UNIDAD 2

Tipos y arquitecturas de redes locales

Sistemas Informáticos
1º de DAM Semipresencial
IES San Vicente 2020/2021

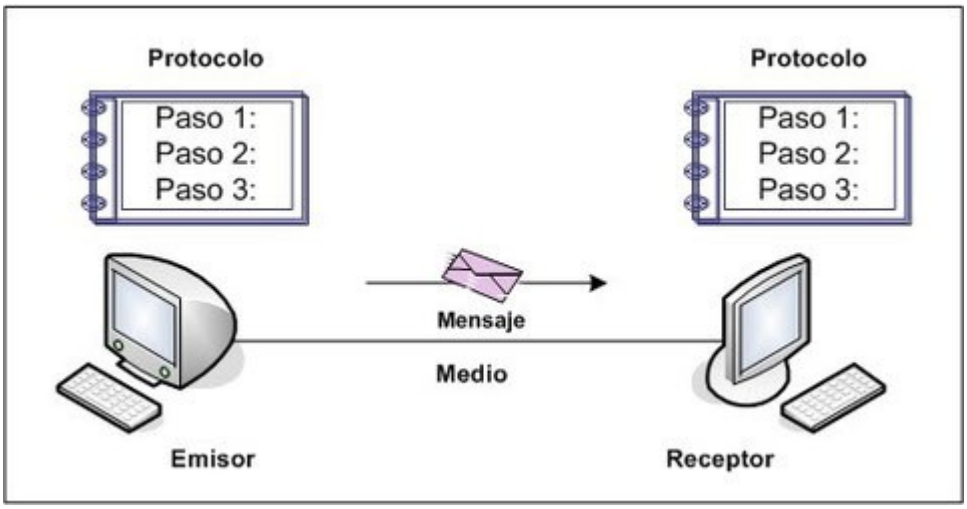
Index

Tipos y arquitecturas de redes

Sistema de comunicación

Conjunto de dispositivos interconectados por un sistema que permite la comunicación entre ellos.

- **Mensaje**: Información a transmitir
- **Emisor**: Dispositivo que genera el mensaje
- **Receptor**: Dispositivo destino del mensaje
- **Medio**: Medio físico utilizado para la transferencia
- **Protocolo**: Reglas que se aplican a la transmisión de los datos.



Tipos de red según cobertura

Según la extensión geográfica de una red se le suele denominar:

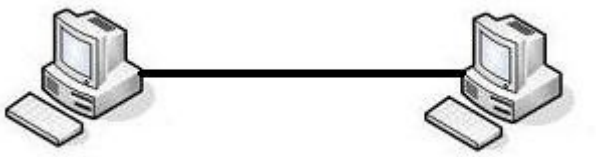
- **LAN (Local Area Network)** → Los ordenadores están en el mismo edificio, o en general, en un entorno próximo.
- **MAN (Metropolitan Area Network)** → Cubren un aréa que no supera el ámbito urbano (o interurbano entre 2 localidades muy cercanas). Suele ser una colección de redes locales (LANs) interconectadas entre sí mediante tecnologías como fibra óptica, cable de cobre trenzado, cable coaxial, WiMax, etc.
- **WAN (Wide Area Network)** → Conexiones entre equipos que están en diferentes localidades, provincias, e incluso países. Básicamente es lo que sería internet. Se suelen usar grandes infraestructuras de fibra óptica para la

conexión entre ciudades, países o continentes (cables submarinos).

Topologías de red

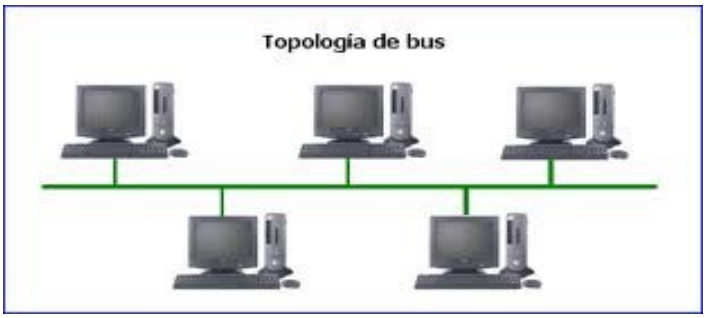
Según estén interconectados los equipos de una red, local tenemos diferentes distribuciones o topologías:

- **Punto a punto:** Básicamente consite en 2 equipos interconectados entre sí directamente.



- **Topología en Bus:** Utilizada hasta los años 90. Se basa en un único canal de comunicaciones (bus) al cual se conectan todos los dispositivos. Si en algún punto se corta la comunicación, la red entera deja de funcionar

  - Todos los equipos transmiten a la vez por el mismo medio, por lo que las capacidades de ampliación son muy limitadas, ya que cuantos más equipos, más colisiones de datos (fallo de trasmisión), y más se degrada el rendimiento.



- **Topología en anillo (Ringbus)**: Los equipos están conectados de forma parecida al bus pero formando un anillo.

  - En cada momento un equipo diferente tiene el "testigo" que le permite transferir (se evitan colisiones). Ese testigo se mantiene durante un tiempo y después pasa al siguiente. Si el equipo no ha terminado de transmitir debe esperar a que le vuelva a llegar el testigo para seguir.

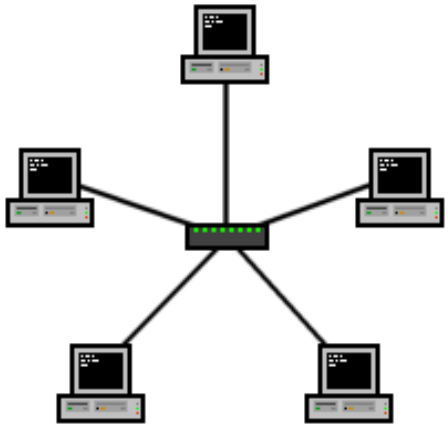
  - Tiene el mismo problema de que si se corta la comunicación en un nodo, se cae la red entera

  - No puede crecer mucho ya la información pasaría por demasiados equipos y afectaría al rendimiento, además de que el testigo tardaría en llegar. Existen mecanismos como el doble anillo pero tampoco mejora tanto el rendimiento.

