Planificación y Administración de Redes

Versión 1.0

José Antonio Muñoz Jiménez

02 de junio de 2018

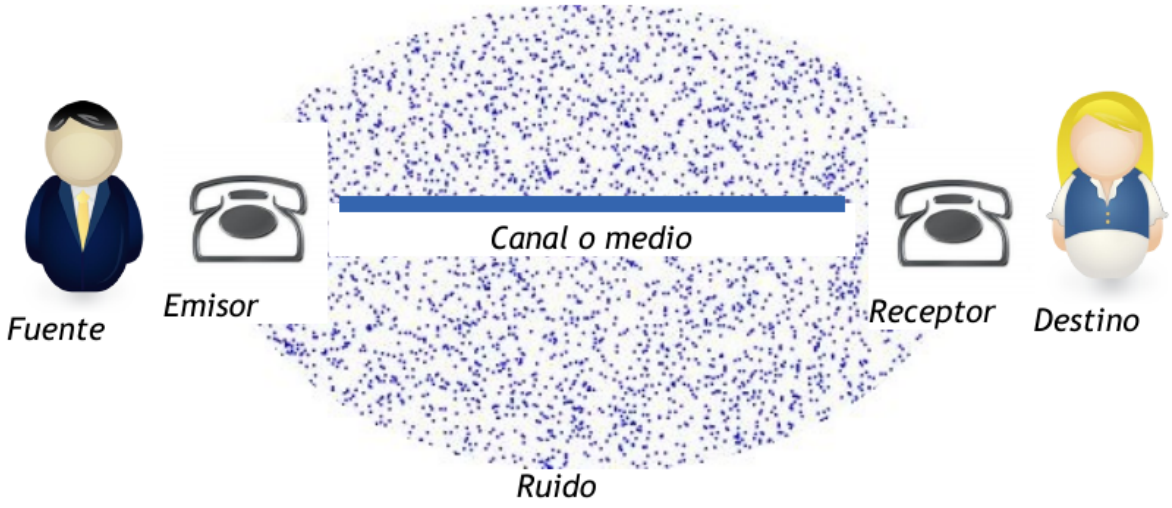
CONTENIDOS

CAPÍTULO 1

INTRODUCCIÓN A LAS REDES

1.1 Un modelo para las comunicaciones

En cualquier comunicación se pueden distinguir los 6 componentes que se indican a continuación:



El **fuente** es el origen del cual procede la información. Normalmente es una persona.

El **emisor** es el elemento que se encarga de transformar la información proporcionada por la fuente para adaptarla al canal o medio por el cual se transmitirá.

El **canal o medio** es el elemento por el cual se transmite la información. Este puede ser algún tipo de cable o, en el caso de comunicaciones inalámbricas, el aire.

El **ruido** es cualquier perturbación sobre el medio que afecte a la información. Esto hace que la información llegue con modificaciones.

El **receptor** es el elemento que se encarga de extraer la información del canal y transformarla para que pueda ser interpretada correctamente por el destino.

El **destino** es el lugar o entidad que consume la información. Normalmente es una persona.

1.2 Componentes de una red

Una red de computadoras, también llamada red de ordenadores, red de comunicaciones de datos o red informática, es un conjunto de nodos o hosts (equipos informáticos) y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

En una red de computadoras podemos distinguir los siguientes elementos:

Equipos finales

Son los ordenadores de los usuarios fuente o destino de la información. Y los ETCS

Equipos intermedios

Son los dispositivos que se hallan en el camino de la comunicación entre dos equipos finales. En Internet el más importante es el router o encaminador". En redes locales es el switch o conmutador y hub

Elementos de interconexión

Son los medios físicos utilizados para transportar los datos. Son el cableado y las ondas electromágneticas.

1.3 Tipos de redes

1.3.1 Según quién puede usarlas

Públicas

Una red pública se define como una red que puede usar cualquier persona. Es una red de computadoras interconectados, capaz de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica. Un ejemplo de red pública es Internet.

Privadas

Una red privada es aquella que sólo está disponible para ciertas personas. La mayoría de las redes privadas son LAN usadas en exclusiva por la organización propietaria. También se suelen llamar intranets.

1.3.2 Según el medio de transmisión

Cableadas

El medio de transmisión es un cable. Los principales son el cable coaxial, la fibra óptica y los pares trenzados.

Inálambricas

El medio es el aire. A través de éste se envían ondas electromagnéticas que pueden ser de diversas frecuencias: radio, microondas, infrarrojos.

1.3.3 Según su extensión

LAN (Local Area Network, Red de Área Local)

Su extensión abarca a lo sumo a un edificio, de modo que cualquier aula de informática u oficina normalmente tiene una red de este tipo. Utiliza para la conexión de ordenadores un cableado privado (o unos elementos repetidores de radiofrecuencias privados).

MAN (Metropolitan Area Network, Red de Área Metropolitana)

Su extensión abarca a varios edificios de la misma ciudad. Por ejemplo, una red para todos los centros educativos de una localidad, o para todos los edificios de un campus. Los medios que usa pueden ser privados o públicos pero alquilados en exclusiva.

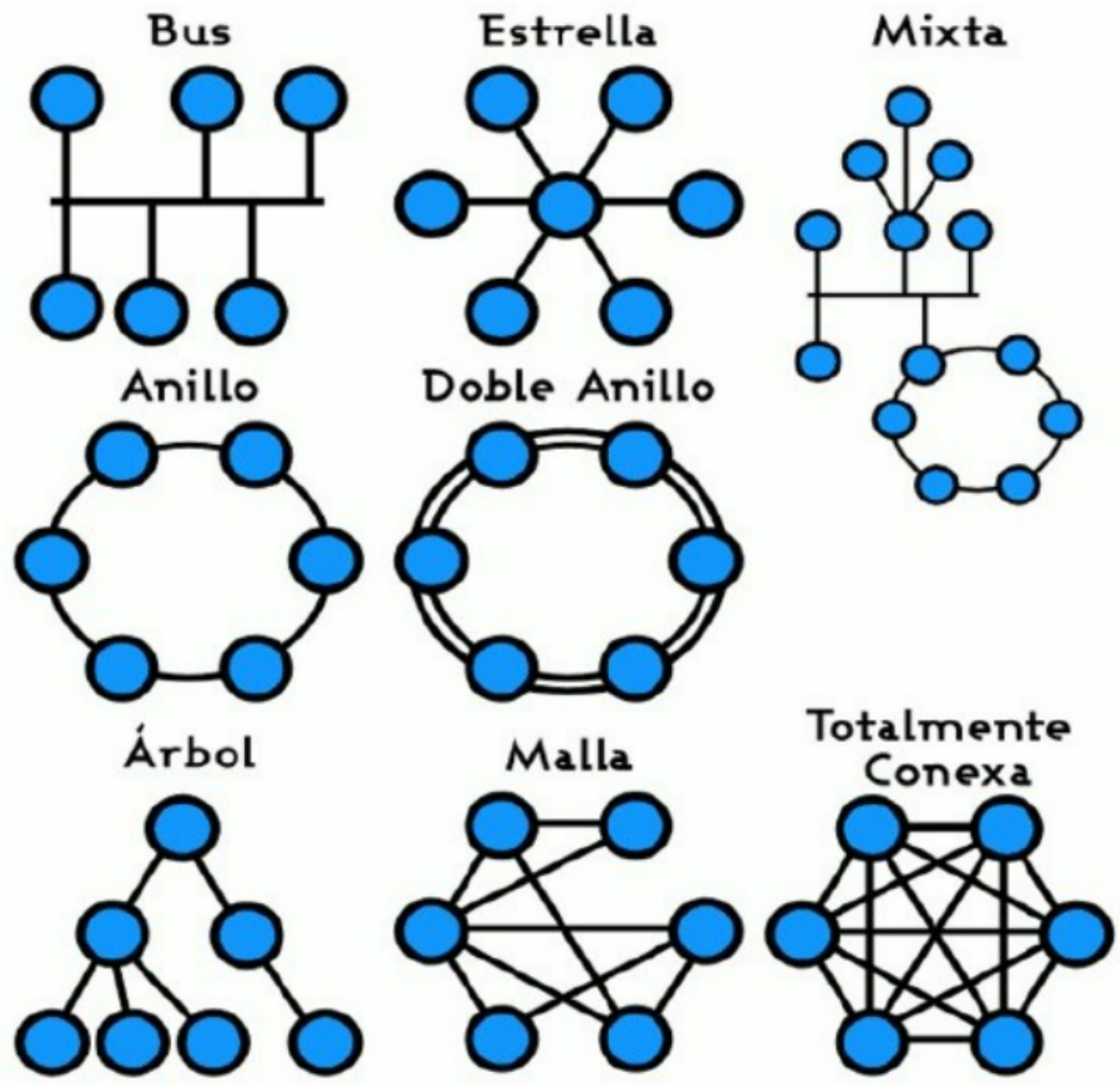
WAN (Wide Area Network, Red de Área Amplia)

Su extensión abarca localidades, provincias e incluso países distintos, usando normalmente medios públicos. El ejemplo más importante es la red Internet, que utiliza, entre otras, la red telefónica mundial.

