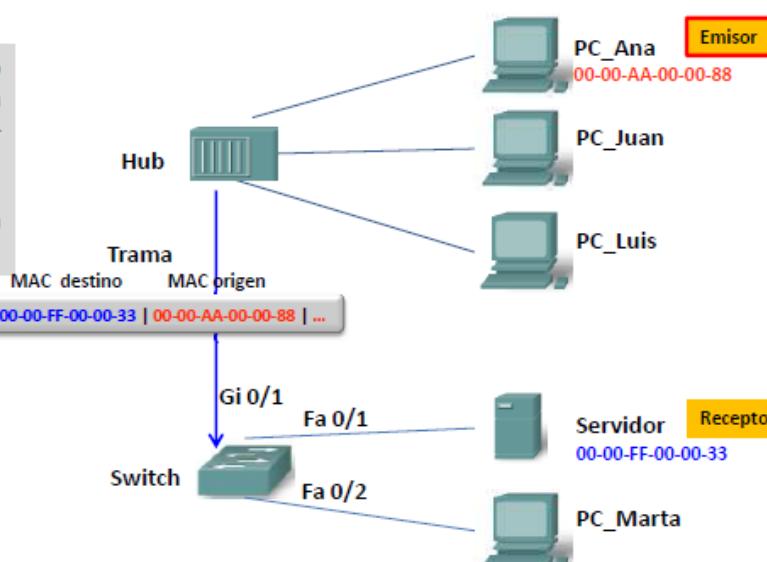
Paso 3

El switch recibe la trama por el puerto Gi0/1. Con este hecho, el switch acaba de **aprender** que la mac 00-00-AA-00-00-88 está en el puerto Gi0/1.

El switch añade lo aprendido a su tabla CAM.

Tabla CAM del switch

Dirección física	Puerto
00-00-AA-00-00-88	Gi0/1



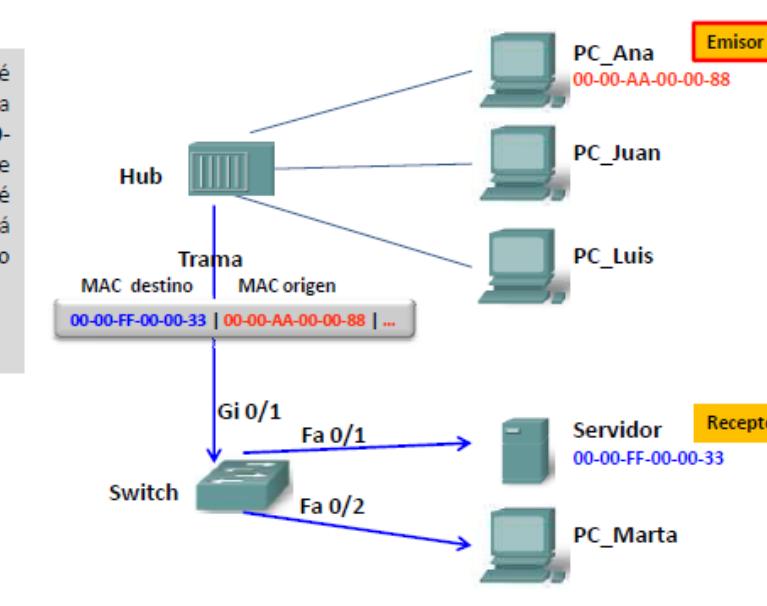
Paso 4

El switch tiene que decidir por qué puerto enviar la trama. Para ello, busca en su tabla CAM la MAC destino 00-00-FF-00-00-33. Como no la tiene registrada todavía, no sabe por qué puerto enviar la trama. Así que enviará la trama por todos los puertos, excepto el de origen (**inundación**).

Finalmente, el servidor recibe la trama.

Tabla CAM del switch

Dirección física	Puerto
00-00-AA-00-00-88	Gi0/1





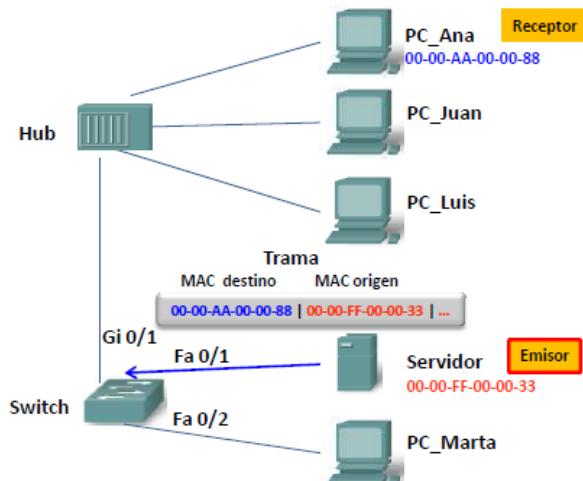
Paso 5

Ahora es el servidor el que envía una trama a PC_Ana. Cuando el switch recibe la trama por el puerto Fa0/1, **aprende** que la mac **00-00-FF-00-00-33** está en ese puerto.

El switch registra lo aprendido en su tabla CAM.

Tabla CAM del switch

Dirección física	Puerto
00-00-AA-00-00-88	Gi0/1
00-00-FF-00-00-33	Fa0/1



Paso 6

El switch tiene que decidir por qué puerto enviar la trama. Para ello, busca en su tabla CAM la MAC destino **00-00-AA-00-00-88**. Como la tiene registrada, sabe que la trama tiene que enviarla por el puerto Gi0/1 (esta vez no hay inundación).

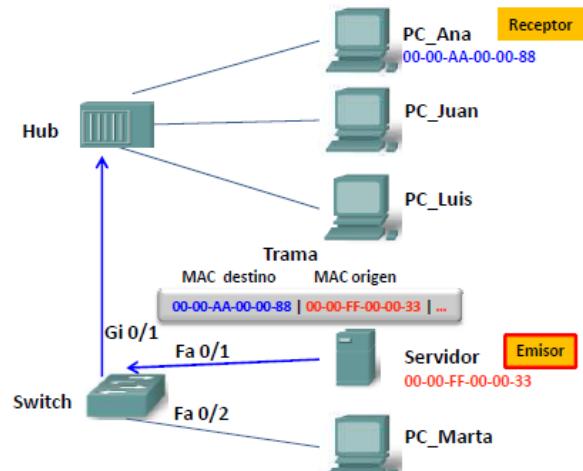


Tabla CAM del switch

Dirección física	Puerto
00-00-AA-00-00-88	Gi0/1
00-00-FF-00-00-33	Fa0/1

Paso 7

Cuando el hub recibe la trama, la envía por todos sus puertos, excepto por el origen.

Finalmente, PC_Ana recibe la trama.

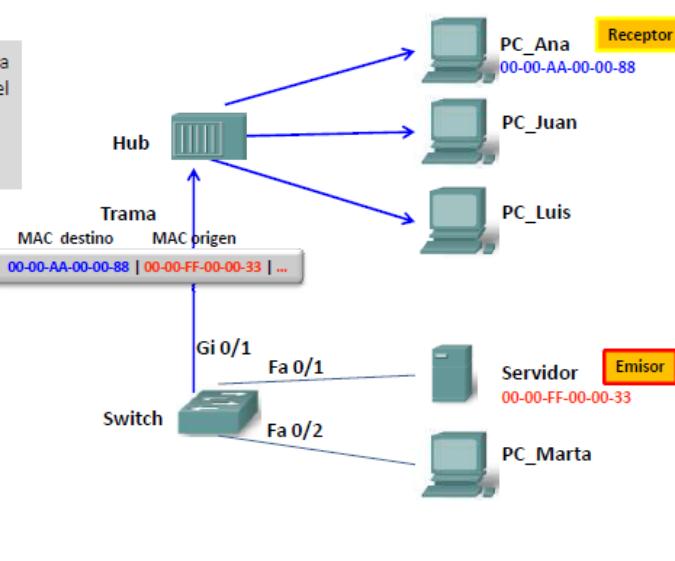


Tabla CAM del switch

Dirección física	Puerto
00-00-AA-00-00-88	Gi0/1
00-00-FF-00-00-33	Fa0/1

PoE (Power over Ethernet)

La **alimentación a través de Ethernet** es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar.

Permite que la **alimentación eléctrica** se suministre a un **dispositivo de red** (switch, punto de acceso, router, teléfono o cámara IP, etc) usando el mismo **cable** que se utiliza para la **conexión de red**.

Elimina la necesidad de utilizar **tomas de corriente** en las ubicaciones del **dispositivo alimentado** y permite una aplicación más sencilla de los sistemas de **alimentación ininterrumpida (SAI)** para garantizar un funcionamiento las 24 horas del día, 7 días a la semana.

Se regula en una norma denominada IEEE 802.3af.

Actualmente existen **switches** o **hubs** que soportan esta tecnología.

Para implementar PoE en una red que no dispone de dispositivos que la soporten directamente se usa una **unidad base** (con conectores RJ45 de entrada y de salida) con un **adaptador de alimentación** para recoger la electricidad y una **unidad terminal** (también con conectores RJ45) con un **cable de alimentación** para que el dispositivo final obtenga la energía necesaria para su funcionamiento.



Red de área local inalámbrica creada mediante un punto de acceso alimentado por PoE.

Tema 4

Capa de red 1^a Parte: Generalidades sobre IPv4

Funciones principales

- Direccionamiento lógico.
- Encapsular los segmentos en paquetes.
- Establecer comunicación con otras redes.
- Establecer la ruta (enrutar) por la que se enviarán los paquetes.

Dispositivos de la capa de red

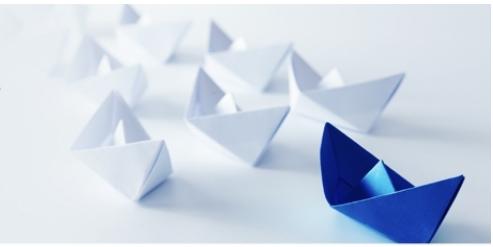


Protocolos de la capa de red



Protocolo IPv6

Es otra versión del protocolo de IP que ha sido diseñada para reemplazar a la IPv4 que actualmente está implementada en la mayoría de los dispositivos que tienen conexión a internet y está empezando a restringir el crecimiento de Internet debido a su número de direcciones sobre todo en países muy poblados como China o India.



Ángel M. Gamaza

-**IPv4** tiene 232 direcciones de host, unas 4.294.967.296 direcciones, un número inadecuado para dar una dirección a cada persona del planeta.

-**IPv6**, en cambio, tiene 2128 direcciones de host, que son unas 340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones, cerca de 670 mil billones de direcciones por cada milímetro cuadrado de La Tierra.

Ejemplo de IPv6:

2002:0000:0000:0000:0000:7ef6:ba01

Las IPv6 se escriben en grupos de 4 dígitos en hexadecimal separados por dos puntos. Para simplificar, si hay un grupo de cuatro ceros, podemos simplificarlo dejando un cero solamente:

2002:0:0:0:0:7ef6:ba01

Y si además hay varios grupos seguidos podemos simplificarlo poniéndolo así:

2002::7ef6:ba01

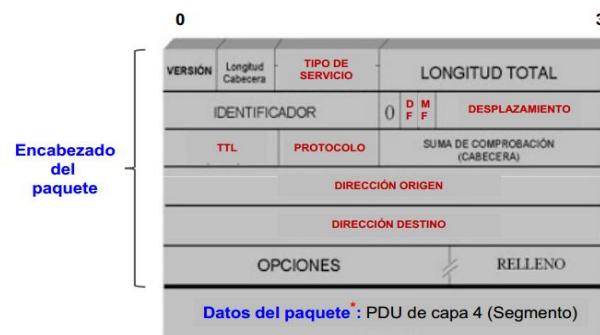
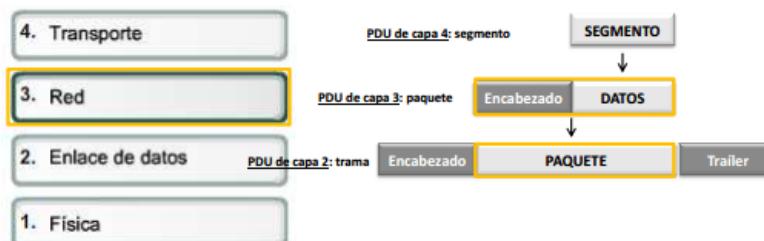
Este método no vale si hay dos grupos de ceros separados ya que podría dar lugar a equivoco a la hora de reconocer la IP.

Formato de un paquete IPv4

El paquete tiene dos partes:

-**Encabezado.**

-**Datos:** generalmente es la PDU de capa 4.



* Generalmente es la PDU de capa 4 (segmento), pero no siempre es así, por ejemplo, podría ser un mensaje ICMP.

La capa de red opera independientemente de la tecnología de red, el transporte de paquetes IP no está limitado a una tecnología en particular (los paquetes pueden circular por diferentes tecnologías indistintamente).

Es responsabilidad de la capa de enlace, tomar un paquete y prepararlo para su transmisión por una tecnología específica.

Existe una característica de la capa de enlace que sí tiene que tener en cuenta la capa de red, la Unidad Máxima de Transferencia (MTU). El tamaño de los paquetes nunca debe superar la MTU establecida por la capa de enlace. Si un paquete tiene una longitud superior a la MTU de la tecnología de red por la que va circular, el router se verá obligado a fragmentarlo.

Señalizador de No Fragmentar (DF)

DF = 1 → No se permite la fragmentación del paquete. En este caso, si un router necesitase fragmentar el paquete, no podría y tendría que descartar ese paquete.

DF = 0 → El paquete puede ser fragmentado si el router lo requiere.

Señalizador de Más Fragmentos (MF)

Si **MF = 1** significa que no es el último fragmento de un paquete. El host receptor analiza el campo Desp. para ver dónde ha de colocar este fragmento en el paquete reconstruido.

Si **MF = 0** y **Desp ≠ 0** significa que es el último fragmento del paquete. El host receptor coloca ese fragmento como la última parte del paquete reconstruido.

Si **MF = 0** y **Desp = 0** significa que es un paquete NO fragmentado.

Desplazamiento de fragmentos (Desp)

Un router tiene que fragmentar un paquete cuando éste va a pasar a una tecnología de red que tiene una MTU menor (longitud máxima de la trama constituye la MTU de una tecnología de red). Cuando se produce una fragmentación, el host destino utiliza los campos Desp y MF para reconstruir el paquete. El campo Desp identifica el orden de ese fragmento.

