FUNDAMENTOS DE REDES

1. INTRODUCCIÓN

En esencia, una red es un conjunto de equipos informáticos interconectados entre sí. En toda red, hay una parte física y otra parte lógica. La parte física, está compuesta por todos los elementos materiales (hardware), y los medios de transmisión. La parte lógica (software), son los programas que gobiernan o controlan esa transmisión y la información o datos que es transmitida.

De este modo, una red de ordenadores puede ser entendida desde dos vertientes distintas:

- Conjunto de equipos interconectados entre sí con el fin de compartir recursos y transmitir información.
- Sistema de comunicación de datos entre equipos distintos.

Una red es, en definitiva, como un sistema de dos o más ordenadores (autónomos) que, mediante una serie de protocolos, dispositivos y medios físicos de interconexión, son capaces de comunicarse con el fin de compartir datos, hardware y software, proporcionando así acceso a un mayor número de recursos con un menor coste económico y facilitando su administración y mantenimiento.

ORIGEN

Aunque los primeros avances en el estudio de redes de ordenadores se dieron en los Estados Unidos, el elemento detonador de todo el proceso es necesario buscarlo en otro país, la URSS. Tras el primer lanzamiento del satélite artificial Sputnik, por parte de la URSS, en los Estados Unidos se sentían derrotados en la guerra fría y necesitaban una revisión de las políticas de desarrollo científico y tecnológico que se habían realizado hasta entonces. En este marco es en el que surge en 1957 la agencia ARPA (*Advanced Research Projects Agency*) dependiente del Departamento de Defensa. Sus objetivos estaban vinculados con el desarrollo tecnológico aplicado a la defensa, pues se consideraba altamente peligroso que la URSS fuese por delante en las distintas carreras emprendidas en la guerra fría.

No se producen verdaderos avances hasta comienzos de la década de los 60, y estos avances se centran más en aspectos conceptuales que tecnológicos. Así en 1962, J.C.R. Licklider (psicólogo e informático) en ARPA propuso la interconexión de ordenadores para el desarrollo de trabajo colaborativo entre investigadores. Simultáneamente, en el MIT (*Massachusetts Institute of Technology*) L. Kleinrock escribió el primer artículo "Flujo de información entre Redes amplias de comunicación" sobre tecnología de comunicación por cable mediante conmutación de paquetes, sentando así las bases para la comunicación entre ordenadores.

En 1964 J.C.R. Licklider abandona ARPA y marcha al MIT para trabajar junto a W. Clarck. Fruto de esta colaboración es su publicación "*Online Man Computer Communication*" donde presentan la necesidad de la colaboración a través del uso de ordenadores. Un año después, P. Barand realiza la primera propuesta realmente viable para la utilización de redes de ordenadores basando su comunicación en la conmutación de paquetes.

Con el patrocinio de ARPA, un año después, dos máquinas, situadas en el MIT (XT-2) y en *System Developmen Corporation* de Santa Mónica (AN/FSQ-32), se unen mediante una línea dedicada cuya velocidad de transmisión era de 1200bits por segundo.

A partir de la publicación en 1966 de "*Towards a Cooperative Network of Time-Shared*" por parte de L.G. Roberts del MIT, se sientan las bases para la creación de ARPANET (red de ordenadores de ARPA) y de la primera red de ordenadores. Tres años después y tras la creación de la primera interfaz

para enrutar la comunicación entre distintos nodos (router) el IMP (*Interfase Message Processor*), se construye ARPANET con cuatro nodos situados en la Universidad de California-Los Ángeles, el *Stanford Reseach Institute* (San Francisco, California), la Universidad de California en Santa Bárbara y la Universidad de Utah.

La primera comunicación se produjo entre Stanford y UCLA el 20 de octubre de 1969, exactamente tres meses después de que el hombre pisara por primera vez la luna. Se había dado el primer paso para la mayor revolución tecnológica del siglo XX. Internet, la comunicación entre ordenadores, el correo electrónico, el teletrabajo, la videoconferencia, son elementos que se han integrado en nuestra rutina y que van a provocar la mayor revolución cultural que haya expedientado la humanidad en el siglo XXI.

1.1. COMPONENTES DE UNA RED

Para determinar los elementos que componen una red debemos diferenciar entre los elementos físicos y los componentes lógicos. Entendemos por componentes físicos todo el hardware y medios físicos necesarios para la comunicación entre ordenadores. Los componentes lógicos son los protocolos de comunicación y el software que permite esa comunicación.

Resulta evidente que, dependiendo del tamaño de la red y las prestaciones que deseemos que nos ofrezca, estos componentes pueden aumentar en número y complejidad. Para facilitar su comprensión, vamos a centrarnos inicialmente en una red formada por dos ordenadores:

- Elementos físicos:
  - Dos equipos.
  - Una entrada y salida física de comunicación entre cada uno de los equipos y el medio físico de comunicación.
  - Un medio físico para la transmisión de datos.
- Elementos lógicos:
  - Software.
  - Protocolos de comunicación.

La unión física entre ambos ordenadores podrá realizarse a través de puerto serie, del paralelo, a través de USB o, como es más habitual, a través de un cable de red conectado a un concentrador, aunque si se tratara de dos equipos sólo, se puede hacer a través de un cable de red de tipo cruzado. Esta comunicación entre ordenadores puede acoger tecnologías de última generación como las redes inalámbricas basadas en el estándar 802.11x (Wi-Fi) o las basadas en BlueTooth.

Cuando nos encontramos con redes constituidas por más de dos equipos, debemos empezar a emplear otros tipos de mecanismos de interconexión. En estos casos, la red estaría constituida por:

- Ordenadores autónomos.
- Elementos de interconexión:
  - Puertos o adaptadores de red. Permiten la comunicación entre el equipo y el medio físico de comunicación.
  - Medio físico para el transporte de datos.
    - Medios guiados: cable coaxial, par trenzado, fibra óptica,...
    - Medios no guiados: ondas de radio, infrarrojos, etc.
  - Mecanismos de interconexión: concentradores, conmutadores, puentes, enrutadores, cortafuegos, transceptores, módem, MSAU, etc. Los mecanismos de interconexión aparecen cuando es necesaria la comunicación de varios equipos con un nivel de eficiencia alto.
  - Otros: terminales, acopladores, repetidores, conector RJ45, BNC, etc.
- Software de conexión y protocolos de comunicación.

1.2. RECURSOS

RECURSO

Un recurso es un elemento instalado en un equipo que puede ser utilizado por el resto de equipos y usuarios de la red. Los principales recursos compartidos, clasificados según su tipo, son:

- Hardware:
  - Unidades de almacenamiento: permite
    - ahorro en la adquisición de estos materiales
    - información centralizada, evitando la repetición y la dispersión de estos archivo
    - facilita el trabajo en común
    - garantiza la seguridad ante pérdidas o deterioro de la información, ya que al estar centralizada, las copias de seguridad son más sencillas de realizar
  - impresoras
    - poder minimizar el número de ellas, redunda en un importante ahorro de coste
  - distintos periféricos de entrada o salida, escáneres, cámaras, etc.
- Software: cualquier tipo de aplicaciones, paquetes de programas, programas, etc.
  - Servidores de aplicaciones
- Información: todo tipo de datos; de texto, numéricos, bases de datos, imágenes, audio, etc.
  - Acceso a Internet empleando una única conexión pudiendo establecer una serie de medidas de seguridad mediante un cortafuegos que evite el acceso a contenidos inadecuados a la vez que se protege la red del ataque de intrusos

ARQUITECTURA CLIENTE-SERVIDOR

Es la base para la utilización de los recursos disponibles en una red:

- Servidor: un ordenador conectado a una red que tiene algún recurso que puede ofrecer a los demás. Normalmente, el servidor es un ordenador más potente y con más prestaciones que el cliente, pero no siempre es así.
- Cliente: entendemos como tal cualquier ordenador conectado a la red que utiliza los recursos que le ofrecen los equipos servidores.

Como vemos estos dos términos son inseparables, el cliente solicita algún recurso y el servidor los ofrece. Es un proceso cooperativo entre cliente y servidor.

Una red cliente-servidor puede ser de arquitectura:

- **Centralizada**: los recursos estarán centralizados en un ordenador servidor (aunque pueden ser varios los servidores), y los demás ordenadores accederán a él solicitando sus recursos siendo solamente clientes.

  En una red con Active Directory hay un ordenador central, llamado Controlador de Dominio, que centraliza el control de acceso de los usuarios y el acceso de estos a los recursos. Aunque una impresora esté conectada a un equipo cliente X, el resto de usuarios de la red podrán acceder a ella previa solicitud y autorización del Controlador de Dominio

- **Distribuida**: (red entre iguales) en este caso los recursos estarán distribuidos entre los distintos ordenadores que conforman la red y cada uno podrá, o no, ofrecer a los demás los recursos de que disponga. Cada equipo es servidor cuando ofrece un recurso a los demás y cliente cuando usa los recursos de los demás.

> En una casa tenemos una conexión de Internet y seis equipos: 2 ordenadores de sobremesa (conectados por cable), 2 portátil, 1 tablet y 1 móvil (conectados por Wi-Fi). Uno de los equipos de sobremesa tiene conectada una impresora de inyección compartida. Y el otro una láser. Podremos imprimir desde cualquiera de los equipos en cualquiera de las impresoras previa solicitud y autorización del equipo que tiene su conexión física

- **Mixta**: es una mezcla de ambas, con parte distribuida y parte centralizada. El grado de centralización puede ser variable en cada caso.

> En un aula tenemos una red LAN con 15 equipos para alumnos y 1 para el profesor. Todos están conectados entre sí mediante una red entre iguales, pero para acceder a Internet los alumnos deben hacerlo a través de un software de servidor Proxy instalado en el equipo del profesor. Así, el acceso a Internet está centralizado mientras que el acceso a otros recursos, como la impresora o las carpetas compartidas, es distribuido.

La seguridad es un tema clave a la hora de determinar una arquitectura. Cuando se utiliza un modelo centralizado se garantiza la seguridad desde todos los puntos de vista, sin embargo, en las redes entre iguales se obtiene un nivel de seguridad mucho más bajo.

Normalmente en una red centralizada los servidores, debidamente configurados por el administrador de red, son los encargados de identificar a los usuarios, conceder los permisos pertinentes para acceder a los distintos recursos, etc.

En una red entre iguales, el control de acceso lo realiza cada ordenador individualmente y el acceso a los recursos es menos restringido.

1.3. TIPOS DE REDES

1.3.1 POR SU TECNOLOGIA DE TRANSMISIÓN

BROADCAST O DE DIFUSION

Hay un único canal de comunicación, compartido por todos los ordenadores de la red. Los ordenadores envían mensajes cortos, denominados tramas, que llegan al resto de los ordenadores de la red. Sin embargo, esto no quiere decir que todos los mensajes tengan como destinatarios, siempre, la totalidad de los ordenadores de la red.

Los protocolos que se utilizan en estas redes deben permitir determinar cuándo un mensaje se envía a todos los ordenadores o cuándo lo hacen únicamente a uno, del mismo modo, deben preocuparse de controlar que no se produzcan colisiones.

En la trama, aparte de la información propiamente dicha, hay un campo que indica el origen y el destino de dicha información. Pudiendo determinarse si el mensaje se envía a todos, a uno, o varios ordenadores en concreto.

Cuando el mensaje se dirige a todos los equipos de la red estamos enviando un mensaje broadcast. Todos los ordenadores reciben el mensaje y lo procesan. Sin embargo, si el mensaje no es broadcast, al ser un medio compartido y, dependiendo del dispositivo de interconexión, puede que todos los equipos lo reciban, pero, en este caso, si la trama no iba dirigida a él, la ignora.

Se usan mensajes broadcast en muchas situaciones, por ejemplo, cuando un ordenador se conecta a una red envía un mensaje de este tipo en busca de un servidor que le pueda asignar una dirección IP. También, cuando desconoce una dirección MAC (dirección de la tarjeta de red) de un equipo, envía un mensaje de broadcast al resto de los equipos de la red para que alguno le pueda proporcionar esta información.

Un mensaje multicast es el que se dirige a varios de los equipos de la red.

Un mensaje unicast es el que se envía a un único equipo.

> Un ejemplo de transmisión por difusión puede ser la señal de televisión por cable. Todos los clientes (televisores) reciben los mismos mensajes. En la emisión en abierto, los mensajes son broadcast por lo que todos pueden cogerlos.
>
> Si es una emisión de pago, se transmiten mensajes multicast que sólo podrán recoger los abonados a dicho canal.
>
> Por ultimo, si es un canal interactivo, se mandaran mensajes unicast individuales a cada uno de los abonados que ha hecho una petición.

En este tipo de redes, el problema principal, es la asignación del canal (medio de transmisión), ya que éste es único, y debe ser compartido por todos los ordenadores. Para solucionar esto, se han creado múltiples protocolos, que pertenecen al nivel MAC (Control de Acceso al Medio). Hay dos métodos:

- **Asignación estática**: se divide el ancho de banda[1] del canal entre los ordenadores que lo usan. Es decir, si un canal posee 100 Mbps de ancho de banda y disponemos de diez equipos conectados al medio, éste es dividido en diez partes de 10 Mbps, reservando una de ellas para cada uno de los equipos. Este sistema de asignación permite que cada ordenador no dependa del resto para comunicar aunque, si sólo necesita enviar datos uno de ellos, los otros 90 Mbps están desaprovechados. Su mayor ventaja es que se evitan las interferencias y colisiones.
- **Asignación dinámica**: que permite gestionar la utilización de un único medio en función de las necesidades de comunicación de los equipos en cada momento, repartiendo el ancho de banda entre los usuarios conectados en un momento dado. Si se conecta o desconecta algún usuario, se puede procede a repartir de nuevo. Así, en el caso anterior si sólo hay 2 equipos conectados, cada uno podrá disponer de 50 Mbps. Al conectarse un tercer equipo, se redistribuye el ancho de banda, pasando a ser de 33Mbps por equipo.

REDES PUNTO A PUNTO

En este caso, las conexiones son punto a punto, entre pares de ordenadores. Se establece una comunicación directa entre los dos ordenadores.

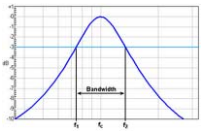
Hasta que un mensaje llega a su destino, puede pasar por varios nodos intermedios. Dado que existe más de un camino posible, hay algoritmos de encaminamiento (routing), que lo gobiernan.

Este tipo de redes, usa tres tecnologías diferentes:

- **Conmutación de circuitos**: en la que se establece un "circuito virtual" entre los dos puntos, mientras dura la conexión. Dicho circuito se crea buscando conexiones libres entre los distintos nodos que componen la red (routing).

> Con este método funciona el sistema telefónico. Al hacer una llamad se establece un circuito temporal entre el emisor y el receptor. Durante el tiempo que dure la conversación, el circuito queda bloqueado al resto de usuarios (circuito dedicado). Al terminar la llamada, el circuito temporal se libera.

[1] El ancho de banda de una señal analógica es la longitud, medida en Hz, del rango de frecuencias en el que se concentra la mayor parte de la potencia de la señal. Así, en una señal, el ancho de banda viene determinado por el rango de frecuencias en el que la transmisión es fiable, descartándose las frecuencias superiores o inferiores en que la señal puede ser deteriorada



Determina la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período dado. El ancho de banda se indica generalmente en bits por segundo (bps), kilobits por segundo (Kbps), o megabits por segundo (Mbps).

- **Conmutación de mensajes**: El emisor añade al mensaje la dirección de destino pasando de un nodo al siguiente sin establecer un circuito físico entre los nodos que se comunican. Se certifica sin están libres de errores antes de reenviarlos al nodo siguiente.

  > Sería similar a enviar un sobre con un conjunto de documentos por medio de correos. Se echa el sobre al buzón. Un empleado de correos recoge el sobre del buzón y lo lleva a la distribuidora local. Otro empleado lo traslada desde la distribuidora local hasta la distribuidora del destino. El cartero traslada el sobre hasta el buzón del destinatario.

- **Conmutación de paquetes**: en las que el mensaje se divide en partes, denominadas paquetes -grupos de bits- que tienen una parte destinada a los datos propiamente dichos y otra a las señales de control como son el origen y el destino, los mecanismos de recuperación de errores, etc. Tienen una longitud máxima permitida y si se excede pueden ser divididos en paquetes más pequeños. Los paquetes se envían independientemente unos de otros, incluso desordenados y por distintos caminos, hasta su destino, donde se debe reordenar y recomponer el mensaje. Se retransmiten nodo a nodo igual que en la conmutación de mensajes.

  > Supongamos que mandamos una serie de paquetes (con los distintos componentes de un mueble de Ikea) con distintos mensajeros a un único destino. Cada mensajero cogerá un camino distinto según el resto de entregas que tenga que realizar. Por tanto, los paquetes llegan a destino desordenados y en distintos periodos de tiempo. Nuestro montador deberá esperar a tener todos los paquetes ya que si falta alguno (por ejemplo, los tornillos) no podrá montar el mueble.

- **Conmutación de celdas**: Es una solución similar a la anterior, si bien, en este caso, el formato de los paquetes (en este caso celdas), debe ser homogéneo.

Broadcast	**Punto a punto**
Fundamentalmente empleada en redes locales (LAN)	Fundamentalmente empleada en redes de largo alcance (WAN)
El software es más simple puesto que no necesita emplear algoritmos de routing y el control de errores es de extremo a extremo.	Los algoritmos de routing pueden llegar a ser muy complejos. Se necesitan dos niveles de control de errores: entre nodos intermedios y entre extremos.
Para que la estación reciba el mensaje, debe reconocer su dirección en el campo de destino.	La información se recibe. Una vez leído el mensaje se procesa si va dirigido a la estación, o se reenvía si tiene un destino diferente.
Un único medio de transmisión debe soportar todos los mensajes de la red, por lo que son necesarias líneas de alta velocidad (>1 Mbps)	Varias líneas de comunicación pueden funcionar en paralelo, por lo que pueden usarse líneas de baja velocidad (2-50 Kbps)
Los principales retrasos son debidos a las esperas para conseguir el acceso al medio.	Los principales retardos son debidos a la retransmisión del mensaje entre varios nodos intermedios.
El medio de transmisión puede ser totalmente pasivo y, en ese caso, más fiable (no puede ser interferido).	El medio de transmisión incluye nodos intermedios por lo que es menos fiable (puede ser interferido).
Se necesitaría duplicar las líneas en caso de que se quiera asegurar la funcionalidad ante fallos.	La redundancia es inherente siempre que el número de conexiones de cada nodo sea mayor de dos.
Los costes de cableado de la red son menores. Sólo es necesaria una tarjeta de interfaz por estación.	Los costes de cableado son superiores, y la estación requiere al menos dos tarjetas de interfaces.

1.3.2 POR EL TAMAÑO

REDES DE ÁREA LOCAL (LAN: LOCAL AREA NETWORK)

Son redes privadas con un medio físico de comunicación propio. Se consideran restringidas a un área geográfica determinada: centro docente, empresa, etc. aunque puedan extenderse en varios edificios empleando distintos mecanismos y medios de interconexión. En las redes de área local, la longitud máxima de los cables, que unen los diferentes ordenadores, puede ir desde 100 metros, con cable de par trenzado, hasta algunos kilómetros en segmentos unidos por fibra óptica. La velocidad de transmisión típica va desde los 10 Megabit/s hasta 1 Gigabit/s en la actualidad.

REDES METROPOLITANAS (MAN: METROPOLITAN AREA NETWORK)

Este tipo de redes es similar en su estructura y funcionamiento a las LAN, si bien ocupan una mayor extensión geográfica y pueden ser públicas o privadas. Disponen de una serie de estándares específicos que las diferencian de las redes LAN y WAN. Uno de estos estándares es conocido como DQDB (Bus Dual de Cola Distribuida) y está adaptado a las características de las redes MAN, que no necesitan elementos de conmutación y dirigen la información empleando dos cables unidireccionales, es decir, un bus doble en el que cada uno de los cables opera en direcciones opuestas.

En este tipo de redes no se pueden producir colisiones ya que se procuran métodos para el control de acceso al medio, los generadores de tramas emiten de forma regular una estructura de trama que permite la sincronización de los equipos a la hora de transmitir, ya que podrán acceder al medio cuando un contador interno (sincronizado por la trama enviada por el generador) se ponga a cero.

Cada nodo recibe la información por un bus de los nodos posteriores y envía por el otro, de manera que puede estar emitiendo y recibiendo información de forma simultánea.

REDES DE ÁREA EXTENSA (WAN: WIDE AREA NETWORK)

Consisten en ordenadores y redes de área local y metropolitanas, unidas a través de grandes distancias, conectando equipos y redes a escala nacional o internacional. La comunicación se consigue mediante routers (encaminadores) y en algunos casos gateways (llamados también convertidores de protocolos o pasarelas).

Sus características son:

- Velocidades de transmisión lentas comparadas con redes de área local.
- Alta tasa de errores, necesitando sistemas de detección y recuperación de errores.
- Posibilidad de reconfiguración de las redes debido a su menor fiabilidad.
- Técnicas de almacenamiento y reenvío (*Store and Fordward*) en los nodos de comunicación.

Están compuestas por un conjunto de nodos interconectados donde los datos son encaminados a través de los mismos desde un emisor hasta el receptor. Utilizan transmisión punto a punto.

INTERNET

Internet es una red de redes, aún más, es “la red de redes”. Conecta multitud de redes, de distinta índole, tamaño, características, etc., distribuidas por todo el mundo. Las redes pueden ser públicas (institucionales, educativas, etc.) o privadas (empresariales, de ocio, etc.) La conexión es posible entre redes de distintas plataformas y ambientes. Esta conexión, entre redes tan distintas, es posible porque todas utilizan el mismo protocolo de comunicación, el TCP/IP. En realidad son dos protocolos, TCP (*Transmisión Control Protocol*) e IP (*Internet Protocol*).

Los redes intermedias se comunican entre si usando la tecnología punto a punto, por medio de paquetes, que contienen, por un lado, la dirección del origen y el destino, y por otro, los datos a transmitir. Todo este proceso, está regido por una serie de normas incluidas en los protocolos TCP/IP.

Cada ordenador está identificado inequívocamente por su dirección IP. Además de la dirección IP, también puede identificarse un ordenador por su nombre de dominio (nombre DNS, *Domain Name System*). Estos tienen una estructura jerárquica. Son una serie de letras separadas por puntos, de la forma google.com. Esta forma es más fácil de recordar, ya que cada palabra entre puntos puede tener un significado (google.com, mail.google.com)

Entre la dirección IP y el nombre de dominio hay una relación biunívoca. De esta forma siempre que se da el nombre DNS de un ordenador, en realidad se da su dirección IP.

1.4. MODELOS CONCEPTUALES

Siempre que se pretende una comunicación del tipo que sea, se deben cumplir una serie de requisitos básicos, como son el tipo de lenguaje a utilizar, el tipo de información a transmitir, el momento, el modo, etc. Cuando dos equipos intentan establecer una comunicación deben hablar el mismo lenguaje y ponerse de acuerdo en una serie de normas. Estas normas son lo que denominamos **protocolo**. Protocolo es, por tanto, el conjunto de normas mutuamente aceptadas que van a regir el diálogo entre los equipos de una red.

> En la comunicación humana, su equivalente sería cada uno de los idiomas con sus respectivas reglas gramaticales y vocabulario. Así, la comunicación entre un hablante chino y otro español no es posible ya que usan distintos protocolos.

Pero, ¿cómo se comunican dos ordenadores? Evidentemente, estamos ante un tema complejo, ya que se están poniendo en juego múltiples elementos. Pensemos, por ejemplo en el proceso que aparece desde que damos la orden en un procesador de textos para que se imprima un documento en un equipo, hasta que esa orden llega a otro ordenador que está compartiendo la impresora y se imprime el archivo.

En principio disponemos de EMISOR que, a través de un MEDIO y empleando un CÓDIGO, envía un MENSAJE a un equipo RECEPTOR, pero, el código que van a emplear los ordenadores para comunicarse debe adaptarse al medio por el que debe circular el mensaje, por lo que se deben implementar unos elementos que codifiquen y decodifiquen la información para que pueda circular por el medio físico del que disponga esa red.

La manera de solucionar este problema fue tratar de dividirlo en subproblemas más fáciles de atacar. A estos subproblemas los denominamos niveles o capas. Así, la comunicación entre ordenadores queda estructurada por niveles y forma lo que llamaríamos una **arquitectura de protocolos de comunicaciones.** Trabajando con estas arquitecturas, la comunicación entre máquinas era un hecho, sin embargo, uno de los problemas que se tenía al principio era que cada fabricante trabajaba con su propio protocolo, encontrándonos con redes imposibles de interconectar debido a que trabajaban con distintas arquitecturas y protocolos. Eran los modelos llamados "cerrados o propietarios". En estos casos, la comunicación entre equipos pertenecientes a redes con distintos protocolos era totalmente inviable. Evidentemente se requería una arquitectura normalizada que sirviera como estándar o modelo de referencia.

1.5. MODELO DE REFERENCIA OSI

En el modelo de referencia OSI se pueden distinguir tres características fundamentales:

- **Arquitectura**, en la que se definen los aspectos básicos de los distintos niveles. Todos los niveles trabajan para dar un servicio al usuario del ordenador que desea comunicarse u obtener un servicio de otro equipo interconectado. La arquitectura OSI, divide todas las tareas en una serie de niveles que cooperan entre sí. Cada nivel se relaciona con el inmediatamente superior e inferior mediante el concepto de interfaz, formado por un conjunto de elementos físicos y lógicos que relacionan dos niveles adyacentes. Los interfaces entre un nivel n y sus niveles adyacentes n-1 y n+1, están definidos por los servicios ofrecidos. Por ejemplo, un nivel puede ofrecer al nivel superior la traducción, a un lenguaje común, de la comu-

nicación que se desea enviar (es su traductor), y una vez que ha efectuado su trabajo, cuenta con un nivel inmediatamente inferior que, por ejemplo, va a envolver la información ya traducida, sería su "empaquetador".

A su vez, para el intercambio de información entre unidades funcionales del mismo nivel, se definen un conjunto de reglas denominadas protocolos.

- **Servicios**, proporcionados por un nivel al nivel inmediatamente superior.

  Para entablar una comunicación, cada nivel, empezando por el más alto, envía la información al nivel lindante inferior hasta llegar al nivel más bajo que accede directamente al medio físico (cable, ondas de radio, etc.) En la máquina receptora la información seguirá el camino ascendente hasta llegar al nivel superior. Cada nivel utiliza los servicios del nivel inmediatamente inferior e incorpora una serie de mecanismos que le permiten mejorar dichos servicios ofreciendo al nivel superior servicios más sofisticados. Sin embargo, un nivel no conoce la forma en que el nivel inferior ha realizado el servicio ofrecido, está diseñado para realizar una función con independencia de lo que puedan hacer los otros niveles.