- En caso de error, es difícil de detectar que segmento de la red ha fallado.

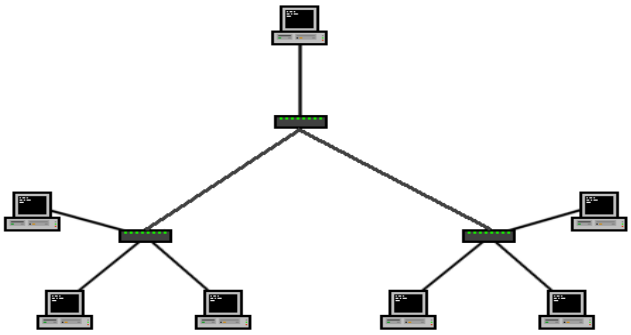
- **Topología en estrella**: Los equipos se conectan todos a un dispositivo central (switch) y las comunicaciones se hacen a través de este. Es la topología más usada hoy en día.

  - La red se cae sólo si el nodo central falla
  - Los datos sólo se transmiten a los equipos que participan en la comunicación (menos colisiones y mejor capacidad de ampliación)
  - Se pueden interconectar varios dispositivos de comunicación entre sí para ampliar la capacidad de la red formando una topología en árbol.



- **Topología en árbol:** Es la combinación de varias topologías (segmentos) en estrella unidas entre sí:

  - Si los segmentos son muy grandes (muchos equipos) puede saturarse la comunicación entre segmentos (los datos de muchos equipos viajan a través de un sólo cable)
  - Si se cae un nodo central se cae ese segmento de red entero (aunque en el ejemplo, si se cae el de arriba se quedan todos los segmentos desconectados)



Medios de transmisión

Los datos se pueden transmitir por diversos medios: Mediante cable (impulsos eléctricos o luminosos, como la fibra óptica), o mediante ondas (inalámbrico). En función del medio elegido varía el coste de la infraestructura necesaria, la velocidad de transmisión, la escalabilidad de la red, o la tolerancia a ruido (electromagnético).

Cable de par sin trenzar

Se usaba principalmente para la transmisión de voz analógica (teléfono), y todavía se usa para el acceso a internet mediante ADSL. Es muy vulnerable al "ruido" electromagnético (interferencias). También se le conoce como cable de categoría 1.

El conector se denomina RJ-11, y se compone de 2 cables de cobre en paralelo recubiertos de aislante (plástico).

Cable de par trenzado

Cables de cobre trenzados en parejas, para así reducir las interferencias electromagnéticas. El conector para este tipo de cables suele ser el RJ-45. Estos son los cables que se utilizan en la red Ethernet para montar una red local.

Son cables de bajo coste que hoy en día permiten transmisiones de hasta 10 Gbits/seg. Para ethernet de más velocidad (hasta 100Gbps), se usan cables de fibra óptica o cables de cobre con un diseño diferente.

Según sus características y velocidad que son capaces de alcanzar, los cables RJ45 se clasifican en las siguientes categorías:

- **Categoría 3** → Cable sin apantallar (malla de protección), usado sobre todo a principios de los 90, que sólo permite velocidades de hasta 10Mbits/seg.
- **Categoría 5** → 2 pares de cables trenzados mínimo (hasta 100Mb/s). Con 4 pares trenzados permite alcanzar hasta 1Gb/seg (Gigabit ethernet).
- **Categoría 5e** → La única diferencia con la anterior es que cumple con unos estándares más estrictos de calidad. Por ejemplo, el cable está más trenzado lo que le da mayor protección ante interferencias electromagnéticas.
- **Categoría 6** → Soportan hasta 1Gb/seg (máx. 100m.) Hasta 10Gb/s en distancias más reducidas.
- **Categoría 6a** → Hasta 10Gbits/seg, máx 100m.

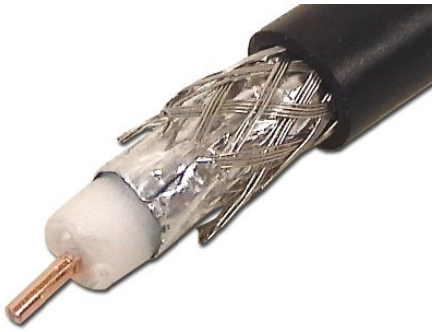
Según su nivel de protección frente a ruidos electromagnéticos mediante una

lámina de aluminio (Folded → F) o una malla (Shielded → S), los cables se clasifican también en:

- **UTP** → No lleva ningún tipo de malla protectora, sensible al ruido, pero fácil de manipular (más flexible).
- **FTP** y **STP**→ A cada par trenzado le rodea una lámina protectora de aluminio (FTP) o malla trenzada (STP → Mejor ya que hace de Jaula de Faraday).
- **S/UTP** y **F/UTP** → La lámina o malla engloba todos los pares en lugar de cada par individualmente.
- **S/FTP** y **F/FTP** → A cada par una lámina de alumnio (FTP) y englobando todo una malla (S) o una lámina (F)
- **SF/UTP** → Una malla trenzada y una lámina cubren todos los cables.

Cable coaxial

Consta de un cable de cobre que transporta la señal, rodeado de un aislante, que a su vez está rodeado por una malla metálica que sirve de pantalla para los ruidos electromagnéticos. Todo esto está envuelto en una cubierta protectora de plástico.