Tipo de servicio (TOS)

Define la prioridad del paquete. Este valor permite aplicar un mecanismo de Calidad del Servicio (QoS) a paquetes de alta prioridad, como aquéllos que son de telefonía IP. El router puede ser configurado para enviar primero los paquetes que tengan una prioridad mayor.

Tiempo de vida (TTL) -8 bits

Indica el número máximo de saltos que puede dar un paquete. Si el TTL es **x**, significa que como máximo podrá dar **x** saltos. Cada vez que el paquete da un salto, es decir, que pasa por un router, el TTL se decrementa en una unidad. Si el TTL llega a valer 0 en un salto, ese router quitará el paquete de circulación. Este mecanismo sirve para evitar que los paquetes circulen indefinidamente por las redes cuando no encuentran el destino.

Protocolo

Indica el tipo de contenido del campo datos del paquete. Por ejemplo:

Si protocolo = 1 entonces datos = mensaje ICMP

Si protocolo = 6 entonces datos = segmento TCP

Si protocolo = 17 entonces datos = segmento UDP

Interfaces de un router

Un **router** puede tener interfaces (**puertos**) de diferentes tecnologías (Ethernet, DSL, etc).

Cada interfaz pertenece a una subred/red diferente y funciona como puerta de enlace (**gateway**) de los hosts de esa subred/red.

A cada interfaz hay que asignarle una IP de su subred/red.

Los **switches** y **puntos de acceso** no requieren direcciones IP para funcionar. Pero, si queremos acceder a estos dispositivos vía telnet, entonces sí que hay que asignarles una IP.

Asignación de direcciones IP

Asignación estática

Realizada por el administrador de red, el cual configura en el host la dirección IP, la máscara, la puerta de enlace y los servidores DNS.

Es recomendable, incluso necesario, realizar la asignación estática en:

-**Puerta de enlace** (normalmente, se asigna a la puerta de enlace la dirección más baja o la más alta de la red).

-**Impresoras de red.**

-**Servidores.**

-**Cualquier dispositivo de red que requiera una dirección predecible.**

Asignación dinámica

Realizada por un servidor **DHCP** (Dynamic Host Configuration Protocol). Este servidor asignará automáticamente a los hosts de la red: dirección IP, máscara, puerta de enlace y servidores DNS.

La mayoría de los routers contienen un servidor DHCP. Otra opción, sería instalar el servidor DHCP en cualquier servidor de la organización.

Configuración del servidor DHCP: hay que definir el bloque de direcciones IP (pool de direcciones) que se utilizará para asignar IPs a los hosts de la red. Es necesario excluir del pool de direcciones, las IPs que se vayan a asignar de forma estática.

Clases de redes

	CLASE	1 ^{er} OCTETO (decimal)	1 ^{er} OCTETO (binario)	MÁSCARA
	A	1-126	0XXXXXXX	255.0.0.0
	B	128-191	10XXXXXX	255.255.0.0
	C	192-223	110XXXXX	255.255.255.0
Direcciones Multicast	D	224-239	1110XXXX	255.255.255.255
Direcciones Experimentales *	E	240-255	1111XXXX	255.255.255.255

Direcciones privadas/Direcciones públicas

Sin direcciones privadas, el rápido crecimiento de Internet habría agotado la cantidad actual de direcciones IP.

Direcciones privadas

Son las que se utilizan en las redes internas de organizaciones, empresas y viviendas. Cualquiera puede utilizar estas direcciones en su red interna. Esto implica que distintas redes internas puedan tener las mismas direcciones privadas (no da lugar a conflicto).

PROBLEMA: los paquetes que contienen estas direcciones no pueden circular (enrutarse) por una red pública como Internet.



Ángel M. Gamaza

Direcciones públicas

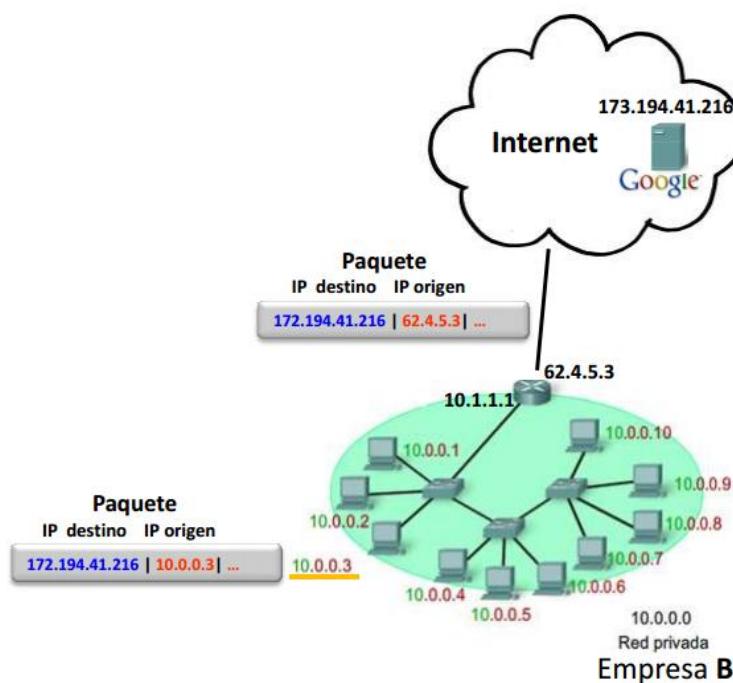
Utilizadas por dispositivos que tienen presencia en Internet, como servidores web, servidores DNS, puerto ADSL de nuestro router, etc.

El espacio de direcciones es gestionado por IANA. En Europa, IANA delega esta función en RIPE. RIPE es un registro regional de internet. <http://www.ripe.net>

Para obtener una IP pública normalmente hay que solicitarla al ISP.

CLASE	1 ^{er} OCTETO (decimal)	1 ^{er} OCTETO (binario)	MÁSCARA	Nº DE HOSTS	DIRECCIONES PRIVADAS (decimal)
A	1-126	0XXXXXXX	255.0.0.0	$2^{24} - 2$	10.x.x.x
B	128-191	10XXXXXX	255.255.0.0	$2^{16} - 2$	172.16.x.x – 172.31.x.x 169.254.x.x
C	192-223	110XXXXX	255.255.255.0	$2^8 - 2$	192.168.x.x

169.254.x.x → Espacio utilizado para las direcciones Link-Local.



PROBLEMA:
Los paquetes que tienen una dirección IP origen privada no pueden circular por Internet.

SOLUCIÓN:
Un router nunca dejará pasar a internet paquetes que tienen una dirección IP origen privada. ¿Entonces? El router convertirá esa dirección IP origen privada en pública gracias al sistema NAT.

Sin NAT un host con dirección IP privada no podría acceder a Internet.

La UCA utilizó una red pública.

-**NAT** (Network Address Translation) mapea una dirección IP privada a una dirección pública. El router asignará a cada dirección IP privada una dirección pública distinta.

-**PAT** (Port Address Translation). Variante de NAT, conocida también como NAT con sobrecarga. También mapea una dirección IP privada a una dirección pública pero, en este caso, el router asigna la misma dirección pública a todas las direcciones privadas de la red (o a un conjunto). PAT utiliza los números de puerto para diferenciar las direcciones privadas.

NAT y PAT pueden funcionar a la vez en el mismo router.

Tipos de comunicaciones

-**Unicast**. Los datos se envían a un único host.

-**Broadcast**. Los datos se envían a todos los hosts de una subred/red.

Broadcast dirigido

Utilizado cuando un dispositivo quiere comunicarse con todos los hosts de una subred/red distinta a la suya.

Dirección IP destino: dirección broadcast de esa subred/red, es decir, dirección cuyo HOST-ID tiene todos los bits a 1.

Por defecto, los routers no reenvían broadcasts dirigidos a otras subredes/redes. Pero pueden configurarse para que sí lo hagan.

Broadcast limitado

Utilizado cuando un dispositivo quiere comunicarse con todos los hosts de su propia subred/red.

Dirección IP destino: 255.255.255.255.

Los routers nunca reenvían broadcasts limitados a otras subredes/redes. Por ello, se dice que un router demarca el dominio de broadcast.

Usos:

-Solicitar una dirección IP utilizando el protocolo DHCP.

-Intercambiar información de enrutamiento por medio de protocolos de enrutamiento.

-**Multicast**. Los datos se envían a un conjunto específico de hosts.

Un grupo multicast está representado por una sola dirección multicast.

Los hosts que desean pertenecer a un **grupo multicast** específico y recibir este tipo de comunicación se denominan clientes multicast. Los clientes multicast usan servicios iniciados por un programa cliente para suscribirse al grupo multicast.

Usos:

- Distribución de audio y video en tiempo real (streaming) a un grupo de hosts.
- Distribución de software, como imágenes de arranque de sistemas operativos.
- Intercambio de información de enrutamiento por medio de protocolos de enrutamiento.

Si la comunicación fuera unicast, la dirección física destino se obtendría haciendo uso del protocolo ARP.

En el caso de una comunicación multicast, no se puede usar ARP y habrá que obtener la dirección física asociada mediante un procedimiento diferente.

Anycast. Los datos se envían a cualquier host de un conjunto determinado, ese host generalmente es el que está más cerca del dispositivo emisor.

Direcciones IP especiales

Existen una serie de direcciones IP especiales que no se pueden asignar a ningún host. Estas son:

- Dirección de broadcast limitada.
- Dirección de broadcast dirigida.
- Dirección de red/subred.
- Dirección Loopback.
- Dirección de ruta predeterminada.
- Dirección Link-Local.

Dirección Loopback

Direcciones loopback: desde 127.0.0.0 hasta 127.255.255.255 (127.x.x.x \equiv 127.0.0.0 /8). Generalmente se utiliza 127.0.0.1.

Es una dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos. Un ping a la dirección de loopback sirve para verificar si la configuración TCP/IP de ese host está funcionando correctamente.

Ruta predeterminada

Direcciones para ruta predeterminada: desde 0.0.0.0 hasta 0.255.255.255 (0.x.x.x \equiv 0.0.0.0 /8). Generalmente sólo se utiliza 0.0.0.0.

Esta dirección es utilizada para definir la ruta por defecto (o predeterminada) en una tabla de enrutamiento.

El router envía los paquetes por la ruta predeterminada cuando la dirección IP destino de los paquetes no concuerda con los destinos de las demás rutas que hay en la tabla de enrutamiento.

Dirección Link-Local

**Direcciones Link-Local: desde 169.254.0.0 hasta 169.254.255.255 (169.254.x.x
≡ 169.254.0.0 /16)**

Función de autoconfiguración (también denominada auto-IP, APIPA o Zeroconf). Si un equipo no tiene asignada una dirección IP y su sistema operativo tiene habilitada esta función, configurará automáticamente una IP Link-Local. El método de asignación es el siguiente:

- 1.** Al equipo se asigna una IP aleatoria del rango Link-Local.
- 2.** El equipo lanza a la red una consulta ARP para asegurarse de que esa IP no está en uso. Si la dirección ya está en uso, se reasigna otra IP.

Los equipos que tienen una dirección Link-Local no tienen acceso a Internet, sólo podrán comunicarse con equipos que están en la misma red, el router nunca dejará pasar estos paquetes.

Possibles usos:

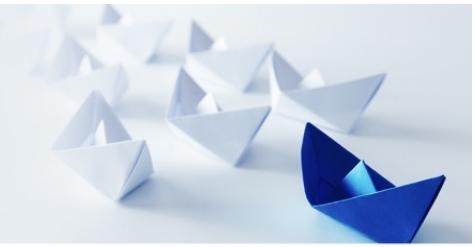
- Conexión punto a punto entre dos PCs.
- Un host no puede contactar con el servidor DHCP para que le proporcione una IP.



INESEM
BUSINESS SCHOOL

Escuela de líderes

Becas | Prácticas | Empleo



Ángel M. Gamaza

Tema 4

Capa de red 2ª Parte: Enrutamiento

Enrutamiento

La función principal de un router es enviar un paquete hacia su destino, para llevar a cabo esta acción el router busca información en su tabla de enrutamiento.

La tabla de enrutamiento almacena información de rutas hacia:

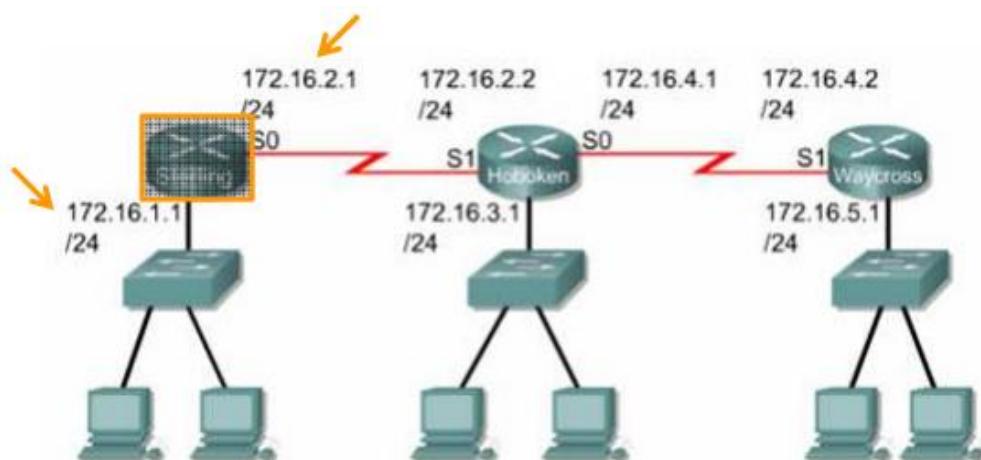
- Redes que están conectadas directamente al router.**
- Redes remotas.**

En la ruta se establece por qué interfaz del router tienen que salir los paquetes para alcanzar su destino.

Redes conectadas directamente

Una red conectada directamente al router es una red que está directamente vinculada a una de las interfaces del router.

Cuando se asigna una dirección IP y una máscara a la interfaz del router, automáticamente se crea una ruta en la tabla de enrutamiento con la dirección de esa subred como destino.



Redes remotas

Una red remota es una red que no está directamente conectada al router. Para llegar a esa red remota, el router tiene que enviar los paquetes a otro router.

Las rutas hacia redes remotas se agregan en la tabla de enrutamiento de dos formas:

- Protocolos de enrutamiento.** Rutas configuradas dinámicamente por protocolos de enrutamiento como RIP, EIGRP, OSPF, etc.

- Rutas estáticas.** Rutas configuradas manualmente por administradores de red.