  Un nivel solicita los servicios del nivel inferior utilizando una serie de primitivas de servicio. Mediante la primitiva se especifica la función a realizar y con los parámetros que se pasan se transfiere la información de datos y control. Podemos comparar las primitivas de servicio con una serie de mensajes u órdenes (siempre las mismas) que se emplean para poder realizar un servicio.
- **Protocolos**, es decir, la información de control transmitida entre los sistemas y los procedimientos necesarios para su interpretación. Tal como hemos descrito, la comunicación entre dos equipos se hace mediante la relación (lógica) que establecen los niveles similares de los distintos nodos. Así, las entidades de un mismo nivel, emplean protocolos propios.

1.5.1 LOS NIVELES OSI

> Supongamos que deseo enviar un ramo de flores a alguien. Dependo de la floristería para comprarlo y que lo forme, pero el encargado de la tienda debe buscar a otra persona que se encargue de recoger el ramo y llevarlo a su destinatario, y ya con su regalo, alguien debe desenvolverlo y ponerlo en agua. Se ha establecido una cadena de dependencias y servicios entre unas personas y otras. Si no hay florista no hay ramo que enviar, pero sin mensajero el ramo no llegaría nunca.
>
> En este ejemplo tenemos 5 niveles de ejecución: encargar el ramo, hacerlo, transportarlo a destino, recibirlo y colocarlo. Cada uno de los niveles es independiente y no tiene por que saber nada de cómo se realiza el trabajo en los otros niveles.

En el modelo OSI se trabaja con 7 niveles, cada uno de los cuales que ofrece un servicio distinto a la comunicación entre equipos y utiliza un conjunto de protocolos independientes entre sí.

Estos servicios tienen un doble sentido, cuando los datos van bajando hasta el último nivel y cuando, en el equipo receptor ascienden hasta el nivel de superior.

NIVEL FÍSICO

Se encarga de la **transmisión de bits** por un medio de transmisión, ya sea un medio guiado (un cable) o un medio no guiado (inalámbrico). Esta capa define el medio de transmisión y los conectores desde cuatro puntos de vista:

- Funcionales: tipo de conectores, número y uso de los pines, etc.
- De procedimiento: secuencia de eventos por la cual cadenas de bits son intercambiadas.
- Mecánico: tipo de cable (fibra óptica, cable par trenzado, enlace vía satélite...), aislante, etc.
- Eléctrico: voltaje que representa un 1 y el que representa un 0, frecuencia, tipo de onda, velocidad de transmisión de cada bit, etc.

La capa física no interpreta la información que está enviando: sólo transmite ceros y unos determinando cómo se va a producir un cero o un uno empleando para ello distintos mecanismos en función del medio por el que deba propagarse los datos. Es decir, traduce a señal eléctrica, lumínica o de radio una serie de datos que ha recibido en formato digital.

Un protocolo de este nivel es el RDSI.

NIVEL DE ENLACE

Envía tramas de datos entre nodos de una misma red. Su función es conseguir que exista una **transmisión fiable** solventando los problemas de ruido que pueda haber en la red ya que se pueden provocar situaciones que deterioren la señal que transmite los datos (eléctrica, de radio, luz, etc.) de manera que si se enviara un flujo continuo de información y se deteriorara una pequeña parte, se perdería todo el mensaje, ya que no se llegaría a comprender. Así, se información acompañada de una serie de códigos para permitir saber donde empieza y termina cada porción de información y si ha llegado en correcto estado.

> Si repetimos rápidamente la palabra "jamón" observamos que se termina juntando y no sabemos lo que decimos,...
>
> jamónjamónjamónjamónjamónjamónjamónjamónjamónjamón
>
> monja o jamón. Sin embargo, si establecemos una clara señal a la hora de separar cada una de las palabras sabremos lo que estamos diciendo, no se mezclarán los sonidos. Además, sabremos si se nos ha quedado cortada alguna de las palabras.
>
> empiezojamóntermino empiezojamóntermino

Otra de las funciones que realiza esta capa es la de control de flujo para evitar la saturación del equipo que recibe la información, estableciendo un acuerdo sobre cuánta capacidad de información puede asumir el equipo receptor.

Ofrece la transmisión y recuperación **fiable** de datos, con varias funciones: Control de errores (detección/corrección), delimitación o sincronización de tramas, función de transparencia y control de flujo.

Algunos protocolos del nivel de enlace: LAPD, PPP, RDSI y Paso testigo.

NIVEL DE RED

Se encarga del **encaminamiento de paquetes** entre el origen y el destino, atravesando tantas redes intermedias como sean necesarias. Los datos se fragmentan en paquetes y cada uno de ellos se envía de forma independiente (modo datagrama). Este nivel se encarga de mandar los paquetes de información por el camino más adecuado para que llegue en el menor tiempo posible y evitando, a la vez, que las redes se lleguen a saturar.

Aparte, este nivel, se ocupa de la conexión y desconexión de redes, su sincronización, control de flujo de la información entre redes, detección de errores de transmisión y recuperación de los errores que se puedan producir.

Tarea importante del nivel de red es ocuparse de **evitar la congestión**, por exceso de paquetes en alguna rama de la subred.

Dentro de un ordenador, este nivel decide si, el mensaje que acaba de llegar, tiene como destino ese equipo y, por lo tanto, lo debe dejar pasar a los niveles superiores del sistema o debe devolverlo a la red.

Su función sería similar a la de un cartero que recogiera todas las cartas que circulan y rechazara las que no van a su zona, dejando pasar las que sí estuvieran bien dirigidas.

Ejemplos de protocolos del nivel de red son: Frame Relay y ATM.

Esta capa ofrece como servicio, a los niveles superiores, la identificación de la procedencia y destino de los paquetes de datos, y utiliza al nivel inferior para que los organice de forma efectiva.

NIVEL DE TRANSPORTE

Es el corazón del modelo OSI. Ofrece mecanismos fiables para el **intercambio de datos** de un extremo a otro, realiza servicios de detección de errores que aseguran la integridad de los datos así como los niveles de calidad de los servicios y se encarga de la multiplexación entre aplicaciones distintas.

El nivel de transporte tiene la función de recomponer la información para que tenga sentido. Es el encargado de **eliminar las tramas repetidas** y ponerlas todas en el **orden correcto**. Se ocupará de subsanar las posibles deficiencias del nivel de red.

Por último, se encarga de establecer la conexión entre el equipo de origen y de destino, de manera que se pueda controlar todo el tráfico de la información.

NIVEL DE SESIÓN

Proporciona funciones de organización y sincronización para que las aplicaciones dialoguen entre si. El diálogo se realiza a través del uso de una conexión que se llama sesión. Son mecanismos complejos que consiguen determinar en que punto se encuentra exactamente una comunicación si ocurre un error fatal. No se suele usar, son para aplicaciones muy específicas.

NIVEL DE PRESENTACIÓN

Se encarga de la **presentación de los datos** intercambiados entre entidades de nivel de aplicación, es decir, la sintaxis de estos datos. Actúa como un traductor de manera que, cualquiera que sea la aplicación que desea emplear los servicios de la red, los datos se traducen a un formato universal, un “esperanto” de la comunicación entre equipos informáticos.

Independiza las sintaxis locales manejadas por el nivel 7 a través de una **sintaxis de transferencia universal**, ocupándose de los aspectos de representación de la información y del tipo de codificación de los datos previamente establecido. También se ocupa de la compresión y encriptación de datos.

NIVEL DE APLICACIÓN

Este nivel **enlaza directamente con el usuario real**. Son funciones de uso común para muchas aplicaciones, las cuales estarían por encima (emulación de terminales, transferencia de ficheros, correo electrónico...).

1.6. MODELO IEEE

Con un fin similar al que inspiró a la ISO para crear el modelo OSI, el *Institute of Electrical and Electronic Engineers* desarrolló una serie de estándares de comunicación de dispositivos para redes LAN y WAN de manera que se pudieran compatibilizar los productos de las distintas empresas orientados a este sector de comunicación. Así, se creó el Comité 802 que elaboró, entre otros, el estándar

802.3 (Ethernet), siendo esta familia de protocolos la más extendida en la actualidad, afectando a los niveles físico y de enlace del modelo OSI en redes LAN.

- **Nivel físico**: Cumpliría exactamente las mismas funciones que se le asignan a este nivel en el modelo OSI.
- **Nivel de enlace**: El estándar IEEE subdivide este nivel en dos capas:
  - Control de enlace lógico (LLC, Logical Link Control): Maneja los distintos tipos de servicios de comunicación
  - Control de acceso al medio (MAC, Media Access Control): Aporta la dirección física del equipo y las herramientas para el uso del medio.

El resto de los niveles del sistema OSI no los contempla. La IEEE es la responsable de la elaboración de la mayoría de los estándares creados hasta este momento y que están vigentes en la comunicación de ordenadores.

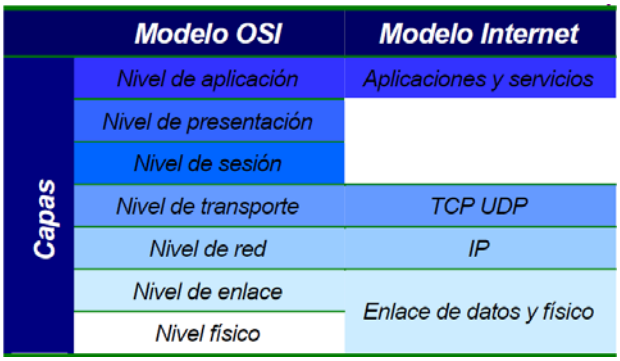
Por ejemplo el IEEE 802.11a, 802.11b, 802.11g para comunicación inalámbrica, IEEE 802.5 para redes Token Ring, el IEEE 802.3u para redes Fast Ethernet, etc.

1.7. MODELO DE REFERENCIA TCP/IP (INTERNET)

La arquitectura de este modelo es el resultado del desarrollo de un sistema capaz de mantenerse efectivo aún cuando estuvieran destruidos parte de los canales de comunicación. Nos encontramos con que se debe transmitir información entre ordenadores de distintos fabricantes y a través de distintos medios. A la vez, se buscaba un modelo de comunicación en el que no se necesitara un control centralizado. Se puede decir que es un modelo surgido de la experiencia ya que se trata de una pila de protocolos que han configurado, posteriormente, una arquitectura.

Así, se generó una arquitectura cuya función fundamental era lograr la supervivencia de la información empleando como estrategia la partición de los datos en “pedazos” de información más pequeños.

Este modelo, asociados a los protocolos TCP/IP que estudiaremos más adelante, genera cuatro capas o niveles que cubren las funcionalidades de los siete niveles del modelo OSI (recordemos que la arquitectura IEEE sólo llega al nivel de enlace del modelo OSI).



Si analizamos los protocolos asociados a cada capa observamos que no hay ninguno definido para la capa de enlace de datos y físico, ya que el modelo TCP/IP se acoge a los definidos por otros estándares. Habitualmente utiliza el conjunto de protocoles IEEE 802.

El nivel de red tendría como función crear datagramas de información que, siguiendo distintos caminos, deberían llegar al equipo de destino. Sin embargo, no se tiene en cuenta ningún mecanismo que garantice que no se va a perder ningún datagrama ni la aplicación del equipo de destino, pero debe evitar que se produzcan congestiones en la red.

En la capa de transporte se establece comunicación de extremo a extremo. Esta comunicación, dependiendo del protocolo que emplee puedes estar orientada a conexión, reservando así una ruta mientras se produce la transmisión de datos,) y fiable (TCP) y otra no orientada a conexión y no fiable

(UDP). Esta capa se encarga de servir de intermediario entre las aplicaciones y el nivel de red y dota de fiabilidad a la comunicación que establece el nivel de red, procurando que los paquetes pasen ordenados y sin pérdidas.

Por último, en la capa de aplicaciones y servicios se definen una serie de protocolos con funciones muy diversas (FTP, SNMP, http, etc.) extraídos de los programas empleados por los usuarios, se encarga de que se comuniquen las aplicaciones situadas en distintos equipos.

2. REDES LAN

Las redes locales son las estructuras de comunicación entre ordenadores que abarcan un área limitada. Son las redes que encontramos más próximas a nosotros.

Las características de una red LAN son:

- **Medio compartido**: Todos los ordenadores están conectados a un medio de comunicación, por lo que para su utilización deben competir por él.
- Utilizan conmutación de paquetes o de celdas.
- Son redes de **difusión**: al disponer de un medio compartido pueden enviar mensajes al resto de los equipos de forma simultánea.
- **Zona geográfica limitada**: son redes que no se extienden en ámbitos geográficos amplios aunque usando fibra óptica pueden extenderse a grandes distancias.
- **Privadas**.
- **Económicas**: Los costes de cableado de la red son bajos. Sólo es necesaria una tarjeta de interfaz por estación.
- Redes **optimizadas**: permiten una gran rapidez y fiabilidad a la hora de transmitir datos.

El desarrollo de las LAN ha buscado siempre una mayor fiabilidad, rapidez y costes más asequibles a la vez que se intentaba solucionar los problemas que el acceso al medio de comunicación empleado presentaba.

EL ACCESO AL MEDIO COMPARTIDO

Si varias personas intentan hablar a la vez (podemos pensar en algunas tertulias televisivas o de radio), es muy difícil que podamos llegar a entender nada. Se producen interferencias en el mecanismo de comunicación y no llegamos a captar el mensaje. Esto es debido a que un único medio debe repartirse entre los distintos sonidos que se están emitiendo a la vez y, por lo tanto, las ondas sonoras, al ser de la misma frecuencia se interfieren. Así, debemos establecer un mecanismo que permita hablar a todos, pero que evite las interferencias, por ejemplo, un turno de palabra.

Esta misma situación se produce cuando en una red, de medio compartido, pretenden comunicarse varios ordenadores de forma simultánea, se producen interferencias y colisiones.

Por lo tanto se debe establecer un método de acceso que garantice la circulación de los datos sin peligro de colisiones e interferencias o que estas se minimicen. El control de acceso al medio responde a las cuestiones ¿cómo pongo los datos en la red?, ¿cómo puedo tomar los datos del medio?

En general, el acceso al medio puede ser realizado de dos formas:

- **Acceso por contienda** (no determinista): Los ordenadores compiten por el medio de transmisión, no esperan a tener un permiso, simplemente envían sus datos, pudiéndose producir choques.

  Cuando se detecta esta situación, los ordenadores esperan un cierto tiempo y vuelven a emitir. Un ejemplo de este método es CSMA/CD (Método de acceso al medio por detección de portadora, por detección de colisiones) donde los equipos escuchan hasta que la red no

contiene tráfico y en ese momento envían sus tramas de datos y, si se produjera una colisión emplearían un algoritmo de demora para volver a emitir.

> Es la misma situación que se presenta cuando un vehículo quiere acceder a una rotonda. El conductor examinará el tráfico hasta que se produzca un hueco que le permita entrar. Si calcula mal, se producirá una colisión.

- **Acceso controlado** (determinista): existe un mecanismo de control que gestiona el tiempo para la transmisión de datos por parte de cada uno de los ordenadores. Esta función la puede realizar un equipo, o bien puede depender de la posesión de un testigo que circula de forma regular por la red.

> En este caso el acceso a la rotonda esta regulado por un policía. El conductor tendrá que esperar a que el policía le de paso para acceder.

El método más empleado en las redes LAN es el acceso por contienda, que ha sido implementado en las redes Ethernet con el protocolo CSMA/CD que se basa en escuchar si la red está ocupada y emitir si no se detecta portadora (que se esté emitiendo un mensaje).

LA IDENTIFICACIÓN DE LOS EQUIPOS

Una de las características de una red LAN es ser una red de difusión, es decir, que todos los equipos conectados a esa red reciben los mensajes enviados por todos los ordenadores aunque no sean los receptores de dichos mensajes. Esto supone que se deba establecer un mecanismo que permita identificar tanto al emisor del mensaje como al receptor, de manera que un equipo pueda saber si se dirige o no a él la trama de datos que le acaba de llegar y, si fuera necesario, establecer un diálogo entre los equipos.

En las redes LAN se toma como sistema prioritario de identificación la dirección MAC (*media access control*) de la tarjeta, es decir, una serie de dígitos en sistema hexadecimal que sirven para identificar la tarjeta de red que tiene instalada un equipo, y, por lo tanto, permite determinar un ordenador en concreto.

> La dirección MAC de una tarjeta sería como el número de bastidor del motor de un coche o nuestro DNI.

El formato de la dirección MAC se representa con HH:HH:HH:HH:HH:HH. Los primeros 24 bits (los 6 primeros dígitos) corresponden al fabricante y los 24 bits últimos a la tarjeta. La dirección para mensajes broadcast es FF:FF:FF:FF:FF:FF

Investiga 1:

1. Calcula cuantas tarjetas de red distintas puede crear un fabricante.
2. ¿Cuántas tarjetas de red puede haber a nivel mundial?
3. ¿Qué probabilidades crees que hay de que se agoten en corto tiempo, digamos 20 años?

2.1. ADAPTADORES DE RED

Un adaptador de red (NIC *Network Interface Card*) es el dispositivo físico que conecta el medio de comunicación con el ordenador (interfaz). Normalmente suelen ser internas al ordenador o, en bastantes casos, está integrada en la placa base. Es un dispositivo

de hardware que integra un software (firmware) almacenado en una memoria ROM.

Una se encarga, en el nivel físico del sistema de referencia OSI, de transformar el flujo de información que le envía el ordenador 1 y 0) en una señal electromagnética que pueda propagarse a través del medio de transmisión y viceversa.

Para realizar esta función, una tarjeta de red debe desempeñar las siguientes tareas:

- Recepción y almacenamiento de los datos procedentes desde la RAM del ordenador o desde la red. A través del bus de conexión con la placa base la tarjeta (PCI o USB) se comunica con la RAM del ordenador, recibe los datos procedentes de ésta y los almacena en su memoria para poderlos tratar y adaptar la velocidad de transmisión de datos a la de la red. En el caso de que la información proviniese de la red el proceso sería inverso

- Construcción o interpretación de la trama de datos en función del protocolo de nivel 2 de la red en la que se encuentre el equipo.
- Controlar el momento en que es posible acceder al medio de comunicación de manera que se eviten colisiones.
- Convertir los datos que recibe del bus del ordenador de paralelo (32 o 64 bits de datos simultáneos) a serie y viceversa.
- Codificar y descodificar los datos de manera que una secuencia de bits se transforme en impulsos eléctricos, luminosos, etc. y viceversa.
- Transmisión de los datos.

Este trabajo no lo realiza únicamente una tarjeta, para que exista comunicación entre dos equipos, se debe establecer un diálogo entre los dos adaptadores instalados en cada ordenador. En este diálogo deben aclarar algunos aspectos de la comunicación:

- Tamaño de los paquetes de datos y cantidad de estos paquetes enviados antes de esperar una confirmación de la recepción.
- Tiempos entre paquetes de datos enviados, y de espera antes de enviar la confirmación.
- Velocidad de transmisión.

2.2. MEDIOS DE TRANSMISIÓN

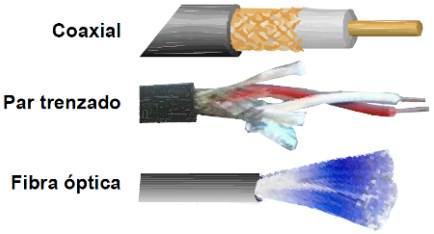
Los medios de transmisión se clasifican en **guiados** y **no guiados**. Los primeros son aquellos que utilizan un medio sólido (un cable) para la transmisión.

Los medios no guiados utilizan el aire para transportar los datos: son los medios inalámbricos.

2.2.1 MEDIOS GUIADOS

Los cables, medios guiados, transmiten impulsos eléctricos o lumínicos determinadas por el protocolo que implemente esa red.

La velocidad de transmisión, el alcance y la calidad (ausencia de ruidos e interferencias) son los elementos que caracterizan este tipo de medio. La evolución de esta tecnología ha estado orientada por la optimización de estas tres variables.



- Uno de los principales problemas de la transmisión de un flujo de datos por un cable eléctrico consiste en el campo magnético que se genera por el hecho de la circulación de los electrones. Este fenómeno es conocido como **inducción electromagnética**.

La existencia de un campo magnético alrededor de un cable genera interferencias en los cables próximos debido a este mismo fenómeno.

- La **atenuación** que sufre la señal según va circulando por el cable, y que es mayor cuanta más distancia debe recorrer, limita considerablemente la longitud de cable que se puede instalar sin regenerar la señal.

  Generalmente, en los cables de cobre un mayor grosor del conductor hace que la atenuación sea menor.

Cada tipo de cable aporta una solución a los tres problemas definidos anteriormente. El cable de par trenzado permite que los campos electromagnéticos generados por la corriente eléctrica se acoplen y se evite así la interferencia. El cable coaxial, con su malla exterior, proporciona una pantalla para las interferencias y el mayor grosor de su cable interior permite mayores distancias, aunque la mejor solución a la atenuación de la señal y el problema de las interferencias es el cable de fibra óptica.

CABLE PAR TRENZADO

El par trenzado es parecido al cable telefónico, consta de 8 hilos trenzados dos a dos identificados por colores para facilitar su instalación. Se trenza con el propósito de reducir interferencias. Dependiendo del número de trenzas por unidad de longitud, los cables de par trenzado se clasifican en categorías. A mayor número de trenzas, se obtiene una mayor velocidad de transferencia gracias a que se producen menores interferencias.

Los cables par trenzado pueden ser a su vez de dos tipos:

- UTP (*Unshielded Twisted Pair*, **par trenzado no apantallado**)
- STP (*Shielded Twisted Pair*, **par trenzado apantallado**)

Los cables sin apantallado son los más utilizados debido a su bajo coste y facilidad de instalación. Los cables STP están embutidos en una malla metálica que reduce las interferencias y mejora las características de la transmisión. Sin embargo, tienen un coste elevado y al ser más gruesos son más complicados de instalar.

Este tipo de cable debe emplear conectores RJ45 (*Registered Jack*) para unirse a los distintos elementos de hardware que componen la red.

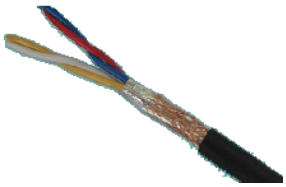
El cable UTP

Actualmente, de los ocho cables sólo cuatro se emplean para transmitir datos.

Generalmente para construir una pequeña red con par trenzado se usa un concentrador (hub) o un conmutador (Switch), que distribuye la información a las estaciones de trabajo.

El cable STP

Es el cable que conocemos como de par trenzado apantallado. Esta constituido por dos pares de hilos trenzados y se caracteriza por poseer una malla metálica que evita las interferencias del ruido electromagnético exterior. Su función es convertir el ruido exterior en una corriente eléctrica, algo que se consigue cuando todos los dispositivos utilizados mantienen una adecuada conexión a tierra, teniendo que estar también apantallados.



El apantallamiento debe estar formado por un material que conduzca la electricidad, de forma similar al cable que rodea y puede estar constituida por una malla de cables o por una fina lámina metálica (ScTP o FTP)

CABLE COAXIAL

El cable coaxial es similar al cable utilizado en las antenas de televisión: un hilo de cobre en la parte central rodeado por una malla metálica y separados ambos elementos conductores por un cilindro de plástico, protegidos por una cubierta exterior.

Los tipos de cable coaxial para redes LAN son:

- **Thicknet** (Ethernet grueso): Fue el primer cable montado en redes Ethernet. Tiene 1,27 cm Ø y capacidad para transportar la señal a más de 500 m. Al ser un cable grueso, se hace mucho más difícil su instalación y está, prácticamente, en desuso. Este cable se corresponde al estándar RG-8/U y posee un característico color amarillo con marcas cada 2,5 m que designas los lugares en los que se pueden insertar los ordenadores al bus.

- **Thinnet** (Ethernet fino): de 0,64 cm Ø y con capacidad para transportar una señal hasta unos 185 m. Es un cable flexible y de fácil instalación (comparado con el cable coaxial grueso). Puede tener su núcleo constituido por un cable de cobre o una serie de hilos entrelazados.

El cable coaxial es menos susceptible a interferencias y ruidos que el cable de par trenzado y puede ser usado a mayores distancias que éste. Puede soportar más estaciones en una línea compartida. Es un medio de transmisión muy versátil con un amplio uso. Las más importantes son:

- Redes de área local
- Transmisión telefónica de larga distancia
- Distribución de televisión a casas individuales (Televisión por cable).

Transmite señales analógicas y digitales, su frecuencia y velocidad son mayores que la del par trenzado.

Uno de los mayores inconvenientes de este tipo de cable es su grosor, superior al del cable de par trenzado, que dificulta mucho su instalación, encareciendo ostensiblemente el coste por mano de obra, de ahí, que pese a sus ventajas en cuanto a velocidad de comunicación y longitud permitida, no se presente de forma habitual en las redes LAN.

Elementos de conexión

Las redes que utilizan Thinnet requieren que los adaptadores de red tengan un conector apropiado: los ordenadores se conectan entre si formando una fila y usando conectores en **T** (denominados BNC ET). Uno de los extremos se utiliza para la conexión al ordenador, y los otros dos para la unión del cable.

En ocasiones es necesario acoplar dos cables para alargar la longitud del bus, para realizar esta función se emplea un conector **barrel**.

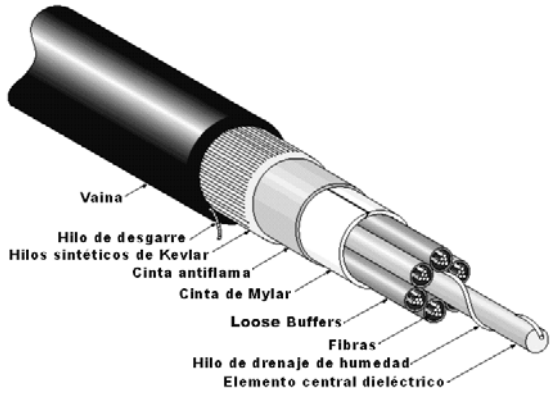
En los extremos del bus hay que colocar un **terminador**, que no es más que una resistencia de 50 ohmios que evita que la señal se repita al llegar al final del cable y produzca colisiones con otras señales.

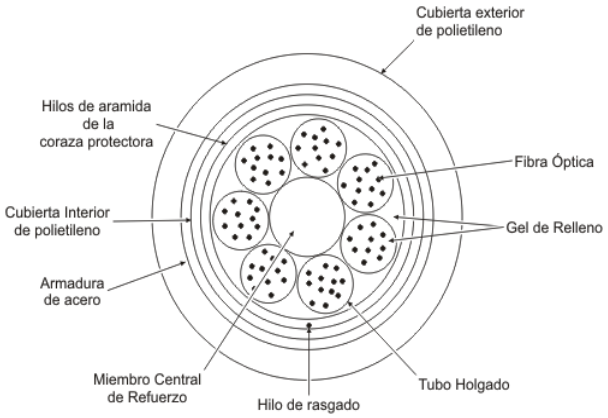
CABLE DE FIBRA ÓPTICA

En los cables de fibra óptica la información se transmite en forma de pulsos de luz. En un extremo del cable se coloca un diodo luminoso (LED) o bien un láser, que emite la señal luminosa. Al otro extremo se sitúa un detector de luz. Este cable permite que la atenuación sea mínima y que no se produzca la interferencia de campos magnéticos, de manera que la longitud a la que se pueden transmitir los datos empleando un solo cable y la cantidad y velocidad en que se hace sea muy alta.