Tiene diversas aplicaciones:

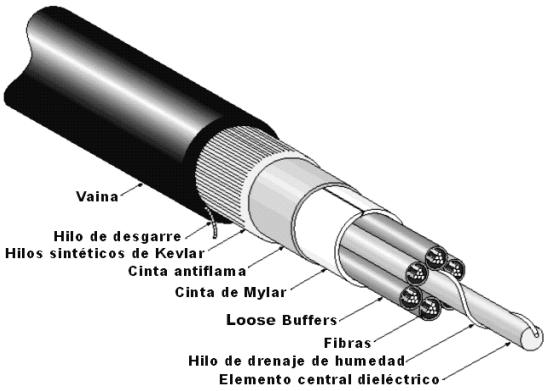
- Conectar televisión a la antena.
- Redes interurbanas (MAN) de televisión por cable e internet (poco a poco la fibra óptica desplaza al cable coaxial).
- Redes locales ethernet antiguas (10mbps, topología en bus).

Para la transmisión de datos a alta velocidad, los proveedores de internet utilizan la tecnología DOCSIS (similar a la usada en el ADSL sobre el cable telefónico), que aumenta el ancho de banda (aprovechando un mayor rango de frecuencias) desde 10Mbits/seg de las redes ethernet antiguas, hasta 10Gb/s de bajada y subida (estándar DOCSIS 3.1) en las infraestructuras más modernas.

Fibra óptica

Está compuesto por filamentos de fibras de vidrio o plásticas que son capaces de

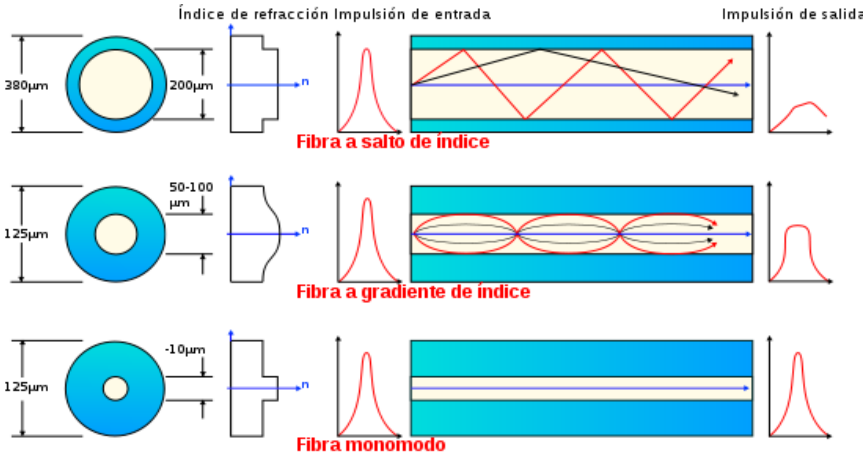
transmitir señales luminosas. Cada filamento tiene un núcleo con un alto índice de refracción (velocidad en la propagación de la onda de luz), rodeado por material similar pero de menor refracción que actúa de capa de protección. De esta manera se evitan interferencias entre filamentos contiguos. Todo esto se recubre de capas protectoras aislantes y absorbentes de luz.



Existen 2 técnicas para transmitir haces de luz a través de cables de fibra:

Multimodo → Los haces de luz circulan con diferentes índices de refracción en el cable (no llegan todos a la vez). Es más económico y fácil de conectar ya que el núcleo tiene un gran tamaño, sólo apto para distancias menores de 1km.

Monomodo → El haz de luz se transmite sólo en línea recta, reduciendo mucho el radio del núcleo. Permiten alcanzar grandes distancias (hasta 400km con un láser de alta intensidad) y grandes velocidades (varios Gb/s).



Dispositivos de interconexión de redes

Existen diversos dispositivos para interconectar equipos entre sí para formar una red local como el switch, o para interconectar diferentes redes.

CableMódem

Un módem sirve para modular una señal y distribuirla por un medio físico. En este caso el medio físico es la infraestructura de cable coaxial donde también se transmite la señal de televisión (por diferentes frecuencias).

Los cablemodems se encargan generalmente de interconectar redes locales (ethernet) con la red del provedor de internet (ISP) mediante una conexión punto a punto. Utilizan el estándar DOCSIS que en la versión 3.1 permite hasta 10Gb/s.

Módem ADSL

Al contrario que los modems originales que enviaban señales analógicas por el cable telefónico (par de cobre sin trenzar), la tecnología ADSL la envía en formato digital.

Al utilizar un medio muy sensible a ruido electromagnético, tiene ciertas limitaciones de velocidad. El estándar VDSL2 permite hasta 300Mb/s en distancias de hasta 300m. Esta disminuye cuanta mayor distancia de la centralita (imposible más de 5km).

Switch

También llamado conmutador. Interconecta varios equipos formando una red local con topología de estrella (es el nodo central). Cuando un mensaje llega desde un equipo dirigido a otro, el switch sabe en que puerto está conectado el destino y retransmite el mensaje por ahí.

Antiguamente se utilizaba otro dispositivo llamado hub o concentrador, que transmitía los paquetes por todos los puertos (saturaba más la red).

Se pueden interconectar entre sí varios de estos dispositivos para aumentar la capacidad de la red, formando una topología en árbol.

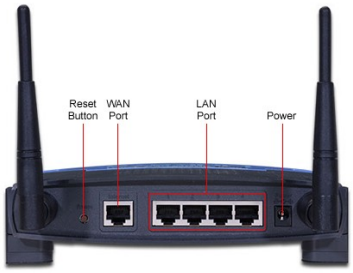
Punto de acceso Wifi

Tiene la misma función que el switch, sólo que en este caso, interconecta por medio de una red inalámbrica (WIFI).

Se pueden interconectar también varios puntos de acceso (por cable o WIFI, aunque se recomienda cable, así hay menos saturación en la red wifi → menos ondas que chocan)

También se puede interconectar un punto de acceso a un switch para formar una red mixta (o comprar un dispositivo híbrido).