Tabla de enrutamiento de un router

El comando para visualizar la tabla de enrutamiento es **Router# show ip route**.

```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      + - candidate default, U - per-user static route, o - ODR
      p - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/30 is subnetted, 4 subnets
R        10.10.10.0 [120/1] via 10.10.10.5, 00:00:12, Serial3/0
C        10.10.10.4 is directly connected, Serial3/0
C        10.10.10.8 is directly connected, Serial2/0
R        10.10.10.12 [120/2] via 10.10.10.5, 00:00:12, Serial3/0
R        192.168.10.0/24 [120/2] via 10.10.10.5, 00:00:12, Serial3/0
R        192.168.20.0/24 [120/1] via 10.10.10.5, 00:00:12, Serial3/0
C        192.168.30.0/25 is subnetted, 1 subnets
          192.168.30.0 is directly connected, FastEthernet1/0
C        192.168.40.0/25 is subnetted, 1 subnets
          192.168.40.0 is directly connected, FastEthernet0/0
Router#
```

-Los datos de esta tabla no se corresponden con la topología de la diapositiva anterior-

Métrica

La métrica es un valor de la ruta que mide la dificultad (coste) de alcanzar el destino. Cada protocolo de enrutamiento utiliza su propia fórmula para calcular la métrica.

PROTOCOLO DE ENRUTAMIENTO	PARÁMETROS QUE INTERVIENEN EN EL CÁLCULO DE LA MÉTRICA
RIP	<ul style="list-style-type: none"> ▪ Número de saltos
OSPF	<ul style="list-style-type: none"> ▪ Ancho de banda
EIGRP*	<ul style="list-style-type: none"> ▪ Ancho de banda ▪ Retardo ▪ Carga ▪ Confiabilidad

*Protocolo propietario de Cisco, no se encuentra disponible en routers de otras marcas. Es el que posee una métrica más precisa.

Si un router aprende más de una ruta hacia el mismo destino, deberá evaluar cuál es la mejor y registrará esa ruta en la tabla de enrutamiento. El router considera que la mejor ruta es la que tiene la métrica más baja.

EJEMPLO: Un router que utiliza el protocolo RIP aprende dos rutas hacia el mismo destino:

-Ruta A: métrica = 2

-Ruta B: métrica = 7

La Ruta A tiene la métrica más baja, por tanto, esta será la que el router registre en su tabla de enrutamiento.

Puede ocurrir que un router esté utilizando varios protocolos de enrutamiento a la vez (por ejemplo, RIP y OSPF).

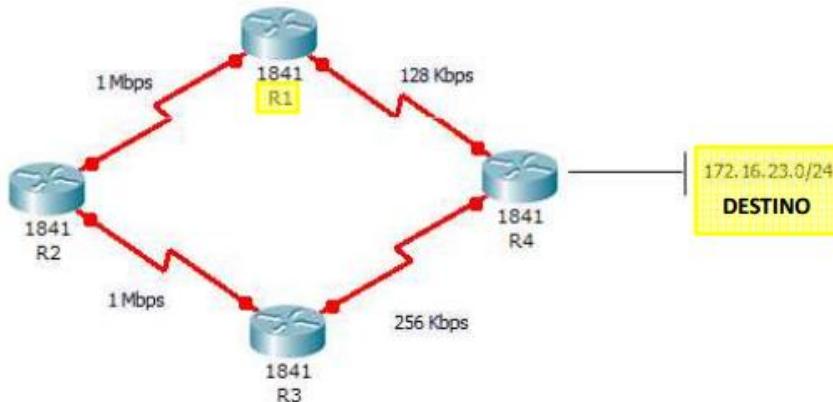
Si un router tiene que comparar varias rutas que han sido calculadas con diferentes protocolos, NO se puede utilizar la métrica como medida comparativa porque los valores pueden ser muy dispares.

PROTOCOLO DE ENRUTAMIENTO	PARÁMETROS QUE INTERVIENEN EN EL CÁLCULO DE LA MÉTRICA	VALOR MÁXIMO (en decimal)
RIP	<ul style="list-style-type: none"> ▪ Número de saltos 	15
OSPF	<ul style="list-style-type: none"> ▪ Ancho de banda 	65.535
EIGRP	<ul style="list-style-type: none"> ▪ Ancho de banda ▪ Retardo ▪ Carga ▪ Confiabilidad 	4.294.967.295



Ángel M. Gamaza

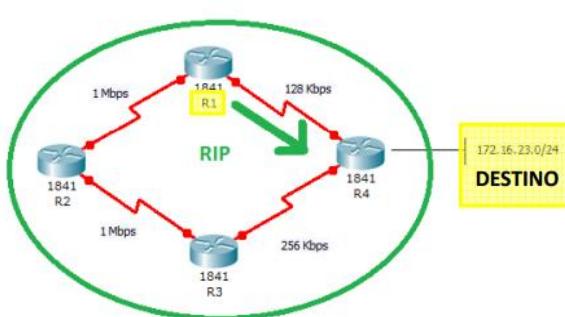
En este ejemplo, R1 debe determinar cuál es la mejor ruta hacia la subred 172.16.23.0/24. Este router utiliza los protocolos RIP y OSPF.



Dos alternativas para llegar al destino:

Ruta 1: R1-R4

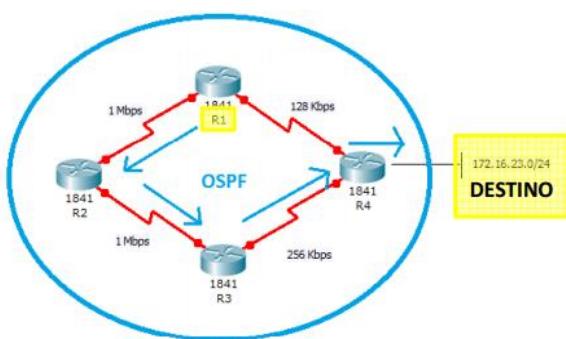
Ruta 2: R1-R2-R3-R4



Ruta 1: un salto

Ruta 2: tres saltos

Ruta seleccionada por RIP: ruta 1 con **MÉTRICA = 1**



Ruta 1: 782

Ruta 2: 591

Ruta seleccionada por OSPF: ruta 2 con **MÉTRICA = 591**

Esto no significa que la ruta calculada por RIP sea mejor que la calculada por OSPF.

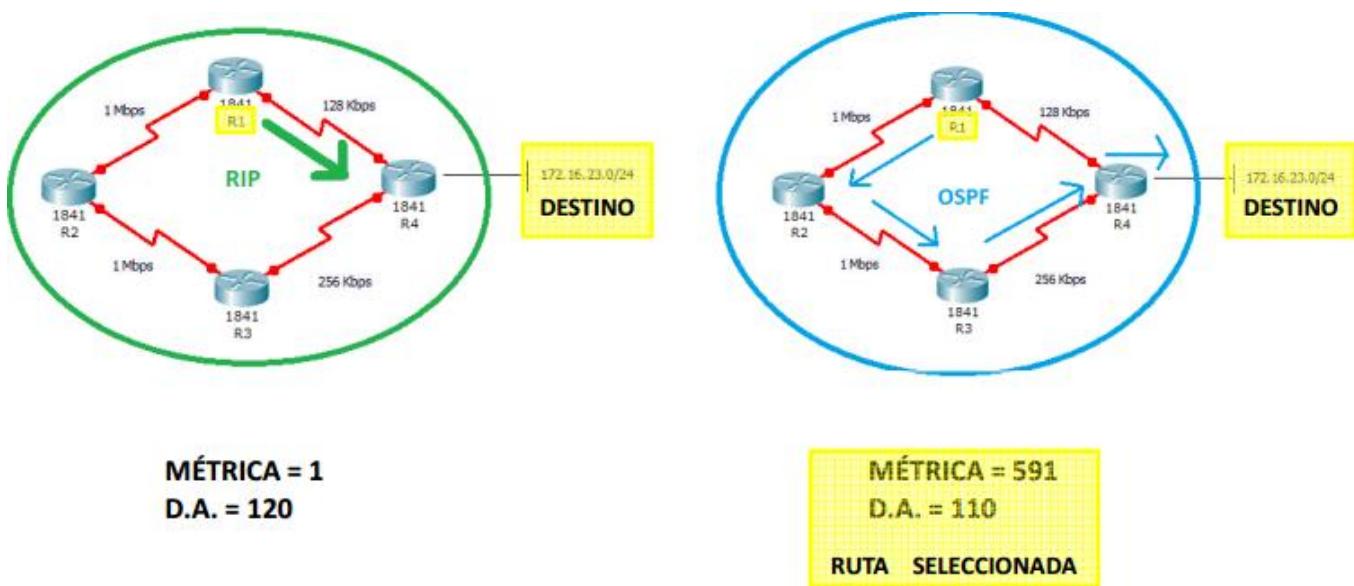
Distancia administrativa

Para resolver la comparativa anterior, el router utiliza la distancia administrativa, que es un valor de 8 bits (0- 255) que mide la confiabilidad de una métrica.

Los valores por defecto son:

ENRUTAMIENTO	D.A.
Estático	1
EIGRP	90
OSPF	110
RIP	120

Si hay varias rutas hacia un destino calculadas con diferentes protocolos, el router seleccionará la ruta que tenga menor distancia administrativa.



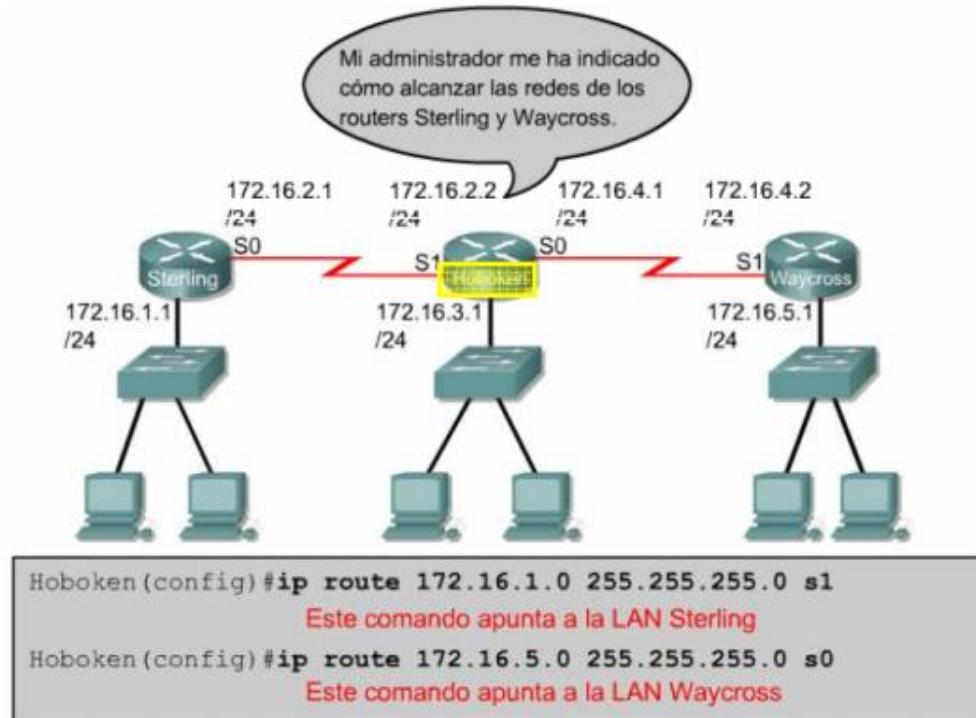
Conclusiones:

- Si las rutas a comparar han sido calculadas con el **mismo protocolo** de enrutamiento, el router utilizará la **MÉTRICA** para elegir la mejor ruta.
- Si las rutas a comparar han sido calculadas con **distintos protocolos** de enrutamiento, el router utilizará la **DISTANCIA ADMISNITRATIVA** para elegir la mejor ruta.

Enrutamiento estático

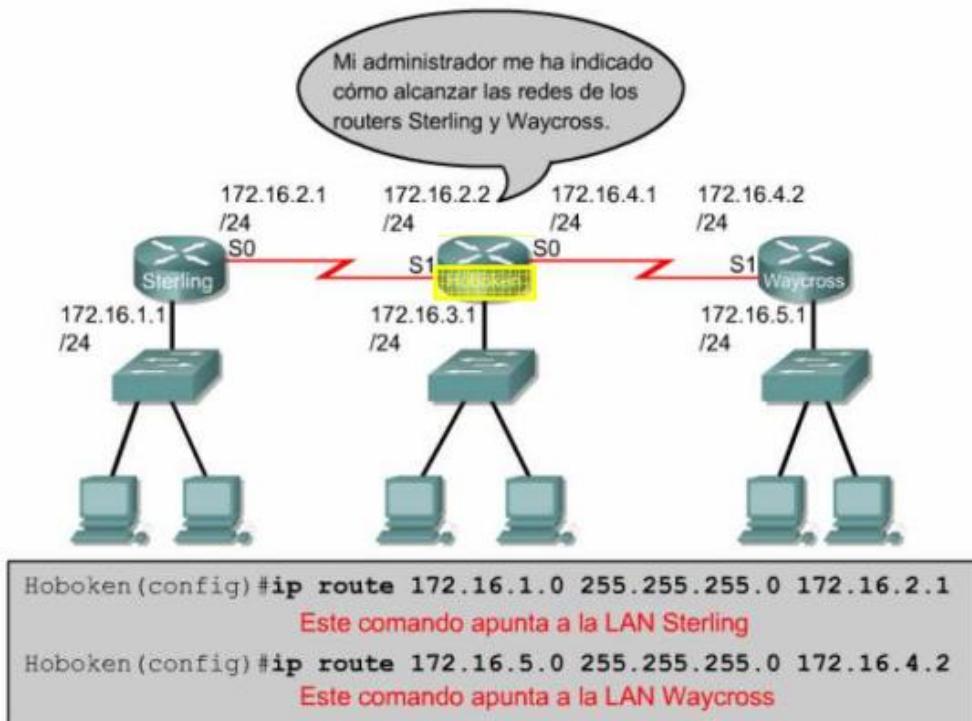
Una ruta estática es una ruta que introduce manualmente el administrador de red utilizando el comando:

```
Router(config)# ip route <dirección_red> <máscara> <interfaz>
```



Otra opción, es poner la dirección del siguiente salto en lugar del nombre de la interfaz:

```
Router(config)# ip route <dirección_red> <máscara> <dirección_salto>
```



La D.A. por defecto de una ruta estática es 1. Si queremos introducir una ruta estática que tenga una D.A. diferente hay que especificar ese valor al introducirla:

```
Router(config)# ip route 172.16.5.0 255.255.255.0 172.16.4.2 95 → D.A.
```

A veces, las rutas estáticas se utilizan como **rutas de respaldo**, una ruta que sólo se utilice cuando falle la ruta dinámica.