El medio de transmisión consiste básicamente en dos cilindros coaxiales de vidrios transparentes y de diámetros muy pequeños. El cilindro interior se denomina núcleo y el exterior se denomina envoltura, siendo el índice de refracción del núcleo algo mayor que el de la envoltura. En la superficie

de separación entre el núcleo y la envoltura se produce un fenómeno de reflexión total de la luz, debido a la diferencia en el índice de refracción. Como consecuencia de esta estructura óptica todos los rayos de luz que se reflejan totalmente en dicha superficie se transmiten guiados a lo largo del núcleo de la fibra. Este conjunto está envuelto por una capa protectora.

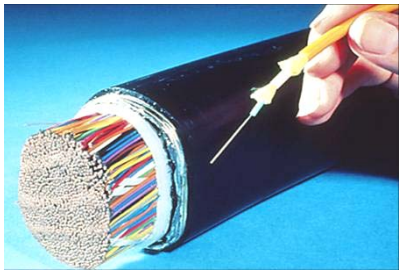




Existen dos formas de transmisión:

- **Monomodo**: La luz, generada por un láser, viaja por el núcleo sin reflejarse en las paredes, presentando una única longitud de onda. El cable empleado es grueso y apenas si se puede emplear en instalaciones LAN debido a que soporta muy bajo ángulo de curvatura.
- **Multimodo**: La luz es producida por un led y viaja reflejándose en las paredes del cable transportando múltiples longitudes de onda

La velocidad de transmisión es muy alta, 10 Mb/seg siendo en algunas instalaciones especiales de hasta 500 Mb/seg. Sin embargo, su instalación y mantenimiento tiene un coste elevado. Este tipo de cable, además, permite que la señal se transmita a longitudes mayores que el par trenzado o el cable coaxial, de manera que se emplea cuando es necesario cubrir largas distancias o la cantidad de información es alta.

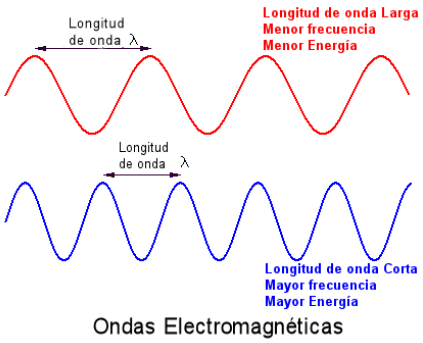


2.2.2 MEDIOS NO GUIADOS

Los medios no guiados se basan en la propagación de ondas electromagnéticas por el espacio. Una radiación electromagnética tiene una naturaleza dual, como onda y como corpúsculo y su comportamiento dependerá de las características ondulatorias de la radiación, especialmente de la longitud de onda.

- **Ondas de radio**. Ondas electromagnéticas cuya longitud de onda es superior a los 30 cm. Son capaces de recorrer grandes distancias, y pueden atravesar materiales sólidos, como paredes o edificios. Son ondas multi-direccionales: se propagan en todas las direcciones. Su mayor problema son las interferencias entre usuarios.

  Estas ondas son las que emplean las redes WI-FI o BlueTooth.



Ondas Electromagnéticas

- **Microondas**. Se basa en la transmisión de ondas electromagnéticas cuya longitud de onda varía entre 1 mm y 30 cm. Estas ondas viajan en línea recta, por lo que emisor y receptor deben estar alineados cuidadosamente. Tienen dificultades para atravesar edificios. Debido a la propia curvatura de la tierra, la distancia entre dos repetidores no debe exceder de unos 80 Kms de distancia. Es una forma económica para

comunicar dos zonas geográficas mediante dos torres suficientemente altas para que sus extremos sean visibles.

- **Infrarrojos**. Son ondas electromagnéticas (longitud de onda entre 750 nanómetros y 1 milímetro) direccionales incapaces de atravesar objetos sólidos (paredes, por ejemplo) y están indicadas para transmisiones de corta distancia. Las tarjetas de red inalámbricas utilizadas en algunas redes locales emplean esta tecnología: resultan muy cómodas para ordenadores portátiles. Sin embargo, no se consiguen altas velocidades de transmisión.
- **Láser**. Son unidireccionales. Se pueden utilizar para comunicar dos edificios próximos instalando en cada uno de ellos un emisor láser y un foto-detector. A mayor longitud de onda de la radiación, el comportamiento se asemeja más al ondulatorio, mientras que si se disminuye la longitud de onda de la radiación, se produce una aproximación al comportamiento de la materia.

Investiga 2:

Los medios no guiados mencionados arriba se usan para comunicar equipos que están situados en la Tierra.

¿Cómo se transmite la información por el espacio? ¿Cómo puede haber comunicación entre la Estación Espacial Internacional y la Tierra?

¿Y entre el robot Curiosity y la Tierra?

2.3. MECANISMOS DE INTERCONEXIÓN

2.3.1 CONCENTRADORES (HUBS)

Los concentradores aparecieron como solución al problema de las redes que se conectaban a un único cable (redes en bus), ya que si este cable se deterioraba, la red dejaba de ser operativa. El hub hace de punto central de todas las conexiones de manera que si un cable de conexión de un equipo a la red se estropea, el resto de la red puede seguir operativa.

Un concentrador es un dispositivo **pasivo** que actúa como punto de **conexión central** entre equipos, para formar un segmento LAN independiente. Los equipos conectados al propio concentrador son miembros de dicho segmento LAN, y comparten el ancho de banda del concentrador para sus comunicaciones.

Otra de las tareas que debe desempeñar un concentrador es la ampliación y regeneración de la señal que están enviando los equipos, ya que la señal eléctrica enviada a través del cable pierde potencia. Además, toman la señal de uno de sus puertos y la envían al resto de los equipos de la red.

Básicamente actuaría como un medio de conducción para los datos. Al poseer múltiples puertos, cuando una trama llega a uno de sus puertos, ésta es copiada a los demás puertos, así los demás segmentos de la LAN pueden verla. El concentrador no sabe ni entiende a quien va dirigida esa señal o trama. Simplemente la *copia* a todos los demás puertos. Esto, evidentemente, consume recursos de la red. Además en una LAN basada en concentradores, éstos deben competir por el medio compartido: se producen colisiones y retardos.

El hub actúa en el nivel 1 del modelo OSI ya que simplemente regenera y transmite la señal, no es capaz de identificar hacia dónde va la trama de datos y en función de ello filtrar el tráfico; igualmente, tampoco pueden ser empleados para seleccionar la mejor ruta para dirigir las tramas.

El funcionamiento es muy sencillo, todos los equipos de la red se conectan a un núcleo central, el hub, mediante un cable. Cuando un equipo envía un mensaje, los datos llegan al concentrador y

este los regenera (mejora su calidad eléctrica) y los retransmite a todos los puestos que están conectados a cada uno de sus puertos.

Al no filtrar el tráfico y reenviar los datos a todos los puestos puede suceder que, cuando un equipo quiera enviar una trama de datos encuentre su zona de la red ocupada por datos que no se le han enviado, o que se produzca una colisión entre los datos enviados por otro equipo y los que acaba de enviar él. Si un hub tiene conectados doce equipos a sus puertos, cuando llega un mensaje, se multiplica por doce, ya que los envía por todos sus puertos, lo que aumenta enormemente el tráfico.

> Supongamos que en una urbanización circular hay un único buzón en el centro. El cartero coloca la correspondencia de todas las viviendas en ese buzón. Los habitantes de las casa pasan periódicamente por el buzón para recoger su correo y dejar el correo que envían al exterior. Puede ocurrir que un día el cartero o uno de los habitantes no puedan dejar su correo porque el buzón esta lleno de correspondencia no recogida.
>
> El buzón sería el equivalente al hub

Hoy en día están prácticamente en desuso.

2.3.2 CONMUTADORES (SWITCHES)

Se les conoce técnicamente como concentradores conmutados. Filtran y dirigen tramas entre los segmentos de la LAN proporcionando un ancho de banda dedicado: forman un circuito virtual entre el equipo emisor y el receptor, y disponen de todo el ancho de banda del medio durante la fracción de segundo que tardan en realizar la transmisión.

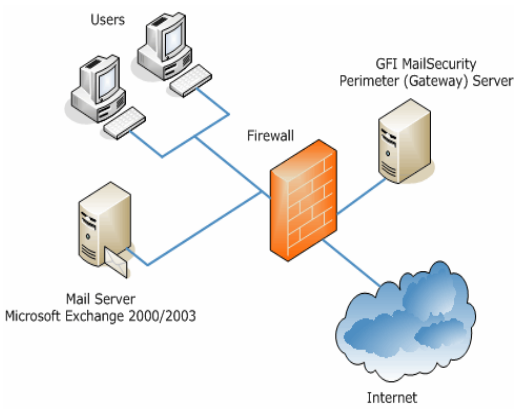
La función de un switch consiste en tomar la dirección MAC de una trama de datos y, en función de ella, enviar la información por el puerto correspondiente. En comparación con el hub, actúa más inteligentemente ya que filtra el tráfico y tiene capacidad de reconocimiento. Los datos pueden conducirse por rutas separadas, mientras que en el hub, las tramas son conducidas por todos los puertos.

> Siguiendo el ejemplo anterior, si el cartero va de casa en casa dejando y recogiendo la correspondencia estaría actuando como un switch.

Los conmutadores son capaces de realizar esto troceando el ancho de banda en franjas, llamadas canales, lo suficientemente grandes como para dar servicio a cada puerto de conmutación.

Las redes conmutadas son más rápidas puesto que el ancho de banda perdido por colisiones se elimina. Por ejemplo, si un concentrador de 24 puertos tiene un dominio de colisión de 24, un conmutador de 24 puertos tendría un dominio de colisión de 1. Evidentemente son algo más complejos de configurar y administrar que los concentradores, y por supuesto más caros.

Aunque ocasionalmente, y con las nuevas tecnologías, operan en el nivel 3 (red), para nosotros actúan el nivel de enlace. No usan direcciones IP y, por lo tanto, no tienen la capacidad de los enrutadores para encontrar trayectorias a través de las redes, simplemente leen la dirección física de los mensajes y los redireccionan al equipo adecuado.



2.3.3 CORTAFUEGOS (FIREWALLS)

Un cortafuegos es un sistema diseñado para prevenir accesos no autorizados. Generalmente se utilizan para proteger las redes privadas de intentos de acceso desde

Internet no autorizados, pero también se puede configurar el cortafuegos a la inversa: para que los usuarios de la Intranet no tengan acceso a ciertos hosts. El cortafuegos puede ser hardware, software, o una combinación de ambos. Muchas veces son enrutadores especializados que comprueban que cada paquete cumple las políticas de seguridad con las que ha sido programado. Un cortafuegos forma un *cuello de botella* intencionado del tráfico y monitoriza constantemente las conexiones internas/externas para verificar que se cumple la seguridad.

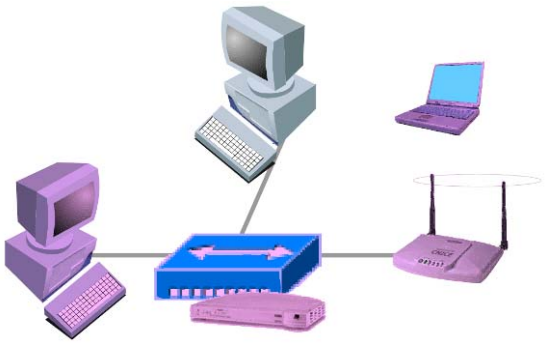
2.3.4 PUENTES (BRIDGES)

Un puente es un dispositivo que conecta dos redes de área local (LAN) o dos segmentos de la misma LAN.

Las funciones de un puente son:

- Dividir una red LAN en dos subredes. Cuando una LAN se hace demasiado grande, en cuanto a número de puestos o extensión, debe ser dividida para que su funcionamiento sea mejor.
- Interconectar dos redes LAN, pudiendo tener protocolos de nivel dos o medios de transmisión distintos. Interconexión de una red inalámbrica a una de cable o una red Ethernet a otra Token Ring.
- Controlar las tramas defectuosas.

Independientemente del objetivo por el que se haya conectado el puente a la red su funcionamiento será siempre el mismo. Básicamente los puentes reciben todos los paquetes enviados por cada red acoplada a él, y los reenvían selectivamente entre las LANs, utilizando solo las direcciones MAC (de enlace) para determinar donde retransmitir cada paquete. Los puentes reenvían solo aquellos paquetes que están destinados a un nodo del otro lado del puente, descartando (filtrando) aquellos que no necesitan ser retransmitidos o haya detectado que son defectuosos.



Para poder realizar esta tarea, cada puente va almacenando en memoria una tabla de direcciones MAC asignada a cada uno de sus puertos, de esta manera, cuando llega una trama, comprueba la dirección MAC, la compara con el "mapa" que posee en memoria y la envía por el puerto adecuado.

En el momento en que se instala un puente por primera vez, no tiene ninguna información sobre los equipos de las redes que interconecta. Según va recibiendo tramas de datos y analiza las direcciones de procedencia, crea el mapa de direcciones, que usará posteriormente. Si en alguna ocasión desconoce la dirección a la que debe enviar una trama, transmitirá por todos sus puertos, garantizando así que lleguen los datos a su destino; cuando el equipo de destino envía el acuse de recibo, podrá incorporar su dirección a su memoria.

Un puente también sirve para conectar dos segmentos de red por medio de comunicaciones inalámbricas, en este caso se les conoce como **punto de acceso**. En la ilustración se observa cómo se sitúa el puente entre cada segmento de red (LAN e inalámbrico).

2.3.5 PASARELAS (GATEWAYS)

El concepto de pasarela es quizás algo abstracto. Básicamente es un sistema de hardware o software que hace de puente entre dos aplicaciones o redes incompatibles para que los datos puedan ser transferidos entre distintos ordenadores.

Cuando un usuario se conecta a Internet, realmente se está conectando a un servidor que le proporciona las páginas Web. Tanto el usuario como el servidor son nodos **host** de una red. Una pasarela es, por ejemplo, un módem-router que dirige el tráfico desde una estación de trabajo a la red exterior que sirve las páginas Web. O, en el caso de acceso telefónico, la pasarela sería el ISP que conecta el usuario a Internet.

2.4. TIPOS DE REDES LAN POR SU TOPOLOGÍA

Cuando hablamos de topología nos referimos estructura que posee la red. Sin embargo, esa estructura puede ser física o lógica.

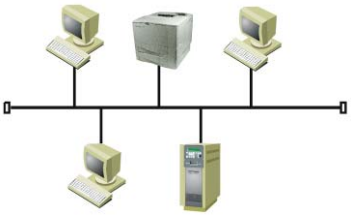
- **Topología física** es la distribución física del cableado y los elementos físicos, y su forma de interconexión.
- **Topología lógica**, es la forma de circulación y la regulación de la información.

Además del cable, que es el medio físico tradicional de transmisión de datos, también puede conseguirse la comunicación, por radio, infrarrojos o microondas, son las comunicaciones inalámbricas. Si nos referimos a las redes locales cuyo medio de transmisión sea el cable, las topologías físicas típicas son:

El tipo de topología influye en:

- El coste de la red.
- El rendimiento.
- La fiabilidad.
- La complejidad del software.
- La facilidad /dificultad para las modificaciones

2.4.1 RED EN BUS



También llamada de **Canal de distribución**. Todos los equipos están unidos a un cable continuo, a través de interfaces físicas, llamadas tomas de conexión, como un bus lineal, de ahí su nombre. Hay terminales (impedancias) a cada extremo del bus para que las señales no se reflejen y vuelvan al bus.

El cable puede ir por el suelo, techo, etc., pero siempre será un segmento continuo. Los equipos se unen al cable mediante unos transceptores, que pueden estar integrados en la propia tarjeta adaptadora de red.

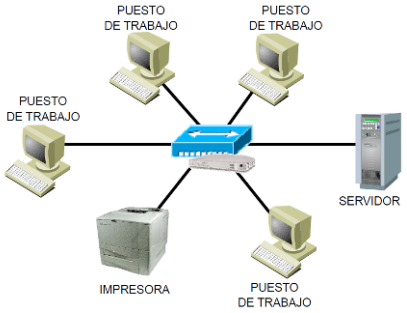
Típicas redes de este tipo son las primeras Ethernet; los otros dos son Thicknet (red gruesa, con cable coaxial 10Base5) y Thinnet (red delgada, utiliza 10Base2).

Características:

- Los mensajes circulan en ambas direcciones.
- No hay ningún nodo central que controle la red.
- La información se transmite por todo el bus. Por ello, todos los nodos del bus pueden escuchar las señales (mensajes broadcast). Para evitar que varios equipos accedan a la vez al canal o bus, con las consiguientes interferencias, se usan protocolos de acceso al bus y detección de colisiones.
- Este tipo de redes puede segmentarse mediante repetidores, aumentando su seguridad, independizando cada segmento y ampliando su longitud y número de nodos en la red, si bien tiene la limitación de la atenuación de la señal

Ventajas	Inconvenientes
Su sencillez y bajo coste. Sólo se tiene que instalar un cable y los adaptadores-transceptores.	La rotura del cable principal dejaría sin servicio a todos los dispositivos de la red.
Es sencillo añadir nuevos nodos.	
El software de comunicaciones no necesita incluir algoritmos de routing.	

2.4.2 RED EN ESTRELLA



En este tipo de redes, está formado por un nodo central –hub o switch– al cual están conectados todos los equipos de la red. El nodo central puede tener dos formas de funcionamiento; como mero repetidor de las tramas que le llegan (cuando le llega una trama de cualquier estación, la retransmite a todas las demás), en este caso, la red funciona de forma parecida a un bus; otra forma es repetir las tramas solamente al destino (usando la identificación de cada estación y los datos de destino que contiene la trama).

Redes de este tipo son: 10Base-T, Fast Ethernet y GigaBit Ethernet sobre cables de par trenzado.

Características:

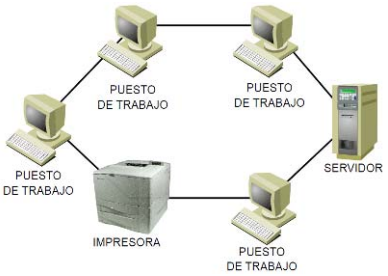
Cuando el nodo central está formado por un switch, se realizan dos funciones básicas: proceso de datos y conmutación de líneas o mensajes. La transmisión será por conmutación de circuitos. El nodo central activa y desactiva la línea con el nodo que debe enviar/recibir la información.

Ventajas	Inconvenientes
Fácil administración.	Si se avería el nodo central, no funciona la red.
Sencillo añadir/desconectar nuevos nodos	Hay que instalar una línea para cada nodo
	La entrada /salida del nodo central puede convertirse en un cuello de botella

Un caso especial de este tipo de red es la red en estrella jerárquica que se produce al unir los nodos centrales de varias redes en estrella, pasando por un único nodo principal central. Los sistemas estructurados de cableado tienen una unión física de este tipo.

2.4.3 RED EN ANILLO

Redes de este tipo son Token Ring (norma 802.5), que utiliza par trenzado como cable y FDDI (*Fiber Distributed Data Interface*) sobre fibra óptica.



Características:

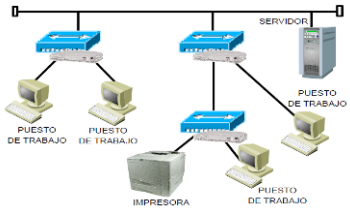
- La transmisión de información es por conmutación de paquetes. Circula en una sola dirección.
- Cada nodo transmite o recibe un paquete.
- No hay principio ni final.
- No hay ningún nodo central que controle la red.
- Cualquier nodo puede recibir el paquete que circula por el anillo, si es para él, se lo queda, si no, lo pasa al siguiente.
- Aunque eléctricamente la señal realice un bucle, recorriendo una por una todos los ordenadores de la red, en muchas implementaciones, su topología, es en estrella, pasando por un único punto centralizado antes de ir a la máquina siguiente en el anillo, lo cual permite una mas fácil administración y resolución de incidencias de la red, en caso de necesitar introducir un nuevo nodo o aislarlo.

Ventajas	Inconvenientes
Localización de errores fácil	El fallo de un enlace provoca el fallo de todo el anillo
El software es sencillo, no necesita algoritmos de encaminamiento o routing	Difícil adición de nodos
	El repetidor de cada nodo ralentiza la velocidad de transmisión
	Instalación de cableado compleja

Una topología que derivaría de esta es la de anillo doble: Son dos anillos concéntricos, donde cada máquina está conectada a ambos anillos, aunque éstos no lo están directamente entre sí. El segundo anillo al conectar los mismos dispositivos incrementa la confiabilidad y flexibilidad de la red.

2.4.4 RED EN ÁRBOL

Es un conjunto de redes formando ramas como en un árbol. Las ramas de la red parten de un nodo principal, los demás nodos se pueden ramificar a su vez formando un árbol. Cada rama puede considerarse una red en bus. Suele usarse en sistemas de control, puesto que refleja la jerarquía de los diferentes niveles de control.



Características:

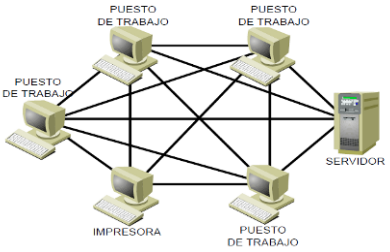
Las mismas que la topología en bus.

Inconvenientes:

Un fallo puede aislar una rama de la red.

2.4.5 RED EN MALLA

Los nodos de la red se conectan con el resto, de la manera más corta posible, si es de malla completa. También las hay incompletas, es el caso de las redes de área extensa que utilizan métodos de telecomunicación como ATM (*Asynchronous Transfer Mode*).

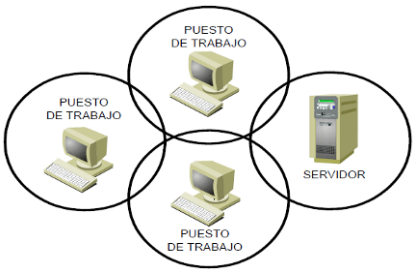


Características:

Esta topología permite que la información circule por varias rutas alternativas.

Ventajas	Inconvenientes
Si algún enlace deja de funcionar, la información puede ir por otro camino	Es cara y compleja

2.4.6 RED CELULAR



La red está compuesta por áreas circulares o hexagonales, llamadas celdas, cada una de las cuales tiene un nodo en el centro. Es la topología usada por las redes inalámbricas.

Características:

Esta tecnología funciona por medio de ondas electromagnéticas (radio, infrarrojos, microondas, etc.).

Ventajas	Inconvenientes
Eliminación de los cables	Problemas típicos de las señales electromagnéticas
	Problemas de seguridad

2.5. TIPOS DE REDES LAN POR SU TECNOLOGÍA FÍSICA DE CONEXIÓN

2.5.1 REDES POR CABLE

ETHERNET

Ethernet es la alternativa más económica y de mayor velocidad de la tecnología LAN. Son, posiblemente, las de uso mas generalizado y son todavía usadas para distancias medias-altas donde son requeridos niveles medios de fiabilidad. Podemos encontrar redes Ethernet sobre cable coaxial de distintos tipos, fibra óptica, par trenzado... El medio de transporte generalmente es el cable de par trenzado. La fibra óptica consigue niveles de fiabilidad y velocidad muy superiores, pero el coste es elevado. El protocolo Ethernet es característico de las redes en los que los ordenadores están conectados a un medio compartido y deben competir por su utilización. LAN IEEE 802.3 es una evolución de Ethernet.

Por su tecnología, las Ethernet son redes broadcast o de difusión, donde cada host envía sus datos hacia todos los demás hosts del medio de red. Las estaciones no siguen ningún orden para utilizar la red, siendo el primero que entra, el primero que se sirve. Así, las redes Ethernet son de carácter no determinista (acceso por contienda), es decir, las estaciones de una LAN de tipo CSMA/CD pueden acceder a la red en cualquier momento.

Ethernet permite que todos los dispositivos puedan comunicarse en el mismo medio, aunque sólo pueda haber un único emisor en cada instante. De esta forma todos los sistemas pueden ser receptores de forma simultánea, pero la información tiene que ser transmitida por turnos.

El método de acceso CSMA/CD que se usa en Ethernet ejecuta tres funciones:

1. Transmitir y recibir paquetes de datos.
2. Decodificar paquetes de datos y verificar que las direcciones sean válidas antes de transferirlos a las capas superiores del modelo OSI.
3. Detectar errores dentro de los paquetes de datos o en la red.

Ocurre con frecuencia que varias máquinas o host que han estado esperando, cuando aprecian que la red está libre, empiecen a transmitir tramas a la vez. Esto da lugar a que en los medios físicos se produzca un encontronazo o choque entre dos tramas diferentes que quieren pasar por el mismo sitio a la vez. Este fenómeno se denomina colisión, y la porción de los medios de red donde se producen colisiones se llama dominio de colisiones.

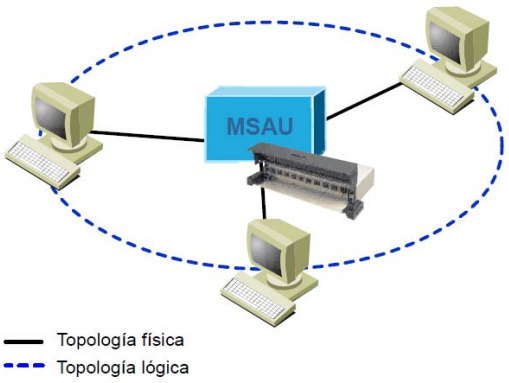
Para intentar solventar esta pérdida de paquetes, las estaciones CSMA/CD pueden detectar colisiones, y poseen algoritmos de postergación que determinan el momento en que las estaciones que han tenido una colisión pueden volver a transmitir. El algoritmo es distinto en cada equipo y consiste, básicamente, en un contador que retarda la nueva emisión del paquete. Al ser distinto en cada equipo, se evita que se vuelva a producir la colisión.

Existen varios estándares, siendo el más usado Ethernet 10Base-T, en el que cada equipo tiene una conexión con un concentrador central, y los cables usados son normalmente de par trenzado y no apantallado. Los cables tienen un límite de sólo 100 metros.

FAST ETHERNET

Con la idea de paliar algunos de los fallos contemplados en las redes Ethernet 10Base-T y buscar una alternativa a las redes FDDI que no han sido bien aceptadas, se desarrolló el estándar 802.3u, también conocido como Fast Ethernet. Para hacerla compatible con Ethernet 10Base-T se preservan los formatos de los paquetes y las interfaces, pero se aumenta la rapidez de transmisión, con lo que el ancho de banda sube a 100 Mbps.

TOKEN RING



Sigue siendo la tecnología de LAN más importante de IBM, y desde el punto de vista de implementación, ocupa el segundo lugar después de Ethernet aunque a una gran distancia.

Token Ring se distingue más por su método de transmitir la información que por la forma en que se conectan los equipos.

A diferencia de Ethernet, aquí, un Token o testigo, es pasado de equipo a equipo constantemente. Cuando un equipo desea mandar información debe de esperar a que le llegue el testigo. De esta manera no se producen colisiones, aunque el problema reside en el tiempo que debe esperar un equipo para obtener el Token.