Router



Los routers sirven para interconectar redes locales o de cualquier tipo entre sí. Los routers domésticos suelen interconectar 2 redes locales, o una red local con internet, pero hay routers que interconectan más redes simultáneamente.

Poseen mecanismos para evitar la congestión de la red repartiendo el tráfico de forma automática o en base a reglas (QoS → Quality of Service, etc.).

Muchas veces se utilizan para aislar una red local del exterior creando una zona privada y otra pública: los equipos externos de la parte pública no pueden acceder directamente a un equipo interno. Los routers domésticos funcionan así: las tomas LAN pertenencen a la red privada, mientras la toma WAN es la parte pública, que normalmente da acceso a internet.

Se comunican con otros routers para saber por donde deben enviar los paquetes de datos y que lleguen a su destino (encaminamiento). Los routers domésticos, suele integrar la funcionalidad de switch y punto de acceso WIFI, junto a la de router (dispositivo híbrido).

Servicios en la red

Ya sea a través de la red local, o a través de internet (redes locales diferentes), la comunicación en red permite crear infraestructuras donde se ofrecen servicios de diversa índole. Estos servicios pueden ser distribuidos (peer2peer o P2P), o centralizados (cliente-servidor).

Arquitectura Cliente/Servidor

Un servidor es un ordenador que comparte recursos y ofrece servicios a otros ordenadores (clientes) a través de la red. Algunos ejemplos de estos servicios son:

Servidor de archivos → Comparte carpetas.

Servidor de impresión → Comparte impresoras.

Servidor de correo electrónico.

Servidor web → Almacena y sirve a petición de los clientes los documentos web almacenados.

Servidor de base de datos.

Servidor FTP → Almacenamiento y descarga de archivos.

Servidor Proxy → Monitoriza el acceso del resto de equipos a la red exterior, sirve también para filtrar el tráfico permitiendo y denegando el acceso a ciertos sitios.

Normalmente una servidor sea dedicado, es decir, no se usará como estación de trabajo, sino únicamente para la tarea asignada. Hoy en día podemos tener varios servidores en una única máquina física, ejecutándose de manera independiente mediante la virtualización.

Servidor DNS

Cuando nos comunicamos con un ordenador que está en internet, a menudo usamos el nombre del dominio (gmail.com, youtube.es,...) en lugar de directamente usar la dirección IP.

Los servidores DNS proveen servicios en internet que se encargan de traducir estos nombres de dominio a sus respectivas IP y viceversa. Podmemos ver la IP de un dominio mandándole un ping a esa dirección, por ejemplo → Ejecutamos el comando: “ping nombre_dominio”.

Servidor DHCP

Dentro de una red local, cuando no necesitamos tener una dirección IP fija en un equipo (los servidores suelen necesitar una IP fija), la opción más sencilla es que se le asigne de forma automática. Para ello algún equipo de la red, normalmente el router, debe tener instalado un servidor DHCP.

El servidor DHCP se encargará de suministrar una ip automática (dentro de un rango definido) a los equipos que se lo pidan, también envía la configuración de los servidores DNS y la puerta de enlace (IP del router que da salida fuera de la red)

De forma temporal, el servidor DHCP guarda a que equipo (MAC) le ha asignado IP. Muchas veces esta IP asociada caduca (leasing time) y se le proporciona otra nueva.

Ethernet

Ethernet es un conjunto de tecnologías para la comunicación de dispositivos a través de la red local.

Utiliza cables de par trenzado de cobre, o de fibra óptica para distancias mayores a 100m, para el envío de información. Pudiendo llegar a velocidades de hasta 100Gb/s utilizando el cableado y los dispositivos adecuados. Acualmente se están desarrollando estándares para llegar a los 200 y 400Gbps.

Las especificaciones de esta tecnología vienen detalladas por el estándar IEEE 802.3. Para las conexiones mediante par trenzado de cobre, se utiliza un conector llamado RJ-45 para los extremos de cada cable.

Conector RJ-45

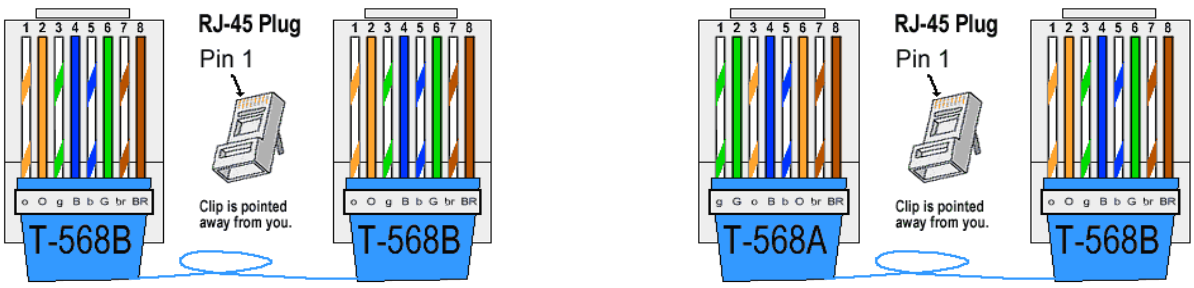
Este es el esquema de colores que deben tener los conectores de un cable RJ-45 según la normativa. Hay 2 variantes:

T-568A: Blanco-Verde, Verde, Blanco-Naranja, Azul, Blanco-Azul, Naranja, Blanco-Marrón y Marrón.

T-568B: Blanco-Naranja, Naranja, Blanco-Verde, Azul, Blanco-Azul, Verde, Blanco-Marrón y Marrón.

Si se va a conectar un equipo con un dispositivo de interconexión (switch, router con funciones de switch integradas), se debe usar un cable “paralelo” (ambos extremos iguales).