Ruta por defecto

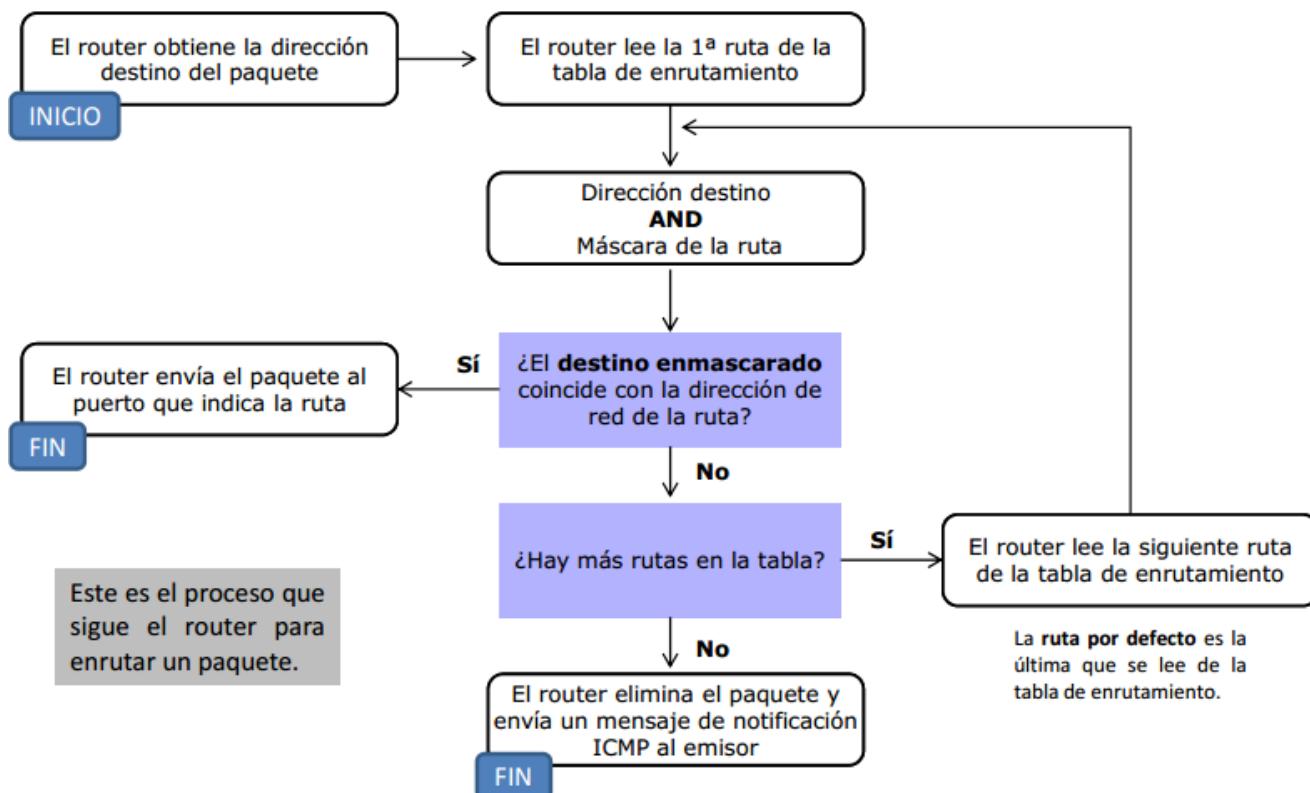
La ruta por defecto se usa para enviar paquetes a destinos que no coinciden con ninguna ruta de la tabla de enrutamiento.

Generalmente, los routers están configurados con una ruta por defecto para el tráfico que se dirige a Internet.

Para definirla, introducir cualquiera de estos dos comandos:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 interfaz
Router(config)# ip route 0.0.0.0 0.0.0.0 dirección_salto
```

Determinación de ruta





Ángel M. Gamaza

Tabla de enrutamiento de un host

Para ver la tabla de rutas de un host se utiliza el comando **route print**.

IPv4 Tabla de enrutamiento

Rutas activas:					
Destino de red	Máscara de red	Puerta de enlace	Interfaz	Métrica	
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.101	25	
127.0.0.0	255.0.0.0	En vínculo		127.0.0.1	306
127.0.0.1	255.255.255.255	En vínculo		127.0.0.1	306
127.255.255.255	255.255.255.255	En vínculo		127.0.0.1	306
192.168.1.0	255.255.255.0	En vínculo		192.168.1.101	281
192.168.1.101	255.255.255.255	En vínculo		192.168.1.101	281
192.168.1.255	255.255.255.255	En vínculo		192.168.1.101	281
224.0.0.0	240.0.0.0	En vínculo		127.0.0.1	306
224.0.0.0	240.0.0.0	En vínculo		192.168.1.101	281
255.255.255.255	255.255.255.255	En vínculo		127.0.0.1	306
255.255.255.255	255.255.255.255	En vínculo		192.168.1.101	281

Tema 4

Capa de red 3ª Parte: Protocolos ICMP, ARP

Protocolo ICMP

ICMP (Protocolo de Mensajes de Control de Internet) es utilizado por los dispositivos para:

- Notificar errores al dispositivo emisor.
- Suministrar información de control a otros dispositivos.

ICMP es utilizado por el administrador de red para:

- Diagnosticar fallas de red.

Mensajes ICMP

Como ICMP es un protocolo de capa 3, los mensajes ICMP se crean en la capa 3 (no vienen de la capa 4).



Algunos de los tipos de mensajes ICMP:

Tipo	
0	Respuesta de eco
3	Destino inalcanzable
8	Petición de eco
11	Tiempo agotado
12	Problema de parámetros

Tipo	
9	Publicación de router
10	Selección de router
13	Petición de marca horaria
14	Respuesta de marca horaria

Mensajes de control

Mensajes de notificación de errores

Funciones

Notificación de errores

Un paquete puede no llegar a su destino por diversas razones:

- Fallas de hardware.
- Configuración de red inadecuada.
- Información de enrutamiento incorrecta.

La capa de red de un dispositivo utiliza ICMP para notificar de estos errores al emisor. ICMP no corrige el problema, sólo informa.

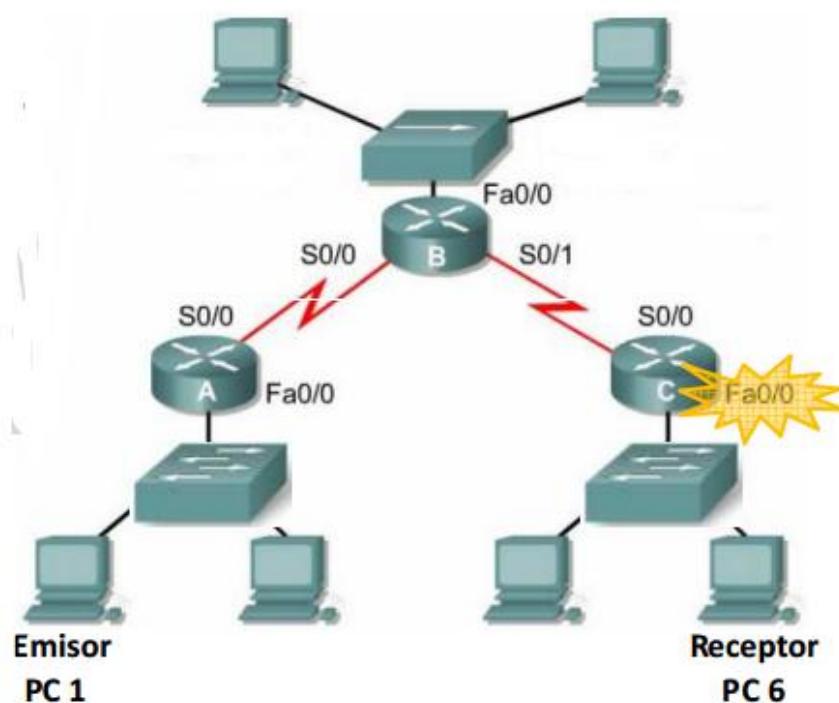
Dado que los paquetes ICMP se transmiten del mismo modo que cualquier otro paquete, están sujetos a las mismas fallas en la entrega.

Ejemplo:

En este ejemplo, PC1 envía un paquete al PC6. Pero hay un problema: la interfaz Fa0/0 del router C ha dejado de funcionar.

El router C utiliza ICMP para enviar una notificación del error a PC1.

El router C sólo notifica del error al emisor del paquete, es decir, a PC1. No notifica ni al router A ni al router B.



Suministrar información de control

Algunos dispositivos utilizan ICMP para suministrar información de control o parámetros de configuración a otros equipos, por ejemplo, información sobre congestión de la red.

Diagnosticar fallas de red

Ping

El protocolo ICMP se puede usar para verificar la conectividad con un destino en particular. Para ello se utiliza el comando ping. Cuando se ejecuta el comando ping se generan cuatro mensajes de petición de eco ICMP.

Si el dispositivo destino recibe los mensajes de petición de eco, crea los mensajes de respuesta de eco hacia el origen de la petición.

Si el emisor recibe la respuesta, se confirma que el dispositivo destino se puede alcanzar (hay conectividad).

A veces, al enviar un mensaje ICMP eco, no se obtiene respuesta. Lo más lógico, sería pensar que el equipo no se encuentra conectado a la red. Sin embargo, puede ocurrir que el equipo sí esté conectado a la red, pero tenga instalado un filtro para no responder a mensajes ICMP.

Tracert

El comando tracert informa del camino exacto que siguen los paquetes de datos desde el equipo origen hasta el equipo destino.

Va mostrando información de cada salto:

- Número del salto.
- Tiempo empleado en ir y volver desde el equipo emisor al salto.
- Dirección IP del salto.

Un salto es un equipo intermediario de capa 3 o superior, normalmente un router.



Ángel M. Gamaza

¿Cómo consigue esto este comando? ENVIANDO paquetes de petición de eco ICMP.

Para averiguar el primer salto de la ruta, el equipo origen envía paquetes eco con TTL igual a 1 (por defecto envía 3 paquetes). Cuando los paquetes eco llegan al primer salto, el TTL se decrementa en una unidad.

Como, ahora, el TTL vale 0, el equipo intermediario envía mensajes ICMP de "Tiempo agotado" al equipo origen. Con este hecho, el equipo origen conoce la IP del primer salto.

Para averiguar el segundo salto de la ruta, el equipo origen envía paquetes eco con TTL igual a 2 (por defecto envía 3 paquetes). Cuando los paquetes eco llegan al primer salto, el TTL se decrementa en una unidad.

Ahora, el TTL vale 1. Cuando llegan al segundo salto, el TTL se vuelve a decrementar en una unidad. Como, ahora, el TTL vale 0, el segundo equipo intermediario envía mensajes ICMP de "Tiempo agotado" al equipo origen. Con este hecho, el equipo origen conoce la IP del segundo salto.

Este es el modo de proceder hasta llegar al equipo destino.

Por defecto se imprimen trazas con un máximo de 30 saltos. Con la opción –h del comando tracert se puede modificar este valor.

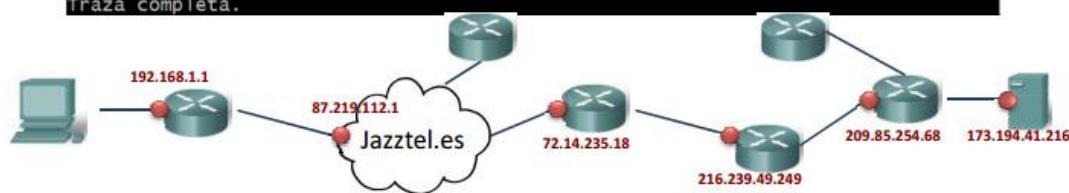
En cada salto se indican los tres tiempos que han empleado los tres paquetes eco en ir y volver desde el origen hasta el equipo intermediario. Un asterisco (*) indica que no se obtuvo respuesta. Se puede utilizar tracert para averiguar en qué lugar se detuvo la conexión.

```
Desplazar C:\windows\system32\cmd.exe
C:\Users\mercedes>tracert www.google.es

Traza a la dirección www.google.es [173.194.41.216]
sobre un máximo de 30 saltos:

 1  2 ms    2 ms    1 ms  COMTREND [192.168.1.1]
 2  36 ms   56 ms   36 ms  1.112.219.87.dynamic.jazztel.es [87.219.112.1]
 3  37 ms   35 ms   37 ms  10.255.19.254
 4  50 ms   50 ms   52 ms  98.217.106.212.static.jazztel.es [212.106.217.98]
]
 5  51 ms   50 ms   50 ms  97.217.106.212.static.jazztel.es [212.106.217.97]
]
 6  47 ms   46 ms   49 ms  2.217.106.212.static.jazztel.es [212.106.217.2]
 7  50 ms   48 ms   48 ms  72.14.235.18
 8  62 ms   59 ms   62 ms  216.239.49.249
 9  61 ms   64 ms   59 ms  209.85.254.68
10  64 ms   66 ms   60 ms  lis01s05-in-f24.le100.net [173.194.41.216]

Traza completa.
```



ANALIZANDO POSIBLES PROBLEMAS en este ejemplo:

Si no hubiese respuesta en el salto 1, el problema lo tenemos en la puerta de enlace de nuestra propia red.

Si la respuesta se pierde entre los saltos 2 y 6, quien está interrumpiendo la conexión es nuestro proveedor de acceso a Internet (en nuestro ejemplo, Jazztel).

En los saltos intermedios intervienen otras redes de tránsito de diferentes operadores. A veces se deja de tener respuesta porque están congestionadas de tráfico. En estos casos es recomendable repetir la orden tracert pasado un tiempo.

Si no hubiese respuesta en el salto 9, el problema está en el servidor de google.

Protocolo ARP

El protocolo ARP (Address Resolution Protocol) se encarga de descubrir la dirección MAC de un dispositivo sabiendo su dirección IP.

Cada host mantiene en la memoria caché de su adaptador de red una tabla de equivalencias entre direcciones IP y direcciones MAC (esta tabla se llama tabla ARP). El contenido de esta tabla se puede ver con el comando arp -a.

Las entradas de la tabla ARP no persisten al reiniciar el sistema.