Para implementar una red Token Ring necesitamos tarjetas y concentradores específicos de esta tecnología, aunque podemos usar los conectores y cables que utilizamos con Ethernet. Cada equipo se conecta a través de cable par trenzado ya sea apantallado o no a un concentrador llamado MSAU (*Multistation Access Unit*), y aunque la red queda físicamente en forma de estrella, lógicamente funciona en forma de anillo por donde da vueltas el Token. En realidad es la MSAU la que contiene internamente el anillo y si falla una conexión automáticamente la ignora para mantener cerrado el anillo.

Un MSAU puede soportar hasta 72 equipos conectados y el cable del MSAU al equipo puede ser hasta de 100 metros utilizando par trenzado apantallado, o 45 metros sin apantallar.

En redes de pequeñas a medianas con tráfico de datos pesado Token Ring es más eficiente que Ethernet. Por el otro lado, el ruteo directo de datos en Ethernet tiende a ser un poco mejor en redes que incluyen un gran número de equipos con tráfico bajo o moderado.

La especificación IEEE 802.5 (método de acceso Token Ring) se basó en la red Token Ring de IBM, es prácticamente idéntica y absolutamente compatible con ella. El término Token Ring se refiere tanto al Token Ring de IBM como a la especificación 802.5 del IEEE.

2.5.2 REDES INALÁMBRICAS (WIRELESS)

Cuando se precisa movilidad en las comunicaciones el cable se convierte más en un inconveniente que en una ayuda. Depender de un enlace físico supone una seria limitación para conseguir una absoluta libertad de movimientos. Para salvar estos obstáculos las redes inalámbricas son la alternativa perfecta. Esta tecnología comenzó a finales del siglo XX, pero ahora es cuando está en pleno auge, debido al abaratamiento de los costes y a su estandarización.

La ampliación de una red cableada con una red inalámbrica se conoce como topología de infraestructura. Para ello, se requiere una estación base, denominada **punto de acceso**, que funciona como puente entre las dos redes incorporando una tarjeta inalámbrica y otra de cable. Además el punto de acceso actúa como controlador central de la red inalámbrica.

- La topología usada por este tipo de redes, es la celular.
- Las principales ventajas de una red inalámbrica son:
- La movilidad y libertad de movimientos de los equipos.
- La conveniencia, vista como la facilidad de implementar la red en un tiempo mucho menor que el que llevaría con una red convencional y sin afectar la infraestructura existente. Se consiguen conexiones que serían inviables con otro tipo de medio por limitantes arquitectónicos o de distancias, o por estar prohibido tender cableado.
- La flexibilidad, porque con la misma facilidad con que se instala, se desinstala. Esto elimina la necesidad de levantar el cableado existente en el caso de un traslado.

REDES INALÁMBRICAS POR INFRARROJOS

Los rayos infrarrojos tienen una longitud de onda cercana a la de la luz, y por lo tanto, un comportamiento similar, con sus ventajas e inconvenientes:

- Son muy rápidos, alcanzando grandes velocidades de transmisión (algunos a 100 Mbps) y, debido a su alta frecuencia, presentan una fuerte resistencia a las interferencias electromagnéticas de otros dispositivos. Utiliza componentes sumamente económicos y de bajo consumo energético, lo que favorece en gran medida su uso en aparatos portátiles.
- La transmisión por infrarrojos no requiere autorización especial en ningún país, aunque los organismos de salud limitan la potencia de la señal emitida. Esto limita la cobertura de las redes a unas decenas de metros.

Como principal freno a su capacidad de difusión está la imposibilidad de atravesar objetos sólidos como paredes, por ejemplo. Además la luz solar directa, las lámparas incandescentes, y otras fuentes de luz brillante interfieren seriamente la señal. Resumiendo, a pesar de sus grandes ventajas, no es un método ampliamente.

REDES INALÁMBRICAS POR ONDAS HERTZIANAS

Wi-Fi

Basadas en el protocolo IEEE 802.11, conocido como Wi-Fi, y cuyo trabajo comenzó en 1991, aunque el estándar fue aprobado en 1997.

Existen diversos tipos de Wi-Fi, basado cada uno de ellos en un estándar IEEE 802.11 aprobado:

- Los estándares IEEE 802.11b, IEEE 802.11g e IEEE 802.11n disfrutan de una aceptación internacional debido a que la banda de 2.4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbps , 54 Mbps y 300 Mbps, respectivamente.
- En la actualidad ya se maneja también el estándar IEEE 802.11a, conocido como WI-FI 5, que opera en la banda de 5 GHz y que disfruta de una operatividad con canales relativamente limpios y, además, no existen otras tecnologías (BlueTooth, microondas, ZigBee, WUSB) que la estén utilizando, por lo tanto existen muy pocas interferencias. Su alcance es algo menor que el de los estándares que trabajan a 2.4 GHz (aproximadamente un 10%), debido a que la frecuencia es mayor (a mayor frecuencia, menor alcance).
- Existe un primer borrador del estándar IEEE 802.11n que trabaja a 2.4 GHz y a una velocidad de 108 Mbit/s. Sin embargo, el estándar 802.11g es capaz de alcanzar ya transferencias a 108 Mbit/s, gracias a diversas técnicas de aceleramiento. Actualmente existen ciertos dispositivos que permiten utilizar esta tecnología, denominados Pre-N.

BlueTooth

Es un estándar diseñado especialmente para dispositivos de bajo consumo, que requieren corto alcance de emisión y basados en transceptores de bajo costo, como teléfonos móviles, Asistentes Personales Digitales (PDA), ordenadores, etc., utilizando radiofrecuencia y conexiones de corto alcance. Está pensado para oficinas, hogar e incluso el automóvil. Puede soportar voz, vídeo y datos a una velocidad máxima de 1 Mbps.

Los sistemas BlueTooth utilizan una señal que opera en la banda de 2,4 GHz y que realiza múltiples saltos de espectro para reducir las posibles interferencias con otros dispositivos. No necesita licencia y está disponible en casi todo el mundo. Su radio de acción es de unos 10 metros, es decir, se trata de un sistema de corto alcance aunque su cobertura pueda llegar a 100 metros con repetidores.

Anecdóticamente comentaremos que el ejército francés utiliza la misma banda para sus transmisiones, por lo que se negó a cambiar la frecuencia de éstas para dar paso a BlueTooth. El problema se solucionó limitando los saltos de la tecnología inalámbrica. De este modo, los dispositivos del país galo utilizan la misma frecuencia pero con saltos a 23 frecuencias en lugar de sobre 79

Hiperlan/2

Es un proyecto del Instituto de Estándares de Telecomunicaciones Europeo (ETSI), cuyo objetivo es mejorar las prestaciones ofrecidas por el estándar IEEE 802.11, el estándar Hiperlan/1 trabaja con una velocidad de transmisión de 23,5 Mbps, mientras que 802.11b ofrecía como máximo 11 Mbps.

Actualmente se dispone de la especificación Hiperlan/2, que mejora notablemente a sus antecesoras y ofrece una velocidad de transmisión de 54 Mbps.

Para ello, emplea el sofisticado método de modulación OFDM (*Orthogonal Frecuency Digital Multiplexing*) para la transmisión de las señales analógicas. Asimismo, y por encima de la capa física, el protocolo de acceso al medio (MAC) es totalmente nuevo y presenta un método duplex de división dinámica del tiempo para permitir una mayor eficiencia en la utilización de los recursos de radio ampliamente las ofrecidas por el resto de sus rivales en el sector del mercado inalámbrico. Sin embargo, este novedoso estándar se encuentra en una fase de evolución demasiado prematura, lo que puede influir en su consolidación en el mercado.

Algunos creen que los estándares IEEE 802.11 ya han ocupado el nicho comercial para el que se diseñó HIPERLAN, aunque con menor rendimiento pero mayor penetración comercial, y que el efecto de la red instalada impedirá la adopción de HIPERLAN. También dicen que como el uso principal de las WLANs es proporcionar acceso a Internet, la falta de soporte para calidad de servicio (QoS) en la Internet comercial hará que el soporte de QoS en las redes de acceso sea irrelevante.

Otros creen que el rendimiento superior de HIPERLAN/2 puede ofrecer nuevos servicios que las variantes de 802.11 son incapaces de suministrar.

2.6. INTRANET Y EXTRANET

2.6.1 INTRANET

Una Intranet es una red privada que utiliza los estándares de Internet. Podríamos decir que se trata, básicamente, de una LAN implementada con la misma tecnología que se utiliza en Internet: protocolos, mecanismos de interconexión, servidores web, de correo, etc. Intranet es un sitio web al público, con la diferencia que sólo puede ser usado por los usuarios (profesores, alumnos, etc.) de un centro y por personas externas autorizadas. Su uso es, básicamente, privado, y debe resultar tan completa como lo es Internet para los usuarios comunes.

Al igual que en Internet, la pieza clave de la Intranet es el World Wide Web, por tanto, los usuarios disponen de navegadores WWW para acceder a las páginas o recursos disponibles en la Intranet.

Una herramienta esencial, es el correo electrónico (e-mail), pero éste es interno, es decir, no sale del ámbito de la empresa.

Igualmente, se utilizan el resto de herramientas de Internet: transferencia de ficheros (FTP), acceso remoto, charlas interactivas (chat), videoconferencia...

En empresas pequeñas puede satisfacer la necesidad de comunicarse a tiempo con otros usuarios; también, puede ayudar a que las políticas y los procedimientos de la empresa, ylos documentos estén a disposición de los usuarios todo el tiempo. Y lo más importante, evita tener material impreso innecesario. Hay un importante ahorro de papel, y todo lo que el papel conlleva, almacenamiento, gestión, etc.

2.6.2 EXTRANET

Es una extensión de la intranet privada y que usa la tecnología World Wide Web para mejorar la comunicación con sus otros centros. Una extranet permite tener acceso limitado a la información que necesitan de su intranet, con la intención de aumentar la velocidad y la eficiencia de su relación de negocio o centro.

La comunicación entre los equipos distantes se realiza mediante redes públicas de transmisión de datos y emplean métodos de encriptamiento que evitan que se puedan descifrar las comunicaciones.

De trata de un espacio en línea donde se pueden incorporar aplicaciones y herramientas tecnológicas para acelerar los procesos diarios de trabajo. Por ejemplo, se pueden crear aplicaciones para realizar órdenes de compra en forma automatizada, o bien crear reportes de venta. Además, las extranets ayudan a disminuir los costos de operación, debido a que reducen los gastos administrativos, los de telefonía y papel.

Además, cualquier empleado puede conectarse a la Intranet desde casa mediante un nombre de usuario y contraseña y acceder a toda la información y documentos en función de las políticas de seguridad y acceso que se hayan establecido para cada tipo de usuario.

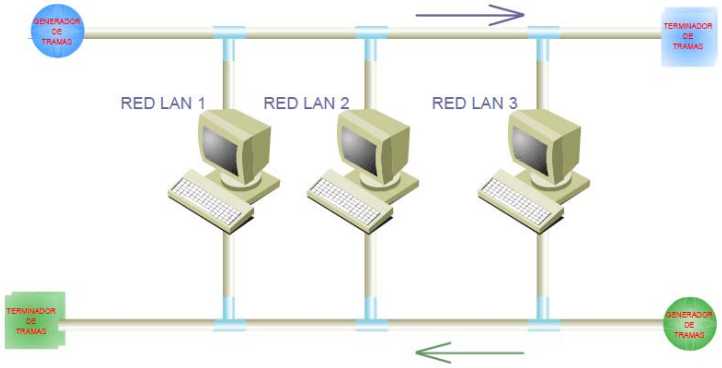
3. INTERCONEXIÓN DE REDES LAN: LAS REDES MAN

Cuando se llega a un cierto punto deja de ser poco práctico, e incluso imposible, seguir ampliando una LAN. Las limitaciones físicas, técnicas o económicas impiden seguir ampliando una LAN hasta alcanzar una amplia zona geográfica o conectar centros, edificios etc. separados por grandes distancias.

Este tipo de redes es similar en su estructura y funcionamiento a las LAN, si bien ocupan una mayor extensión geográfica y pueden ser públicas o privadas. Disponen de una serie de estándares específicos que las diferencia de las redes LAN y WAN.

3.1. DQDB

Este estándar es conocido como DQDB (Bus Dual de Cola Distribuida) y está adaptado a las características de las redes MAN, que no necesitan elementos de conmutación y dirigen la información empleando dos cables unidireccionales, es decir, un bus doble en el que cada uno de los cables opera en direcciones opuestas.



En este tipo de redes no se pueden producir colisiones ya que no es un medio Ethernet, sino que se procuran métodos para el control de acceso al medio, los generadores de tramas emiten de forma regular una estructura de trama que permite la sincronización de los equipos a la hora de transmitir, ya que podrán acceder al medio cuando un contador interno (sincronizado por la trama enviada por el generador) se ponga a cero.

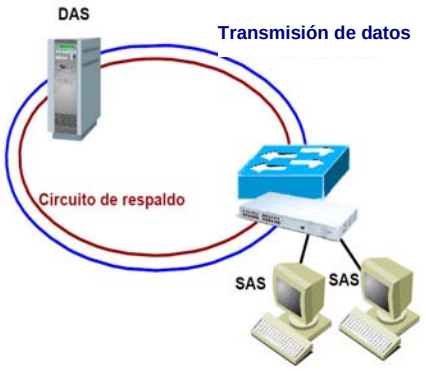
Cada nodo recibe la información por un bus de los nodos posteriores y envía por el otro, de manera que puede estar emitiendo y recibiendo información de forma simultánea.

3.2. FDDI

FDDI (Interfaz de Datos Distribuida por Fibra) es una LAN de anillo doble de token que corre con una velocidad de 100 Mbps sobre distancias de hasta 200 metros, soportando hasta 1000 estaciones

conectadas, y su uso más normal es como una tecnología de bus para conectar entre sí LANs de cobre u ordenadores de alta velocidad en una LAN.

El tráfico de cada anillo viaja en direcciones opuestas. Físicamente, los anillos están compuestos por dos o más conexiones punto a punto entre estaciones adyacentes. Los dos anillos de la FDDI se conocen con el nombre de primario y secundario. El anillo primario se usa para la transmisión de datos, mientras que el anillo secundario se usa generalmente como respaldo.



Las estaciones Clase B, o estaciones de una conexión (SAS), se conectan a un anillo, mientras que las de Clase A, o estaciones de doble conexión (DAS), se conectan a ambos anillos.

Las SAS se conectan al anillo primario a través de un concentrador que suministra conexiones para varias SAS. El concentrador garantiza que si se produce un fallo o interrupción en el suministro de alimentación en algún SAS determinado, el anillo no se interrumpa. Esto es particularmente útil cuando se conectan al anillo equipos que se encienden y se apagan con frecuencia.

FDDI utiliza una estrategia de transmisión de tokens muy similar a la de Token Ring, y como en éstas, no se producen colisiones.. La FDDI realiza la gestión del ancho de banda mediante la definición de dos tipos de tráfico: sincrónico y asíncrono. El tráfico sincrónico puede consumir una porción del ancho de banda total de 100 Mbps de una red FDDI, mientras que el tráfico asíncrono puede consumir el resto.

Tráfico sincrónico

El ancho de banda sincrónico se asigna a las estaciones que requieren una capacidad de transmisión continua, en tiempo real. Esto resulta útil para transmitir información de voz y vídeo. El ancho de banda restante se utiliza para las transmisiones asíncronas.

Tráfico asíncrono

El ancho de banda asíncrono se asigna utilizando un esquema de prioridad de ocho niveles. A cada estación se asigna un nivel de prioridad asíncrono. FDDI también permite diálogos extendidos, en los cuales las estaciones pueden usar temporalmente todo el ancho de banda asíncrono. El mecanismo de prioridad de la FDDI puede bloquear las estaciones que no pueden usar el ancho de banda sincrónico y que tienen una prioridad asíncrona demasiado baja.

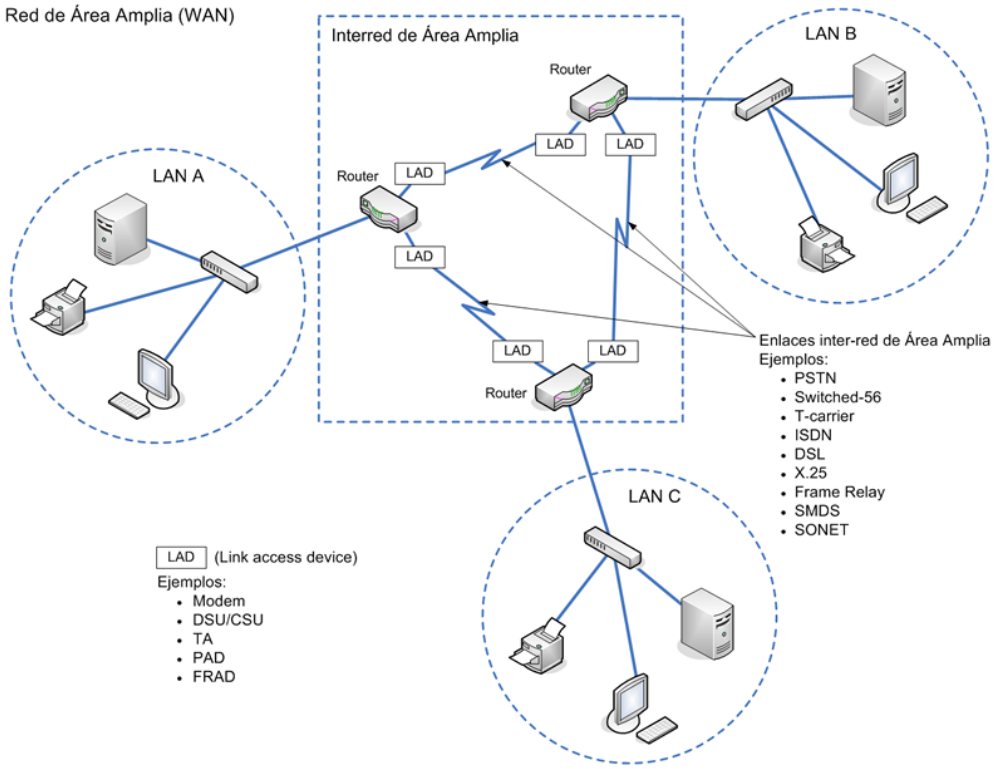
FDDI especifica una LAN de dos anillos de 100 Mbps con transmisión de tokens, que usa un medio de transmisión de fibra óptica.

4. REDES WAN

Una red WAN (*Wide Area Network*) es aquella que se encuentra formada por la interconexión de otras redes en un área geográfica amplia empleando, para ello, sistemas de telecomunicaciones. Normalmente, estos enlaces, no son administrados por los gestores de la red ya que son aportados por compañías externas (operadoras telefónicas).

Realmente, deberíamos hablar de conexiones WAN, más que de redes WAN, pues son los sistemas de conexión los que van a poder definir con más claridad este tipo de red.

Al ser las distancias entre máquinas considerablemente mayores es necesaria una tecnología diferente que garantice adecuadamente la transmisión de datos. Es en este punto donde mencionamos la tecnología ATM o la Red Digital de Servicios Integrados (RDSI).



4.1. DISPOSITIVOS DE INTERCONEXIÓN

En las redes LAN existe un estándar de comunicación con una implantación mayoritaria, LAN Ethernet y los dispositivos de interconexión presentan un abanico de posibilidades reducido, basado, fundamentalmente, en su funcionalidad.

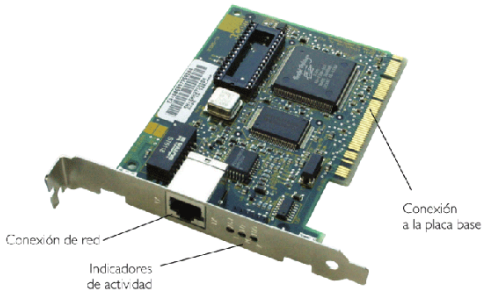
Sin embargo, en las redes WAN, si bien se encuentran rígidamente estandarizadas a nivel mundial, no existe un interfaz que predomine sobre el resto, esto supone que para una misma función existan distintos tipos de dispositivos en función de la tecnología de comunicación. Los mas comunes son el módem y sus evoluciones.

4.1.1 MÓDEM

Cuando se planteó la generalización de las comunicaciones entre equipos y la necesaria independencia de las redes privadas que empleaban medios propios de comunicación se comprobó que la solución más adecuada era el uso de las líneas telefónicas ya existentes cuya extensión es prácticamente mundial, la tecnología muy conocida y no necesita de la implementación de nuevos dispositivos.

Sin embargo, se planteaba el problema de la señal que circula por las líneas telefónicas. Mientras que los ordenadores se comunican con señales digitales, la línea telefónica transmite información analógica en una banda de frecuencias audible.

Para solucionar este problema debemos utilizar un módem, cuya función consiste en transformar la señal digital que procede del ordenador a una señal analógica utilizable por las líneas telefónicas. Igualmente, realiza la operación inversa, transformar la señal analógica que procede de la línea telefónica en una señal digital "entendible" por el ordenador.



Del mismo modo que dos personas hablan a la vez usando una línea telefónica (aunque tal vez no se entienda muy bien), dos módems pueden mantener comunicación simultánea en ambos sentidos (full-duplex). Esto es gracias a que en un módem los 1 y 0 se "oirán" de forma distinta que en el otro. No olvidemos que los módems usan cable telefónico que transmite en frecuencias audibles para el oído humano (300–3400 Hz).

La transmisión de datos se realiza en la misma banda de frecuencias que la voz, por ello, no se pueden transmitir datos y voz simultáneamente por una única línea. La velocidad de acceso de estas líneas es de 56,6 Kbps ([2]) de descarga y hasta 48 Kbps de subida.

Además de las funciones de modulación y demodulación, los módem deben ponerse de acuerdo en cómo va a realizarse la conexión y qué protocolos van a utilizar.

El equipo de usuario necesario para conectarse es un ordenador, un módem y una línea telefónica convencional. Además, necesitaríamos instalar software que permita este tipo de conexión y los protocolos de comunicación adecuados. Un módem ser interno (conectado a un puerto PCI) o externo (conectado a través de un puerto COM o USB).

Por regla general, un módem da acceso a un único ordenador, sin embargo, dicho ordenador puede actuar como servidor de acceso, permitiendo que el resto de los equipos de la red se conecten a Internet.

4.1.2 BRIDGE

Estos dispositivos ya han sido tratados en el apartado 2.3.4. Al situar un puente en cada una de las redes conectado a un módem, se puede filtrar en gran medida el tráfico que se va a dirigir a través de la conexión WAN, a la vez que permite mensajes de broadcast, algo que los enrutadores no permiten (salvo escasas excepciones).

Al existir una gran diferencia entre las velocidades de transmisión de las tecnologías WAN y LAN, un puente remoto (como son conocidos estos tipos de puente) debe contener un buffer interno (memoria de almacenamiento) que recoja la información de la red LAN y la transmita a través de la conexión WAN a menor velocidad.

4.1.3 ROUTERS (ENRUTADORES)

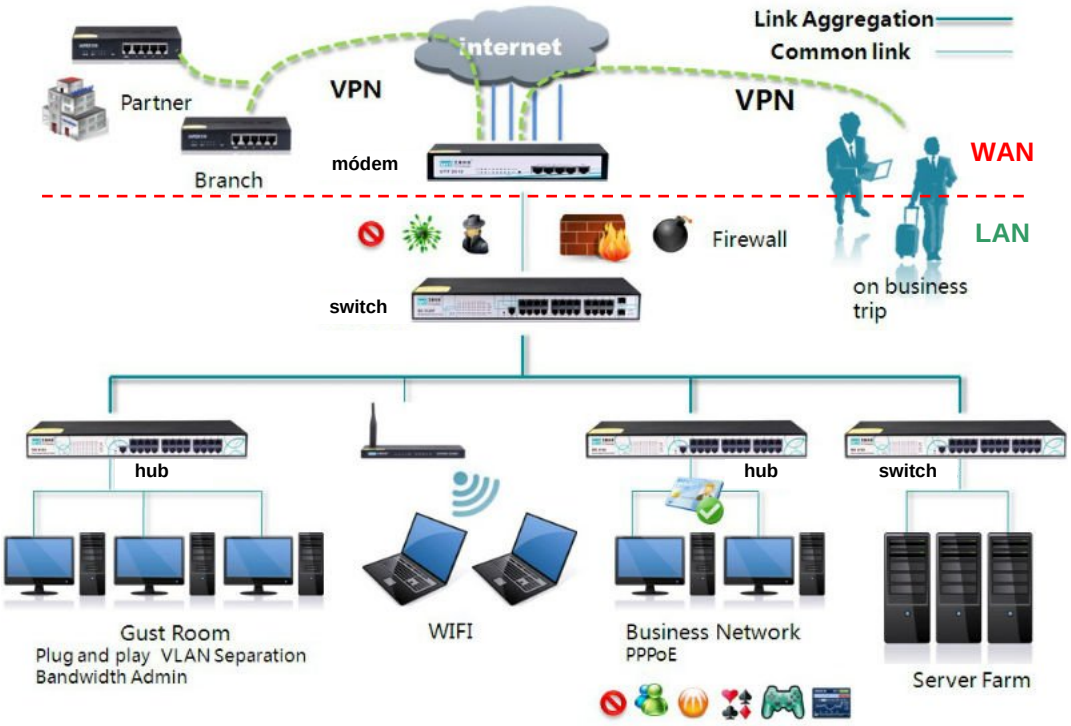
Podríamos definir al router como el dispositivo básico de comunicación entre redes. Un router es un dispositivo inteligente (similar a un ordenador) que determina la trayectoria a lo largo de la cual se puede establecer un enlace, y transmite los paquetes a lo largo de dicha trayectoria. Mientras

[2] La velocidad de transmisión de datos se mide en bits por segundo. En ocasiones podemos oír hablar de baudios. Los baudios son el número de veces que cambia el estado del medio de transmisión por unidad de tiempo. Los primeros módems enviaban un sólo bit en cada baudio. Cuando se alcanzó el límite de baudios por unidad de tiempo (1200 baudios por segundo) que permitían las líneas telefónicas, la velocidad de transmisión mejoró aumentando el número de bits que se incorporaban en un periodo de transferencia de datos

que los switchs y hubs tienen puertos donde se conectan los equipos independientes, los routers tienen interfaces a las que se conectan redes LAN.

Es un dispositivo de entrada y salida que, a través de un interfaz (puerto), enlaza distintas redes. Este interfaz es físico, es decir, se debe emplear un medio de interconexión (cable, microondas, etc.). Esta interconexión permite el paso de información en forma de datagramas de una red a otra, ofreciendo un servicio de calidad, ya que busca el mejor camino por el que dirigir el datagrama para que llegue a su destino.

Trabajan en la capa de red y utilizan las direcciones IP de los mensajes para dirigir el tráfico. Básicamente lo que hace un enrutador es mover paquetes de datos entre segmentos LAN adjuntos.



Por regla general, emplean protocolo IP y tecnologías de acceso WAN (RDSI, ADSL, Frame Relay), haciendo de forma efectiva virtualmente compatibles a todos los equipos en la capa de red. Para comunicarse con otros routers utilizan protocolos de enrutamiento o rutas estáticas.