1.3.4 Según su topología

La topología define la estructura de una red. La definición de topología puede dividirse en dos partes. la topología física, que es la disposición real de los cables (los medios) y la topología lógica, que define la forma en que los hosts (equipos) acceden a los medios.

Topología física



Las topologías físicas que se utilizan comúnmente son de bus, de anillo, en estrella, en estrella extendida, jerárquica y en malla.

La **topología de bus** utiliza un único segmento backbone (cable) al que todos los hosts se conectan de forma directa.

La **topología de anillo** conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.

La **topología en estrella** conecta todos los cables con un punto central de concentración. Por lo general, este punto es un hub o un switch.

La **topología en estrella extendida** se desarrolla a partir de la topología en estrella. Esta topología conecta estrellas individuales conectando los hubs/switches. Esto permite extender la longitud y el tamaño de la red.

La **topología jerárquica** se desarrolla de forma similar a la topología en estrella extendida pero, en lugar de conectar

los hubs/switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.

La **topología en malla** se utiliza cuando no puede existir absolutamente ninguna interrupción en las comunicaciones, por ejemplo, en los sistemas de control de una central nuclear. De modo que, como puede observar en el gráfico, cada host tiene sus propias conexiones con los demás hosts. Esto también se refleja en el diseño de la Internet, que tiene múltiples rutas hacia cualquier ubicación.

Topología lógica

La topología lógica de una red es la forma en que los hosts se comunican a través del medio.

En redes locales, los dos tipos más comunes son:

Topología lógica de bus: existe un medio compartido entre varios hosts y éstos compiten por el uso del medio (Acceso al medio por contienda). Cada host envía sus datos hacia todos los demás hosts de la red. Las estaciones no siguen ningún orden para utilizar la red, el orden es el primero que entra, el primero que se sirve. Esta es la forma en que funciona Ethernet.

Topología lógica de anillo: existe un medio compartido entre varios hosts y éstos deben recibir un testigo (token) para poder transmitir. Esta transmisión controla el acceso al medio mediante la transmisión de un token electrónico a cada host de forma secuencial. Cuando un host recibe el token, eso significa que el host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, pasa el token (testigo) al siguiente host y el proceso se vuelve a repetir.

1.3.5 Según uso del medio o canal

Red punto a punto (Point-To-Point)

Es aquella en la que existe multitud de conexiones entre parejas individuales de máquinas. Este tipo de red requiere, en algunos casos, máquinas intermedias que establezcan rutas para que puedan transmitirse paquetes de datos. Internet funciona de esta forma mediante una serie de nodos conectados en forma de malla denomidados routers o encaminadores.

Red de difusión

Se caracteriza por transmitir datos por un sólo canal de comunicación que comparten todas las máquinas de la red. En este caso, el paquete enviado es recibido por todas las máquinas de la red pero únicamente la destinataria puede procesarlo. Las equipos unidos por un concentrador, o hub, forman redes de este tipo. Muchas redes locales funcionan de esta forma.

1.3.6 Según relación funcional

Arquitectura Cliente-servidor

Consiste básicamente en computadores cliente que realizan peticiones a computadores servidor que dan respuesta (proporcionan un servicio).

Arquitectura Peer-to-peer

También denominada red entre iguales, es aquella red en la que los computadores se comportan como cliente y servidor a la vez.

1.4 Referencias

- Planificación y Administración de Redes. Editorial Ra-ma.
- Redes Locales. Editorial Macmillan.
- Certificaciones CISCO

1.5 Actividades

1. Elabora un resumen, menor de una página, donde expongas la historia de Internet. Indica los momentos más decisivos y la evolución de sus tecnologías asociadas.
2. Busca información acerca del dispositivo denominado hub o concentrador. Indica en que tipo de redes se usa (LAN, MAN, WAN) y la topología física y lógica de la red.
3. Busca información acerca de los dispositivos AUI y MAU. Indica en que tipo de redes se usa (LAN, MAN, WAN) y la topología física y lógica de la red.
4. Busca en Internet las siguientes tipos de redes según su extensión. Indica qué extensión abarca cada una.
   - PAN
   - VLAN
   - WLAN
   - WMAN
   - WWAN
   - CAN
   - HAN
5. Haz un esquema de cada una de las topologías físicas y encuentra una red donde se aplique.
6. Busca información acerca de la topología celular. ¿Qué forma tiene? ¿Dónde se utiliza?

CAPÍTULO 2

NORMALIZACIÓN EN LAS REDES

2.1 Estándares y organismos de normalización

Un estándar puede definir, por ejemplo, el tipo de conector a emplear, las tensiones e intensidades empleadas, el formato de los datos a enviar, etc. En resumen, **un estándar es un conjunto de normas, acuerdos y recomendaciones técnicas que regulan la transmisión de los sistemas de comunicación**. El empleo de estos estándares presenta las siguientes ventajas:

- Los productos de diferentes fabricantes que cumplen los estándares son totalmente compatibles y, por tanto, pueden comunicarse entre ellos sin necesidad de utilizar adaptadores.
- El mercado se amplía, ya que al existir compatibilidad entre los productos de diferentes fabricantes, la oferta de productos será mayor, pudiendo derivar en precios más competitivos. Esto se traduce en una mayor flexibilidad a la hora de elegir y utilizar dispositivos.
- Se asegura la compatibilidad con productos futuros empleando la misma tecnología.
- Se reducen los costes de los productos.
- De esta forma, la estandarización evita que las empresas posean arquitecturas cerradas que derivan en monopolios, favoreciendo la interoperabilidad entre dispositivos de varios fabricantes y la flexibilidad del mercado.

Existen dos tipos de estándares:

- **De facto**: son estándares con gran aceptación en el mercado, establecidos normalmente por grupos de empresas y organizaciones, pero que aún no son oficiales.
- **De iure**: son estándares definidos por organizaciones o grupos oficiales.

Puede ocurrir que una empresa o corporación posea una normativa establecida para el desarrollo de sus productos y servicios, siendo ésta propiedad absoluta de la empresa o corporación. Esta manera de actuar es seguida por muchas empresas con la intención de atar a los clientes a sus productos. A esta normativa con frecuencia se le denomina «estándar propietario», y si alcanza una penetración en el mercado considerable, puede llegar a convertirse en estándar de facto e incluso de iure.

En este sentido, los estándares pueden clasificarse, atendiendo a la propiedad, en dos tipos, **abiertos y cerrados**. Al primer tipo pertenecen los estándares de facto y iure, ya que pueden ser consultados por cualquiera. No obstante,

existen organismos que cobran una cuota por acceder a sus estándares prohibiendo su distribución, aunque en la mayoría de los casos la utilización de este estándar no requiere el pago de un canon. A este tipo de estándares se les denomina estándares de distribución restringida. En el otro extremo se sitúan los estándares cerrados, también denominados propietarios, que representan normas únicamente accesibles para los miembros de la empresa propietaria.

Centrándonos en los estándares abiertos, existen dos tipos de organizaciones que pueden definirlos, los consorcios de fabricantes y los organismos oficiales.

Los **consorcios de fabricantes** están formados por grupos de empresas que cooperan para establecer acuerdos y reglas que permitan obtener la interoperabilidad de sus productos empleando una tecnología determinada. Como ya se mencionó anteriormente, asegurando dicha interoperabilidad, se consigue un aumento del mercado que se traduce en un mayor número de clientes potenciales para sus productos. En este caso, las empresas o personas interesadas pueden unirse al consorcio y participar en los grupos de trabajo que definen los documentos técnicos de la norma. ADSL Forum, ATM Forum, Zigbee Alliance, y PLC forum son ejemplos de consorcios de este tipo.