```
C:\Users\mercedes>arp -a
Interfaz: 10.141.153.174 --- 0xb
          Dirección de Internet      Dirección física      Tipo
          10.141.1.1                2c-6b-f5-3c-40-00    dinámico
          10.141.1.3                aa-30-0a-8d-01-03    dinámico
          10.141.1.4                aa-30-0a-8d-01-04    dinámico
          10.141.2.139              00-e0-4d-0c-a5-9f    dinámico
```

Necesitamos saber la MAC de un equipo para poder identificarlo a nivel físico.

Funcionamiento

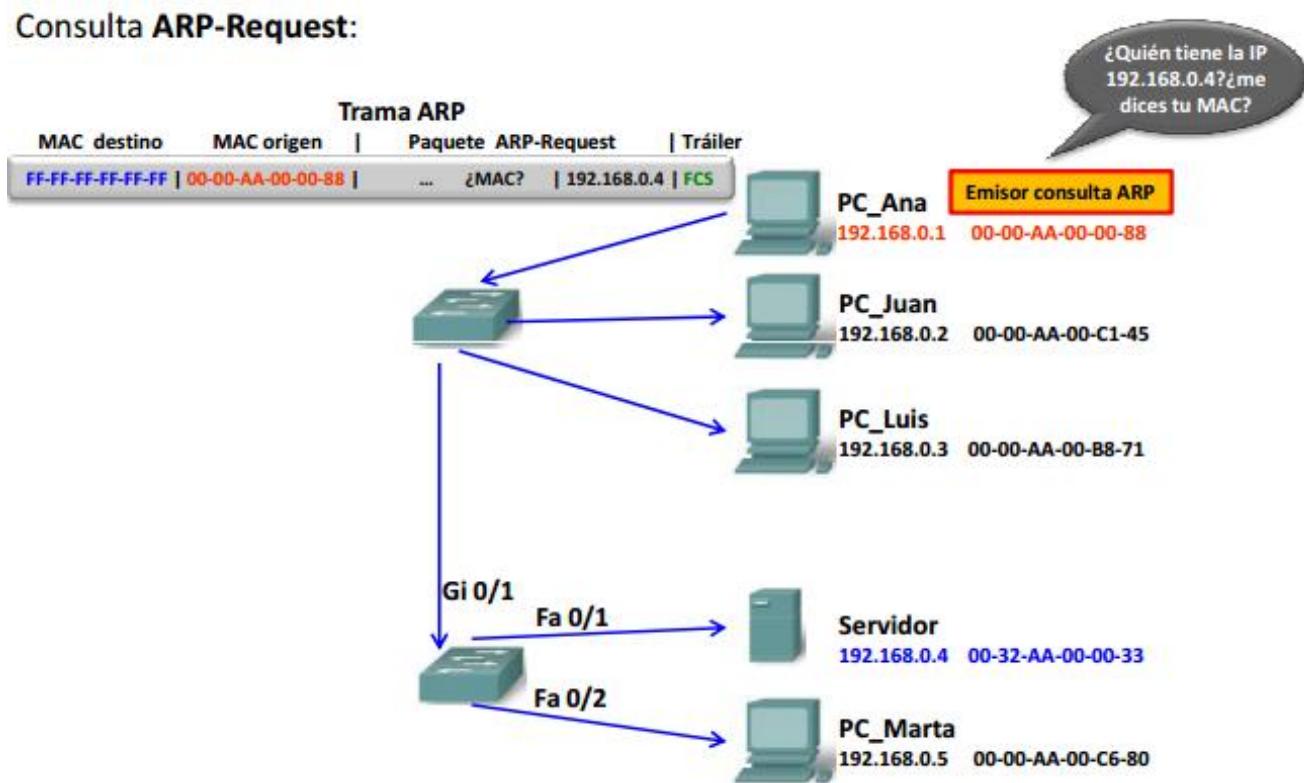
Ejemplo:

Sea un equipo emisor al que llamaremos PC_Ana. PC_Ana desea enviar un mensaje al equipo 192.168.0.4, pero no conoce su MAC y necesita introducirla en el encabezado de la trama.

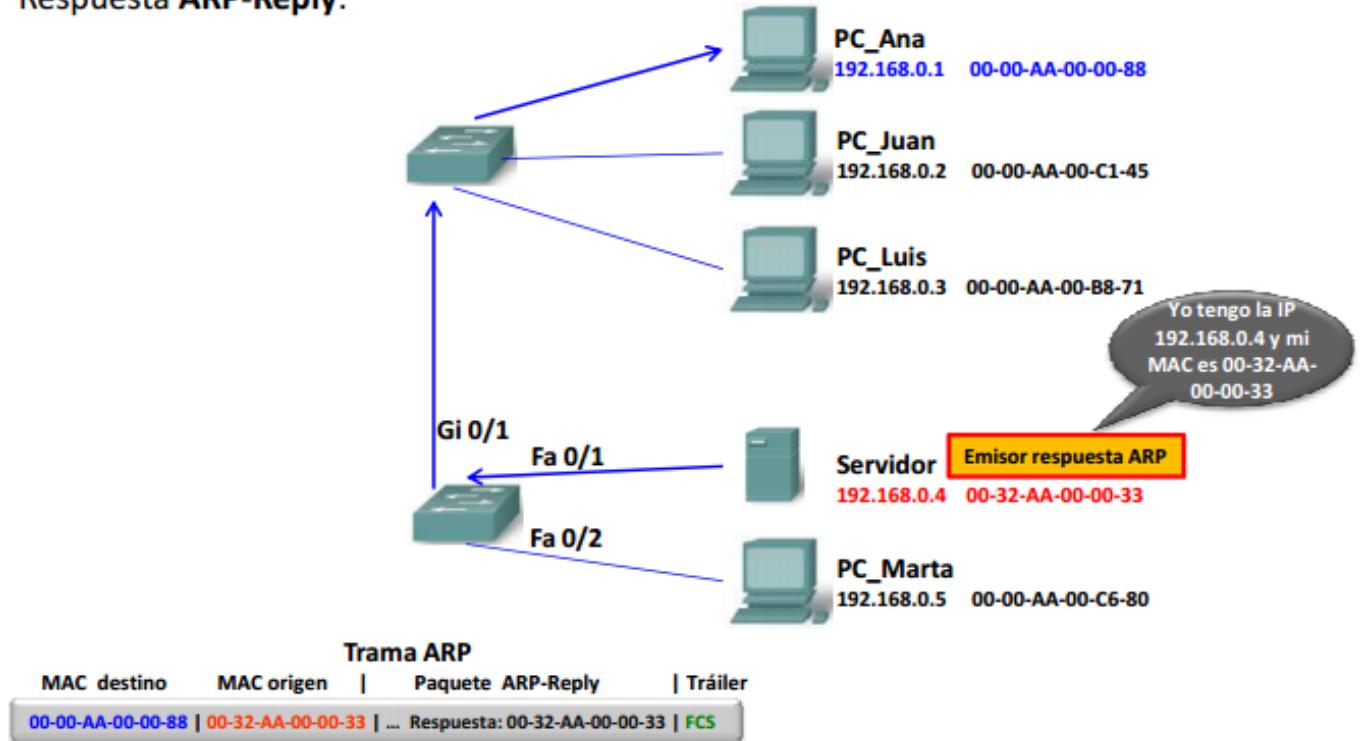
PC_Ana, para averiguar la MAC del equipo 192.168.0.4 debe seguir estos pasos:

1. PC_Ana consulta su tabla ARP, comprueba si la dirección MAC está en la tabla.
2. Si la dirección MAC está en la tabla ARP, PC_Ana toma esa dirección y la inserta en el encabezado de la trama. FIN
3. Si la dirección MAC no está en la tabla ARP, entonces
 1. PC_Ana envía una consulta (ARP-Request) a todos los equipos de la subred/red.
 2. El equipo de la red que tiene esa IP envía una respuesta (ARP-Reply) a PC_Ana comunicándole su MAC.
 3. Cuando PC_Ana averigua la MAC, la registra en su tabla ARP para uso futuro. Finalmente, inserta la MAC en el encabezado de la trama. FIN

Consulta ARP-Request:



Respuesta ARP-Reply:



¿Qué ocurre si el dispositivo destino no está en nuestra subred/red?

En este caso, el dispositivo origen envía el mensaje a la puerta de enlace y será ésta la que se encargue de enrutarlo a su destino.

Existe un método diferente llamado Proxy-ARP que no veremos en esta asignatura.

Paquetes ARP

Existen dos tipos de paquetes ARP:

- ARP-Request.
- ARP-Reply.

Como ARP es un protocolo de capa 3, el contenido de estos paquetes se crea en la capa 3 (no viene de la capa 4).



NOTA: un paquete ARP no tiene la típica cabecera de capa 3.



INESEM
BUSINESS SCHOOL

Escuela de líderes

Becas | Prácticas | Empleo



Ángel M. Gamaza

Tema 5

Capa de Transporte

Funciones de la capa de transporte

Segmentar los datos.- Generalmente, el conjunto de bytes de datos que se quieren transmitir en un mensaje es demasiado grande para ser enviado a la vez. La capa 4, se encarga de dividir el conjunto de bytes en segmentos (PDU de la capa 4) para permitir su correcta transmisión.

En el destino, determinar a qué proceso (aplicación) dirigir los datos.- La capa 4 es responsable de hacer llegar los datos al proceso correcto, para ello, identifica cada proceso con un número de puerto.

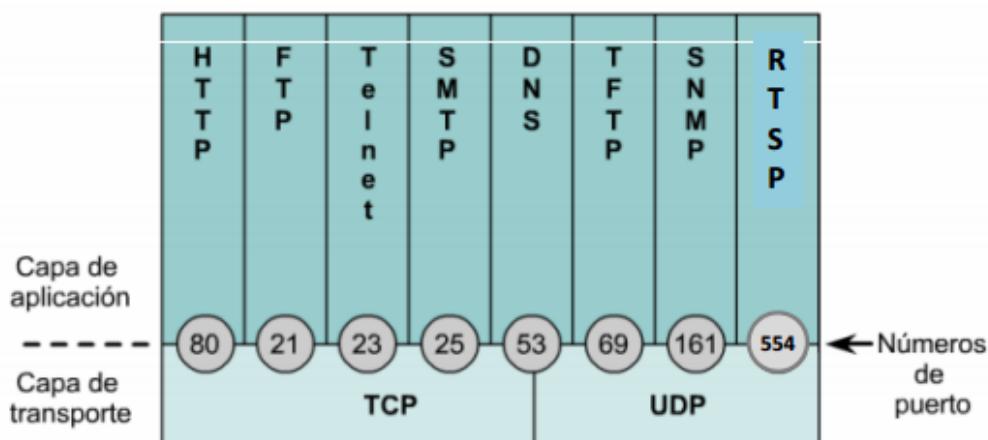
Control de flujo (si el protocolo es TCP).- No saturar de datos el buffer del dispositivo receptor.

Entrega confiable (si el protocolo es TCP).- Garantizar la entrega de los datos.

Protocolos de la capa de transporte

TCP (Protocolo de Control de Transmisión): es un protocolo orientado a conexión.

UDP (Protocolo de Datagrama de Usuario): es un protocolo NO orientado a conexión.



Protocolo TCP

El protocolo IP de la capa de red no garantiza la entrega de paquetes (IP envía paquetes sin saber si han sido recibidos por el equipo destino), es un protocolo no confiable.

En su defecto, esta garantía la puede proporcionar la capa de transporte mediante el protocolo TCP.

TCP garantiza la entrega y control de flujo.

En una conexión TCP existen 3 etapas:

- Establecimiento de la conexión (sincronización).**
- Transferencia de datos.**
- Fin de la conexión.**

Encabezado de un segmento TCP

Los campos más importantes del encabezado de un segmento TCP:

- Puerto origen.
- Puerto destino.
- Tipo de segmento.
- Número de secuencia.
- Acuse de recibo (ACK).
- Ventana deslizante.

TCP Header																																	
Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset	Reserved	N S R E G K H T	C W C R E G K H T	E C R C S E G K H T	U A P C S S Y I N N	A P R C S S Y I N N	R S Y I N N	Window Size																							
16	128	Checksum																Urgent pointer (if URG set)															

Número de secuencia

1-La capa 4 recibe de la capa 5 los bytes que se quieren transmitir.

Bytes de datos

2-La capa 4 asocia un número de secuencia a cada byte para identificarlo.

Capa 4

3-La capa 4 agrupa estos bytes en segmentos.



El número de secuencia que aparece en el encabezado del segmento es el número de secuencia del primer byte del segmento.



Bytes identificados con un número de secuencia



Segmento	Encabezado	1	2	3
----------	------------	---	---	---

Acuse de recibo (ACK)

Objetivo de un ACK

Confirmar al dispositivo emisor los bytes de datos que se han recibido correctamente.

¿Qué es un ACK?

Es el número de secuencia del siguiente byte que se espera recibir, quedando confirmados los bytes anteriores.

Por ejemplo, si ACK es igual a 100 significa que se han recibido correctamente los 99 primeros bytes y se está esperando recibir del byte número 100 en adelante.

¿Puedo enviar el siguiente segmento sin esperar el ACK del envío anterior?



Rol de emisor

¿Es necesario enviar un ACK nada mas recibir un segmento?



Rol de receptor

Sí, el emisor puede seguir enviando segmentos (siempre que la cantidad de bytes de ese conjunto de segmentos **no se supere la ventana de recepción del equipo B**). Si para enviar un nuevo segmento hubiese que esperar el ACK del segmento anterior, se desperdiciaría buena parte del ancho de banda de la red.

No, el receptor puede esperar y emitir un ACK para un conjunto de segmentos (siempre que la cantidad de bytes de ese conjunto **no se supere la ventana de recepción del equipo A**).



El host A tiene dos ventanas:

- **V-Envío_A** para controlar los bytes que se envían. Define la cantidad máxima de bytes que el equipo A puede enviar antes de recibir un ACK.
- **V-Recepción_A** para controlar los bytes que se reciben. Define la cantidad máxima de bytes que el equipo A puede recibir antes de enviar un ACK. Esta es la que aparece en la cabecera de sus segmentos.



El host B tiene dos ventanas:

- **V-Envío_B** para controlar los bytes que se envían. Define la cantidad máxima de bytes que el equipo B puede enviar antes de recibir un ACK.
- **V-Recepción_B** para controlar los bytes que se reciben. Define la cantidad máxima de bytes que el equipo B puede recibir antes de enviar un ACK. Esta es la que aparece en la cabecera de sus segmentos.

Los bytes confirmados de la ventana de recepción pasan la capa 5.

Establecimiento de conexión

Antes de transmitir datos, cada host debe poner en conocimiento del otro: su número de secuencia inicial y el tamaño de su ventana de recepción.