Las funciones de un router son:

- Interconectar redes (física y lógicamente).
- Averiguar las direcciones IP de las redes y host que están conectados a sus puertos para realizar un envío óptimo de los paquetes.
- Evitar la congestión de las redes recibiendo los paquetes de datos y almacenándolos para distribuirlos progresivamente en función de la situación de la red.

Estas funciones las realizan gracias a que disponen de una memoria con unas tablas de enrutamiento, donde se han almacenado las rutas más apropiadas para dirigir los datagramas a través de las "marañas" de redes interconectadas. Como ya hemos destacado, aprenden automáticamente nuevas trayectorias y configuran la mejor ruta entre dos máquinas.

En resumen, un router acepta paquetes de datos por uno de sus puertos y los envía por otro en función de la dirección de red que tenga ese paquete de datos.

4.2. TIPOS DE REDES WAN

El criterio más eficiente para la clasificación de las conexiones WAN es la utilización o no de circuitos dedicados. Debemos considerar los **circuitos dedicados** como aquellos en los que el medio de

transmisión entre los puntos permanece permanentemente abierto. Por el contrario hablamos de **circuitos conmutados** cuando se deben estar conectando los distintos canales físicos para establecer la conexión entre los puntos.

- **WAN Conmutada**: Redes mediante conmutación de circuitos. Se crea, mantiene y finaliza un circuito físico de conexión dedicado, proporcionado por una compañía de telecomunicaciones (por ejemplo Telefónica). Esta tecnología sería similar a la que se emplea en las llamadas telefónicas y mantiene un ancho de banda estable.
  - RTB. Hasta 56 Kbps.
  - RDSI. Hasta 128 Kbps o 1,544 Mbps
  - X25. De 64 Kbps a 2 Mbps.
- **WAN dedicada**: Se trata de conexiones permanentes entre redes LAN, también se denominan enlaces punto a punto y proporcionan una ruta de comunicación específica implementando un router en cada red LAN. Los interfaces más habituales son:
  - xDSL. Hasta 2048 Mbps.
  - G703
  - V35

Investiga 3:

Realiza una tabla con las características de transmisión de: RTB, RDSI, ADSL, HDSL (velocidad de bajada y subida, frecuencia, etc)

4.3. TECNOLOGÍAS DE ACCESO REMOTO

Al tratarse de redes de comunicación públicas, las tecnologías empleadas deben ser las que ya están implementadas por las grandes compañías, comenzando con la simple conexión telefónica a través de un módem hasta las conexiones vía satélite. De todas ellas vamos a estudiar aquellas que más se emplean en la actualidad.

4.3.1 CONEXIONES CONMUTADAS

RED TELEFÓNICA BÁSICA

No requiere de una gran infraestructura local ni dispositivos de hardware, se implementa sobre la red telefónica y se requiere la utilización de un módem en uno de los equipos de la red LAN y que actúe como proveedor de acceso del resto de los equipos.

Las conexiones que se realizan suelen ser bajo demanda, ya que cuando trabajamos con conexiones conmutadas se suele pagar en función del tiempo que dure la comunicación; de este modo, cuando un equipo desea conectarse a su servidor de correo electrónico, el ordenador con el módem establece la conexión con el nodo de acceso (ISP o Proveedor de Servicios de Internet) que conectará con el servidor de correo. El módem mantiene la conexión mientras dura el intercambio de información y, por último, “cuelga”, cancela la conexión con el servidor.

Como ya hemos indicado, la conexión se realiza mediante un cable telefónico normal, lo que limita bastante el ancho de banda de las conexiones.

RED DIGITAL DE SERVICIOS INTEGRADOS

Se basa en una serie de normas que posibilitan la transmisión completamente digital de voz y datos sobre los mismos hilos de cobre que utiliza la RTB.

La diferencia entre una transmisión analógica y otra digital es que, mientras en una transmisión analógica RTB la comunicación que se origina en la línea del usuario es analógica, aunque en alguna centralita pueda ser tratada digitalmente, la RDSI es tratada, punto a punto, de forma digital.

Con la RDSI se mejora el tramo de cableado telefónico que existe desde el Punto de Presencia (centralita telefónica) de la compañía al domicilio del usuario (tecnología de la última milla) y se consigue que la transmisión sea digital en todos los tramos de la línea.

La principal ventaja es la mayor velocidad y calidad de la transmisión (no se producen las pérdidas de señal de las transmisiones analógicas) y su principal desventaja se encuentra en el adaptador (tarjeta RDSI) que es más caro que un módem para RTB, y también, el coste de la línea RDSI es mayor que el de una línea convencional.

En cualquier acceso RDSI existen dos tipos de canales, los canales B, que operan a 64 Kbps y que se utilizan para la transmisión de voz, datos, imágenes, etc. y un D que sirve para transmitir la información de control (conexión y desconexión de la comunicación, por ejemplo) y que puede funcionar a 16 ó 64 Kbps.

Una tarjeta RDSI para el ordenador es similar a una tarjeta Ethernet pero su circuitería debe adaptarse a la comunicación por un par de cobre y con los protocolos normalizados para este fin.

El esquema de conexión es idéntico al de la RTB (mediante servicio de marcación), excepto que la conexión entre nuestro equipo y el nodo de acceso correspondiente es a través de RDSI en lugar de RTB. Además, la conexión con la línea se hace a través de un dispositivo conocido como TR1, en el que encontramos dos conexiones RJ45 para extraer de ellas las dos líneas RDSI.

Aun cuando las llamadas a través de una línea RDSI tienen la misma tarifa que una llamada analógica, la transmisión de datos, la mayor velocidad y seguridad de la RDSI suponen un ahorro de costes porque se envía más información en menos tiempo.

Tipos de acceso RDSI

Los tipos de acceso RDSI se distinguen por el número de canales disponibles y por su velocidad de conexión. Existen dos tipos de acceso RDSI:

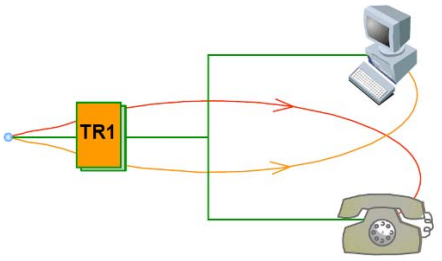
- **Acceso Básico (BRI)**: consiste en dos canales de 64 Kbps cada uno (canales B) que pueden usarse indistintamente para voz y datos, sólo para voz o sólo para datos, y un canal de 16 Kbps (canal D) para señalización y provisión de servicios suplementarios, como por ejemplo, el control de la conexión y desconexión de la llamada.

  Con un acceso básico, si utilizamos un único canal B para conectarnos a Internet se pueden alcanzar velocidades de hasta 64 Kbps, pero si utilizamos los dos canales B simultáneamente la velocidad será de hasta 128 Kbps. Evidentemente, al tratarse de un servicio de conmutación de circuitos, si empleamos los dos canales para la transmisión de datos no podríamos hablar simultáneamente.
- **Acceso Primario (PRI):** permite la conexión de 30 canales B y un canal D de 64 Kbps. El acceso PRI puede proporcionar un ancho de banda de 2,048 Mbps y permite elegir entre varias configuraciones de canales.

La tarificación de los canales se realiza por separado, así que, si usamos varios canales simultáneamente el coste será equivalente al de varias llamadas.

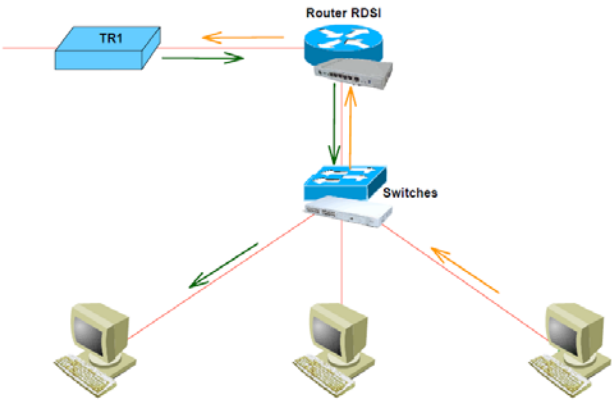
Elementos de una red RDSI

En primer lugar conviene distinguir entre terminales digitales (ET1) que pueden conectarse directamente a la línea RDSI y terminales analógicos (ET2) que necesitan un adaptador (AT) para conectarse a la línea digital. El adaptador AT tiene un interfaz de entrada y salida para cada dispositivo, es decir, una conexión para, por ejemplo, el teléfono analógico, y otro para conectarse a la línea RDSI.



Además de estos dispositivos, tenemos los equipos de terminación (TR1), que constituyen la frontera entre la línea de la compañía telefónica y la línea del usuario. Un TR1 es el dispositivo que ofrece la compañía proveedora para que los usuarios accedan a la línea RDSI. Dicho de otro modo, la caja a la que se conectan los dispositivos del usuario.

En ocasiones, la conexión no se hace directamente a los dispositivos TR1, es decir, que disponemos de una LAN conectada a un hub o switch y queremos acceder a la red RDSI, para ello, conectaríamos un router RDSI al hub o switch y a la línea RDSI. El router sería un equipo de terminación TR2.



La conexión mediante RDSI pareció ser una alternativa para las empresas de cara a obtener una conexión rápida y flexible de acceso a Internet o para crear conexiones WAN. Sin embargo, la forma en que las compañías telefónicas realizaban este tipo de conexión, su precio y la aparición del ADSL, han provocado que este tipo de conexión no se haya impuesto.

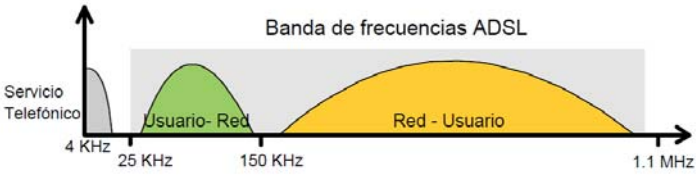
No obstante, es la alternativa al ADSL en las localidades donde aun no ha llegado este servicio.

4.3.2 CONEXIONES DEDICADAS

BUCLE DE ABONADO DIGITAL ASIMÉTRICO (ADSL):

La tecnología xDSL utiliza el ancho de banda disponible por encima del requerido por el servicio telefónico de voz hasta el límite permitido por la propia línea.

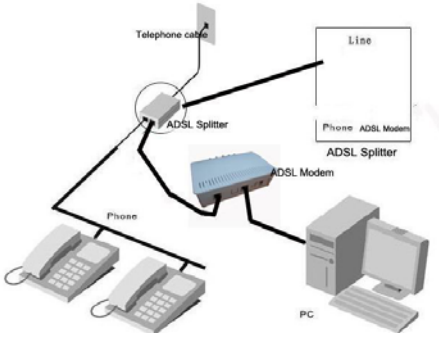
Se puede observar que la banda de frecuencias que utiliza ADSL se divide en dos subbandas, una para las señales enviadas desde el usuario hacia la red (velocidad ascendente) y otra mayor, para las señales recibidas por el usuario desde la red (velocidad descendente).



Esta asimetría permite alcanzar mayores velocidades en sentido red→usuario, lo cual se adapta perfectamente a los servicios de acceso a la información (Internet, correo, etc.) en los que normalmente, el volumen de información recibido es mucho mayor que el enviado.

Esto permite alcanzar elevadas velocidades de transmisión en el bucle de abonado, velocidades que dependerán de diversos factores tales como longitud del bucle, calibre de los pares, existencia de ramas múltiples, paso por zonas ruidosas, etc. En condiciones óptimas, ADSL permite alcanzar velocidades de hasta 24 Mbps en sentido red→usuario y, simultáneamente 3,5 Mbps en sentido usuario→red.

Conseguir este mayor ancho de banda en el acceso exige la incorporación de equipamiento específico tanto en el domicilio del usuario como en la central local.



Concretamente, es necesaria la instalación de sendos módems ADSL (uno ubicado en el domicilio del usuario y otro en la central local) que permitan el intercambio de señales a la frecuencia requerida. Adicionalmente, es necesario incorporar filtros separadores (*splitters*) que permitan discriminar la señal de las frecuencias de banda vocal y ADSL, posibilitando la coexistencia junto con el servicio telefónico básico.

Ventajas

Las ventajas que presenta el uso de tecnologías basadas en ADSL son:

- **Simultaneidad** y compatibilidad con el servicio telefónico. Sobre la misma línea es posible hacer, recibir y mantener una llamada telefónica simultáneamente a la conexión con Internet sin que se vea afectado en absoluto ninguno de los servicios.
- La separación de equipos permite aplicar a los servicios basados en ADSL políticas de precios independientes del servicio telefónico lo que ha hecho posible la introducción de la denominada **'tarifa plana'** para el acceso a Internet.
- Los usuarios están **siempre conectados** a la red, por lo que no existen fases de marcación y desconexión de la llamada, y no se pierde tiempo en la interconexión.
- Frente a otras soluciones de alta velocidad como el cable, es aplicable a la casi totalidad de líneas telefónicas ya instaladas, mientras que el cable necesita de un tendido de cable nuevo o su modificación. Por esto, su **implantación es económica** (no hay que hacer un gran desembolso, sólo en equipos terminales) y el alcance de este servicio es mayor que el de otras soluciones.

Otra ventaja del ADSL es que se trata de un **servicio dedicado para cada usuario**, con lo que la **calidad del servicio es constante**, mientras que con el cable se consiguen velocidades de hasta 400 Mbps (para uso doméstico 100 Mbps) pero la línea se comparte entre todos los usuarios conectados, degradándose el servicio conforme hay más usuarios y el tráfico aumenta.

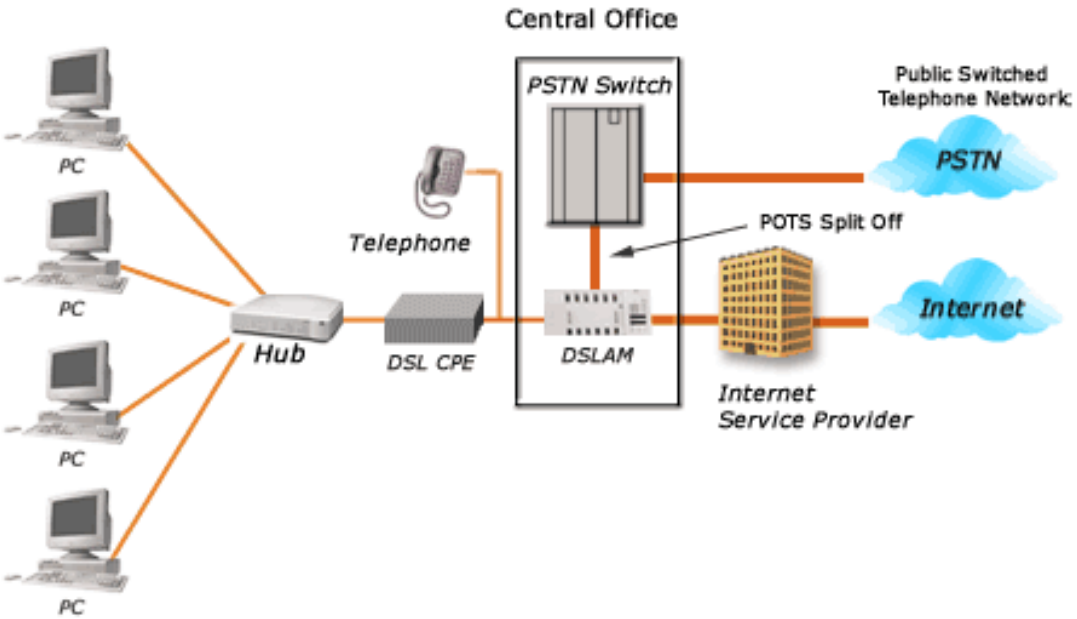
El servicio ADSL es más rápido y seguro que el cable ya que este último comparte el medio y utiliza técnicas de cifrado y tunelización de protocolos.

Esquema de conexión

El abonado está conectado permanentemente a un Nodo o central ADSL donde se van a separar por una parte, el servicio de voz, y, por otra, el servicio de datos ADSL. Se trata de la Central Local a la que llega el bucle de abonado y que debe estar provista de accesos ADSL.

La Central Local (Nodo ADSL) transmite los datos al ISP (o PSI) a través de una red de acceso de banda ancha, con recursos reservados suficientes que permitan sacar todo el partido a la conexión ADSL.

Por otro lado, transmitirá los datos de voz a la red telefónica básica.



4.4. PROTOCOLOS DE COMUNICACIÓN WAN

4.4.1 X-25

Es un protocolo utilizado principalmente en las redes públicas de transmisión de datos. Funciona por conmutación de paquetes, esto es, que los bloques de datos contienen información del origen y destino de los mismos para que la red los pueda entregar correctamente aunque cada uno circule por un camino diferente.

Esta diseñado para operar efectivamente sin importar los tipos de sistemas conectados a la red.

El servicio que ofrece es orientado a conexión (previamente a usar el servicio es necesario realizar una conexión y liberarla cuando se deja de usar el servicio), fiable, en el sentido de que no duplica, ni pierde ni desordena (por ser orientado a conexión), y ofrece multiplexación, esto es, a través de un único interfaz se mantienen abiertas distintas comunicaciones.

X.25 trabaja sobre servicios basados en circuitos virtuales (CV) o canales lógicos en el cual el usuario (DTE *Data Terminal Equipment* o terminal de usuario) piensa que es un circuito dedicado a un sólo ordenador; pero la verdad es que lo comparte con muchos usuarios o clientes mediante técnicas de multiplexado estadístico entrelazando paquetes de distintos usuarios de un mismo canal lógico (LCN).

El servicio X.25 es un diálogo entre dos entidades: DTE y DCE (*Data Circuit-terminating Equipment*) o red de paquetes.

Para que las redes de paquetes y las estaciones de usuario se puedan interconectar se necesitan unos mecanismos de control, siendo el mas importante desde el punto de vista de la red, el control de flujo, que sirve para evitar la congestión de la red.

También el DTE ha de controlar el flujo que le llega desde la red. Además deben existir procedimientos de control de errores que garanticen la recepción correcta de todo el trafico. X.25 proporciona estas funciones de control de flujo y de errores.

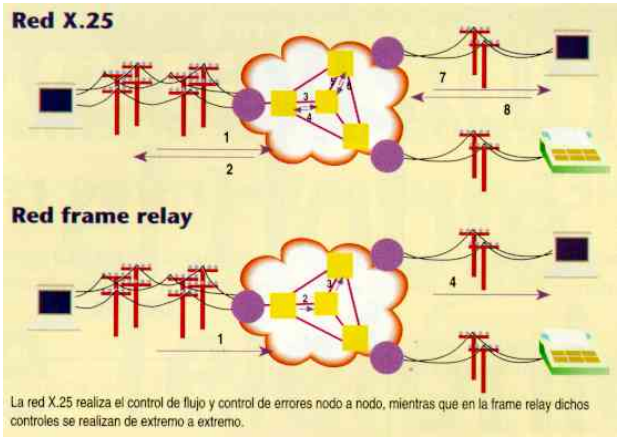
La X.25 se define como la interfaz entre equipos terminales de datos y equipos de terminación del circuito de datos para terminales que trabajan en modo paquete sobre redes de datos publicas.

Es el método de transmisión de información por RTB en Europa.

4.4.2 FRAME RELAY

Frame Relay se basa en conmutación de paquetes (tramas) de longitud variable proporcionando transmisiones de alta velocidad a través de líneas alquiladas digitales. Cuando se contrata un servicio de este tipo a un operador de telecomunicaciones se deben establecer:

- Velocidad de información comprometida: ancho de banda mínimo garantizado.
- Velocidad de información de ráfaga comprometida: ancho de banda máximo disponible en ráfagas. Este ancho de banda extra se consigue "robándolo" de otras conexiones.



La red X.25 realiza el control de flujo y control de errores nodo a nodo, mientras que en la frame relay dichos controles se realizan de extremo a extremo.

Este servicio se puede implementar sobre cable de cobre de par trenzado o fibra óptica. Este sistema supone que se implementa en redes de alta confiabilidad por lo que los mecanismos de control de errores que utiliza son muy simples.

LOS CIRCUITOS VIRTUALES DE FRAME RELAY

Cuando conectamos dos redes a través de Frame Relay se crean circuitos virtuales, es decir, que el operador de telecomunicaciones proporciona un circuito conmutado entre los distintos puntos. Este circuito se identifica con un código de 10 bits (DLCI) de manera que cada camino queda unívocamente identificado, de manera que las tramas que circulan por la red toman siempre el mismo camino, lo que aumenta la velocidad de transmisión.

El circuito puede ser permanente si se contrata así, de manera que se emplee siempre la misma ruta (con lo que se consigue mayor velocidad) o conmutado que serán rutas temporales a través de la nube de Frame Relay, creadas de forma dinámica en función de las necesidades del tráfico. En cualquier caso, aunque el circuito virtual sea permanente, se crea empleando el sistema de conmutación de circuitos.

4.4.3 ASYNCHRONOUS TRANSFER MODE (ATM)

ATM se trata de un protocolo para redes WAN y LAN, independiente del medio físico, que divide el tráfico de datos en celdas de un tamaño fijo lo que permite una utilización óptima del ancho de banda.

Las características básicas de la arquitectura ATM son:

- Es orientada a conexión.
- No tiene errores de control. Se maneja entre puntos finales.
- Es escalable. Diseñado para diferentes velocidades y tipos de medios.
- Diseñado para redes LANs y WANs.
- Posibilita transporte integrado de datos, audio y vídeo.

ATM está considerado como un modo de transferencia de paquetes orientado, basado en celdas de longitud fija. Cada celda está compuesta por 53 bytes, de los cuales 48 forman el cuerpo de información y los restantes son usados para campos de control o cabecera. La cabecera identifica la celda mediante un *Virtual Circuit Identifier* VCI y determina el camino que será utilizado con un *Virtual Path Identifier* VPI. Así, se define el tipo de conexión y el enrutamiento de celdas. Las celdas son enrutadas individualmente según los conmutadores incluidos en estos identificadores VPI y VCI.

4.5. RED DE CABLE

En ADSL no todo son ventajas, en un par de cobre, la atenuación por unidad de longitud aumenta a medida que se incrementa la frecuencia de las señales transmitidas. Y cuanto mayor es la longitud del bucle (tramo de cable entre 2 repetidores), tanto mayor es la atenuación total que sufren las señales transmitidas. Ambas cosas explican que el caudal máximo que se puede conseguir mediante los módems ADSL varíe en función de la longitud del bucle de abonado.

Entonces, frente a un servicio en ADSL cuyo potencial se basa en la reutilización del par de cobre tradicional y donde una de las características básicas (velocidad de acceso) se ve limitada por la longitud del bucle se encuentra el servicio ofrecido por los Operadores de Cable.

Algunas de las características que hacen competitivas a las Redes de Cable como redes de transmisión de datos de banda ancha son:

- **Velocidad y ancho de banda:** Las redes de cable proporcionan mayor ancho de banda disponible en el hogar del abonado que otras soluciones basadas en la red telefónica.
- **Conexión permanente:** Los usuarios permanecen conectados 24 horas, con acceso constante a la red, lo que permite la eliminación del establecimiento previo de la llamada puesto que los dispositivos estarán siempre recibiendo información sin coste. Podemos disponer en tiempo real de correo multimedia o un servicio de videoconferencia sin necesidad de procesos complejos de señalización.

- **Medio compartido:** La utilización de un medio compartido como es la red de cable en el que los usuarios no tienen un ancho de banda fijo en recepción permite reducir los costes de mantenimiento y operación frente a tecnologías como la RDSI o la RTB en las que por cada usuario conectado simultáneamente al sistema debe existir una "línea física" entre el usuario y la central local. Esto no sólo supone el desperdicio en costes por mantener la línea ocupada, cuando no existe transmisión de datos, sino también por el gran número de dispositivos y complejidad del equipamiento de la central cuando el número de usuarios es elevado.

  Además, en las redes de telefonía, existe la posibilidad de no disponer de capacidad de transmisión si todas las líneas están ocupadas, a diferencia del medio compartido, en el que el acceso está garantizado, aunque el ancho de banda disponible sea bajo.

4.5.1 ESQUEMA DE CONEXIÓN

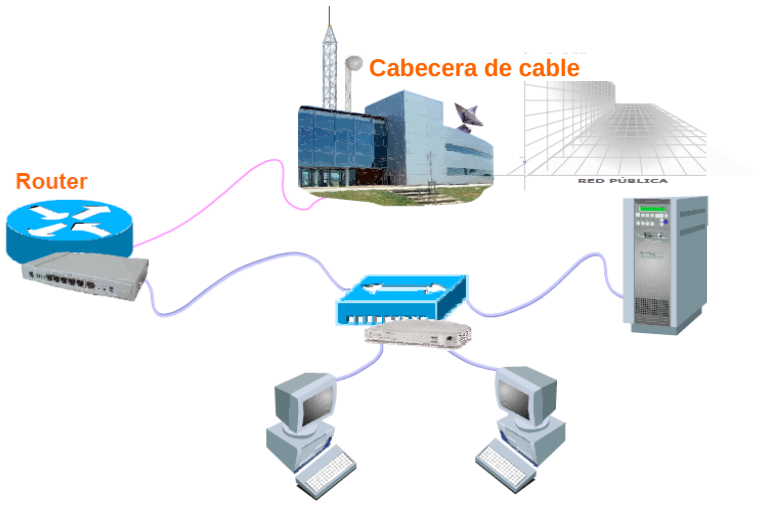
La red de cable la podemos estructurar en varias partes:

- **Cabecera de red de cable:** Es el órgano central desde donde se gobierna todo el sistema. Suele disponer de una serie de antenas que reciben los canales de televisión y radio de diferentes sistemas de distribución (satélite, microondas,...), así como de enlaces con otras cabeceras o estudios de televisión y con redes de otro tipo (ej. Internet) que aporten información susceptible de ser distribuida a los abonados a través del sistema de cable.

  En la cabecera se encontraría el CMTS (*Cable Modem Terminal Server*), es decir, el equipo encargado de comunicarse con los dispositivos terminales de transmisión de datos (módem de cable, set-top box[3]) instalados en la red.

  Gestiona el acceso y la transmisión de los equipos terminales de usuario a la red, bien asignándoles una frecuencia de transmisión o un instante de tiempo para transmitir, etc.

  También asigna direcciones a cada dispositivo para identificarlos en la red, ya sea a nivel MAC (nivel 2 del modelo OSI) o a nivel IP (nivel 3).
- **Router/Switch, cable-módem:** Todas las comunicaciones de un dispositivo terminal se realizan con la cabecera.
  - **Modulador:** Convierte las señales de datos enviadas por los dispositivos terminales de usuario en señales aptas para ser introducidas en la red de distribución.
  - **Demodulador:** Las señales de retorno provenientes de la red de distribución se suman, ya que provienen de diferentes nodos mediante fibras separadas y se combinan en la cabecera antes de pasarlas al demodulador.



[3] Set-top Box (STB), Receptor de televisión o Decodificador: es el nombre con el que se conoce el dispositivo encargado de la recepción y opcionalmente decodificación de señal de televisión analógica o digital (DTV), para luego ser mostrada en un dispositivo de televisión.