Si se conectan 2 dispositivos de interconexión (switch) entre sí, o 2 equipos entre sí directamente, se debe usar un esquema cruzado (T-568A → T-568B). De esta manera, los cables de envío de datos en un equipo (1 y 2) se convierten en los de recepción en el otro (3 y 6) y viceversa.

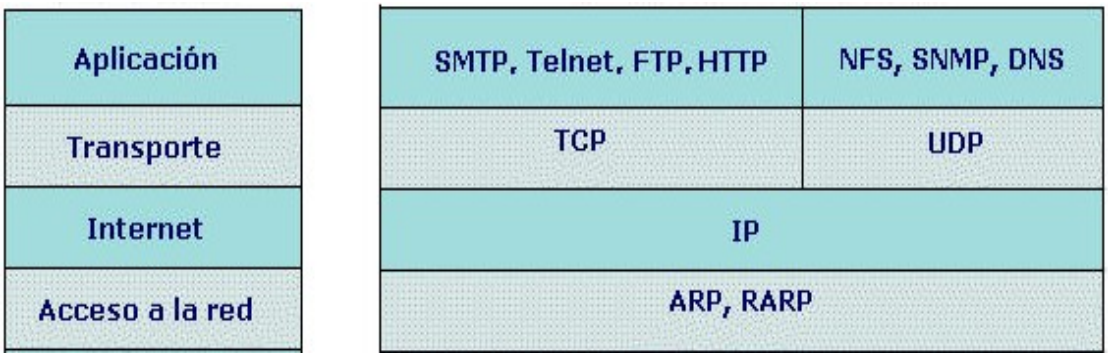


En cualquier caso, los dispositivos de interconexión (switches) hoy en día detectan el tipo de cable conectado y son capaces de cruzar internamente las conexiones si es necesario.

Protocolo TCP/IP

Es el modelo usado para las comunicaciones a través de las redes locales e internet. Las capas de arriba hacen uso de los servicios que le ofrecen las capas de abajo. En cada capa hay unos protocolos que se encargan de que los servicios de dicha capa funcionen correctamente.

Ejemplo: El protocolo IP (internet), necesita del protocolo ARP (Acceso a la red) para poder llegar a su destino dentro de una red local.



Acceso a la red – ARP

La capa de acceso a la red utiliza el protocolo ARP para lograr que un paquete de datos llegue a su destino dentro de una red local. Los dispositivos de interconexión como los switches trabajan a este nivel.

En las comunicaciones dentro de la LAN se utiliza la dirección MAC, sin embargo la dirección que configuramos es una dirección IP, y esta es la que se utiliza cuando queremos acceder a otro ordenador de la red.

El protocolo ARP se encarga de almacenar las equivalencias y traducir entre direcciones IP y direcciones MAC, y consiste en lo siguiente:

- Un ordenador A se quiere comunicar con otro B (sabe únicamente su IP)
- A envía un mensaje ARP a TODOS (broadcast) los ordenadores de la red preguntando por la MAC del que tiene esa dirección IP
    - La dirección de destino (Broadcast) será FF:FF:FF:FF:FF:FF (todos los bits a 1)
    - (A envía su propia MAC también)
- El ordenador B recibe ese mensaje y contesta a A, indicándole su dirección MAC
- A apunta la IP y la MAC de B en una tabla ARP, y B hace lo mismo.
- Si B no responde en un determinado tiempo de espera, A deja de esperar (no lo

encuentra).

- Cada cierto tiempo las entradas de la tabla ARP se van borrando (se puede cambiar una tarjeta de red de un equipo o la IP) y hay que volver a preguntar

- Se pueden crear entradas estáticas.

Comandos para ver la tabla ARP

Linux → arp -n

Windows → arp -a

```
Interface  220.0.0.80
Internet Address         Physical Address   Type
220.0.0.160              00-50-04-62-F7-23  static
192.128.0.3              00-54-0A-14-AC-13  dynamic
```

Dirección MAC

Identifica de forma única a una interfaz de red (cableada o inalámbrica) de un equipo o dispositivo en la red local (LAN). Las direcciones MAC vienen asignadas de fábrica a los dispositivos de red.

Se compone de 6 cifras de 8 bits (48 bits total), separadas por ":", y se suelen representar con 2 dígitos hexadecimales cada una (4+4 bits)

Ejemplo → E1:AC:30:00:6F:A7

Las 3 primeras cifras (24 bits) identifican al fabricante del dispositivo, mientras que las 3 últimas identifican de forma ÚNICA al dispositivo.

Una cifra hexadecimal está en base16 y va del 0 al 9 y de la A a la F (para representar dígitos mayores que el 9), por lo que tenemos 16 posibles dígitos. Internamente, un dígito hexadecimal se almacena usando 4 bits ($2^4 \rightarrow 16$).

Aquí puedes ver una equivalencia entre números decimales, hexadecimales, octales y binario:

http://www.sitiosargentina.com.ar/categorias/internet/formatos/tabla_conversion.htm

Internet (IP)

La capa de internet, provee de servicios para poder hacer llegar un paquete a su destino a través de internet. Los dispositivos de encaminamiento IP (routers), se encargan de redirigir los datos a su destino usando tablas de rutas IP y otras técnicas para optimizar el tiempo de llegada.

En la siguiente sección hablaremos de como funciona el encaminamiento de paquetes.

Capa de transporte

La capa de red (o capa de enlace) se encarga de transportar datos a través de las redes locales, y la capa de internet, de transportarlos por medio de routers a otra red diferente.

La capa de transporte se encarga, entre otras cosas, del control de errores en la comunicación, control de congestión, direccionamiento de aplicaciones mediante los puertos. Las aplicaciones que reciben comunicaciones de datos “escuchan” los puertos (16 bits → hasta el 65535) para recibir datos.