Esta primera fase también es denominada saludo de tres vías, por ser un proceso de tres pasos.

Ángel M. Gamaza

Ventanas deslizantes

¿Para qué se utiliza una ventana deslizante?

Se utiliza para regular la cantidad de bytes que se pueden enviar consecutivamente al equipo receptor sin saturarlo. Esto se conoce como control de flujo.

¿Cuántas ventanas existen en cada equipo?

Dos, una para controlar los bytes que se envían y otra para controlar los bytes que se reciben.

Ataque de denegación de servicio (DoS): SYN Flooding (inundación SYN)

Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios; por eso se le denomina "denegación", pues hace que el servidor no dé abasto a la cantidad de solicitudes. Esta técnica es usada por los llamados crackers para dejar fuera de servicio a servidores objetivo.

Protocolo UDP

UDP no garantiza la entrega y ni el control de flujo.

Ciertas aplicaciones prefieren utilizar el protocolo UDP porque es más rápido, aunque éste no garantice la entrega. En este caso, son los protocolos de la capa de aplicación los que brindan la detección de errores.

¿Qué aplicaciones utilizan UDP?

-Aplicaciones que requieren velocidad. En estos casos, resulta más importante transmitir a alta velocidad que garantizar la entrega de paquetes. Ejemplo: VoIP, streaming, juegos on-line.

-Aplicaciones que transmiten pequeñas cantidades de datos. Estas pequeñas cantidades de datos no justifican toda la información de control que se debe transmitir durante las fases de establecimiento y finalización de la conexión en el protocolo TCP, resulta más eficaz reenviar los datagramas defectuosos. Ejemplo: la mayoría de las consultas-respuestas DNS.

Streaming utiliza el protocolo de aplicación RTSP (Real-Time Streaming Protocol), que a su vez usa el protocolo de transporte UDP y el puerto bien conocido UDP 554).

¿Por qué es más rápido?

-No hay fases de establecimiento y finalización de conexión, es decir, es no orientado a conexión.

-No se envían acuses de recibo (ACK).

Encabezado de un segmento UDP

UDP no utiliza:

- Acuses de recibo (ACK).**
- Ventanas.**

Lógicamente, el encabezado de un segmento UDP es diferente al encabezado de un segmento TCP.

Bits 0 - 15	16 - 31
Puerto origen	Puerto destino
Longitud del Mensaje	Suma de verificación

Encabezado de un segmento UDP, los campos sombreados son opcionales.

Puertos

Definición de puerto (Tema 1).

La combinación de la dirección IP y el número de puerto se denomina socket. Un socket identifica un proceso de red de manera única en Internet.

Una conexión tiene dos sockets, uno por cada host. Este par de sockets identifica la conexión de manera única en Internet.

Clasificación de los puertos según IANA

Definición en el Tema 1.

Listado de números de puerto según IANA

Muchas aplicaciones pueden funcionar tanto con TCP como con UDP. Por ejemplo, la aplicación HTTP, siempre se ha dicho que utiliza TCP, sin embargo, hay dos puertos 80 uno para TCP y otro para UDP. Pues bien, HTTP se asocia con TCP porque es el que utiliza con mayor frecuencia.

Por este motivo, los procesos son identificados con la combinación protocolo-puerto.

Los números de puerto que hay que memorizar son:

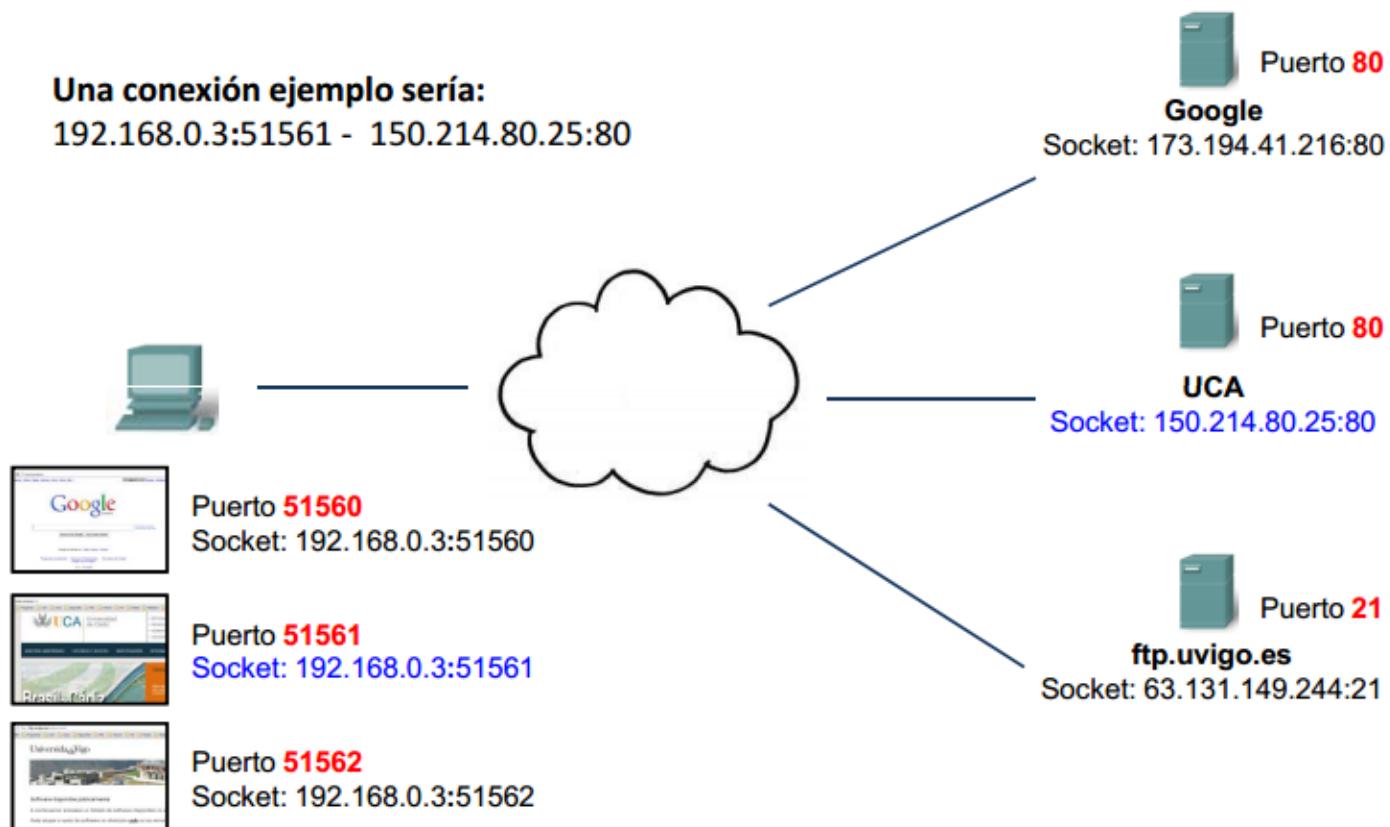
Aplicación	Puerto TCP	Puerto UDP
FTP	21	21
SSH	22	22
Telnet	23	23
SMTP	25	25
DNS	53	53
TFTP	69	69
HTTP	80	80
POP3	110	110
HTTPS	443	443

En la tabla se ha resaltado el protocolo de transporte que utiliza la aplicación con mayor frecuencia.

Funcionamiento

Una conexión ejemplo sería:

192.168.0.3:51561 - 150.214.80.25:80



NETSTAT -N

TCP	192.168.1.129:50774	173.194.34.193:80	ESTABLISHED
TCP	192.168.1.129:50788	150.214.80.25:80	ESTABLISHED
TCP	192.168.1.129:50791	63.131.149.244:21	SYN_SENT



INESEM
BUSINESS SCHOOL

Escuela de líderes

Becas | Prácticas | Empleo



Ángel M. Gamaza

Tema 6

Capa de Aplicación

DNS (Servicio de Nombres de Dominio)

Un dominio o nombre de dominio es el nombre que identifica un sitio en Internet.

Ejemplo: "cisco.com" es el nombre de dominio asociado a la empresa Cisco. Bajo ese dominio se pueden acoger diferentes servicios. Estos servicios deben residir en una máquina concreta y no todos los servicios tienen por qué estar en la misma máquina. Por ejemplo:

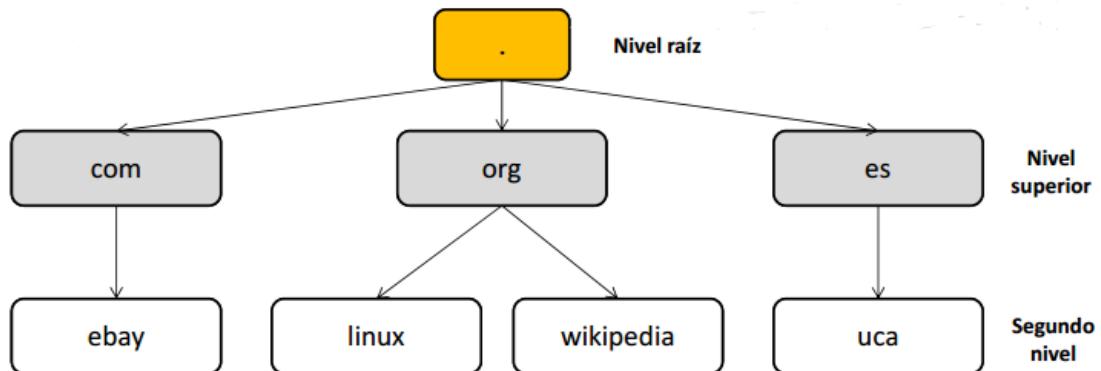
- www.cisco.com: está en el host 233.4.4.56.
- ftp.cisco.com: está en el host 233.4.4.56.
- mail.cisco.com: está en el host 233.4.4.57

DNS proporciona un mecanismo para traducir el nombre de dominio de un servicio en la dirección IP de la máquina donde reside. Esta funcionalidad la proporcionan los servidores DNS.

Espacio de nombres de dominio

El espacio de nombres de dominio es una estructura jerárquica en forma de árbol dividida en niveles:

- Nivel raíz
- Nivel superior
- Segundo nivel
- ...



El nombre completo de un dominio (nombre de dominio completamente cualificado -FQDN-) está constituido por el conjunto de nombres que aparecen en el itinerario desde ese nodo hasta el raíz, separándolos por puntos y terminando en punto. **Ejemplo:** ebay.com.

Nivel Raíz

En el nivel raíz se halla el dominio raíz. Debajo, puede existir un número indeterminado de niveles (normalmente no se superan los 5 niveles).

El dominio raíz no tiene nombre y se representa con un punto.

Nivel superior (TLD)

En el nivel superior están los dominios que descienden directamente del dominio raíz. Estos dominios pueden ser:

- Generic (gTLD): com, org, net, gov, edu, ...
- Country-Code (ccTLD): es, fr, de, ...

Base de datos distribuida

El espacio de nombres de dominio se implementa mediante una base de datos distribuida. Veremos que, por ser distribuida, permitirá una administración descentralizada.

En esta base de datos, se almacena información de cada dominio en registros recursos (RR). Esta información permite identificar el dominio y asociar el nombre de dominio con la dirección IP (resolución de nombres). Campos de un registro de recursos:

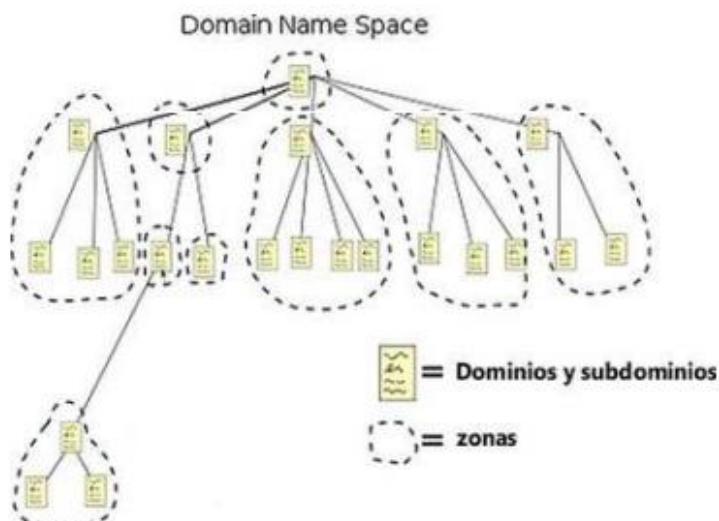
Propietario: nombre de máquina o dominio DNS al que pertenece el recurso. Puede contener el símbolo @, que representa el nombre de la zona descrita.
TTL (Time To Live): tiempo de vida en segundos que puede estar el registro en la caché, expresado en días (d), horas (h), minutos (m) y segundos (s). El cero (0) no se almacena en caché. Se trata de un campo opcional.
Clase: familia de protocolos en uso indicados por IN (de Internet) y que representa una red TCP/IP.
Tipo: varía en función del campo clase. En la tabla 1.2 se indican tipos de registros para la clase IN.