PLANTA DE CABLE

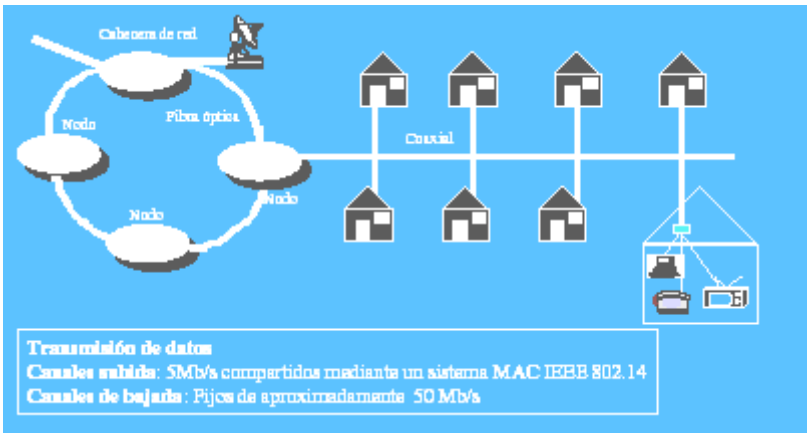
En este concepto agrupamos todo el despliegue de la red de cable desde la cabecera hasta el abonado final .

La red troncal

Es la encargada de repartir la señal generada por la cabecera a todas las zonas de distribución que abarca la red de cable mediante fibra óptica.

En una estructura con anillos redundantes que unen los nodos ópticos entre sí. En estos nodos ópticos es donde las señales descendentes (de la cabecera al usuario) pasan de óptico a eléctrico para continuar su camino hacia el hogar del abonado a través de la red de distribución de cable coaxial.

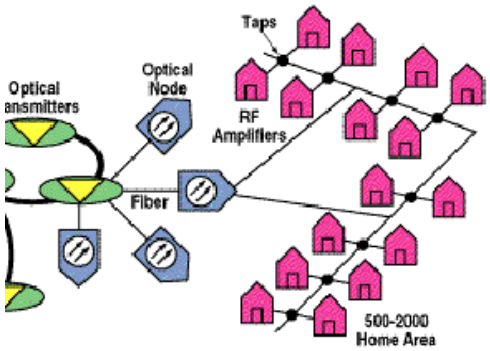
También se encargan de recibir las señales del canal de retorno o ascendentes (del abonado a la cabecera) para convertirlas en señales ópticas y transmitirlas a la cabecera a través de una o varias fibras independientes.



La red de distribución

La red de distribución está compuesta por una estructura de tipo bus de coaxial que lleva las señales descendentes hasta la última derivación antes del hogar del abonado.

Se estima que debe haber un nodo óptico por cada grupo de entre 500 y 2.000 viviendas. Si sacamos del nodo óptico varias ramas de coaxial, podemos tener un buen canal de retorno con no más de 100 ó 200 abonados por rama coaxial. Estas condiciones, en principio, aseguran un nivel de ruido y distorsión aceptables. Dichas ramas salientes del nodo óptico podrían acabar en unos nodos remotos para permitir la evolución hacia nodos ópticos de menor tamaño.



Evidentemente cuanto menor sea el número de usuarios por nodo óptico, mayor ancho de banda tendremos disponible de forma individual para cada usuario y menor número de dispositivos electrónicos entre abonado y cabecera por lo que aumentará la calidad.

La tendencia en la evolución de las redes de cable es acercar lo más posible la fibra a casa del abonado.

Acometida

La acometida a los hogares de los abonados es la instalación interna del edificio, el último tramo antes de la base de conexión.

Red de Abonado

Llamamos red de abonado al conjunto de elementos que se utilizan en el hogar del abonado para distribuir las señales en el interior.

La instalación está realizada en cable coaxial, y generalmente suele ser propiedad del propio abonado. Es aquí donde se generan mayores problemas en la transmisión de las señales de retorno, ya que normalmente el operador no tiene control sobre las modificaciones que pueda efectuar el usuario (conexión de nuevos televisores o dispositivos de amplificación, ampliación de la red a otras partes de la casa, etc.).

4.6. SISTEMAS DE ACCESO VÍA RADIO TERRESTRE

Entendemos por Sistemas de Acceso vía Radio, aquellos sistemas que utilizan el espectro radioeléctrico en el aire, en lugar del par de cobre, cable coaxial o fibra óptica para llevar la red de telecomunicaciones a casa del cliente.

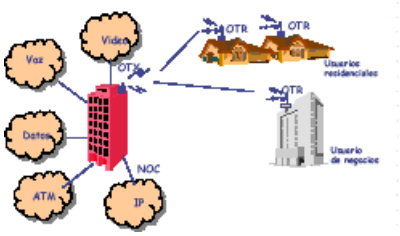
Se les conoce también con el nombre de 'bucle local inalámbrico' (WLL) o 'sistemas de acceso inalámbrico punto – multipunto'.

4.6.1 LMDS

El **sistema LMDS** (*Local Multipoint Distribution Service*) es un sistema de comunicación de punto a multipunto que utiliza ondas radioeléctricas a altas frecuencias. En España las frecuencias utilizadas para este sistema son, la banda de 3,5 GHz y la de 26 GHz.

Debido al ancho de banda disponible, el LMDS puede ser el soporte de una gran variedad de servicios como, por ejemplo, televisión multicanal (difusión, pago por visión, vídeo bajo demanda), telefonía, datos, servicios interactivos multimedia (teleducación, Internet en banda ancha, ...)

El territorio a cubrir se divide en células de varios kilómetros de radio, del orden de 15 Km. en la banda de 3,5 GHz, y del orden de 4 km en la banda de 26 GHz.



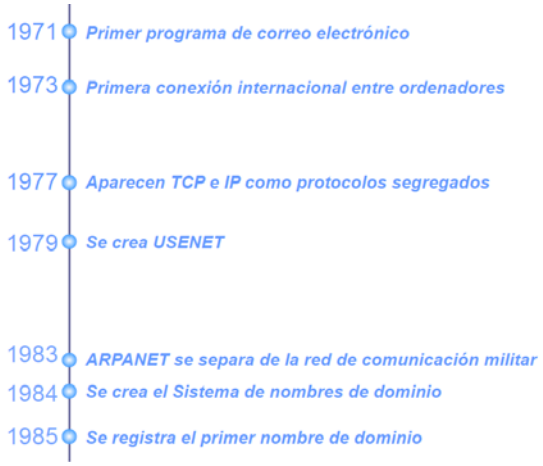
Por otro lado, la frecuencia de 3,5 GHz ofrece hasta 2 Mbps de ancho de banda y la de 26 GHz puede superar los 8 Mbps según las necesidades de los clientes.

Se trata de un esquema análogo al de la red de Cable, en el que podríamos distinguir los siguientes elementos:

- El **ISP** equivalente a la Cabecera de Servicios con funciones como proporcionar acceso a todas las redes a las que se van a conectar los usuarios (como Internet), captación y generación de la información que se va a distribuir..., y **Centro de Gestión de Red** con funciones como monitorización del sistema, gestión de red, provisión y tarificación de servicios, asegurar la calidad de servicio,...
- **La Red de Acceso**, es una Red troncal que une la Cabecera con cada Estación Base y puede ser de fibra óptica como en el caso de la red de Cable, o bien, radioenlaces dedicados punto a punto.
- **La Estación Base**, que es donde se realiza la conversión de la infraestructura de red troncal a infraestructura de acceso inalámbrico. Recibe la información de la Cabecera de Servicios y la retransmite al Estaciones de Usuario después de amplificarla y trasladarla a la banda de frecuencias asignada, y por otro lado, recibe las señales procedentes de las Estaciones de Usuario y las retransmite a la Cabecera de Servicios.
- **Las Estaciones de Usuario**, constan de transceptores CPE *(Customer Premise Equipment)* que captan la señal y la distribuyen entre los equipos correspondientes: gateways, set-top box, módem,... Y también transmite la señal de retorno a la Estación Base.

5. INTERNET

Internet es un sistema mundial de redes de ordenadores interconectadas mediante la pila de protocolos TCP/IP que pueden comunicarse sobre distintos medios y tecnologías. Este sistema de interconexión permite que cualquier usuario de cualquier red pueda acceder a equipos integrados en otras redes de otros países, siempre que tenga permiso para ello, para compartir información o comunicarse empleando, para ello, los distintos servicios de esta red de redes.



Un elemento fundamental para el desarrollo de Internet fue la creación de la pila de protocolos TCP/IP, sin embargo, no fueron estos los primeros protocolos que se emplearon en la primera red creadas por ARPA, ARPANET. El protocolo original era el *Network Control Protocol* (embrión de TCP/IP) y ALOHA, primer protocolo de comunicaciones por conmutación de paquetes vía radio.

En 1971 se crea el primer programa de **correo electrónico**, pero no fue hasta 1972 que se incorporó el popular carácter @ para separar el nombre de usuario y el servidor de correo de dicho usuario. Un año después se realiza la primera demostración pública de ARPANET realizándose, entre otras cosas, una demostración del **chat**. Además, en esa Conferencia Internacional de Comunicación entre Ordenadores, celebrada en Washington, se decide la creación del INWG, grupo internacional de trabajo sobre redes.

En 1973, y un año después de la publicación del RFC[4] sobre **telnet**, se realiza la primera conexión internacional entre ordenadores, y se comienza a estudiar la necesidad de emplear mecanismos de interconexión para la comunicación entre redes. La utilización de **news**, la creación del RFC sobre transferencias de ficheros (**ftp**), demuestran un enorme trabajo de desarrollo que contrasta con el bajo número de usuarios, alrededor de 2000.

Un paso que debemos considerar fundamental para la creación de Internet es la publicación del artículo "*A Protocol for Packet Network Interconnection*" donde se explicaba el protocolo TCP. Un año después se realizaban los primeros ensayos mediante este sistema de comunicación y, en función de los resultados de las distintas pruebas se adopta en 1977 la división del protocolo TCP en dos: TCP e IP. Ya existían programas de correo con funcionalidades similares a los que utilizamos ahora, y se había empleado para una transmisión de email transcontinental.

En 1979 se crea USENET. Un año después se produjo el parón del 27 de octubre en ARPANET debido a la amenaza de la propagación accidental de un virus. Se empieza a ser consciente de los problemas que se pueden asociar al desarrollo de Internet. Entre los años 1981 y 1982 se crean redes privadas y de ámbito nacional.

En 1983 ARPANET se separa de la red de comunicaciones militar. A la vez, se decide la adopción de TCP/IP como el protocolo para ARPANET y en 1984 se crea el sistema de nombre de dominios (**DNS**) para interpretar las direcciones IP[5]. Internet nace como fenómeno social, económico y tecno-

[4] Las *Request for Comments* ("Petición De Comentarios" en español) son una serie de notas sobre Internet, y sobre sistemas que se conectan a Internet, que comenzaron a publicarse en 1969.

Cada una de ellas individualmente es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet (originalmente de ARPANET), que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades.

[5] El *Stanford Research Institute,* dependiente directamente de la Universidad Stanford(en la actualidad SRI International) es una empresa americana y que lleva adelante investigaciones en diferentes dominios científicos y tecnológicos. Entre otro hechos importantes, invento el "entorno de escritorio" y el ratón.

En 1985 se le atribuyo al SRI la responsabilidad de asignar los nombre de dominio que residían en el ISI (*Information Sciences INstitute*), siendo en 1985 cuando se registra el primer nombre de dominio *symbolics.com*

lógico. A partir de ese momento Internet empieza a ser lo que hoy conocemos, con sus debilidades y virtudes, sus hackers, virus, problemas de crecimiento, etc.

La década de los años noventa aparece el hipertexto (**http**) como forma de interactuar con Internet. Se desarrolla el primer navegador en 1993 y en ese mismo año se crea el primer servidor web español.

5.1. LA CONEXIÓN A INTERNET

Podríamos considerar que todos los usuarios de un mismo servidor de acceso a Internet constituyen una red WAN, pues mediante la utilización de una tecnología de telecomunicación llegan a unirse gran cantidad de redes LAN.

5.1.1 PROCESO DE CONEXIÓN

Para poder realizar una conexión a Internet nos debemos dar de alta en un Proveedor de Servicios de Internet (en adelante ISP), como Movistar, Orange, Jazztel, Ono...

Una vez dados de alta tendremos un nombre de usuario y una contraseña y, si se trata de conexión RTB o RDSI, un número de teléfono de un Nodo de Accceso.

La conexión se realiza del siguiente modo: el abonado realiza una conexión telefónica a través del módem conectado a nuestro ordenador. El número de teléfono que marcamos es el del Nodo de Acceso que nos han proporcionado (en ADSL, esta “llamada” la realiza el router al encenderlo).

Una vez realizada la llamada telefónica se establece una conexión con el ISP donde un servidor de autenticación y control de acceso nos permite la conexión hacia Internet tras comprobar que el nombre de usuario y contraseña son válidos.

5.2. PROTOCOLOS TCP/IP

En realidad TCP/IP, no es un único protocolo, sino un conjunto de ellos, que cubren las distintas capas del modelo de referencia OSI. Como los dos protocolos más importantes son TCP e IP, estos son los que han dado el nombre al conjunto.

TCP/IP fue desarrollado a principio de los años 70 por el ministerio de Defensa norteamericano, para la red ARPANET. Adoptó su forma actual en 1983, como consecuencia del proyecto DARPA (*Defense Advanced Research Projects Agency*), de la defensa norteamericana. Nació para interconectar distintas redes en entorno operativo UNIX. Soluciona básicamente el problema de interconectar distintas redes, divididas en subredes, enrutando el tráfico entre ellas

4	Aplicación		HTTP, FTP, SMTP, etc.
3	Transporte		TCP, UDP
2	Red	Internet	IP
		Host a red	ICMP, ARP, etc.
1	Enlace	Acceso a la red	Ethernet, Token Ring, etc.
		Enlace físico	Tipo cable

Como la comunicación entre ordenadores es de una gran complejidad, el problema se ha dividido en otros menos complejos, creándose varios niveles. Cada nivel soluciona un problema en la comunicación y tiene asociado uno o varios protocolos para ello.

El modelo de red Internet tiene 4 capas o niveles, que son:

1. **Aplicación:** aquí están incluidos los protocolos destinados a proporcionar servicios, tales como transferencia de ficheros (FTP), navegación en Internet (HTTP), correo electrónico (SMTP), etc.
2. **Transporte**: aquí están incluidos los protocolos destinados a proporcionar el transporte de los datos con la fiabilidad suficiente.

La información es dividida en paquetes, para que la transmisión sea más eficiente. Cuando llega al receptor, este mismo nivel se encarga de reordenar los paquetes y unirlos para recomponer la información. Los protocolos que se encargan de esto son, TCP (*Transfer Control Protocol*) y UDP (*User Datagram Protocol*).

Equivale a las capas de transporte del modelo de referencia OSI.

3. **Internet o red:** se encarga de enviar cada paquete de información a su destino, es decir encaminar los datos. Para ello coloca los paquetes del anterior nivel en datagramas IP y los envía al nivel inferior. Cuando recibe estos datagramas del nivel inferior, comprueba su dirección IP y los envía al nivel superior o los encamina a otro ordenador, si no son para éste. Los protocolos que actúan en este nivel son:
    - IP (*Internet Protocol*)
    - ICMP(*Internet Control Message Protocol*)
    - IGMP(*Internet Group Management Protocol*)
    - ARP (*Address Resolution Protocol*)
    - RARP (*Reverse Address Resolution Protocol*)
    - BOOTP (*Bootstrap Protocol*)

    Equivale a las capas de red del modelo de referencia OSI.
4. **Enlace:** se encarga de la transmisión a través del medio físico, que une todos los ordenadores de la red. En este nivel no tiene protocolos propios sino que usa los ya existentes para redes LAN y WAN, como Ethernet, X.25, Frame Relay, etc.

    Equivale a las capas física y de enlace del modelo de referencia OSI.

Analogía:

Supongamos que se nos ocurre la peregrina idea de enviar "El Quijote" a un amigo, empleando palomas mensajeras. Una sola paloma no puede llevar todo el libro así que microfilmamos las páginas y a cada paloma le damos un microfilm. Para facilitar el trabajo de nuestro amigo, numeramos las filminas, puesto que ordenar después todo el libro, sin una numeración, resultaría muy difícil.

A lo largo de todo el viaje, alguna paloma puede ser cazada, decidir que se va a otro lugar o, simplemente, perder su mensaje. Cuando esto sucede, nuestro amigo nos manda una paloma diciendo que algo no ha llegado o que ha llegado defectuoso. Así, hasta que complete el libro y lo pase a papel.

Ahora, en lugar de emplear las palomas, envío El Quijote en formato pdf por correo electrónico. Aparentemente, el libro va completo, sin embargo, los protocolos de comunicación realizarán las mismas tareas que tendríamos que hacer mi amigo y yo empleando las palomas.

5.2.1 PPP

El protocolo PPP (*Point-to-point Protocol*) permite establecer una comunicación a nivel de la capa de enlace TCP/IP entre dos ordenadores. Generalmente, se utiliza para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un módem telefónico. Ocasionalmente también es utilizado sobre conexiones de banda ancha (como PPPoE o PPPoA). Además del simple transporte de datos, PPP facilita dos funciones importantes:

- **Autenticación**. Generalmente mediante una clave de acceso.
- **Asignación dinámica de IP.** Los proveedores de acceso cuentan con un número limitado de direcciones IP y cuentan con más clientes que direcciones. Naturalmente, no todos los clientes se conectan al mismo tiempo. Así, es posible asignar una dirección IP a cada cliente en el momento en que se conectan al proveedor. La dirección IP se conserva hasta que termina la conexión por PPP. Posteriormente, puede ser asignada a otro cliente.

PPP también tiene otros usos, por ejemplo, se utiliza para establecer la comunicación entre un módem ADSL y la pasarela ATM del operador de telecomunicaciones.

PPP consta de las siguientes fases:

- **Establecimiento de conexión**. Durante esta fase, un ordenador contacta con otro y negocian los parámetros relativos al enlace: el método de autenticación que se va a utilizar, el tamaño de los datagramas, números mágicos para usar durante la autenticación,...
- **Autenticación**. No es obligatorio. Existen dos protocolos de autenticación. El más básico e inseguro es PAP, aunque no se recomienda dado que manda el nombre de usuario y la contraseña en claro. Un método más avanzado y preferido por muchos ISPs es CHAP, en el cual la contraseña se manda cifrada.
- **Configuración de red.** En esta fase se negocian parámetros dependientes del protocolo de red que se esté usando. PPP puede llevar muchos protocolos de red al mismo tiempo y es necesario configurar individualmente cada uno de estos protocolos. Para configurar un protocolo de red se usa el protocolo NCP correspondiente. Por ejemplo, si la red es IP, se usa el protocolo IPCP para asignar la dirección IP del cliente y sus servidores DNS.
- **Transmisión**. Durante esta fase se manda y recibe la información de red. LCP se encarga de comprobar que la línea está activa durante periodos de inactividad. PPP no proporciona cifrado de datos.
- **Terminación**. La conexión puede terminar en cualquier momento y por cualquier motivo.

5.2.2 TCP

TCP (*Transmission Control Protocol*) es el protocolo de control de transmisión de la capa de transporte, que regula las cuestiones relativas al transporte de la información.

El protocolo TCP se encarga de regular el flujo de la información, de tal forma que éste se produzca sin errores y de una forma eficiente. Proporciona calidad de servicio. Por esto, se dice que este protocolo es:

- **Orientado a la conexión:** esto significa que se establece una *conexión* entre emisor y receptor, previamente al envío de los datos. Se establece un *circuito virtual* entre los extremos. Este circuito crea la ilusión de que hay un único circuito por el que viaja la información de forma ordenada. Esto, en realidad no es cierto, la información viaja en paquetes desordenados por distintas vías hasta su destino y allí, tiene que ser reensamblada.
- **Fiable:** la información llega *sin errores* al destino. Por esto, la aplicación que usa este protocolo, no se tiene que preocupar de la integridad de la información, se da por hecho.

El protocolo TCP actúa de puente entre la aplicación, que requiere sus servicios, y el protocolo IP, que debe dirigir el tráfico por la red, hasta llegar a su destino.

Este protocolo usa la tecnología de conmutación de paquetes. La unidad de información es el byte y estos se agrupan en segmentos, que son pasados al protocolo IP. Estos segmentos viajan encapsulados en los datagramas IP. Es un flujo de información no estructurado, información binaria sin ningún formato. La aplicación de destino tiene que interpretar esta información. Los datos viajan en los segmentos junto a información de control. La transmisión es punto a punto, origen y destino, y full-duplex, es decir en ambas direcciones, para hacer más eficaz el tráfico en la red.

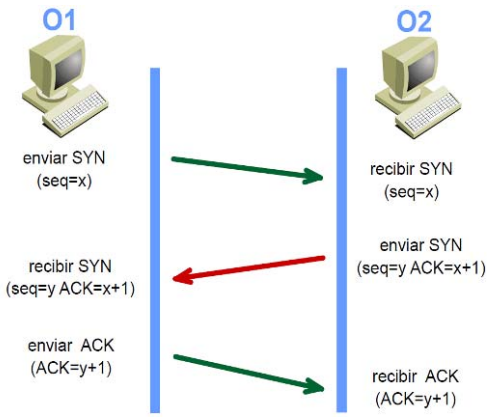
Los datagramas IP no tienen porqué llegar en el orden correcto al destino, pueden llegar en cualquier momento y en cualquier orden, e incluso puede que algunos no lleguen a su destino o lleguen con información errónea. El protocolo TCP se encarga de corregir estos problemas, numerando los datagramas antes de ser enviados y en el destino se encarga de reensamblarlos en el orden adecuado. Además solicita el reenvío de los datagramas que no hayan llegado o sean erróneos. No es necesario normalmente reenviar el mensaje completo.

Como hemos dicho, antes de poder enviar información, hay que establecer una conexión entre los extremos. En una transmisión hay tres fases:

1. Apertura de conexión

Para abrir la conexión se envían tres segmentos, por eso se llama "saludo de tres vías":

1. El ordenador 1 (O1), hace una *apertura activa* y envía un segmento TCP (S1), al ordenador 2 (O2). Este segmento lleva el bit SYN activado (se usa cuando se crea una conexión e indica al otro extremo cuál va a ser el primer número de secuencia con el que va a comenzar a transmitir).
2. O2 recibe el segmento (S1). Si desea abrir la conexión, responde con un segmento acuse de recibo (ACK), con el bit SYN activado, con ACK = x +1 y con su propio número de secuencia inicial (y), y deja abierta la conexión por su extremo. Si no desea abrir la conexión, envía un segmento, con el bit RST activado, a O1.



3. O1 recibe el segmento y envía su segmento de confirmación con ACK = y + 1.
4. O2 recibe la confirmación y decide que la conexión ha quedado abierta y puede enviar mensajes también en el otro sentido. Los números de secuencia usados (x e y), son distintos en cada sentido y son aleatorios para evitar conflictos

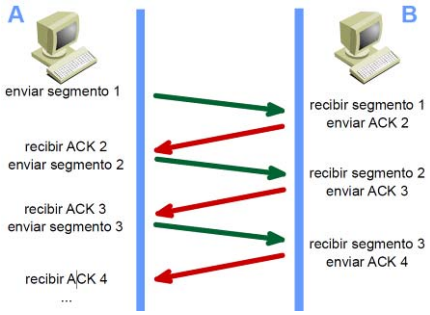
A partir del paso 4 comienza la transmisión de datos hasta el final. Cuando ya no hay más datos que transferir, hay que cerrar la conexión.

2. Transferencia de datos

Para controlar el flujo de la transmisión, el protocolo TCP, usa unas técnicas conocidas con el nombre genérico de “Solicitud de Repetición Automática” (ARQ), que usan el “acuse de recibo positivo con retrasmisión” (PAR), mediante el cual el receptor (O2) envía un mensaje de acuse de recibo (ACK), cada vez que recibe un segmento TCP del emisor (O1).

La técnica más simple es, la conocida como control de flujo mediante sistema de parada y espera. En esencia funciona así:

1. El ordenador 1 (O1), envía un segmento TCP (S1), al ordenador 2 (O2) y espera un ACK antes de enviar el siguiente. También arranca un temporizador con un tiempo de expiración (timeout). Si el temporizador expira antes de que O1 reciba un ACK, retransmite el segmento y reinicia el temporizador.
2. O2 recibe el segmento y envía su segmento de confirmación con ACK.
3. O1 recibe la confirmación y envía el 2º segmento.
4. El proceso continua de esta manera sucesivamente.



Para controlar la transmisión, TCP numera los segmentos secuencialmente. En el receptor, TCP reensambla los segmentos como estaban en el inicio. Si falta algún número de secuencia en la serie, se vuelve a transmitir el segmento con ese número.

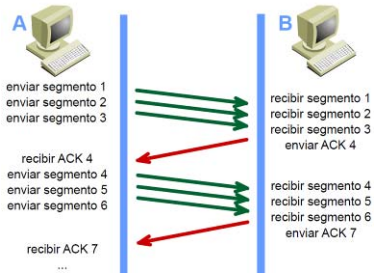
La numeración se hace contando los bytes de cada segmento. Si el primer segmento contiene 100 bytes y empezamos numerando con el 0, el siguiente segmento será el número 100.

La cantidad de datos en bytes que se pueden transmitir antes de recibir un ACK se denomina "tamaño de ventana".

- Con un tamaño de ventana = 1 y ventana simple: esta técnica es la más eficaz para evitar errores en la transmisión. Es muy usada cuando se transmiten tramas muy grandes, pero el canal de transmisión está desaprovechado la mayor parte del tiempo.

Una técnica más avanzada, conocida como "ventana deslizante", hace un uso más eficaz del canal de transmisión. En esta técnica el emisor envía varios segmentos sin esperar los ACK correspondientes.

- Con un tamaño de ventana negociado = 3 y ventana deslizante: Una tarea que tiene que realizar el protocolo TCP, es controlar la *congestión* de la transmisión. Para esto controla dinámicamente el tamaño de la ventana, aumentando o disminuyendo su tamaño, para que no haya congestión.



Comprobación de errores

Hay varias técnicas para detectar y corregir los posibles errores en la transmisión (Comprobación de la paridad, Suma de chequeo (*checksum*), Comprobación de la redundancia cíclica (CRC)).

Los métodos para informar de que ha habido errores en la transmisión son variados: Confirmaciones positivas, Confirmación negativa y transmisión, Expiración de intervalos de tiempo (*timeout*).

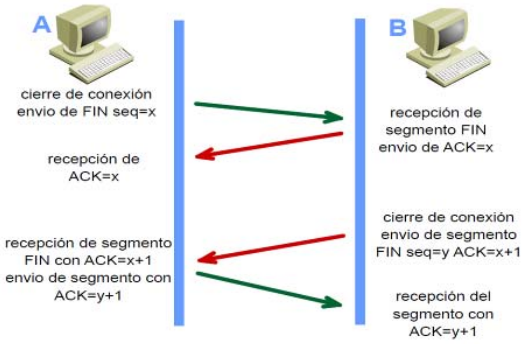
Investiga 4:

Investiga los términos mencionados en el epígrafe “comprobación de errores”. Indica en que consiste cada uno de ellos.