Por otra parte, los **organismos oficiales** están formados por consultores independientes, miembros de los departamentos o secretarías de estado de diferentes países y otros miembros. ISO, IEEE, y ANSI son ejemplos de organismos oficiales. A continuación describiremos algunos de ellos.

2.1.1 Organismos reguladores en el ámbito internacional

ITU (International Telecommunication Union)

La organización ITU (UIT en castellano, Unión Internacional de Telecomunicaciones) es la organización más importante de las Naciones Unidas en lo que concierne a las tecnologías de la información. Esta organización representa un foco global para los gobiernos y el sector privado en el desarrollo de redes y servicios. ITU coordina el uso del espectro radioeléctrico, promoviendo la cooperación internacional para la asignación de órbitas de satélites, trabajando para mejorar las infraestructuras de comunicación mundiales, estableciendo estándares mundiales para la interconexión de un enorme rango de sistemas de comunicación, y haciendo frente a problemas actuales, como el cambio climático y la seguridad en el ciberespacio. Su sede está en Ginebra (Suiza) y está formada por 191 Estados miembros y más de 700 miembros del Sector y Asociados.

Esta organización está compuesta por tres sectores o comités:

- **ITU-R** (anteriormente conocida como CCIR, Comité Consultivo Internacional de Radiocomunicaciones), que se encarga de promulgar estándares de comunicaciones que emplean el espectro electromagnético.
- **ITU-D** que se encarga de la organización, coordinación técnica y actividades de asistencia.
- **ITU-T** (anteriormente conocida como CCITT, Comité Consultivo Internacional de Telegrafía y Telefonía), que se encarga de desarrollar estándares para la telefonía, la telegrafía, interfaces, redes y otros aspectos de las telecomunicaciones.

ISO (International Organization for Standardization)

La organización internacional para la normalización es una agencia internacional sin ánimo de lucro con sede en Ginebra (Suiza), cuyo objetivo es el desarrollo de normalizaciones que abarcan un amplio abanico de materias. Esta organización ha definido multitud de estándares de diferentes temáticas, que van desde el paso de los tornillos hasta arquitecturas de comunicaciones para la interconexión de sistemas abiertos (**OSI - Open Systems Interconnection**).

ISO está formada por organismos de estandarización de diversos países (**ANSI** en EEUU, **DIN** en Alemania, **AENOR** en España, . . .) y por un grupo de organizaciones observadoras, que no poseen capacidad de voto. A pesar de ser una organización no gubernamental, la mayoría de sus miembros son instituciones gubernamentales. Se fundó en 1946 y actualmente reúne a más de 100 países.

IEEE (Institute of Electrical and Electronic Engineers)

IEEE (leído IE cubo) es la mayor asociación profesional para el avance de la innovación y la excelencia tecnológica en busca del beneficio de la humanidad. IEEE y sus miembros inspiran una comunidad global que innove hacia un mejor mañana a través de sus publicaciones enormemente citadas, conferencias, estándares tecnológicos, y actividades profesionales y educativas. Fue fundada en 1884 y desde entonces desarrolla estándares para las industrias eléctricas y electrónicas. Desde el punto de vista de las redes de datos son muy interesantes los **trabajos del comité 802, que desarrolla estándares de protocolos de comunicaciones para la interfaz física de las conexiones de las redes locales de datos**.

IETF (Internet Engineering Task Force)

Este **Grupo de Trabajo de Ingeniería de Internet**, es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad. Fue creada en EE.UU. en 1986. El IETF es mundialmente conocido por ser la entidad que **regula las propuestas y los estándares de Internet, conocidos como RFC (Request For Comments)**.

Es una institución sin fines de lucro y abierta a la participación de cualquier persona, cuyo objetivo es velar para que la arquitectura de Internet y los protocolos que la conforman funcionen correctamente. Se la considera como la organización con más autoridad para establecer modificaciones de los parámetros técnicos bajo los que funciona la red. El IETF se compone de técnicos y profesionales en el área de redes, tales como investigadores, integradores, diseñadores de red, administradores, vendedores, entre otros.

Dado que la organización abarca varias áreas, se utiliza una metodología de división en grupos de trabajo, cada uno de los cuales trabaja sobre un tema concreto con el objetivo de concentrar los esfuerzos.

2.1.2 Organismos reguladores en Estados Unidos

ANSI (American National Standards Instituto)

El Instituto Americano de Normas Nacionales. Organización sin ánimo de lucro encargada de supervisar el desarrollo de estándares que se aplica en los Estados Unidos de América.

TIA (Telecommunications Industry Association)

La Asociación de la Industria de las Telecomunicaciones Organización formada por representantes de las industrias más importantes del sector de las telecomunicaciones y que ha desarrollado también numerosos estándares a nivel internacional relacionados con el mundo de las redes en colaboración con ANSI y la antigua EIA

2.1.3 Organismos reguladores en Europa

ETSI (European Telecommunications Standardas Institute)

Las siglas ETSI hacen referencia al instituto europeo de estándares de las telecomunicaciones.

ETSI es una organización independiente sin ánimo de lucro que produce estándares aplicables globalmente para las tecnologías de la información y comunicación. Este instituto es reconocido por la Unión Europea como una organización de estándares europeos. Posee 766 organizaciones miembro procedente de 63 países de los cinco continentes.

El ETSI ha tenido gran éxito al estandarizar el sistema de **telefonía móvil GSM**.

Cuerpos de estandarización significativos dependientes del ETSI son 3GPP (para redes UMTS) o TISPAN (para redes fijas y convergencia con Internet).

El ETSI fue creado en 1988.

CEN (Comité Europeo de Normalización)

En francés Comité Européen de Normalisation, es una organización no lucrativa privada cuya misión es fomentar la economía europea en el negocio global, el bienestar de ciudadanos europeos y el medio ambiente proporcionando una infraestructura eficiente a las partes interesadas para el desarrollo, el mantenimiento y la distribución de sistemas estándares coherentes y de especificaciones.

El CEN fue fundado en 1961. Sus veintinueve miembros nacionales trabajan juntos para desarrollar los **estándares europeos (EN)** en varios sectores.

2.1.4 Organismos reguladores en España

AENOR (Asociación Española de Normalización)

Es el organismo nacional de normalización que a través de sus Comités Técnicos de Normalización se encarga de la publicación de las **normas UNE** (**UNE acrónimo de Una Norma Española**) y la adopción de las normas europeas. Está relacionado con organismos europeos como CEN (Comité Europeo de Normalización), CENELEC (Comité Europeo de Normalización Electrotécnica) y ETSI.

2.2 Arquitecturas de comunicaciones

Cuando se diseña una red de ordenadores, es necesario resolver una gran cantidad de problemas que aparecen: ¿hay que compartir un único medio de transmisión?; ¿cómo distinguimos unos ordenadores de otros?; ¿qué tipo de información se va a transmitir?; ¿se manejará información confidencial? Es evidente que una persona no debe enfrentarse directamente a todas estas cuestiones, sino que siempre es preferible tratarlas una a una y de forma aislada.

La arquitectura de una red viene definida por tres características fundamentales, que dependen de la tecnología que se utilice en su construcción:

- **Topología**: la topología de una red es la organización de su cableado, ya que define la configuración básica de la interconexión de estaciones y, en algunos casos, el camino de una transmisión de datos sobre el cable.
- **Método de acceso a la red**: todas las redes que poseen un medio compartido para transmitir la información, necesitan ponerse de acuerdo a la hora de enviar información, ya que no pueden hacerlo a la vez. En este caso, si dos estaciones transmiten a la vez en la misma frecuencia, la señal recogida en los receptores será una mezcla de las dos. Para las redes que no posean un medio compartido, el método de acceso al cable es trivial y no es necesario llevar a cabo ningún control para transmitir.
- **Protocolos de comunicaciones**: son las **reglas y procedimientos utilizados en una red para realizar la comunicación**. Esas reglas tienen en cuenta el método utilizado para corregir errores, establecer una comunicación, etc.

Aunque a primera vista parezca que el diseño de un sistema de comunicación parece simple, cuando se aborda resulta mucho más complejo, ya que es necesario resolver una serie de problemas. Algunos de los problemas más importantes a los que se enfrentan los diseñadores de redes de comunicaciones son:

- **Encaminamiento**: cuando existen diferentes rutas posibles entre el origen y el destino (si la red tiene una topología de malla o irregular), se debe elegir una de ellas (normalmente, la más corta o la que tenga un tráfico menor).