RDATA: información específica del tipo de recurso. Por ejemplo, para un registro de clase IN y tipo A, este campo especifica una dirección IP.

Los principales tipos de registros de recursos son: SOA, NS, A, CNAME, MX, PTR, etc.

Nombre del recurso	Tipo de registro	Función
Inicio de autoridad	SOA	Identifica al servidor autoritario de una zona y sus parámetros de configuración.
Servidor de nombres	NS	Identifica servidores de nombres autorizados para una zona.
Dirección	A	Asocia un nombre de dominio FQDN con una dirección IP.
Puntero	PTR	Asigna una dirección IP a un nombre de dominio completamente cualificado. Para las búsquedas inversas.
Registro de correo	MX	Indica máquinas encargadas de la entrega y recepción de correo en el dominio.
Nombre canónico	CNAME	Permite asignar uno o más nombres a una máquina.

Zonas de autoridad

El espacio de nombres de dominio se divide en zonas. Cada zona tiene autoridad para administrar una parte del árbol.



Cada zona controla sus dominios.



Ángel M. Gamaza

Cada zona administra una parte de la base de datos distribuida (base de datos de la zona), concretamente la correspondiente a esa parte del árbol.

Una zona puede tener varios servidores:

- **Servidor primario:** sólo existe uno y contiene la base de datos de la zona. La autoridad de la zona se delega en el servidor primario.
- **Servidores secundarios:** contienen una copia exacta de la base de datos de la zona (son un espejo del servidor primario). Objetivo: servidores de respaldo.

Estos servidores se consideran **autoritarios** en esa zona porque son capaces de responder las consultas de los dominios de la zona.

Los servidores se comunican entre ellos mediante consultas de **transferencia de zona**.

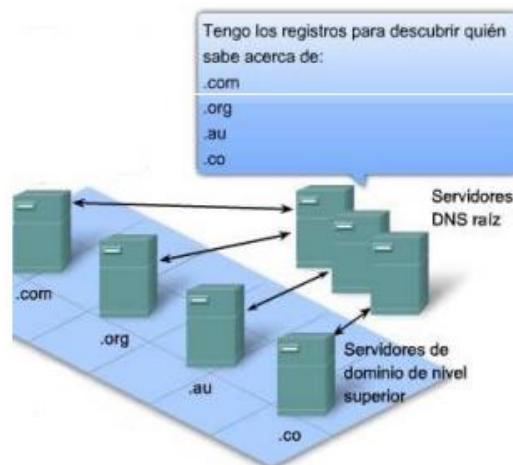
El servicio utiliza el puerto **53-UDP** para atender las consultas de los clientes y el puerto **53-TCP** para atender las transferencias de zona entre servidores.

Base de datos de la zona raíz: Contiene los registros de recursos que permiten obtener la dirección de los servidores DNS autoritarios de las zonas de nivel superior (TDL).

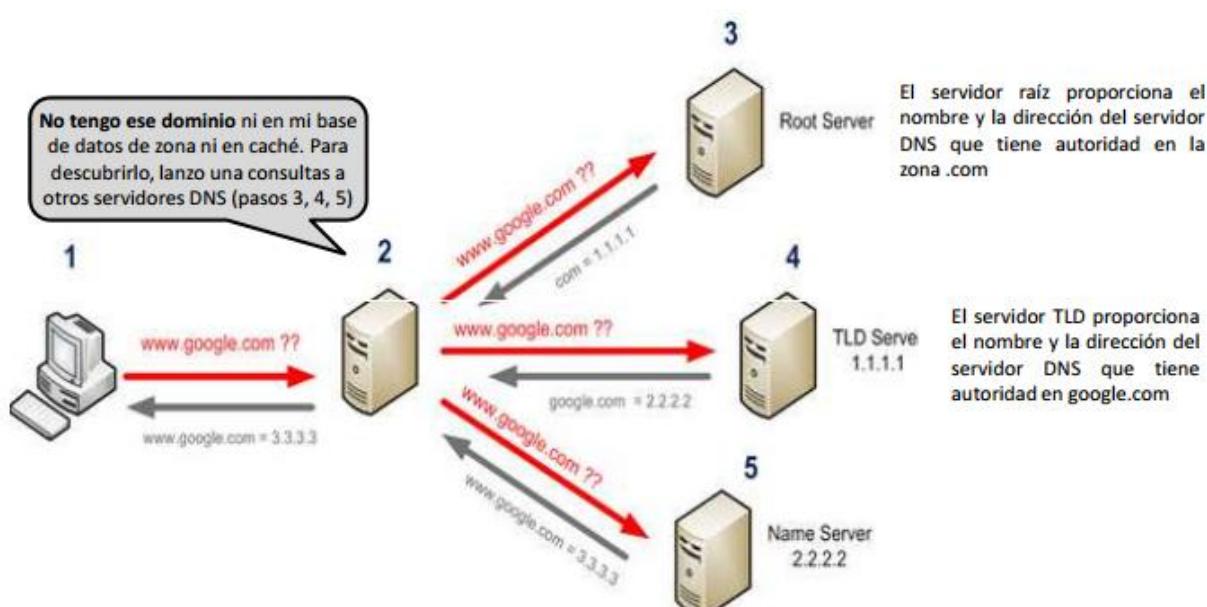
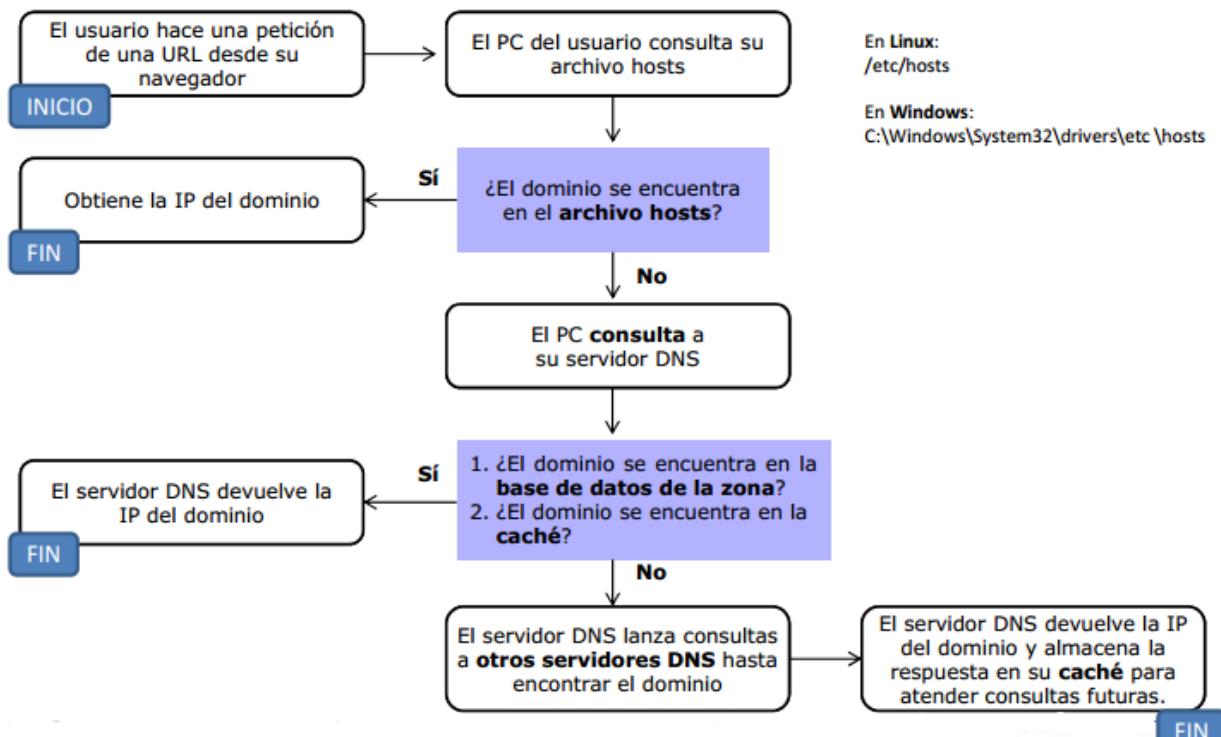
Actualmente existen 13 servidores raíz. Sus nombres tienen la forma

letra.root-servers.net

donde la letra va desde la A a la M. Esto no quiere decir que haya sólo 13 servidores físicos, cada operador utiliza servidores redundantes distribuidos a lo largo del globo terráqueo para ofrecer un servicio fiable.



Resolución de nombres de dominio



Una respuesta se considera autoritativa cuando es respondida por el servidor DNS que posee autoridad sobre el dominio.

Si el servidor DNS local puede resolver el dominio porque está en su base de datos de zona, la respuesta es autoritativa.

Si el servidor DNS local puede resolver el dominio porque está en su caché, la respuesta es NO autoritativa.

Si el servidor DNS local no puede resolver el dominio porque ni está en su base de datos de zona ni en su caché, irá contactando con otros servidores DNS hasta encontrar el servidor DNS autoritario capaz de resolverlo. En este caso, la respuesta es autoritativa. Acto seguido, el servidor DNS local almacenará en memoria caché esa información, por lo que las consultas siguientes se responderán de forma NO autoritativa.

Propagación del dominio

Cuando se produce un cambio en un dominio, por ejemplo, cambia la IP del servidor, esa nueva información debe propagarse entre los servidores DNS de la zona.

Aparentemente debería ser un proceso inmediato, sin embargo, suele tardar unas 48 horas.

¿Por qué? Servidores DNS de otras zonas pueden tener ese dominio en caché.

Hay que esperar que expire (TTL generalmente tiene un valor de 48 horas) la entrada en caché para que, cuando esos servidores reciban una consulta de un cliente, contacten con el servidor DNS autoritario. El servidor DNS autoritario responderá con los datos actualizados.

DNS Dinámico (DDNS)

El DDNS permite la asignación de un nombre de dominio a una máquina con dirección IP dinámica, es decir, dirección IP variable.

Es común que el proveedor de internet (ISP) proporcione a nuestro router una IP pública dinámica. Si en estas circunstancias queremos tener un servidor público en nuestra red con un dominio asociado, debemos hacer uso de DDNS.

DynDNS ofrece este servicio gratuitamente. Para utilizarlo:

1. Crear una cuenta DDNS en DynDNS (www.dyndns.com).
2. Entrar en la cuenta DynDNS y dar de alta al host indicando el dominio asociado.
3. Activar la opción DDNS en el router (habrá que proporcionar los datos de la cuenta DynDNS).

Cada vez que cambia la IP pública del router, éste se la comunicará al servidor DynDNS.

Herramienta nslookup

Los sistemas operativos cuentan con una herramienta llamada nslookup, que permite, entre otras muchas funciones, las siguientes:

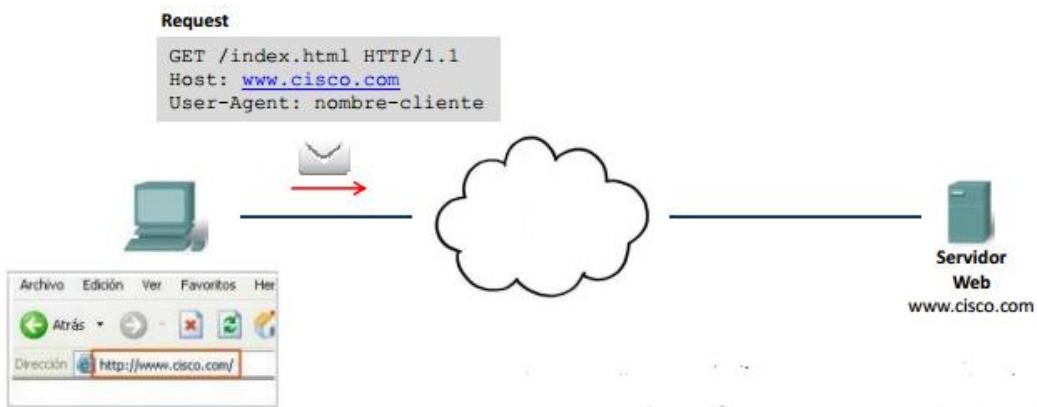
- Obtener información de un servidor DNS.
- Solucionar problemas de resolución de nombres.
- Transferir una zona.

HTTP (Protocolo de Transferencia de HyperTexto)

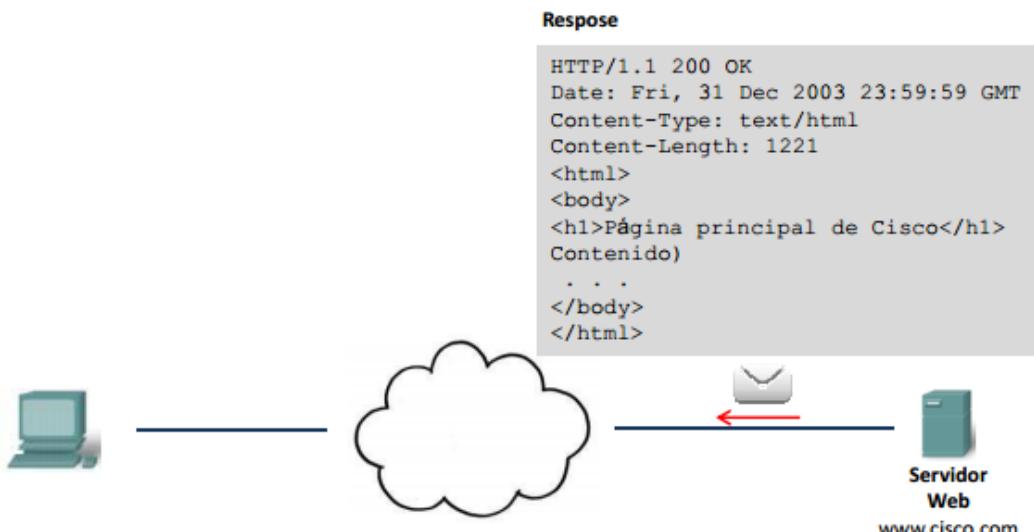
Conexión HTTP

1. El usuario introduce en el cliente web (navegador) la dirección de la página que quiere consultar.

2. El cliente interpreta la dirección y establece una conexión TCP con el servidor web para solicitar la página (Request).



3. El servidor envía la página al cliente (Response) y, si no existe, envía un código de error (por ejemplo, 404 “No encontrado”).

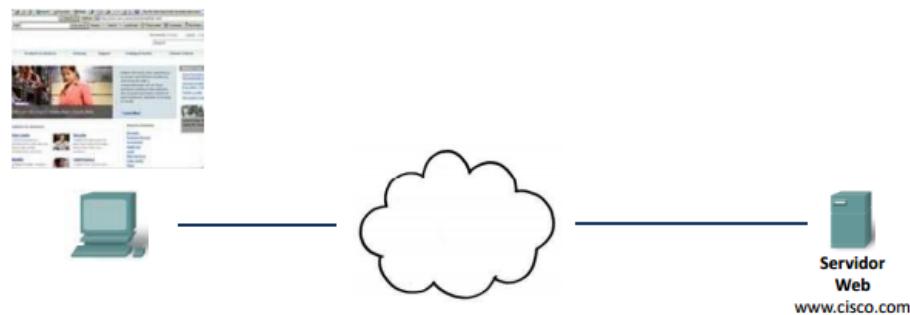




Ángel M. Gamaza

4. Cuando el cliente recibe la página web, interpreta el código HTML-XML y ejecuta el código JavaScript, Java (applet) que pueda contener.

5. El cliente muestra la página.



Métodos de solicitud HTTP

En HTTP 1.1, el cliente puede solicitar al servidor web distintas acciones:

- **GET**: solicitar una página.

- **POST**: cargar información en el servidor web, por ejemplo, los datos introducidos en un formulario web.

- **HEAD**: sólo solicitar la cabecera de la página. Útil cuando sólo se quiere obtener meta-information del encabezado.

- ...

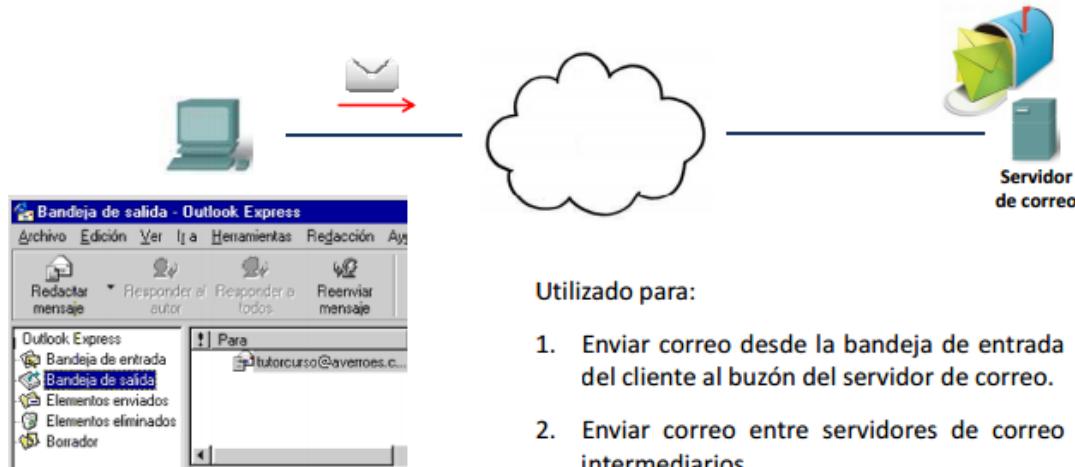
HTTPS

El protocolo SSL permite establecer una comunicación segura y codificada entre el servidor web y el navegador. Puede utilizar cualquier método de cifrado, siempre que lo compartan el servidor y el cliente.

SSL trabaja conjuntamente con el protocolo HTTP, creando un protocolo HTTP seguro: **HTTPS**.

Servicio de correo electrónico

SMTP (Protocolo Simple de Transferencia de Correo)



Utilizado para:

1. Enviar correo desde la bandeja de entrada del cliente al buzón del servidor de correo.
2. Enviar correo entre servidores de correo intermedios.