3. Cierre de conexión

El proceso es una variación del saludo de tres vías:

1. O1 ya no tiene más datos para transferir. Envía un segmento TCP con el bit FIN activado y cierra la conexión activa, en el sentido de envío. La recepción está abierta todavía.
2. O2 recibe el segmento, informa a la aplicación receptora del cierre y devuelve la confirmación (ACK) a O1.
3. O1 recibe el ACK de O2.
4. O2 decide cerrar la comunicación y envía un segmento TCP con el bit FIN activado.
5. O1 lo recibe y envía un ACK a O2.
6. O2 lo recibe y cierra la conexión definitivamente.



PUERTOS Y ZÓCALOS

La noción de **puerto**, es introducida por la capa de transporte para distinguir entre los distintos destinos, dentro del mismo host, al que va dirigida la información.

La capa de red solamente necesita, para dirigir la información entre dos ordenadores, las direcciones IP del origen y el destino. La capa de transporte añade la noción de puerto.

Un ordenador puede estar ejecutando a la vez varios procesos distintos, por ello no es suficiente indicar la dirección IP del destino; hay que especificar el puerto al que va destinado el mensaje.

Cada aplicación utiliza un número de puerto distinto. Cuando una aplicación está esperando un mensaje, lo hace en un puerto determinado, se dice que está "escuchando un puerto”.

Un puerto es un número de 16 bits, por lo que existen 2^{16} números de puerto posibles en cada ordenador. Las aplicaciones utilizan estos puertos para enviar y recibir mensajes. Se llama *conversación* al enlace de comunicaciones entre dos procesos.

> Analogía:
>
> Los puertos de un ordenador son como los andenes de una estación. Madrid-Atocha tiene más de 30 andenes, todos los trenes llegan a Madrid, pero en función de su origen las personas que esperan a los viajeros deben situarse en un andén u otro.

Aparte del concepto de puerto, la capa de transporte, usa el concepto de **socket o zócalo**. Los sockets son los puntos terminales de una comunicación, que pueden ser nombrados y direccionados en una red. Un socket está formado por la dirección IP del host y un número de puerto. Una dirección de socket está formado por la tripleta:

{protocolo, dirección local, proceso local}

Por ejemplo, en el protocolo TCP/IP un socket sería: {tcp, 193.53.214.3, 1345}. Si una aplicación cliente quiere comunicarse con una aplicación servidora de otro host, el protocolo TCP le asigna un número de puerto libre. En el otro extremo, la aplicación servidora permanece a la escucha en su puerto bien conocido.

Para que la transmisión sea más eficaz, los puertos usan una memoria intermedia. Existe un buffer en el origen, usado por la aplicación cliente, y otro en el destino, donde se van almacenando los datos enviados hasta que los pueda recoger la aplicación receptora.

Los primeros 256 puertos son los llamados "puertos bien conocidos" (well-known), y se usan para servicios comunes, como HTTP, FTP, etc. TCP asigna los números de puerto bien conocidos, para aplicaciones servidoras (aquellas que ofrecen servicios) y el resto de los números disponibles a las aplicaciones cliente (aquellas que solicitan servicios), según los van necesitando.

Los números de puerto tienen asignado los siguientes intervalos:

- Del 0 al 255 se usan para aplicaciones públicas.
- Del 255 al 1023 para aplicaciones comerciales.
- Del 1023 en adelante, no están regulados.

Los puertos bien conocidos están definidos en la RFC 1700 y se pueden consultar en http://www.ietf.org/rfc/rfc1700.txt

Al ser los puertos las "puertas" de entrada a un ordenador, pueden usarse por los "piratas" para sus ataques. Son puntos vulnerables. Se recomienda que, en general, no se tengan más puertos abiertos que los que sean imprescindibles.

El ataque puede ser directamente al ordenador cliente, o al servidor a través de éste.

Hay diversas aplicaciones usadas por los piratas informáticos, para accesos no autorizados. Se basan, generalmente, en la apertura de puertos de número mayor que 1023 para estos accesos. Es conveniente, por lo tanto, comprobar los puertos que tenemos abiertos y cerrar los que no necesitemos.

Con el comando **netstat**, podemos ver las conexiones activas y los sockets en uso.

> Investiga 5:
>
> Investiga el comando netstat. Teniendo abiertos el navegador y otras aplicaciones de Internet (por ejemplo descargas y/o subidas de datos a la nube) ¿Qué información nos muestra netstat?
>
> Haz una lista con al menos 10 servicios de Internet, que puerto usan y para que se usa cada servicio.

5.2.3 UDP

El protocolo UDP (*User Datagram Protocol*) proporciona una comunicación sencilla entre dos ordenadores y no consume muchos recursos. Pertenece a la capa de transporte y es:

- **No confiable**: no hay un control de paquetes enviados y recibidos. Estos pueden llegar erróneos o no llegar a su destino.
- **No orientado a conexión**: no se realiza una conexión previa entre origen y destino, como ocurre en el protocolo TCP.

Es un protocolo útil, en casos en los que no es necesario mucho control de los datos enviados. Se usa cuando la rapidez es más importante que la calidad, en los casos en que la información cabe en un único datagrama. Uno de sus usos más comunes es el envío de mensajes entre aplicaciones de dos ordenadores como DNS y SNMP.

Utiliza el protocolo IP para transportar los mensajes, es decir, va encapsulado dentro de un datagrama IP. No añade ninguna mejora a este protocolo, en cuanto a control de errores.

Incorpora los puertos origen y destino en su formato.

No controla errores, cuando se detecta un error en un datagrama, se descarta. Esto hace que deban ser las aplicaciones que lo usen, las que controlen los errores, si les interesa.

UDP no numera los datagramas, tampoco utiliza confirmación de entrega. Esto hace que no haya garantía de que un paquete llegue a su destino, ni que los datagramas puedan llegar duplicados o desordenados.

Algunas situaciones en las que es más útil el protocolo UDP, son:

- Aplicaciones en tiempo real como audio o video, donde no se admiten retardos.
- Situaciones en las que se necesita conectar con un ordenador de la propia red, usando una IP interna o un nombre. Habría que conectar primero con el servidor de red apropiado que transforme dicha dirección en una dirección IP válida.
- Consultas a servidores en las que se envían uno o dos mensajes solamente, como es el caso del DNS.
- En transmisiones en modo multicast (a muchos destinos), o en modo broadcast (a todos los destinos), ya que si todos los destinos enviaran confirmación el emisor se colapsaría.

5.2.4 IP

El protocolo IP (*Internet Protocol*) funciona transmitiendo la información por medio de paquetes. A este sistema se le conoce como "catenet". Da las normas para la transmisión de bloques de datos llamados datagramas, desde el origen al destino. Para hacer esto, identifica a los host origen y destino por una dirección de longitud fija, llamada dirección IP. Se encarga también, si fuera necesario, de la fragmentación y reensamblaje de grandes datagramas para su transmisión por redes de trama pequeña. Es un protocolo que pertenece a la capa de red.

Es un sistema de conmutación de paquetes:

- **no orientado a conexión**, ya que cada paquete viaja independientemente de los demás
- **no fiable**, los paquetes se pueden perder, duplicar o cambiar de orden. Es decir este protocolo no soluciona estos problemas, esta tarea queda para otros protocolos.

Este protocolo utiliza, a su vez, protocolos de redes locales, que se encargan de llevar el datagrama IP a través de la red local hasta su salida, por medio de una pasarela (*gateway*), hasta la próxima red.

El protocolo IP realiza dos funciones básicas:

- **Direccionamiento**: Cada datagrama IP tiene una cabecera en la que figuran la dirección de origen y de destino. El módulo Internet usa estas direcciones para llevar el datagrama hasta su destino. Este proceso se llama encaminamiento o enrutamiento.

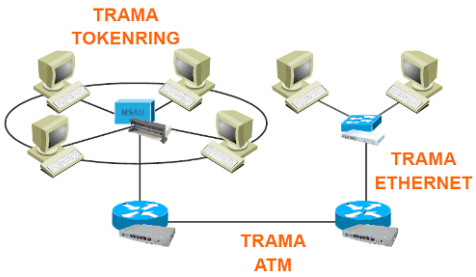
- **Fragmentación:** El módulo Internet usa campos en la cabecera para fragmentar y reensambla los datagramas IP, si fuera necesario, para su transmisión por redes de trama pequeña.

Cada datagrama IP, se trata como una entidad independiente, no relacionada con ningún otro datagrama IP. No existen conexiones o circuitos lógicos (virtuales o de cualquier otro tipo).

> El protocolo IP actúa como las señales en un vía pública. No saben si los coches que circulan por la calle llegan o no llegan a su destino, simplemente informan, si usted quiere ir al zoo, vaya por allí, hasta que se vuelva a encontrar otro cartel indicador o haya llegado ya. Así todos los carteles, uno tras otro, hasta que el coche llega a su destino.

Para transmitir un datagrama de una aplicación a otra, procede de la siguiente manera:

- Supongamos dos hosts, que quieren intercambiar información; cada uno estará integrado en su respectiva red local, y supongamos que hay una pasarela intermedia entre ambos.
- La aplicación remitente prepara sus datos y llama a su módulo Internet local, que se encargará de enviar esos datos como datagramas IP. Para ello, prepara la cabecera del datagrama y adjunta los datos a él con la dirección de destino y otros parámetros como argumentos de la llamada. Decide, por la dirección IP del destino, que debe enviarlo a la pasarela de la red local primera y lo envía a la interfaz de red local. Esta, crea una cabecera de red local (según las normas del protocolo de red la red local que sea), le adjunta el datagrama y envía el resultado a través de la red local.
- El datagrama llega a la pasarela encapsulado en la cabecera de red local.
- Esta pasarela, a su vez llama a su módulo Internet. Este, comprueba si el datagrama debe ser reenviado a otro host en una segunda red. Así sucesivamente, hasta llegar a la red local a la que pertenece el host de destino.



- Este host, a su vez, llama a su módulo Internet, que lo pasa a la aplicación a la cual va dirigido el datagrama, en este host. Pasa los datos a la aplicación en respuesta a una llamada del sistema, pasando la dirección de origen y otros parámetros como resultado de la llamada.

Como vemos, los datagramas van pasando desde un módulo Internet a otro hasta que se alcanza el destino. En el camino puede haber distintas redes interconectadas. Los módulos Internet residen en hosts y pasarelas.

En su ruta, los datagramas pueden necesitar atravesar una red cuyo tamaño máximo de paquete es menor que el tamaño del datagrama. Para salvar esta dificultad, el protocolo IP proporciona un mecanismo de fragmentación.

Todo este proceso se basa en la interpretación de una dirección Internet. Por eso, un importante mecanismo del protocolo IP es la dirección Internet**.**

DIRECCIÓN INTERNET Y DIRECCIÓN IP

Cuando queremos enviar un mensaje a través de un sistema de redes no podemos emplear la dirección física de la tarjeta ya que no existe un modo estandarizado de identificar un host dentro de una red, dentro de un sistema de múltiples redes, que sea efectivo. Así, se ha ideado la dirección IP, que permite identificar la red en la que se encuentra el ordenador y, a la vez, ubicar la posición de este PC dentro de la red.

El sistema de direccionamiento IP consiste en una serie de dígitos. Se representa por cuatro campos separados por puntos, como 193.144.238.1, no pudiendo superar ninguno de ellos el valor 255 (11111111 en binario).

Para poder identificar una máquina en Internet cada una de ellas tiene una dirección IP asignada por **IANA**, organismo internacional encargado de asignar las direcciones IP públicas, aunque se dedi-

ca a asignar las direcciones de red de las empresas proveedoras de Internet y estas ya se encargan de administrarlas para sus clientes.

Las direcciones IP son las que entiende la máquina y se representan por 32 bits con 4 campos de 8 bits cada uno, aunque normalmente se pasan de binario a decimal. Por ejemplo 139.3.2.8 es en numeración binaria 10001011 00000011 00000010 00001000.

Cualquier dirección IP de un host tiene dos partes, por un lado, aquella que identifica la red a la que pertenece el ordenador y por otro, el ordenador dentro de la red en la que se encuentra. Debemos analizar este sistema desde la perspectiva de la gran cantidad de ordenadores que existen conectados a Internet.

La forma de determinar las direcciones IP sería muy similar al antiguo sistema de matriculación de un coche, donde las primeras letras indicarían la provincia, y el resto el coche en concreto, que es distinto si pertenece a León o a Murcia.

- LE-3456-A
- MU-3456-A

Son dos coches distintos que pertenecen a provincias distintas. Lo mismo sucedería con las direcciones IP.

La diferencia radica en que existen distintos tipos de redes y es necesario determinar qué parte de la dirección IP pertenece a la red y cual al ordenador.

Para determinar qué parte de la dirección de Internet se refiere a la red y cuál pertenece al ordenador debemos introducir la máscara de subred que nos permite identificar los dígitos de la dirección IP que pertenecen a cada una de sus partes.

El sistema para realizar esta distinción es el siguiente. Si la dirección IP se compone de cuatro grupos de ocho bits, creamos una máscara en la que, de alguna forma se nos indica cuáles de esos bits pertenecen a la red y cuales al host. Los dígitos de valor uno de la máscara de subred indican la parte de la dirección IP que identifica la red, y los de valor cero, indican el ordenador. Así, la dirección IP de un equipo siempre debe estar asociada a una máscara de subred.

Significado	Red			Ordenador
Máscara de subred	11111111	11111111	11111111	00000000
Dirección IP	11000000	10101000	00000000	10101100

Direcciones IP PRIVADAS

Se denominan así a las direcciones IP que usan las redes privadas de organizaciones que no están directamente conectadas a Internet (esto es, las redes que se conectan por medio de un proxy o un router a una única línea con una única dirección IP dada por un proveedor de servicios).

Estas direcciones IP no son utilizadas por los routers para su comunicación con Internet, y se utilizan sólo dentro de la organización. Estas redes (Intranet) tienen la ventaja de ser mucho menos accesibles a ataques desde el exterior.

Clases de direcciones IP de legado.

Como ya hemos explicado, una parte de los bits representa la red y el resto la máquina (host). Existen cinco clases de direcciones IP según la manera de repartir los bits entre la dirección de red y el número de host.

Esta idea pretende asignar direcciones de red que se adapten a las necesidades de los usuarios. Así, si tenemos una red en donde la máscara de subred es del tipo 255.0.0.0, puede llegar a tener 256^3 mientras que si la máscara de subred es 255.255.255.0 sólo podrá haber 256 direcciones de host distintas.

Utilizando las direcciones IP y las máscaras de subred podemos definir varios tipos de redes.:

		Clase A	Clase B	Clase C	D y E
	Dirección de red	1.0.0.0 - 127.0.0.0	128.0.0.0 - 191.255.0.0	192.0.0.0 - 223.255.255.0	224.0.0.0 - 254.0.0.0
	Máscara de subred	255.0.0.0	255.255.0.0	255.255.255.0	
	IP privada	10.x.x.x	172.16.x.x- 172.31.x.x	192.168.x.x -192.168.x.x	
	Broeadcast	x.255.255.255	x.x.255.255	x.x.x.255	
Número	**Redes**	126	16.384	2.097.151	
Número	**Hosts**	16.777.214	65.534	254	

La clase que se elija para una red dada dependerá del número de máquinas que tenga y las que se prevean en el futuro. Como vimos antes el número de red es asignado por el NIC o por el organismo de cada país en quien él delegue. El número de host lo asignará el administrador que controla la red.

Direccionamiento sin clase

El sistema que utilizamos actualmente se denomina direccionamiento sin clase. Con el sistema sin clase, se asignan los bloques de direcciones adecuados según la cantidad de hosts a las compañías u organizaciones sin tener en cuenta la clase de unicast.

Ya que el sistema que se emplea para identificar cualquier servidor en Internet es su dirección IP, cuando quisiéramos conectar con un equipo, deberíamos identificarlo por esta serie de números, en muchos casos, difíciles de recordar. Así, se desarrolló el sistema de identificación por nombres de dominio. De esta manera, las direcciones del nivel de red en Internet pueden representarse de manera simbólica o numérica. Una dirección simbólica es por ejemplo www.cnice.mecd.es. La correspondencia entre direcciones simbólicas y numéricas las realiza el **DNS** (Domain Name System).

Investiga 6:

Investiga las direcciones IPv6 ¿Cómo funcionan? ¿Cómo se representa el loopback? ¿Qué es una dirección mapeada? ¿Qué es una dirección compatible?

5.2.5 ARP, RESOLUCIÓN DE DIRECCIONES

En una red local, los ordenadores se comunican por medio de tramas físicas.

Por ejemplo, en una red Ethernet, la comunicación se realiza por medio de las tramas Ethernet. En cada trama va un campo con la dirección física de origen y otro campo con la dirección física de destino. Cada hosts está identificado por su dirección MAC.

En una red Internet, la comunicación es por medio de datagramas IP, que van con direcciones IP.

Necesitamos, entonces, obtener la dirección física de un ordenador por su dirección IP.

Esto es lo que hace el protocolo ARP (*Address Resolution Protocol*) (Protocolo de resolución de direcciones).

Supongamos dos redes distintas, en la red 1 está el host1 que quiere enviar un mensaje al host 2, que está en la red 2.

1. El host 1 envía un datagrama, con IP origen 195.53.123.219 y con IP destino 193.47.120.220. Como el host destino está en otra red, el datagrama viajará a través de la red 1, hasta el router, que es la salida de esta red. Para ello hay que conocer la dirección física de la tarjeta de red 1 del router (el router tiene dos tarjetas de red, una para la red local u otra para la conexión WAN).

2. Entra en funcionamiento el protocolo ARP: Se manda un mensaje ARP a todos los ordenadores de la red 1, para ver quien tiene la dirección IP 195.53.123.210. Este mensaje es de multidifusión o broadcast y lleva la dirección física e IP del ordenador origen.
3. El router contesta mandando su dirección física 1, 00-90-E1-F8-91-A1. La respuesta va directamente al host que preguntó.
4. El host 1 manda la trama física, que contiene encapsulado el datagrama IP, al router.
5. El router pasa el datagrama IP a la red 2.
6. Se repiten los pasos 2 a 4 en la red 2.
7. El datagrama es recogido por el host2, ya que su dirección IP de destino coincide con la de él.

Vemos que el protocolo ARP ha hecho dos conversiones de dirección IP a dirección física. Si el recorrido fuera a través de n redes, se haría esto n veces.

Cada ordenador tiene una tabla ARP (caché ARP) que relaciona las direcciones físicas con las IP. Esta tabla la va construyendo según el proceso anteriormente descrito. Cada vez que el protocolo ARP hace una búsqueda, almacena la respuesta en la tabla ARP, así no tiene que repetir siempre el mismo proceso, sino que primero mira la tabla ARP y, si encuentra la respuesta en ella, la manda directamente al ordenador que la requirió.

La tabla ARP se actualiza cada cierto tiempo, para que recoja las modificaciones de direcciones IP que haya podido haber.

5.2.6 RARP

A veces, el problema se plantea al revés, se conoce la dirección física de un host y se necesita conocer la dirección IP. Esto es lo que hace el protocolo RARP (*Reverse Address Resolution Protocol*) (Protocolo de resolución de direcciones inverso).

Una máquina utiliza el protocolo RARP para obtener su dirección IP a partir de un servidor. RARP utiliza el mismo formato de mensaje que ARP y al igual que un mensaje ARP, es encapsulado en la parte de datos de una trama Ethernet. La red debe tener un servidor RARP, que conteste al host, enviándole la dirección IP, a partir de la dirección física.

Esto ocurre en el caso de un ordenador que accede vía módem a Internet, y el proveedor le asigna cada vez una dirección IP, de las que tiene libres en ese momento. El ordenador envía un mensaje broadcast con su dirección física, para que el proveedor le mande la dirección IP.

5.2.7 BOOTP

El protocolo BOOTP (*Bootstrap Protocol*) es algo más eficiente que el anterior, además de la dirección IP del solicitante, se manda información adicional, para facilitar el mantenimiento y movilidad de los ordenadores.

El protocolo BOOTP se utiliza para efectuar arranques remotos en ordenadores que no tienen una dirección IP.

DHCP

El protocolo de configuración dinámica de host (DHCP *Dynamic Host Configuration Protocol*) permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Se definió como una extensión del protocolo *Bootstrap*, porque BOOTP requería intervención manual para completar la información de configuración en cada cliente, y no proporciona un mecanismo para la recuperación de las direcciones IP en desuso.

5.2.8 ICMP

El Protocolo ICMP (*Internet Control Message Protocol*), proporciona un mecanismo que puede informar de los posibles errores. También da información de control, como congestión en la red, cambios de ruta, etc.

Los mensajes ICMP van encapsulados en los datagramas IP. ICMP utiliza el soporte básico de IP como si se tratara de un protocolo de nivel superior. Sin embargo, ICMP es realmente una parte integrante de IP, y debe ser implementado por todo módulo IP.

El protocolo ICMP no está diseñado para ser absolutamente fiable. El propósito del protocolo es darnos información, no solucionar, sobre los problemas que pueda haber en la comunicación. Existe la posibilidad de que algunos datagramas no sean entregados, sin ningún informe sobre su pérdida. Los protocolos de nivel superior que usen IP son los encargados de que la comunicación sea fiable.

Orden ping

Esta orden envía mensajes ICMP, de solicitud de eco, desde un host origen a otro destino y nos muestra los resultados.

Orden tracert

Sirve para saber por donde va pasando la información. Manda mensajes ICMP de solicitud de eco, con tiempos de vida 1,2 3, etc., hasta alcanzar el host destino. El 1º datagrama IP expira en el 1º router, mandando un mensaje tipo 11 (Tiempo excedido) y el router que lo envía. El 2º informa del 2º router y, así sucesivamente. Con esto se consigue tener una traza de los nodos por donde ha ido pasando el datagrama.

5.3. SERVICIOS DE INTERNET

5.3.1 HTTP

El Protocolo de Transferencia de HiperTexto (*Hypertext Transfer Protocol*) es un sencillo protocolo cliente-servidor que articula los intercambios de información entre los clientes Web y los servidores http.

Se diseñó específicamente para el World Wide Web: es un protocolo rápido y sencillo que permite la transferencia de múltiples tipos de información de forma eficiente y rápida. Se puede comparar, por ejemplo, con FTP, que es también un protocolo de transferencia de ficheros, pero tiene un conjunto muy amplio de comandos, y no se integra demasiado bien en las transferencias multimedia.

HTTP está soportado por los servicios de conexión TCP/IP. Cada vez que un cliente realiza una petición a un servidor, se ejecutan los siguientes pasos:

1. Un usuario accede a una URL, seleccionando un enlace de un documento HTML o introduciéndola en el navegador.
2. El cliente Web descodifica la URL, separando sus diferentes partes. Así identifica el protocolo de acceso, la dirección DNS o IP del servidor, el posible puerto opcional (el valor por defecto es 80) y el objeto requerido del servidor.
3. Se abre una conexión TCP con el servidor webs, llamando al socket {tcp, IPlocal, 80}.
4. Se realiza la petición. Para ello, se envía el comando necesario (GET, POST, HEAD,…), la dirección del objeto requerido (el contenido de la URL que sigue a la dirección del servidor), la versión del protocolo HTTP empleada (casi siempre HTTP/1.0) y un conjunto variable de información, que incluye datos sobre las capacidades del navegador, datos opcionales para el servidor…

5. El servidor devuelve la respuesta al cliente. Consiste en un código de estado y el tipo de dato MIME[6] de la información de retorno, seguido de la propia información.
6. Se cierra la conexión TCP.

Este proceso se repite en cada acceso al servidor HTTP. Por ejemplo, si se recoge un documento HTML en cuyo interior están insertadas cuatro imágenes, el proceso anterior se repite cinco veces, una para el documento HTML y cuatro para las imágenes.

En la actualidad se ha mejorado este procedimiento, permitiendo que una misma conexión se mantenga activa durante un cierto periodo de tiempo, de forma que sea utilizada en sucesivas transacciones. Este mecanismo, denominado HTTP *Keep Alive*, es empleado por la mayoría de los clientes y servidores modernos.

- Es un protocolo simple de solicitud-repuesta.
- Es usado por las aplicaciones Web.
- Usa el HTML como lenguaje de transmisión.
- Rápido y simple, aunque carece de estado. Lo que significa que, en principio, un servidor de HTTP carece de medios para relacionar información concerniente a una petición con otra petición anterior o posterior. Cada petición de página se procesa independientemente.

5.3.2 USENET

Usenet (también conocido como News) es un conjunto de protocolos para generar, almacenar y recuperar noticias "artículos" (parecidos a los mensajes mail de Internet) y para intercambiarlos entre lectores, con una distribución generalizada mediante el acceso a foros de discusión o conferencias multitudinarias sobre los temas más diversos.

Del mismo modo que las listas de correo, News es un medio para intercambiar información. Pero se diferencian en que las News no están basadas en el correo electrónico: no es necesario darse de alta en la lista, y los mensajes no se distribuyen a los buzones personales de los usuarios. En este servicio, los mensajes que se envían son públicos: todo el mundo tiene la posibilidad de acceder a ellos. En este sentido, las News son comparables a un gran número de tablones de anuncios públicos, clasificados por temas, a los que todo el mundo puede acceder para dejar un mensaje y/o para leer el resto de mensajes que están expuestos.

5.3.3 FTP

El protocolo FTP corresponde a Protocolo de Transmisión de Ficheros (*File Transfer Protocol*) y es usado para "subir" o "bajar" archivos entre una estación de trabajo y un servidor FTP.

Existen en la red Internet cientos de ordenadores que son servidores de ficheros de acceso público, es decir, que el usuario puede acceder a ellos y obtener ficheros sin necesidad de tener abierta una cuenta.

Existen programas clientes que permiten hacer FTP de una manera sencilla y completa. Aunque también se puede utilizar el propio navegador HTTP (en realidad, el navegador invoca un cliente FTP).

5.3.4 VNC

VNC (*Virtual Network Computing*) permite tomar el control del ordenador servidor remotamente a través de un ordenador cliente. Esencialmente es un sistema remoto de visualización que te permite ver el escritorio de un sistema operativo desde otra máquina diferente. Por ejemplo po-

[6] *Multipurpose Internet Mail Extensions* o MIME (extensiones multipropósito de correo de Internet) son una serie de convenciones o especificaciones dirigidas al intercambio a través de Internet de todo tipo de archivos (texto, audio, vídeo, etc.) de forma transparente para el usuario. Una parte importante del MIME está dedicada a mejorar las posibilidades de transferencia de texto en distintos idiomas y alfabetos

dríamos usar VNC para visualizar en nuestro PC el entorno UNIX de nuestro servidor situado en otra parte del edificio.