Cada aplicación tiene su puerto asignado. Hasta el 1024 son puertos estándar reservados por el sistema, y a partir de ahí, los puede usar cualquier aplicación.

http://es.wikipedia.org/wiki/Anexo:N%C3%BAmeros_de_puerto

Hay 2 protocolos de transporte → **TCP** y **UDP**

El protocolo TCP se encarga de verificar lo siguiente:

- Los datos llegan en orden (los ordena)
- Los datos no tienen errores (si no, pide un reenvío)
- Descarta los datos duplicados (reenvío por error)
- Controla la congestión del tráfico

El protocolo UDP sin embargo, no controla ninguna de estas cosas. Se utiliza para aplicaciones donde es importante que lleguen los datos lo más rápido posible sin importar que se pierdan algunos por el camino o que lleguen desordenados (audio y vídeo en tiempo real por ejemplo, donde no importa si en un momento fijo se han perdido unos cuantos píxeles o baja la calidad de sonido).

Capa de aplicación

Este es el nivel donde actúan las aplicaciones y servicios creados para diversos objetivos como compartir archivos, envío de correos, servidores web, etc. En la sección de Servicios en la red, ya hemos visto algunos ejemplos.

Dirección IP

La dirección IP sirve para identificar un dispositivo en redes que usan el protocolo TCP/IP (Internet por ejemplo). En una red local (LAN) sirve también para identificar a los equipos y dispositivos, aunque para comunicarse dentro de este tipo de red se utiliza realmente la MAC.

Se compone de 4 cifras de 8 bits, que se suelen representar en decimal, pero internamiente se trabaja con ellas en binario.

Ejemplo → 192.168.2.12 →En binario: 1100000.10101000.00000010.00001100

Hay una tabla de equivalencias (decimal-binario) en la subsección de la dirección MAC. En este otro enlace explican 2 métodos para transformar de decimal a binario:

https://es.wikihow.com/convertir-de-decimal-a-binario

Y aquí como hacer lo mismo de binario a decimal:

https://es.wikihow.com/convertir-binario-a-decimal

Máscara de red

Parte de una dirección IP se utiliza para identificar a la red, mientras que otra parte identifica al dispositivo. Para delimitar ambas partes se utiliza la máscara de red.

La máscara se representa como una dirección del mismo tamaño que una IP. Se representa en decimal, pero hay que pasarla a binario para entender cómo funciona. Para simplificar, también se suele indicar simplemente los bits que tiene la máscara de red después de la IP. Ejemplo: 192.168.2.12/**24**.

Los bits de la máscara empezarán con una cantidad de unos seguidos y el resto serán ceros.

- Los bits que están a 1, indican los bits de la IP que identifican a la red. Estos no se pueden alterar y deben permanecer fijos a la hora de asignar diferentes direcciones IP a equipos.
- Los que están a 0 indican qué bits identifican a los equipos de la red. Estos son los bits de la IP que se pueden usar para identificar equipos, salvo 2 excepciones:
    - Cuando todos los bits de la parte del equipo están a cero, hablamos de la dirección IP que identifica a la red actual, o **dirección de red**. Se usa en las tablas de encaminamiento para representar dicha red.
    - Cuando todos los bits de la parte del equipo están a uno, es una dirección

de **difusión** o **broadcast**. Se usa para que un mensaje llegue a todos los equipos de la red.

Tipos de redes locales estándar en función de los bits de la máscara (se puede usar cualquier tamaño de máscara):

- **Tipo A** (8 bits → 255.0.0.0). IPs de red que empiezan entre 1 y 126
- **Tipo B** (16 bits → 255.255.0.0). IPs de red que empiezan entre 127 y 191
- **Tipo C** (24 bits → 255.255.255.0). IPs de red que empiezan entre 192 y 223

Tendremos que traducir la máscara y la IP a binario (sobre todo en tamaños de máscara no estándar, o que no engloben bloques enteros de la IP) para saber identificar la parte que corresponde a la red y cual a los equipos en la IP.

IP → 192.168.2.12 Máscara → 255.255.255.0 (C)

IP (binario)→ 11000000.10101000.00000010.00001100

Máscara (binario) → 11111111.11111111.11111111.00000000

Los bits a 1 (máscara) identifican la red (192.168.2)

Los bits a 0 identifican al equipo (12)

Si tenemos **n** bits para identificar equipos dispondremos de (**2n – 2**) direcciones disponibles ya que como hemos indicado antes, hay 2 direcciones que no podremos usar para identificar equipos (red y broadcast).

Ejemplo → Si queremos una red de 7 equipos necesitaremos como mínimo 4 bits para los equipos → 2^4-2 = 14, mientras que con 3 no es suficiente → 2^3-2 = 6 equipos.

Subredes (Subnetting)

A partir de una dirección de red con una máscara predeterminada, podemos dividir esta en redes más pequeñas, lo que genera zonas independientes con menor cantidad de tráfico y saturación.

Para ello podemos incrementar la máscara tanto como necesitemos en función del número de equipos que queramos situar en cada segmento.

En función de lo que necesitemos bien podemos ir aumentando la máscara según el número de segmentos a crear:

Por ejemplo, a partir de una máscara de 24 bits (255.255.255.0), si la aumentamos en 2 bits (255.255.255.192), podríamos crear 2^2 → 4 subredes diferentes, cada una con capacidad para 2^6 – 2 = 62 equipos.

Encaminamiento

Todos los equipos, y routers sobre todo, tienen una tabla interna donde aparecen las redes a las que pueden acceder, y a que dirección IP (puerta de enlace) deben dirigir el paquete para que llegue a esa red.

Comandos "**route -n**" o "**netstat -n -r**" en linux. "**route print**" en Windows.

La red 127.0.0.0/8 representa a una red interna del equipo (físicamente no existe), la usan las aplicaciones para enviarse mensajes sin salir del equipo.