```

S: 220 Servidor ESMTP
C: HELO miequipo.midominio.com
S: 250 Hello, please to meet you
C: MAIL FROM: <yo@midominio.com>
S: 250 Ok
C: RCPT TO: <destinatario@sudominio.com>
S: 250 Ok

C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: Subject: Campo de asunto
C: From: yo@midominio.com
C: To: destinatario@sudominio.com
C:
C: Hola,
C: Esto es una prueba.
C: Hasta luego.
C:
C: .
S: 250 Ok: queued as 12345
C: quit
S: 221 Bye

```

El cliente abre una conexión TCP con el servidor y éste contesta con el mensaje 220 Servidor SMTP.

El cliente abre una sesión con el servidor mediante la orden HELO y proporciona las cuentas del emisor y del receptor.

El cliente envía el mensaje. DATA indica el comienzo del mensaje y una línea con un punto indica el fin del mensaje.

El cliente solicita cerrar la sesión con la orden QUIT.

POP3 (Protocolo de Oficina de Correos v.3)

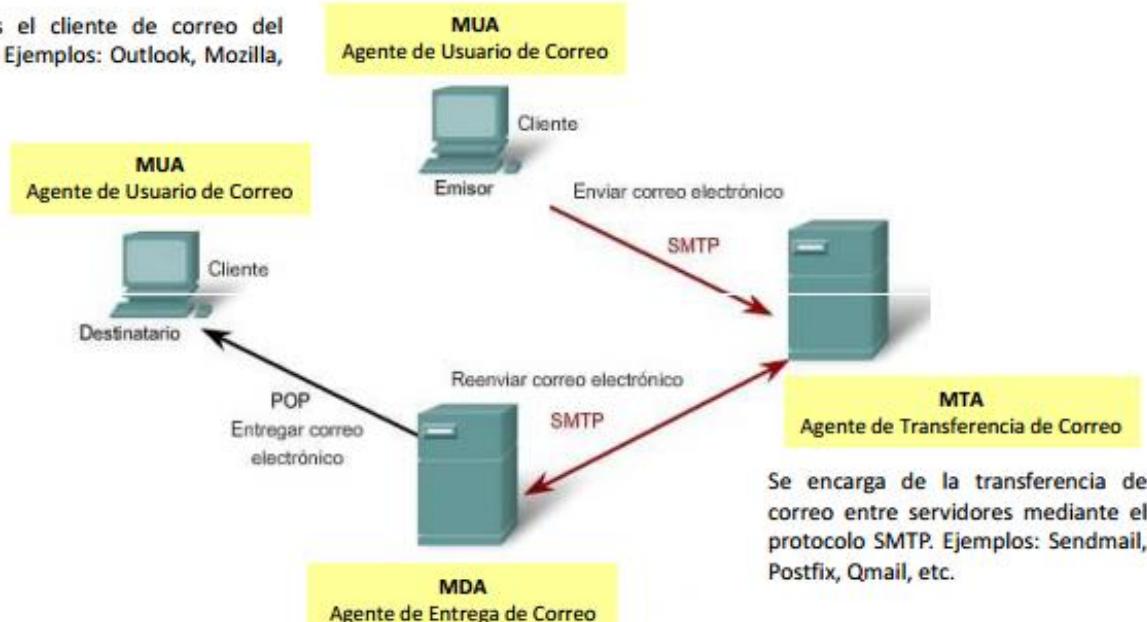


Utilizado para **descargar los e-mails** del buzón del servidor de correo a la bandeja de entrada del cliente.

Permite leer el correo recibido sin estar conectado a la red

Agentes del Servicio de Correo Electrónico

MUA es el cliente de correo del usuario. Ejemplos: Outlook, Mozilla, etc.



Recibe el correo del MTA y lo guarda en el buzón del usuario. El MDA escucha cuando un cliente (MUA) se conecta al servidor y, una vez establecida la conexión, envía el correo al MUA mediante POP3 o IMAP. Ejemplos: Qpopper, Cyrus, etc.

Campos de un mensaje de correo electrónico

```

Delivered-To: smrser@gmail.com

Received: by 10.204.69.68 with SMTP id y4cs104175bki; Sun, 5 Jul 2009
15:15:20 -0700 (PDT)

MIME-Version: 1.0

Received: by 10.223.111.140 with SMTP id s12mr1666698fap.45.124683211
9088;

Sun, 05 Jul 2009 15:15:19 -0700 (PDT)

Date: Mon, 6 Jul 2009 00:15:19 +0200

Message-ID: <22ccb3270907051515s6f038f01k2e84a02d5b0fed25@mail.gmail.
com>

Subject: =?ISO-8859-1?Q?Software_Libre=Publicada_la_versi=F3n_3

From: =?ISO-8859-1?Q?SMR_WEB?= <smrweb2@gmail.com>

To: =?ISO-8859-1?Q?SMR_SER? <smrser@gmail.com>

Content-Type: multipart/alternative; boundary=001636c5a8508d8768046df
cb979

```

Received: servidores de correo por donde ha circulado el mensaje

Direccionamiento de IP

La dirección IP tiene dos partes:

- **NET ID:** identifica la red en la que está ubicado el host.
- **HOST ID:** identifica el host dentro de esa red.

Si en la red se han definido subredes entonces se puede considerar que la dirección IP tiene tres partes:

- **NET ID:** identifica la red en la que está ubicado el host.
- **SUBNET ID:** identifica la subred en la que está ubicado el host.
- **HOST ID:** identifica el host dentro de esa subred.

TIPO DE RED	1 ^{er} OCTETO (decimal)	1 ^{er} OCTETO (binario)	MÁSCARA	Nº HOSTS
A	1-126	0XXXXXXX	255.0.0.0	/8
B	128-191	10XXXXXX	255.255.0.0	/16
C	192-223	110XXXXX	255.255.255.0	/24

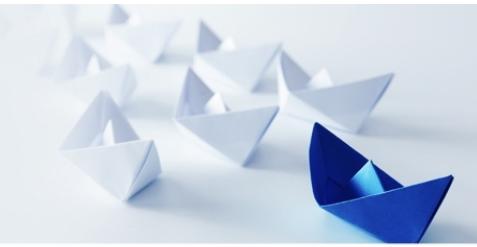
IP:	192.168.1.6	11000000.10101000.00000001.00000110
MÁSCARA:	255.255.255.0	11111111.11111111.11111111.00000000



INESEM
BUSINESS SCHOOL

Escuela de líderes

Becas | Prácticas | Empleo



Máster en Ciberseguridad



Ángel M. Gamaza

Puntos clave prácticas

Puntos clave práctica 1

Generalidades TCP/IP

1. Ejercicio llave (IP).
2. El protocolo ARP sirve para que un equipo (A) obtenga la MAC de otro (B), a través del envío de un paquete especial que pide al equipo (B) que responda con su dirección física. Todo esto se lleva a cabo a partir de la dirección IP.

Porque así no se tienen que estar enviando constantemente paquetes de multidifusión, y se ahorra en costos de comunicación. Antes de realizar la comunicación, se mirará esta tabla por si está en ella la dirección física.

3. Es otro método, además de la IP, para nombrar a un host dentro de internet. Es lo que se llama Sistema de Nombres por Dominios. Facilita la memorización y se puede localizar más fácilmente el área geográfica de un host. Se contrata en la página web www.iana.com.
4. Gestionan los dominios de cada entidad, además de los datos de éstas y de personas de contactos, entre otros.
5. Con este comando se puede comprobar el estado de las conexiones que mantiene el PC (puertos abiertos), también puede mostrar una serie de estadísticas del TCP/IP. Al añadirle el –n, el comando muestra las direcciones y los números de los puertos en formato numérico (en lugar de buscar nombres).

COMANDOS

-**PING**: Se utiliza para comprobar el estado de la conexión con uno o varios hosts.

-**TRACERT**: El nombre de este comando proviene de Trace Route o trazador de rutas. Consiste en una herramienta de diagnóstico que determina el camino más probable que se tomara al establecer la comunicación con un host.

-**NETSTAT**: Con este comando se puede comprobar el estado de las conexiones que mantiene el PC (puertos abiertos), también puede mostrar una serie de estadísticas del TCP/IP.

-**ARP –a**: Muestra las entradas actuales de ARP mediante una consulta de TCP/IP. Si se especifica *dir_inet*, sólo se mostrarán las direcciones IP y físicas del equipo especificado.

Puntos clave práctica 3

Manejo de una Red de Área Local

1. En el Grupo de Trabajo la red está descentralizada y es cada máquina la responsable de la gestión de la red, los usuarios y la seguridad de manera local; sin embargo en el Dominio toda esta gestión es llevada a cabo por una o varias máquinas sobre las que hay instalada un sistema operativo del tipo Windows Server.
2. a) Protocolo TCP/IP. Protocolo de red de área extensa predeterminado que permite la comunicación de varias redes conectadas entre sí.
b) Transforma al PC en un servidor habilitando la compartición de recursos en él.
c) transforma al PC en un cliente capaz de acceder a los recursos compartidos de PCs que tienen instalado el servicio “Compartir impresoras y archivos para redes Microsoft”.
3. Sistema de E/S Básica de Red, que podemos definir como un protocolo de la capa de sesión (capa 5) cuyo objetivo es compartir recursos en una red. Una mala configuración de NetBIOS supone un alto riesgo de intrusión por parte de extraños a los recursos compartidos y por eso es conveniente deshabilitarlo si no se va a utilizar.
4. Poniendo al final del recurso compartido un \$, ese recurso no se verá a través del entorno de red. Existe y funciona de la misma manera que uno no oculto, pero para acceder a él no se usa el entorno de red.
5. Una unidad de red es un área del disco duro de un ordenador cuyo usuario ha hecho accesible a otros ordenadores. Su finalidad es simplificar el intercambio de información (archivos).

COMANDOS

1. a) Net es un conjunto de comandos, cada uno de los cuales se utiliza para habilitar/deshabilitar un servicio de red, así como para su configuración
b) SHARE: mostrar/modificar recursos compartidos. **net share**
recursodered=recurso
VIEW: mostrar dominios enteros o recursos. **net view x /Domain:y**
USE: crear conexiones de red. **net use nombre \\ recurso**
START: inicia el servicio x. **net start x**
STOP: detiene el servicio x. **net stop x**

Puntos clave prácticas 5,6,7,8,9,10

Switches, Routers, Tablas de enrutamiento y Wireshark

1 y 2. Modo exec de usuario (Router>)

Modo exec-privilegiado → enable (Router#)

Modo de configuración global → configure terminal (Router(config)#)

Para salir → end o exit, también disable.

3. El **running-config** es la configuración que se está utilizando es ese momento, el fichero se encuentra en la memoria volátil por lo que los cambios que se realicen no serán permanentes.

El **startup-config** se graba en la memoria no volátil (NVRAM) y será el fichero de configuración utilizado al reiniciar el router.

4. El acceso al router y a su modo exec privilegiado, así como a Telnet.

5. Para las FastEthernet:

```
Router1(config)# interface fa0/0
Router1(config-if)# description Connection to Host1 with crossover cable
Router1(config-if)# ip address address mask
Router1(config-if)# no shutdown
Router1(config-if)# end
Router1#
```

Para las seriales:

```
interface Serial0/1/0
```

6. Una **ruta estática** le dice al router cual es el camino a tomar hacia un destino determinado, pero con la diferencia de que no es el router quien crea o aprende dicha ruta, sino que es el administrador quien fija la misma.

La **ruta por defecto** o gateway de último recurso se utiliza para enviar a otro router un paquete cuando el mio no sabe cómo llegar a un determinado destino, es como el gateway que le configuráis a un PC.

7. Se debe cambiar la IP a un switch cuando se quiera que ésta sea estática en lugar de dinámica.



Ángel M. Gamaza

COMANDOS

1. **show running-config.**
2. **#erase nvram.**
3. **#copy running-config startup-config.**
4. **enable password <<contraseña>>** (Establece una contraseña local para controlar el acceso a los diversos niveles de privilegio.)
enable secret <<contraseña>> (Especifica una capa de seguridad adicional mediante el comando enable password).
5. **interface tipo número** (Configurar).
cdp enable (Activar).
6. **(config)#ip route [metrica]**
7. **#show ip route**