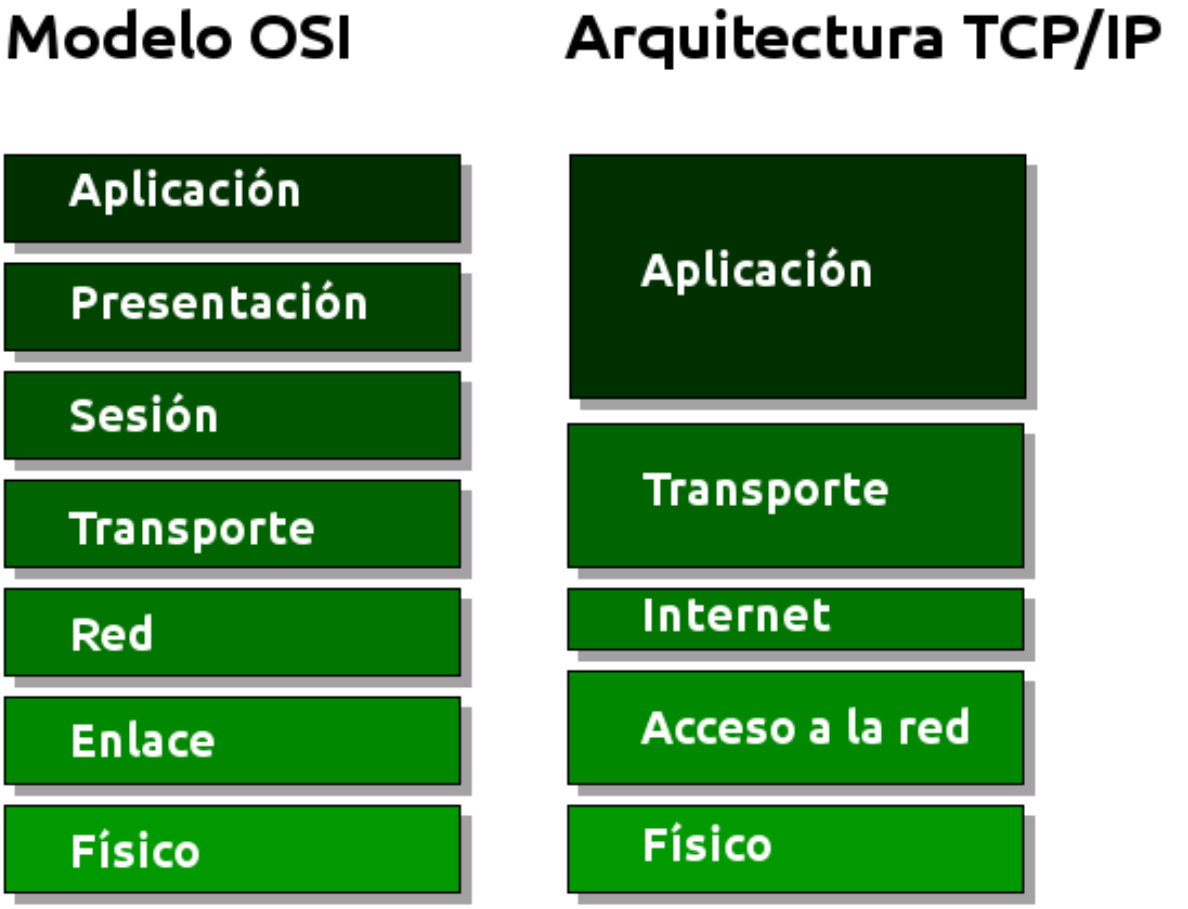
- **Direccionamiento**: puesto que una red normalmente tiene muchos ordenadores conectados, se requiere un mecanismo para que un proceso (programa en ejecución) en una máquina especifique con quién quiere comunicarse. Como consecuencia de tener varios destinos, se necesita alguna forma de direccionamiento que permita determinar un destino específico.
- **Acceso al medio**: en las redes donde existe un medio de comunicación de difusión, debe existir algún mecanismo que controle el orden de transmisión de los interlocutores. De no ser así, todas las transmisiones se interfieren y no es posible llevar a cabo una comunicación en óptimas condiciones. El control de acceso al medio en una red es muy similar a una comunicación mediante walkie-talkie, donde los dos interlocutores deben evitar hablar a la vez o se producirá una colisión. Esta situación es indeseable en las redes que usan un medio compartido, ya que los mensajes se mezclan y resulta imposible interpretarlos.
- **Saturación del receptor**: esta cuestión suele plantearse en todos los niveles de la arquitectura y consiste en que un emisor rápido pueda saturar a un receptor lento. En determinadas condiciones, el proceso en el otro extremo necesita un tiempo para procesar la información que le llega. Si ese tiempo es demasiado grande en comparación con la velocidad con la que le llega la información, será posible que se pierdan datos. Una posible solución a este problema consiste en que el receptor envíe un mensaje al emisor indicándole que está listo para recibir más datos.
- **Mantenimiento del orden**: algunas redes de transmisión de datos desordenan los mensajes que envían, de forma que, si los mensajes se envían en una secuencia determinada, no se asegura que lleguen en esa misma secuencia. Para solucionar esto, el protocolo debe incorporar un mecanismo que le permita volver a ordenar los mensajes en el destino. Este mecanismo puede ser la numeración de los fragmentos, por ejemplo.
- **Control de errores**: todas las redes de comunicación de datos transmiten la información con una pequeña tasa de error, que en ningún caso es nula. Esto se debe a que los medios de transmisión son imperfectos. Tanto emisor como receptor deben ponerse de acuerdo a la hora de establecer qué mecanismos se van a utilizar para detectar y corregir errores, y si se va a notificar al emisor que los mensajes llegan correctamente.
- **Multiplexación**: en determinadas condiciones, la red puede tener tramos en los que existe un único medio de transmisión que, por cuestiones económicas, debe ser compartido por diferentes comunicaciones que no tienen relación entre sí. Así, el protocolo deberá asegurar que todas las comunicaciones que comparten el mismo medio no se interfieran entre sí.

Los primeros ingenieros de comunicaciones se dieron cuenta de que el proceso de comunicación entre computadoras se podía dividir en capas, y de que abordar cada una de estas capas por separado facilitaba enormemente la tarea de diseño de protocolos y estándares para redes.

Al ocuparse cada una de las capas de ciertos aspectos concretos del proceso de comunicación, se libera de tales aspectos al resto de las capas, simplificando así el diseño de la red.

2.2.1 Modelo de referencia OSI y arquitectura TCP/IP

Niveles y equivalencia



Nota: En realidad la arquitectura TCP/IP es una arquitectura de 4 capas:

- 4. Aplicación (capas 5,6 y 7 de OSI)
- 3. Transporte (capa 4 de OSI)
- 2. Internet (capa 3 de OSI)
- 1. Acceso a la red (capas 1 y 2 de OSI)

En estos apuntes usaremos la distribución de capas indicadas en la figura anterior por motivos didácticos al ser la numeración de niveles muy parecida al modelo OSI.

A mediados de los años setenta empezaron a aparecer los primeros estándares para redes. La **ISO** comenzó a elaborar un modelo arquitectónico de referencia al que llamaron modelo de interconexión de sistemas abiertos (OSI: Open Systems Interconnection). Surgió como un intento de unificar esfuerzos, conocimientos y técnicas para elaborar un modelo de arquitectura basado en capas que sirviera como referencia a los distintos fabricantes de la época para

construir redes compatibles entre sí. La publicación final del modelo OSI no llegó hasta 1984 y el modelo obtenido resultó ser demasiado complejo y de difícil implementación.

También durante la década de los setenta, **DARPA** evolucionó su red ARPANET y dio origen a la pila de protocolos TCP/IP, que, por su sencillez y su visión más práctica, empezó a ganar popularidad. TCP/IP acabó convirtiéndose en el estándar de facto de arquitectura en las redes de ordenadores, desbancando así al modelo OSI.

El modelo OSI, sin embargo, continúa siendo de gran importancia, ya que nos permite describir y comprender fácilmente la base conceptual del resto de arquitecturas de red.