Las direcciones que empiezan por 169.x.x.x también están reservadas para para cuando una interfaz no tiene una IP válida (no ha podido ser asignada por algún motivo). Es una dirección que no se puede usar para identificar redes y equipos, sino que se utiliza porque la interfaz debe tener siempre alguna IP asignada.

Ejemplo de tabla de rutas en Windows

Dirección de red	Máscara de red	Puerta de enlace	Interfaz
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.33
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1
192.168.1.0	255.255.255.0	192.168.1.33	192.168.1.33
192.168.1.255	255.255.255.255	192.168.1.33	192.168.1.33

Ejemplo de tabla de rutas en Linux

Destino	Pasarela	Genmask	Indic	Métric	Ref	Uso	Interfaz
0.0.0.0	192.168.2.1	0.0.0.0	UG	0	0	0	eth0
192.168.2.0	0.0.0.0	255.255.255.0	U	1	0	0	eth0

En estas tablas se pueden distinguir 4 elementos fundamentales:

- **Dirección de red** / **Destino** → A la hora de buscar como llegar a un equipo, se mira a qué red pertenece, y se usa esa entrada para saber cómo llegar a él.
- **Máscara de red** / **Genmask** → Junto a la dirección de red, nos sirve para identificar del todo la red. Ambas entradas se pueden resumir en una sola si junto a la dirección de red se indican los bits de la máscara → 192.168.1.0/24.
- **Interfaz** → Interfaz de red del equipo (pueden haber varias cableadas, Wifi, etc.) por donde se enviará el paquete para que llegue a la red de destino. Se suele indicar la IP asignada a dicha interfaz o el nombre de la misma.

- **Puerta de enlace** / **Pasarela** → Dirección IP del router a quien tendremos que dirigir el paquete para que llegue a su destino. Esto indica que la red no está conectada directamente al equipo actual, ya que en ese caso se indicaría con la dirección especial 0.0.0.0.

Construir una tabla de encaminamiento

Primero pondremos la red (o redes) a las que esté conectado directamente el equipo. La puerta de enlace a esas redes será la ip que tenga asignada el equipo en esa tarjeta de red (igual que la interfaz), o también podemos poner “directo” en ese apartado.

Añadimos el resto de redes de nuestra organización, y como puerta de enlace ponemos el router al que le tenemos que enviar el paquete para que llegue.

La última dirección (si queremos tener salida a internet, por ejemplo) es la de por defecto (0.0.0.0) que engloba cualquier otra red que no esté especificada anteriormente. La puerta de enlace es el router que nos dará acceso a internet. En el ejemplo está la primera, pero nosotros la pondremos la última, ya que ese es el orden en el que se comprueba.

La estrategia que seguiremos para simplificar las tablas de rutas será siempre poner como puerta de enlace la IP del router más próximo al actual que lleve al destino. Además pondremos la dirección del router de destino que esté en la misma red que nuestro router.

Otra regla que podemos aplicar es que aquellas redes que para llegar a ellas, la puerta de enlace (router), sea la misma que la que tenemos por defecto, se pueden omitir de la tabla de rutas.

Se publicarán ejemplos de como realizar tablas de rutas a partir de un esquema de red.

PAT/NAT

El PAT (Port Address Translation) o NAT (Network Address Translation) de una única dirección, lo utilizan los router para que un equipo de la red externa pueda responder (o acceder directamente) a otro de la red interna, ya que por defecto, solo podrán dirigirse a la IP pública de dicho router.

NAT estático

Para que pueda establecer conexión directa un equipo de la red externa con uno interno, se debe establecer la traducción de forma manual (NAT estático).

Ejemplo: Si tengo un servidor web en mi red interna (el servicio web escucha en el puerto 80) y quiero que desde el exterior s puedan hacer peticiones a mi servidor (establecer conexión), debo hacer la siguiente equivalencia:

IP_EXTERNA_ROUTER:80 → IP_MAQUINA:80

De esta forma los equipos de fuera harán las peticiones al puerto 80 de la IP externa del router (IP pública) y este se encargará de redirigirlas al equipo interno.

NAT dinámico

Cuando un ordenador de la red interna establece una conexión con otro exterior, el router le asigna automáticamente un puerto (mayor de 1024) a esa conexión.

El equipo externo sólo verá la IP externa de nuestro router, pero también reciben el puerto al que deben responder.

Cuando el equipo manda la respuesta a nuestro router en el puerto asignado a la conexión, el router nos la redirige automáticamente a nosotros. Lo que hace el router es hacer una traducción para que un paquete que vaya hacia un equipo de la red interna (dirección privada) pueda llegar a su destino.

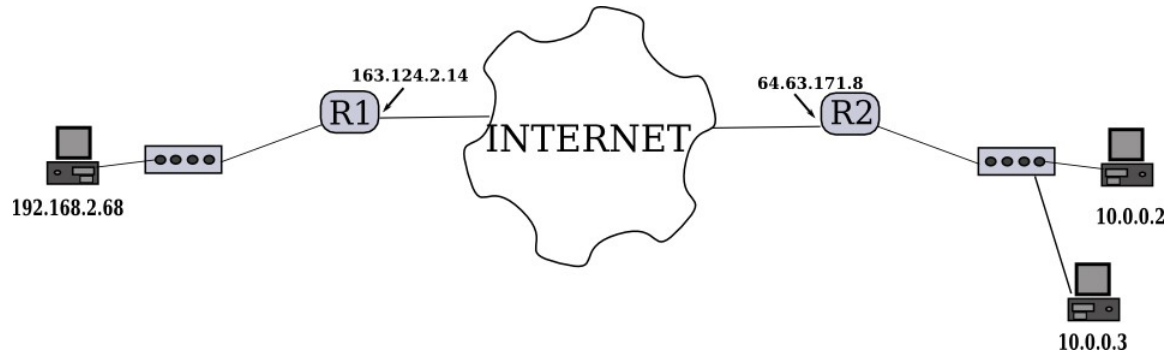
Cuando un equipo envía un paquete además de la IP de destino también tiene un puerto de destino. El equipo establece un puerto de origen, para que la respuesta la envíen a ese puerto.