Un método similar de contacto remoto es la instalación de un servidor X en nuestro PC. Sin embargo VNC se diferencia de otros sistemas en varias características:

- Podemos abandonar la máquina a mitad de un trabajo, ir a otro equipo al otro lado de la puerta o muchos kilómetros más allá, conectarnos y finalizar nuestro trabajo. Con VNC todas las operaciones remotas se mantienen incluso si el PC es reiniciado.
- Es pequeño (se puede transportar en un pendrive) y muy sencillo, y no requiere proceso de instalación.
- Es independiente del tipo de plataforma. Un sistema operativo Linux puede ser visualizado en un PC, y también una máquina Solaris, así como otras muchas arquitecturas. La sencillez del protocolo lo hace posible.
- Un mismo escritorio puede ser visualizado desde numerosos equipos simultáneamente.
- Es gratuito. Se puede descargar y distribuir bajo los términos de la licencia pública GNU. Para más información consultar la siguiente web: http://www.uk.research.att.com/vnc/

VNC consta de dos tipos de componentes: Un servidor, el cual genera un “display” o imagen de la pantalla, y un visor, que realmente captura y muestra el “display” del servidor VNC.

5.3.5 IRC

IRC (*Internet Relay Chat*) es el comúnmente llamado Chat. Es una aplicación de Internet que permite mantener conversaciones en directo a través del ordenador en las que pueden participar varios usuarios a la vez.

Originalmente el Chat se llevaba a cabo por medio de texto escrito en pantalla, y aunque este modo sigue siendo mayoritario ha surgido, apoyado en los equipos multimedia, otro tipo de Chat que se realiza trasmitiendo la voz e imagen.

Para mantener una conversación por Chat es necesario un cliente IRC y una conexión a Internet. El cliente IRC es el programa que esta instalado en la máquina del usuario y envía y recibe los mensajes de un servidor IRC. Este servidor es el encargado de asegurar que los mensajes llegan a todos los miembros de una conversación.

5.3.6 TELNET

El protocolo TELNET proporciona el servicio de conexión remota y es un emulador de terminal que permite acceder a los recursos y ejecutar los programas de un ordenador remoto en la red, de la misma forma que si se tratara de un terminal real directamente conectado al sistema remoto.

El sistema local que utiliza el usuario se convierte en un terminal "no inteligente" donde todos los caracteres pulsados y las acciones que se realicen se envían al host remoto, el cual devuelve el resultado de su trabajo. Para facilitar un poco la tarea a los usuarios, en algunos casos se encuentran desarrollados menús con las distintas opciones que se ofrecen. Generalmente TELNET no ofrece gráficos bonitos o enlaces en el texto, pero es una cómoda y eficiente, si bien rudimentaria, forma de dar acceso remoto a una red a las personas interesadas e incluso al público en general.

Una vez establecida la conexión, se nos pide una identificación para darnos acceso (un nombre o login y una contraseña o password). A partir de ahí, si nos identificamos correctamente, estaremos dentro de la red con acceso a los servicios disponibles para el usuario con el cual nos identificamos.

Es posible ejecutar una aplicación cliente TELNET desde cualquier sistema operativo, pero hay que tener en cuenta que los servidores suelen ser sistemas VMS o UNIX por lo que, a diferencia del protocolo FTP para transferencia de ficheros donde se utilizan ciertos comandos propios de esta aplicación, los comandos y sintaxis que se utilice en TELNET deben ser los del sistema operativo del servidor.

Las direcciones TELNET consisten típicamente IP del servidor de la red que deseamos acceder, por ejemplo telnet://128.183.104.16/

El se encargará automáticamente de ejecutar un programa adicional para TELNET y este establecerá la conexión con el servicio deseado.

5.3.7 DNS

Las siglas DNS corresponden a Servidor de Nombres de Dominio (*Domain Name Server*). Básicamente es un conjunto de software y protocolos que traducen los nombres de dominio en una dirección IP, por ejemplo el dominio www.mec.es se corresponde a la IP 195.147.0.29.

Aunque Internet está basado en direcciones IP pero muy pocas veces usamos una dirección IP para visitar cualquier página en el navegador. Evidentemente, nos es mucho más sencillo el recordar nombres que números, de ahí el sentido de los DNS. Cada vez que usamos un nombre de dominio un DNS se encarga de traducirlo a una dirección IP.

Para ello usa lo que se denomina ***Resolver***: un conjunto de bibliotecas de las aplicaciones clientes, o sea, las que solicitan información acerca de un dominio de nombre.

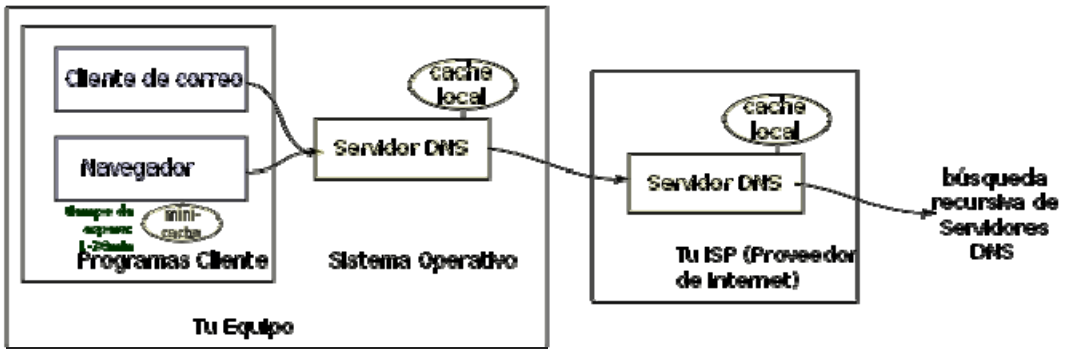
El *Resolver* tiene como tareas:

- Interrogar al servidor de nombres.
- Interpretar respuestas. Que serán registros o errores.
- Devolver información al programa que la solicita.

Primero el servidor de nombres verifica sus tablas de direcciones a ver si allí consigue el nombre por el cual le están preguntando. Si es así, entonces retorna la dirección IP asociada con ese nombre. Si la información pertenece a otro dominio, entonces el servidor de nombres busca en su cache y si no está allí comienza un proceso que se puede comportar de estas dos formas:

- De manera **Recursiva**: En las resoluciones recursivas, el servidor no tiene la información en sus datos locales, por lo que busca y se pone en contacto con un servidor DNS raíz, y en caso de ser necesario repite el mismo proceso básico (consultar a un servidor remoto y seguir a la siguiente referencia) hasta que obtiene la mejor respuesta a la pregunta.
- De manera **Iterativa**: Las resoluciones iterativas consisten en la respuesta completa que el servidor de nombres pueda dar. El servidor de nombres consulta sus datos locales (incluyendo su caché) buscando los datos solicitados. El servidor encargado de hacer la resolución realiza iterativamente preguntas a los diferentes DNS de la jerarquía asociada al nombre que se desea resolver, hasta descender en ella hasta la máquina que contiene la zona autoritativa para el nombre que se desea resolver.

Las bibliotecas del *Resolver* hacen búsquedas recursivas e iterativas, mientras que entre servidores de nombres solo se hacen búsquedas iterativas.



Cada máquina en la red pertenece a un dominio, cuyo servidor de nombres contiene la información acerca de la máquina. Esta información puede incluir direcciones IP, información acerca de enrutamiento de correo, etc. Una máquina también puede tener uno o más alias de dominio, lo cual quiere decir que existen 2 referencias hacia la máquina, una de ellas es un apuntador de un dominio (alias) a su nombre canónico (u oficial).

DNS permite eliminar los problemas que presentaba la existencia de un archivo de datos planos:

- Elimina el problema de nombres repetidos (cada organización tiene un dominio único, pueden existir dos máquinas con el mismo nombre mientras estén en dominios separados).
- Elimina el problema de carga y tráfico de red en una sola máquina ya que la información esta distribuida y disponible de manera redundante.
- Finalmente hay consistencia, ya que la actualización de la información se hace de manera automática, sin intervención del administrador de la red.

NOMBRE DE DOMINIO

Un nombre de dominio usualmente consiste en dos o más partes (técnicamente *etiquetas*), separadas por puntos cuando se las escribe en forma de texto. Por ejemplo, www.example.com o www.wikipedia.es

- A la etiqueta ubicada más a la derecha se le llama dominio de nivel superior (*top level domain*). Como *org* en www.ejemplo.org o *es* en www.wikipedia.es
- Cada etiqueta a la izquierda especifica una subdivisión o subdominio. "subdominio" expresa dependencia relativa, no dependencia absoluta. En teoría, esta subdivisión puede tener hasta 127 niveles, y cada etiqueta puede contener hasta 63 caracteres, pero restringidos a que la longitud total del nombre del dominio no exceda los 255 caracteres, aunque en la práctica los dominios son casi siempre mucho más cortos.
- Finalmente, la parte más a la izquierda del dominio suele expresar el nombre de la máquina (*hostname*). El resto del nombre de dominio simplemente especifica la manera de crear una ruta lógica a la información requerida. Por ejemplo, el dominio es.wikipedia.org tendría el nombre de la máquina "es", aunque en este caso no se refiere a una máquina física en particular.

El DNS consiste en un conjunto jerárquico. Cada dominio o subdominio tiene una o más zonas de autoridad que publican la información acerca del dominio y los nombres de servicios de cualquier dominio incluido. La jerarquía de las zonas de autoridad coincide con la jerarquía de los dominios. Al inicio de esa jerarquía se encuentra los servidores raíz: los servidores que responden cuando se busca resolver un dominio de primer y segundo nivel.

URL

URL (*Uniform Resource Locator*/Recurso de Localización Uniforme) se usa para nombrar recursos en Internet para su localización o identificación.

Un URL se clasifica por su **esquema**, que generalmente indica el protocolo de red que se usa para recuperar, a través de la red, la información del recurso identificado. Un URL comienza con el nombre de su esquema, seguido por dos puntos, seguido por una *parte específica del esquema*. Algunos ejemplos comúnmente encontrados en el uso diario de Internet son:

- **http**, que es el esquema más frecuentemente encontrado al navegar en Internet.
- **https**, que es el esquema usado para páginas seguras de Internet, conocido como SSL.
- **mailto**, esquema usado para direcciones de correo electrónico.
- **ftp**, esquema usado para el protocolo de transferencia de archivos ftp.
- **File,** esquema que indica recursos disponibles en el sistema local, o en una red local

La especificación de los elementos que siguen después de los dos puntos varía en función del esquema. Un **URL** tiene un formato estándar, que es:

esquema://máquina/directorio/archivo

donde *máquina* se corresponderá con un dominio (o un subdominio) o una dirección IP.

También pueden añadirse otros datos, por ejemplo, ftp permite añadir el usuario:

esquema://[usuario[:contraseña]@]máquina[:puerto]/directorio/archivo

Investiga 7:

Describe los componentes de las siguientes URLs:

http://es.wikipedia.org/wiki/Localizador_uniforme_de_recursos

https://accounts.google.com/ServiceLoginAuth

https://mail.google.com/mail/u/0/?shva=1#inbox/18e4519g3589c397

http://www.ideal.es/granada/rc/20130311/deportes/baloncesto/reina-mate-201303111300.html

ftp://j_fernandez@ftp.uca.es/imagenes/globo.gif

El siguiente ejemplo ilustra la diferencia entre una URL y un nombre de dominio:

URL: http://www.ejemplo.net/index.html

Nombre de dominio de nivel superior: net

nombre de dominio: ejemplo.net

nombre de host: www.ejemplo.net

5.3.8 CORREO ELECTRÓNICO

SMTP

SMTP (*Simple Mail Transfer Protocol*) es un protocolo de transferencia de correo entre servidores. El servidor que envía el mensaje establece una conexión TCP al puerto 25 de el servidor destinatario. Escuchando este puerto se halla un *daemon* o demonio que utiliza SMTP. Este demonio acepta los mensajes que llegan y los copia a sus correspondientes buzones de correo. Si el mensaje no puede ser entregado, se genera un mensaje de error que es enviado al remitente.

Una vez establecida la conexión TCP en el puerto 25, el servidor que envía el mensaje y actúa como cliente, espera que el servidor destinatario *hable* primero. El servidor envía un texto con su identidad y si puede o no recibir mensajes. Si no puede, el cliente abandona la conexión y lo intenta más adelante.

Si el servidor está preparado para recibir, el cliente envía información diciendo de quién es el mensaje y a quién va dirigido. Si el servidor reconoce al destinatario, manda un mensaje con la autorización de envío y el cliente manda los mensajes. Cuando se han mandado todos los mensajes en ambas direcciones, se corta la conexión.

SMTP permite que el correo pueda ser enviado desde una aplicación cliente a una aplicación SMTP, la cual almacena el mensaje en un dispositivo o tipo de memoria buffer. Así, el mensaje es incluido en esta estación de espera hasta que el proceso se pueda realizar con absoluta normalidad.

POP

El protocolo POP (*Post Office Protocol*) protocolo es usado para permitir que una estación de trabajo pueda tener acceso a los mensajes de correo que un servidor almacena para ella. El cliente será el ordenador que usa el servicio POP y el servidor el que proporciona este servicio.

POP no intenta proporcionar multitud de operaciones de gestión de correo, normalmente baja los mensajes de correo al ordenador y los borra del servidor.

Inicialmente, el servidor está usando una conexión TCP y escuchando el puerto 110. Cuando un cliente quiere hacer uso del servicio, establece una conexión TCP con el servidor, que le responde

dándole la bienvenida. El cliente y el servidor POP intercambian ordenes y respuestas (respectivamente) hasta que la conexión llega a su fin y es cortada.

Uno de los inconvenientes del protocolo POP es que necesita un gestor de correo en el ordenador cliente. El otro es que, al descargar al ordenador el correo entrante y borrarlo del servidor, dicho correo solo será accesible desde el ordenador donde está instalado el gestor de correo. Así mismo, del correo saliente solo se guarda copia en la máquina cliente.

IMAP

IMAP (*Internet Message Access Protocol*) permite a una aplicación cliente el acceso a los mensajes almacenados en un servidor como si estuvieran localmente almacenados. El correo puede ser manipulado desde distintos equipos. Por ejemplo desde el equipo en casa, la estación de trabajo en la oficina o el portátil mientras se viaja sin la necesidad de transferir archivos entre estos equipos.

Algunas características de IMAP son:

- Es completamente compatible con los estándares usados en los mensajes de Internet, es decir, accesible desde el navegador.
- Permite el acceso y tratamiento de los mensajes desde más de un equipo.
- El software del cliente no necesita saber el formato de almacenamiento del servidor.

El protocolo incluye operaciones para crear, borrar y renombrar buzones de correo, comprobar si hay nuevos correos, borrarlos permanentemente y operaciones de búsqueda entre otras.

El principal inconveniente suele ser el no poder consultar el correo ya recibido si no hay conexión a Internet.

Uno de las situaciones más típicas es que los mensajes leídos no son borrados, sino mantenidos en el servidor y éste se sobrecarga. Por ello se suelen tomar ciertas medidas por parte de los administradores de los servidores de correo como por ejemplo:

- Limitar al usuario la cantidad de espacio libre en el servidor para el almacenamiento del correo. Como consecuencia de ello, cuando la cuota es excedida, el usuario es incapaz de recibir nuevos mensajes. Normalmente los clientes son informados de esta situación.
- Imponer una política de tratamiento del correo. Por ejemplo, un sitio puede borrar los mensajes que no son leídos al cabo de 60 días y borrar los leídos a los 7 días.

5.3.9 SINCRONIZACIÓN HORARIA

Un aspecto que puede pasarnos por alto, pero que sin embargo es muy importante, es el tema de la sincronización horaria de nuestro equipo. En muchos casos es importante que nuestro servidor tenga la hora exacta, o que una red de ordenadores mantenga la misma hora. Para ello existen diversas aplicaciones que conectan nuestras estaciones de trabajo con servidores que supuestamente son más fiables, o están conectados a una fuente horaria casi perfecta. Esta fuente suele ser un reloj atómico o poseer unidades de sincronización GPS.

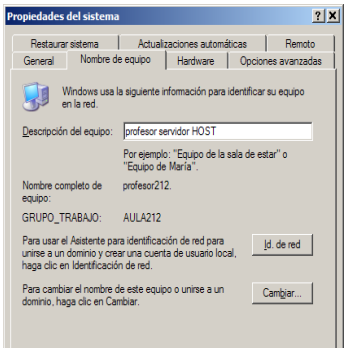
Estos servidores soportan protocolos como NTP, Time/UDP, o Time/TCP.

NTP (*Network Time Protocol*), por ejemplo, es un protocolo basado en TCP/IP que asegura una sincronización al milisegundo de la estación de trabajo con el reloj del observatorio naval de los EE.UU. en Washington. Para ello es necesario que una aplicación cliente esté funcionando en la estación de trabajo. NTP envía peticiones periódicas a servidores, obteniendo información precisa para ajustar el reloj cliente.

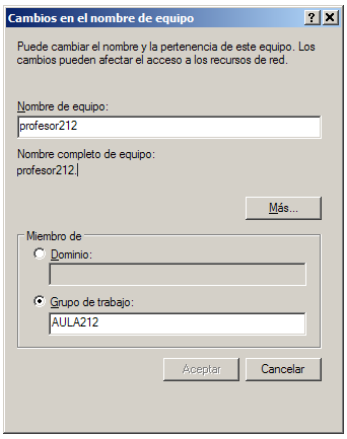
6. CONFIGURACIÓN DE EQUIPOS EN RED

6.1. WINDOWS

6.1.1 NOMBRE DE RED DEL EQUIPO



Lo primero que debemos hacer es identificar el equipo. Para ello , pulsamos botón derecho sobre MiPc\Propiedades→ficha **Nombre de equipo**.

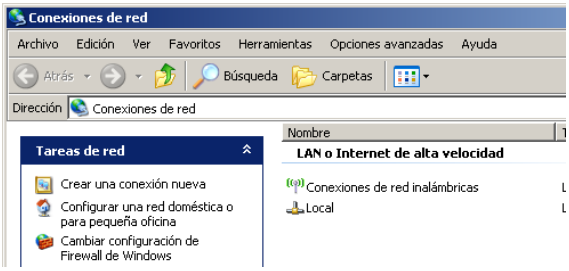


Aquí indicaremos el nombre descriptivo del equipo. Este nombre no es significativo para la red pero ayuda a identificar al usuario del mismo.

A continuación pulsamos el botón Cambiar. Se abrirá una nueva ventana (**Cambios en el nombre de equipo**). En ella debemos indicar el nombre de red del equipo y si nos vamos a unir a un dominio (red centralizada) o a un grupo de trabajo (red entre iguales).

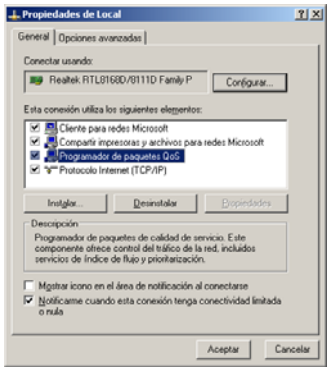
Los cambios se aplicarán tras reiniciar el equipo.

6.1.2 CONFIGURACIÓN TCP/IP



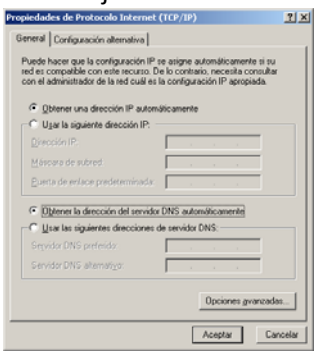
Abrimos **Conexiones de red**:

- Botón derecho sobre Mis sitios de red\Propiedades
- (En el área de notificaciones de la barra de tareas) Botón derecho sobre el icono de la tarjeta\propiedades
- Inicio\Configuración\Panel de control\Conexiones de Red



Sobre la *tarjeta* que queremos configurar, botón derecho\Propiedades (también llegamos aquí directamente a través de Inicio\Configurar\Conexiones de Red*tarjeta-a-configurar*.

Se nos muestran los protocolos instalados para esa tarjeta en concreto. Como mínimo deben aparecer:



- Cliente para redes Microsoft.
- Compartir impresoras y archivos
- Protocolo de Internet TCP/IP

Si no estuviesen hay que instalarlos a través del botón Instalar (hay que tener en cuenta que TCP/IP es un *protocolo*, Compartir… es un *servicio* y el Cliente es eso, un *cliente*).

Seleccionamos Protocolo de Internet TCP/IP y pulsamos Propiedades. Se abre la ventana **Propiedades de Protocolo Internet (TCP/IP)**.

Por defecto, aparece configurada para obtener la IP automáticamente a través del servidor DHCP mediante asignación dinámica.

Si deseamos usar asignación estática, marcaremos la opción *"Usar la siguiente dirección IP"*, lo que nos permitirá indicar los distintos valores.

La asignación de IP estáticas da mas seguridad en las redes locales ya que se impide que equipos ajenos a la red puedan conectarse. Por el contrario, la asignación dinámica permite que los equipos portátiles puedan conectarse a múltiples redes sin tener que tocar la configuración de red.

Si se mantiene la asignación dinámica, aparece la ficha *"Configuración alternativa"* que nos permite especificar (IP secundaria) una asignación estática que será usada en redes sin asignación DHCP. Esto es útil para configurar, sobre todo, portátiles de forma que, en casa o en la empresa, se conecten con una IP fija y, fuera de este ámbito, puedan conectarse a redes Wi-FI abiertas.

6.1.3 EL COMANDO NETSH

El comando NETSH y sus subcomandos nos permiten gestionar tanto la configuración IP como otros aspectos de los servicios de red (DHCP, enrutamiento, etc)

NETSH interface ip set address "Red de área local" static 192.168.1.6
mask=255.255.255.0 gateway=192.168.1.1 auto

Comando relacionados con gestión y configuración de redes

```
PING
TRACERT
NETSTAT
NSLOOKUP
IPCONFIG
ROUTE
NETSH para ip
FTP
NET VIEW
NET START
NET STOP
```

Investiga 8:

Realiza un chuletario con los comandos anteriores indicando para qué sirven y la síntesis con los principales parámetros.

6.2. LINUX

Al igual que el resto de procesos de configuración, la configuración de los adaptadores de red se realiza a través de archivos de texto ASCII. En estos archivos se definen tanto la IP primaria como las secundarias que deseemos para cada tarjeta que tengamos en el sistema así como las direcciones de *resolver*.

/etc/resolv.conf

En donde indicaremos las direcciones IP de los servidores DNS siguendo el formato:

nameserver 194.179.1.100
nameserver 194.179.1.101

/etc/hosts

Contiene las correspondencias de dirección URL <-> dirección IP, ya que esta traducción puede hacerse preguntando a un servidor DNS o utilizando este fichero. Normalmente lo que se hace es utilizar ambas cosas, servidor y fichero, y poner en el fichero sólo las direcciones locales que no se preguntan al DNS.

127.0.0.1 localhost

/etc/networks

Permite asignar un nombre simbólico a las redes.

```
loopback    127.0.0.0
localnet    192.168.0.0
```

/etc/HOSTNAME

Contiene una única línea con el nombre de dominio del equipo.

Configuración IP

Ubuntu

El fichero **/etc/network/interfaces** contiene todas las configuraciones, tanto primarias como secundarias, de todas las interfaces de red.

```
auto lo
    iface lo inet loopback
auto eth0                    IP primaria
    iface eth0 inet static
    address 10.0.10.100
    netmask 255.255.255.0
    gateway 10.0.10.1
    network 10.0.10.0
    broadcast 10.0.10.255
auto eth0:1                  IP secundaria
    iface eth0:1 inet static
    address 192.168.1.10
    netmask 255.255.255.0
    gateway 192.168.1.1
    network 192.168.1.0
    broadcast 192.168.1.255
auto eth1
    iface eth1 inet dhcp
```

La primera sección que nos encontramos es la del bucle **loopback** o interfaz de red virtual que suele tener la IP 127.0.0.1 y se suele utilizar cuando una transmisión de datos tiene como destino el propio host.

La última corresponde a una tarjeta con IP asignada por DHCP

Suse

Las configuraciónes se almacenan en archivos independientes denominados ifcfg-*tarjeta[:nº]* donde *tarjeta* especifica el interfaz y *nº* la IP secundaria.

/etc/sysconfig/network/ifcfg-eth0

```
DEVICE=eth0
IPADDR=10.0.10.100
NETMASK=255.255.255.0
NETWORK=10.0.10.0
BROADCAST=10.0.10.255
ONBOOT=yes
BOOTPROTO=static
USERCTL=no
```

/etc/sysconfig/network/ifcfg-eth0:1

DEVICE=eth0
IPADDR =192.168.1.10
NETMASK=255.255.255.0
NETWORK=192.168.1.0
BROADCAST=192.168.1.255
ONBOOT=yes
BOOTPROTO=static
USERCTL=no

/etc/sysconfig/network/ifcfg-eth1

DEVICE=eth1
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no

Especificaremos ONBOOT=yes si deseamos que la tarjeta se habilite al arrancar. Con BOOTPROTO indicaremos sí el interfaz se acoge al servidor DHCP o no. USERCTL=no indica que solo podrá configurar y controlar esa interfaz el root

6.2.1 PROCEDIMIENTO

Para configurar un adaptador de red basta con modificar o crear el archivo correspondiente. Tanto en SuSe como en ubuntu, los valores *network* y *broadcast* no son obligatorios si corresponde a x.x.x.0 y x.x.x.255 respectivamente.

Se puede hacer con un editor de texto, la interfaz gráfica o herramientas como YaST. O con comandos, aunque en este caso suele ser temporal y se pierde la configuración establecida al reiniciar.

Tras modificar los parámetros de la red hay que relanzar el demonio de red para que actualice los datos con que trabaja:

```
/etc/init.d/networking restart  (network en SuSe)
          service networking restart
```

Para configurar la tarjeta mediante comandos se utiliza:

```
ifconfig interfaz ip [netmask ip]
```

permite configurar todos los parámetros de la tarjeta excepto la puerta de enlace que se establece con:

```
route {add | del}  -net default gw IP
```

Por último para habilitar o deshabilitar una interfaz de red:

```
ifconfig interfaz up            ifup interfaz
ifconfig interfaz ip down       ifdown interfaz
```

Comandos relacionados con gestión y configuración de redes

```
ping
ifconfig
route
ftp
nslookup
/bin/hostname NUEVO_NOMBRE
/etc/init.d/networking restart | stop | start
```

Investiga 9:

Realiza un chuletario con los comandos anteriores indicando para qué sirven y la sintaxis con los principales parámetros.

Práctica:

Configura correctamente tu puesto de trabajo en red, teniendo en cuenta que la red es de tipo C y la puerta de enlace es 192.168.aula.254

- El equipo físico debe tener como IP 192.168.aula.0+puesto
- La MV Windows XP debe tener como IP 192.168.aula.50+puesto
- La MV SuSe debe tener como IP 192.168.aula.150+puesto
- La MV Ubuntu debe tener como IP 192.168.aula.200+puesto
- La MV Windows 2003 debe tener como IP 192.168.aula.100+puesto

Cada máquina tendrá como nombre host:

El equipo físico	puestoNN
La MV Windows XP	virXP-NN
La MV Windows 2003	vir03-NN
La MV Ubuntu	ubuntu-NN
La MV SuSe	suseNN

Siendo NN el número de tu máquina representado con 2 dígitos.

(Sólo máquinas Windows) comparte una carpeta como solo lectura (lectura-NN) y otra carpeta con acceso total (total-NN).

Comprueba que desde cada máquina puedes ver correctamente al resto, tanto físicas como virtuales, y acceder a los recursos que ofrecen.