2.2.2 Niveles OSI

Físico

La capa física abarca el interfaz físico entre los dispositivos y las reglas por las cuales se pasan los bits de uno en uno. Se encarga de proporcionar el **soporte material para la transmisión de la información**. La capa física tiene cuatro características importantes:

- **Mecánicas**: normalmente, incluye la especificación de un conector que une una o más señales del conductor, llamadas circuitos.
- **Eléctricas**: relaciona la representación de los bits y la tasa de transmisión de datos
- **Funcional**: especifica las funciones realizadas por los circuitos individuales de la interfaz física entre un sistema y el medio de transmisión.
- **De procedimiento**: especifica la secuencia de eventos por los que se intercambia un flujo de bits a través del medio físico.

Enlace de datos

Esta capa intenta hacer el enlace físico seguro y proporciona medios para activar, mantener y desactivar el enlace. El principal servicio proporcionado por la capa de enlace de datos a las capas superiores es el de **detección de errores y control**.

Red

Esta capa proporciona los medios para la **transferencia de información** entre sistemas finales a través de algún tipo de red de comunicación. Libera a las capas superiores de la necesidad de tener conocimiento sobre la transmisión de datos subyacente y las tecnologías de conmutación utilizadas para conectar los sistemas.

Transporte

Esta capa proporciona un mecanismo para intercambiar datos entre sistemas finales. El servicio de transporte orientado a conexión asegura que **los datos se entregan libres de errores, en secuencia y sin pérdidas o duplicados**.

Sesión

Esta capa proporciona los mecanismos para **controlar el diálogo** entre aplicaciones en sistemas finales. En muchos casos, habrá poca o ninguna necesidad de los servicios de la capa de sesión, pero para algunas aplicaciones, estos servicios se utilizan. Por ejemplo, definir la disciplina del diálogo: full-duplex o semi-duplex.

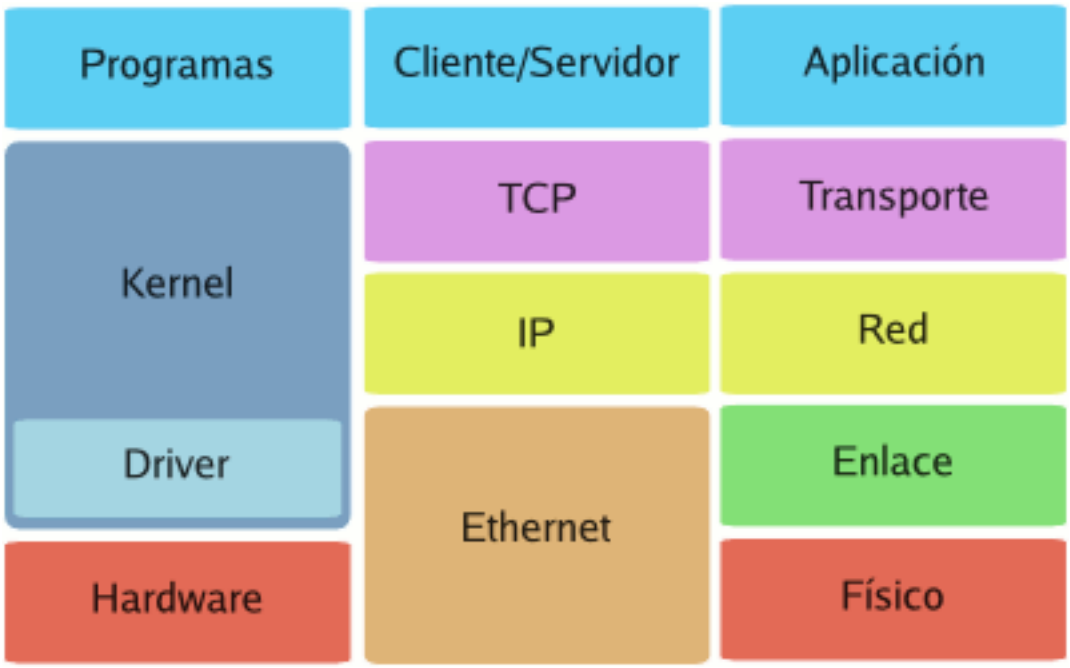
Presentación

Esta capa **define el formato de los datos** que se van a intercambiar entre las aplicaciones y ofrece a los programas de aplicación un conjunto de servicios de transformación de datos. Algunos ejemplos de los servicios específicos que se podrían realizar en esta capa son los de compresión y cifrado de datos.

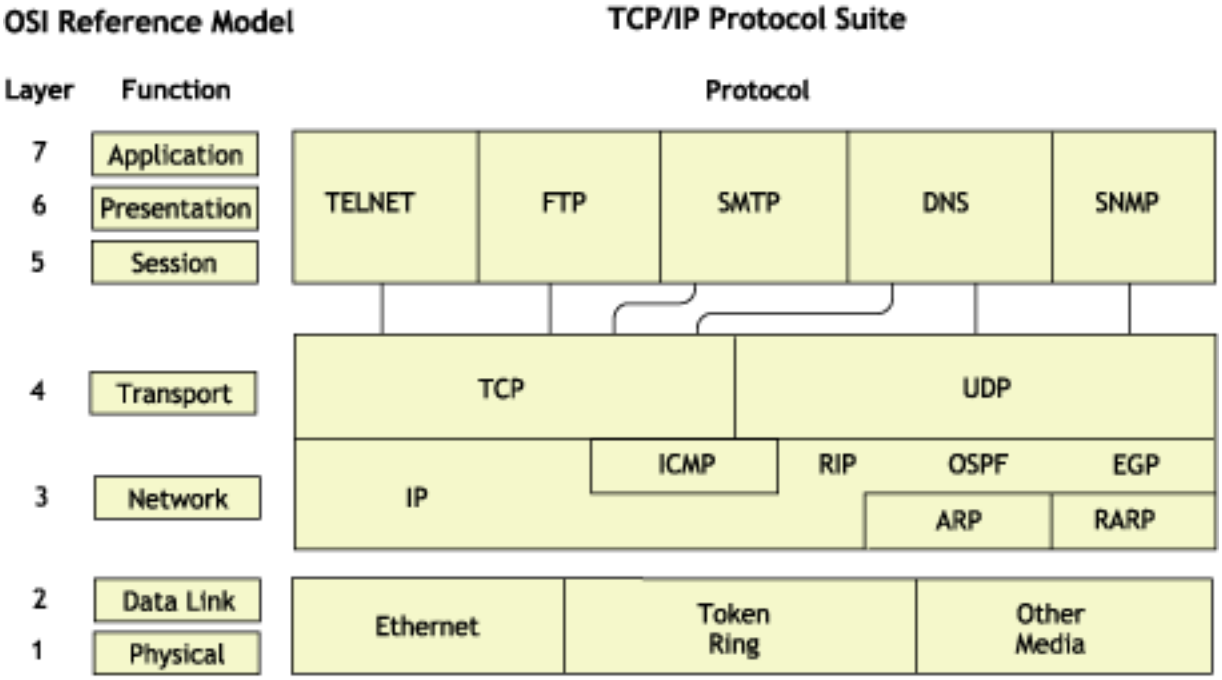
Aplicación

Esta capa proporciona un medio a los programas de aplicación para que accedan al entorno OSI. Se considera que residen en esta capa las aplicaciones de uso general como transferencia de ficheros, correo electrónico y acceso terminal a computadores remotos. **Proporciona un servicio al usuario final**.