Cuando se establece una conexión desde un equipo de la red interna hacia el exterior, el router guarda, mientras dure la conexión un puerto asociado a la IP del router que traducirá al puerto de respuesta del equipo interno.

Ejemplo

A partir de la siguiente situación: Nuestra red es la 192.168.2.0/24 y queremos conectarnos a través de internet con un servidor web que está escuchando en el puerto 80 en otra red privada (10.0.0.2/24). Como no podemos conectarnos directamente a una IP privada de otra red, debemos usar la IP pública del router que da acceso a dicha red (64.63.171.8). Eso significa que el router R2 tendrá una entrada

estática que redirija lo que reciba al puerto 80 de su IP pública



Ahora vamos a ver la secuencia que siguen los paquetes que van desde el cliente al servidor (petición) y la respuesta generada:

1. El equipo 192.168.2.68 realiza una petición al servidor web poniendose él como origen, reservando un puerto aleatorio libre mayor que 1024 para la respuesta. Como destino la IP pública del router R2 (puerto 80).
   - origen (192.168.2.68:1025) → destino(64.63.171.8:80)
2. El router 1 recibe el paquete del cliente. Como no puede mantener la dirección de origen, ya que es privada y no podrían responder desde el exterior, reserva un puerto propio (cualquiera que tenga libre) para recibir la respuesta y cambia la IP de origen por la suya. Además, añade de una entrada NAT dinámica para que cuando le llegue la respuesta sepa a quien redirigirla.
   - origen (163.124.2.14:2020) → destino(64.63.171.8:80)
3. El router 2 recibe la petición y consulta su tabla NAT. Ve que el paquete con esa dirección de destino y puerto le corresponde al servidor web, cambia el destion y le envía el paquete.
   - origen (163.124.2.14:2020) → destino(10.0.0.2:80)
4. El servidor de correo lo recibe y le contesta al origen:
   - origen (10.0.0.2:80) → destino(163.124.2.14:2020)
5. El router 2, antes de enviarlo fuera de la red traduce la dirección del emisor cambiando la ip privada por su ip pública (como tiene una equivalencia en su tabla NAT, la utiliza).
   - origen (64.63.171.8:80) → destino(163.124.2.14:2020).
6. El router 1 recibe el paquete, consulta su tabla NAT y comprueba que lo que llegue a 163.124.2.14:2020 tiene una equivalencia con un equipo de la red interna, así que cambia el destino y lo redirige.
   - origen (64.63.171.8:110) → destino(192.168.2.68:1025)

Las tablas NAT de los routers quedarían así durante la conexión:

Router 1

IP Pública	IP Privada
163.124.2.14:2020	192.168.2.68:1025 (dinámica)

Router 2 (Son NAT estáticas):

IP Pública	IP Privada
64.63.171.8:80	10.0.0.2:80 (estática)

IPv6

Para solventar el problema de la escasez de direcciones IPv4, entre otros, hace años que existe el nuevo estándar IPv6, aunque aún no se utiliza demasiado en la práctica. Este estándar permite hasta 2^128 direcciones posibles (128 bits), por lo que se puede asignar una IP pública única a todos los dispositivos conectados a internet. IPv6 también permite que un único equipo (interfaz de red) tenga múltiples direcciones IP asignadas.

Las direcciones IPv6 se representan con 128bits, separados en 8 grupos de 16bits, cada grupo representado con 8 caracteres hexadecimales.

```
Ejemplo: 2001:0db8:85a3:08d3:1319:8a2e:0370:7334
```

Cuando hay grupos de ceros consecutivos se pueden omitir, pero sólo se puede hacer en una parte de la dirección.

```
2001:0DB8:0000:0000:0000:0000:1428:57ab
```

```
2001:0DB8::1428:57ab
```

Los ceros iniciales también se pueden omitir (en ese caso, se debe hacer en todos los grupos).

```
2001:DB8:0:0:0:F4:428:57ab
```

Si hay más de 1 grupo de ceros no consecutivos, sólo se puede “comprimir” uno de ellos.

```
2001:0db8:0000:0000:1319:0000:0000:7344
```

```
2001:db8::1319:0:0:7344
```

~~2001:db8::1319::7344~~

La razón es que no podemos saber cuantos bloques faltan en cada sitio.

Para representar una dirección IPv4 en formato IPv6 y así tener sistemas híbridos, pasamos la dirección IPv4 a hexadecimal y los representamos como los últimos 32 bits, precedidos de un bloque FFFF.

```
192.168.12.4 → 11000000.10101000.00001100.00000100
```

```
::FFFF:C0A8:0C04
```

Máscara de red (prefijo) en IPv6

En IPv6, la parte invariable de la dirección de red, viene dada por el prefijo asignado a la misma. El funcionamiento es similar a la máscara de red en IPv4. El tamaño de los prefijos es el siguiente:

En IPv6, siempre se usan los últimos 64 bits para la dirección de equipo (2^{64}), por lo que los primeros 64 representan la dirección de red, y se utilizan para crear diferentes subredes.

```
2001:0DB8:0000:0000 (red) :0000:0000:1428:57ab (equipo)
```

Los 48 primeros se utilizan para crear las diferentes redes a nivel global que usaran los ISP (proveedores de internet). A partir de ahí, los siguientes 16 bits se usan para crear subredes.

bits	48 (o más)	16 (o menos)	64
campo	*routing prefix*	*subnet id*	*interface identifier*