2.2.3 Arquitectura TCP/IP



Algunos de los protocolos de TCP/IP



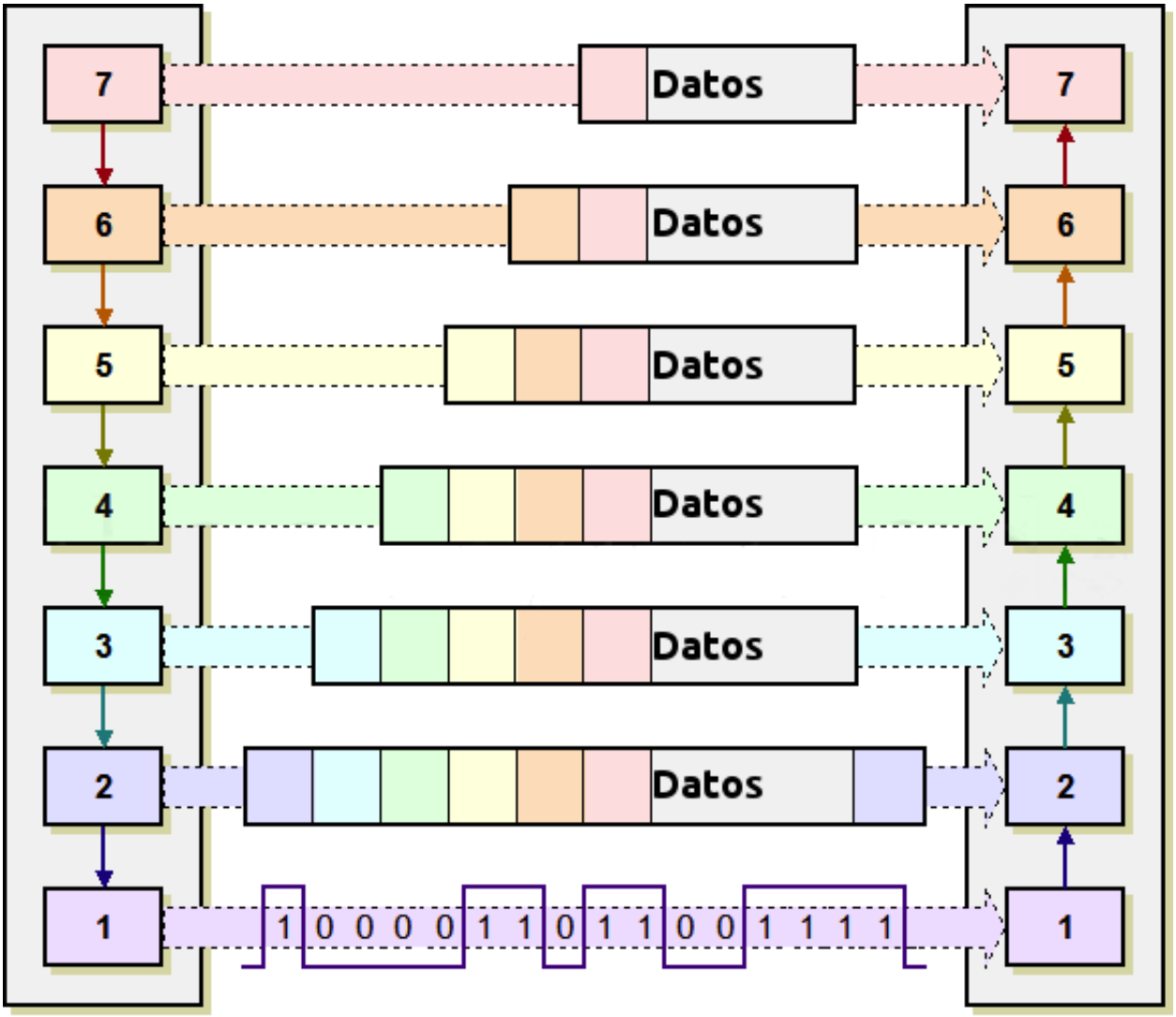
2.2.4 Unidades de Datos de Protocolo (PDU)

PDU es la abreviatura de **Protocol Data Unit** (unidad de datos del protocolo). Su función principal es establecer una comunicación de datos entre capas homologas. Esta forma de establecer conexiones recibe el nombre de comunicación par-a-par.

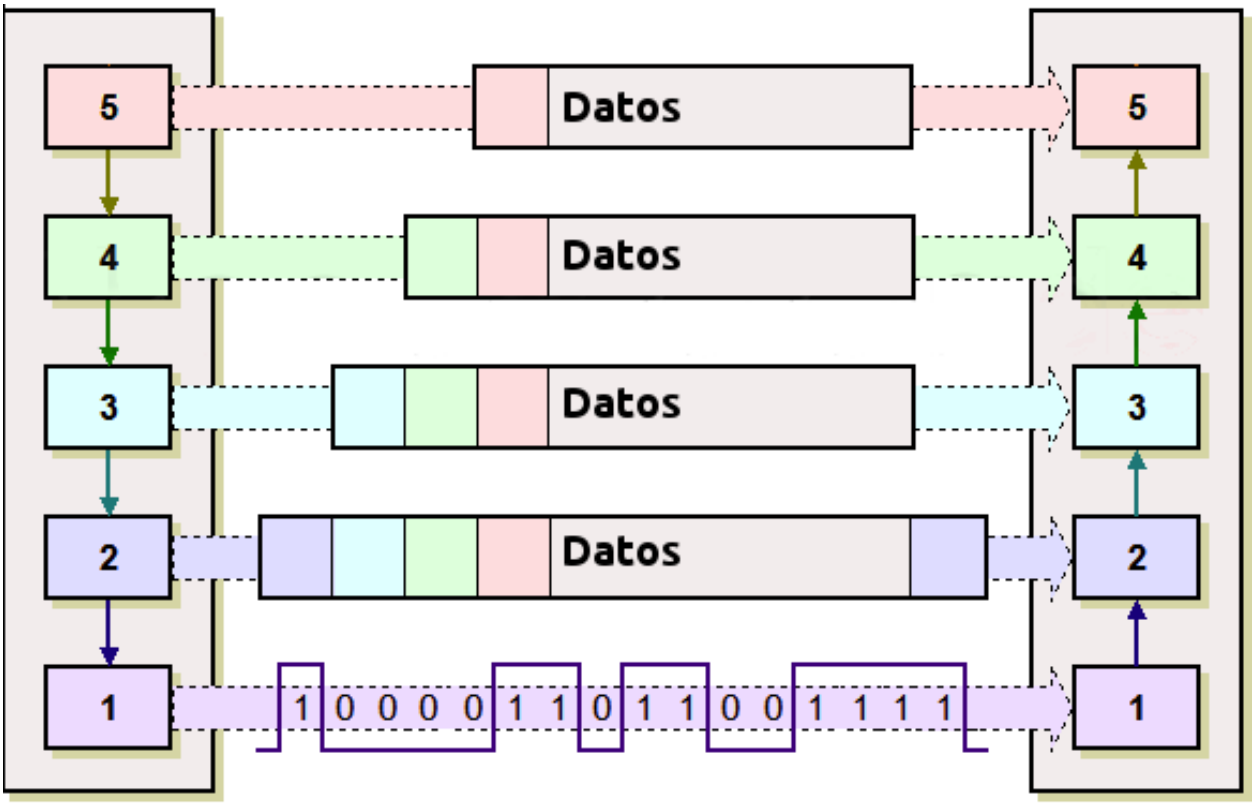
La primera PDU corresponde a los datos que llegan a la capa de aplicación. Aquí se les añade una cabecera y la PDU pasa al nivel siguiente, el de presentación en el modelo OSI, el de transporte en la arquitectura TCP/IP.

A partir de aquí, y en cada uno de los niveles subsiguientes, a la PDU recibida se le añadirá una cabecera y será enviada al nivel inferior, y así sucesivamente hasta llegar al nivel físico, donde los datos serán enviados como bits.

PDUs de OSI


7
6
5
4
3
2
1
Datos
Datos
Datos
Datos
Datos
Datos
1 0 0 0 0 1 1 0 1 1 0 0 1 1 1 1
7
6
5
4
3
2
1

PDUs de TCP/IP



En la arquitectura TCP/IP cada PDU recibe un nombre específico:

- Capa de aplicación: **Datos**
- Capa de transporte: **Segmentos**
- Capa de red: **Datagramas**
- Capa de acceso a la red: **Tramas**
- Capa física: Flujo de bits

Encapsulación

Como se observa en las PDUs, éstas están formadas por una cabecera propia de cada nivel y datos. La PDU (Cabecera y Datos) de una capa superior se trata como datos por la capa inmediatamente inferior. Esta capa inferior le añade su propia cabecera y pasa toda la información a la capa inferior.

El resultado de todo esto es que los datos originales cada vez poseen más cabeceras (una por cada capa) a medida que descienden por la pila.

En el equipo destino se irán quitando las cabeceras en orden inverso a como se añadieron. Cada capa leerá la cabecera que contiene los datos de control destinados a ella.

2.3 Componentes de una red

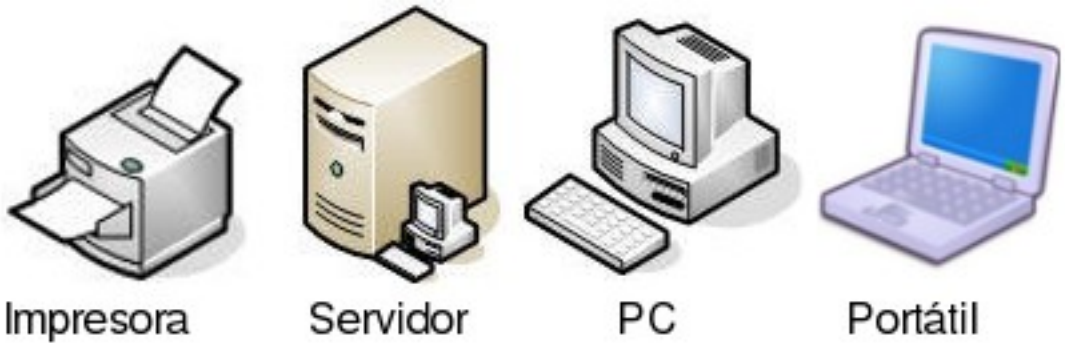
Ahora que tenemos una noción básica sobre el modelo OSI y sobre lo que sucede con los paquetes de datos a medida que recorren las capas del modelo, es hora de que comencemos a echar un vistazo a los dispositivos básicos de redes. A medida que vayamos repasando las capas del modelo de referencia OSI, veremos cuáles son los dispositivos que operan en cada capa según los paquetes de datos vayan viajando a través de ellas desde el origen hacia el destino. Las LAN son redes de datos de alta velocidad y bajo nivel de errores que abarcan un área geográfica relativamente pequeña. Las LAN conectan estaciones de trabajo, dispositivos, terminales y otros dispositivos que se encuentran en un mismo edificio u otras áreas geográficas limitadas.

2.3.1 Nubes

El símbolo de nube indica que existe otra red, por ejemplo Internet. Nos recuerda que existe una manera de conectarse a esa otra red (Internet), pero no suministra todos los detalles de la conexión, ni de la red. Simplemente es útil para realizar los esquemas, si vemos que se conecta a una nube sabemos que esa conexión va a otra red que no es nuestra y que desconocemos, por ejemplo Internet

El propósito de la nube es representar un gran grupo de detalles que no son pertinentes para una situación, o descripción, en un momento determinado. Es importante recordar que solo nos interesa la forma en que las LAN se conectan a las WAN de mayor tamaño, y a Internet (la mayor WAN del mundo), para que cualquier ordenador pueda comunicarse con cualquier otro ordenador, en cualquier lugar y en cualquier momento. Como la nube en realidad no es un dispositivo único, sino un conjunto de dispositivos que operan en todos los niveles del modelo OSI, se clasifica como un dispositivo de las Capas 1-7.

2.3.2 Dispositivos terminales (Capas 1 a 7)



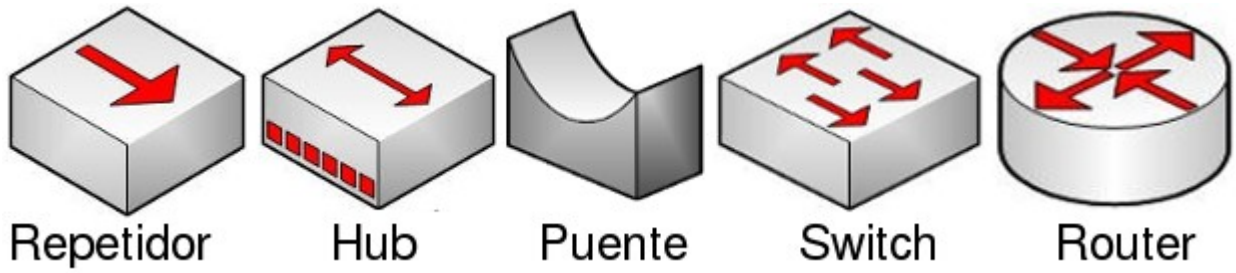
Los dispositivos que se conectan de forma directa a un segmento de red se denominan hosts. Estos hosts incluyen ordenadores, tanto clientes y servidores, impresoras, escáneres y otros dispositivos de usuario. Estos dispositivos suministran a los usuarios conexión a la red, por medio de la cual los usuarios comparten, crean y obtienen información.

Los dispositivos host no forman parte de ninguna capa. Tienen una conexión física con los medios de red ya que tienen una tarjeta de red (NIC) y las demás capas OSI se ejecutan en el software ubicado dentro del host. Esto significa que operan en todas las 7 capas del modelo OSI. Ejecutan todo el proceso de encapsulamiento y desencapsulamiento para

realizar la tarea de enviar mensajes de correo electrónico, imprimir informes, escanear figuras o acceder a las bases de datos.

No existen símbolos estandarizados para los hosts, pero por lo general es bastante fácil detectarlos. Nosotros dibujaremos éstos como si fueran ordenadores:

2.3.3 Dispositivos intermedios (Capas 1, 2 y 3)



Medios (cableado o inalámbrico). Nivel 1

Los símbolos correspondientes a los medios o cableado son distintos según el que realice los esquemas o documentación. Por ejemplo: el símbolo de Ethernet es normalmente una línea recta con líneas perpendiculares que se proyectan desde ella, el símbolo de la red token ring es un círculo con los equipos conectados a él y el símbolo correspondiente a una FDDI (fibra óptica) son dos círculos concéntricos con dispositivos conectados).

Las funciones básicas del cableado, ya sabes, llamado «medios» por ser el medio de conexión, consisten en transportar un flujo de información, en forma de bits y bytes, a través de una LAN. Salvo en el caso de las LAN inalámbricas los medios de red limitan las señales de red a un cable o fibra. Los medios de red se consideran componentes de Capa 1 de las LAN.

Se pueden desarrollar redes informáticas con varios tipos de medios distintos. Cada medio tiene sus ventajas y desventajas. Lo que constituye una ventaja para uno de los medios (costo de la categoría 5) puede ser una desventaja para otro de los medios (costo de la fibra óptica). Algunas de las ventajas y las desventajas son las siguientes:

- Longitud del cable
- Costo
- Facilidad de instalación

El cable coaxial, la fibra óptica o incluso el espacio abierto pueden transportar señales de red, sin embargo, el medio principal que se estudia en esta clase se denomina cable de par trenzado no blindado de categoría 5 (UTP CAT 5) o el categoría 6 (UTP CAT 6).

Repetidores. Nivel 1

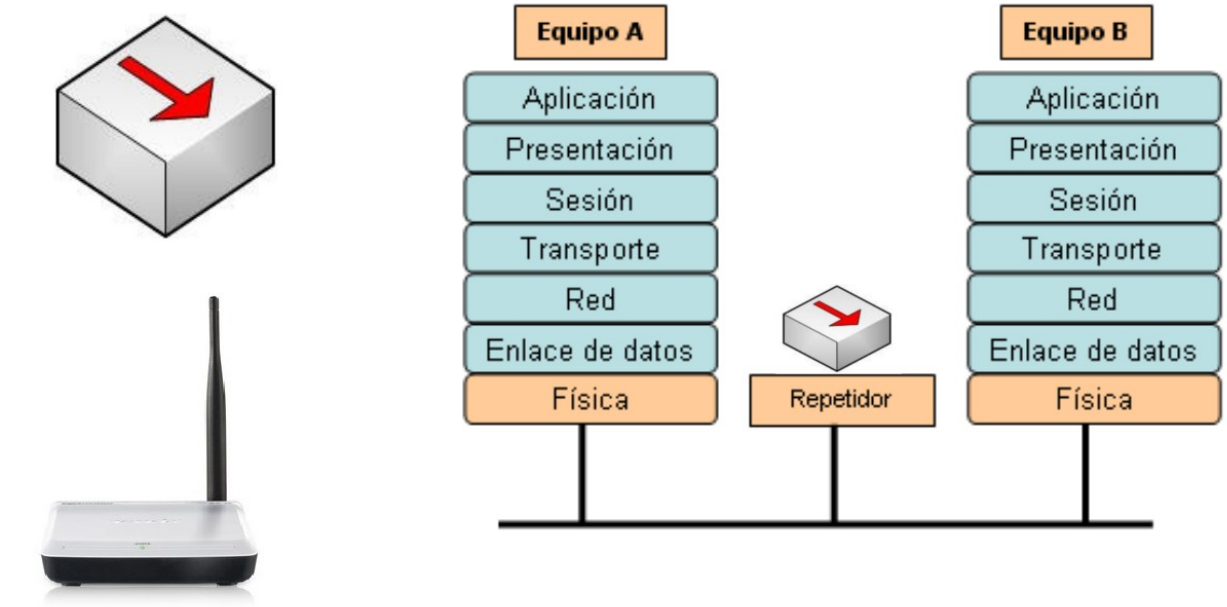
Sabemos pues que según el cableado que utilicemos existen ventajas y desventajas. Por ejemplo una de las desventajas del tipo de cable que utilizamos principalmente (UTP CAT 5) es la longitud del cable. La longitud máxima para el cableado UTP de una red es de 100 metros. Si necesitamos ampliar la red más allá de este límite, debemos añadir un dispositivo a la red llamado repetidor.

El término repetidor se ha utilizado desde la primera época de la comunicación visual, cuando una persona situada en una colina repetía la señal que acababa de recibir de la persona ubicada en la colina de la izquierda, para poder comunicar la señal a la persona que estaba ubicada en la colina de la derecha. También proviene de las comunicaciones telegráficas, telefónicas, por microondas y ópticas, cada una de las cuales usan repetidores para reforzar las señales a

través de grandes distancias, ya que de otro modo en su debido tiempo las señales se desvanecerían gradualmente o se extinguirían.

El propósito de un repetidor es regenerar y retemporizar las señales de red a nivel de los bits para permitir que los bits viajen a mayor distancia a través de los medios. Ten en cuenta la Norma de cuatro repetidores para Ethernet de 10Mbps, también denominada Norma 5-4-3, al extender los segmentos LAN. Esta norma establece que se pueden conectar cinco segmentos de red de extremo a extremo utilizando cuatro repetidores pero sólo tres segmentos pueden tener ordenadores en ellos, curioso ¿no?.

El término repetidor se refiere tradicionalmente a un dispositivo con un solo puerto de «entrada» y un solo puerto de «salida». Sin embargo, en la terminología que se utiliza en la actualidad, el término repetidor multipuerto se utiliza también con frecuencia. En el modelo OSI, los repetidores se clasifican como dispositivos de Capa 1, dado que actúan sólo a nivel de los bits y no tienen en cuenta ningún otro tipo de información. El símbolo para los repetidores no está estandarizado, así que nosotros utilizaremos este:



Repetidor (nivel 1)

Concentradores o hubs. Nivel 1

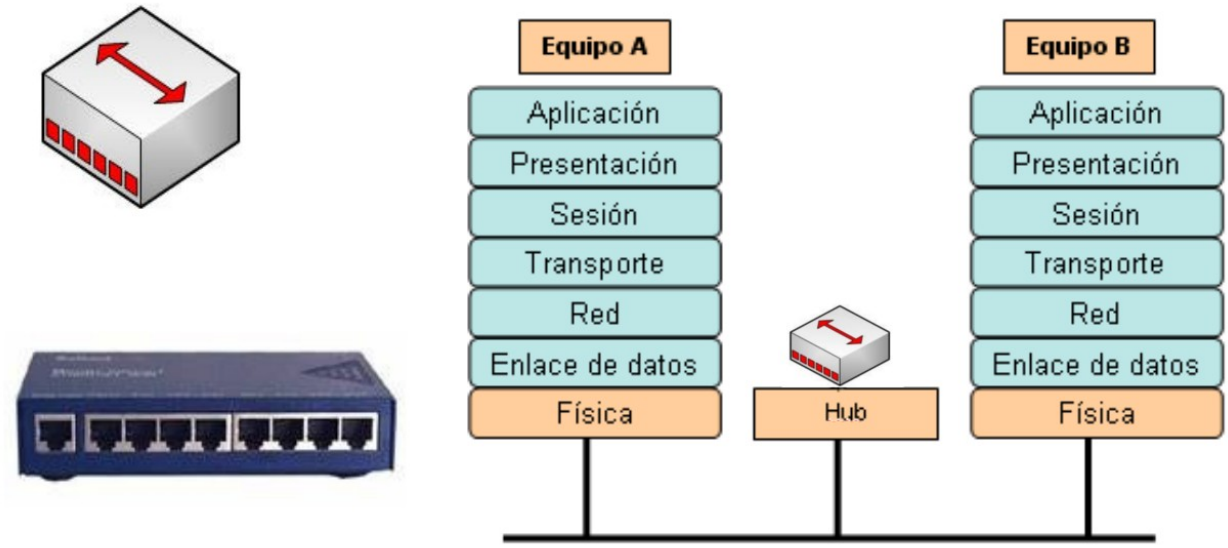
El propósito de un hub es regenerar y retemporizar las señales de red. Esto se realiza a nivel de los bits para un gran número de equipos (por ej., 4, 8 o incluso 24) utilizando un proceso denominado concentración. Como ves es prácticamente la misma definición que la del repetidor, pues si, a los hub también se les llama **repetidor multipuerto**. La diferencia es la cantidad de cables que se conectan al dispositivo, que en este caso admiten varios ordenadores conectados en este hub.

Los hubs se utilizan por dos razones: para crear un punto de conexión central para los ordenadores y para aumentar la fiabilidad de la red. La fiabilidad de la red se ve aumentada al permitir que cualquier cable falle sin provocar una interrupción en toda la red. Esta es la diferencia con la topología de bus, en la que, si un cable fallaba, se interrumpía el funcionamiento de toda la red. Los hubs se consideran dispositivos de Capa 1 dado que sólo regeneran la señal y la envían por medio de un broadcast (ya lo veremos pero consiste en que mandan la información a todos los demás equipos) a todos los puertos.

Hay una pequeña clasificación de los hubs que son los inteligentes y no inteligentes. Los hubs inteligentes tienen puertos de consola, lo que significa que se pueden programar para administrar el tráfico de red. Los hubs no inteligentes

simplemente toman una señal de red de entrada entrante y la repiten hacia cada uno de los puertos sin la capacidad de realizar ninguna administración.

El símbolo correspondiente al hub no está estandarizado pero utilizaremos este.



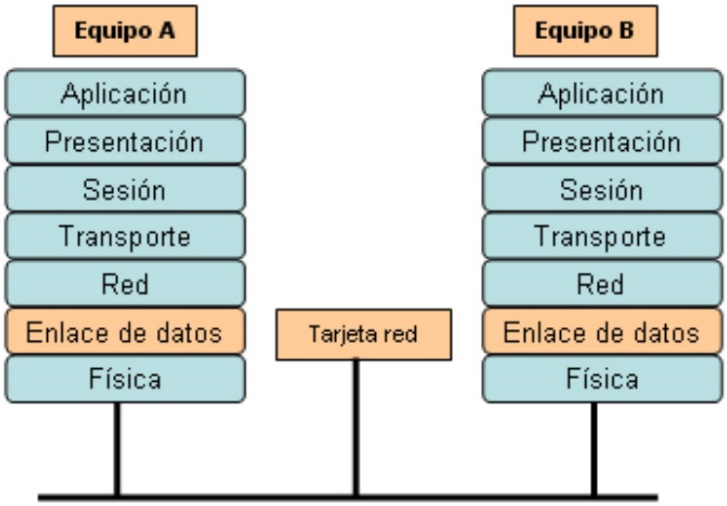
Hub o concentrador (nivel 1)

Tarjeta de red o NIC. Nivel 2

Hasta este momento, en este capítulo nos hemos referido a dispositivos y conceptos de la capa uno. A partir de la tarjeta de interfaz de red, nos trasladamos a la capa dos: la capa de enlace de datos del modelo OSI. En términos de aspecto, una tarjeta de interfaz de red (tarjeta NIC o NIC) es un pequeño circuito impreso que se coloca en un slot de expansión de un bus de la (placa madre) del ordenador, aunque ahora ya casi todos los ordenadores la incorporan de fábrica y no hay que añadirla. También se denomina adaptador de red.

Las NIC se consideran dispositivos de Capa 2, cada tarjeta de red (NIC) lleva un nombre codificado único, denominado dirección de Control de acceso al medio (MAC o MAC Address) y es único en el mundo. Si, como lo lees, cada fabricante tiene asignada una numeración y a cada tarjeta de red le pone esa dirección física única, es como su DNI y nunca pueden existir dos tarjetas de red con ese mismo número interno. Esta dirección es muy importante ya que identifica perfectamente y de forma única al ordenador origen y al destino.

Las tarjetas de red no tienen ningún símbolo estandarizado. Se da a entender que siempre que haya dispositivos de red conectado a la de red, existe alguna clase de NIC o un dispositivo similar aunque por lo general no aparezcan. Siempre que haya un punto en una topología, significa que hay una NIC o una interfaz (puerto), que actúa por lo menos como parte de una NIC.



Tarjeta de red (nivel 2)

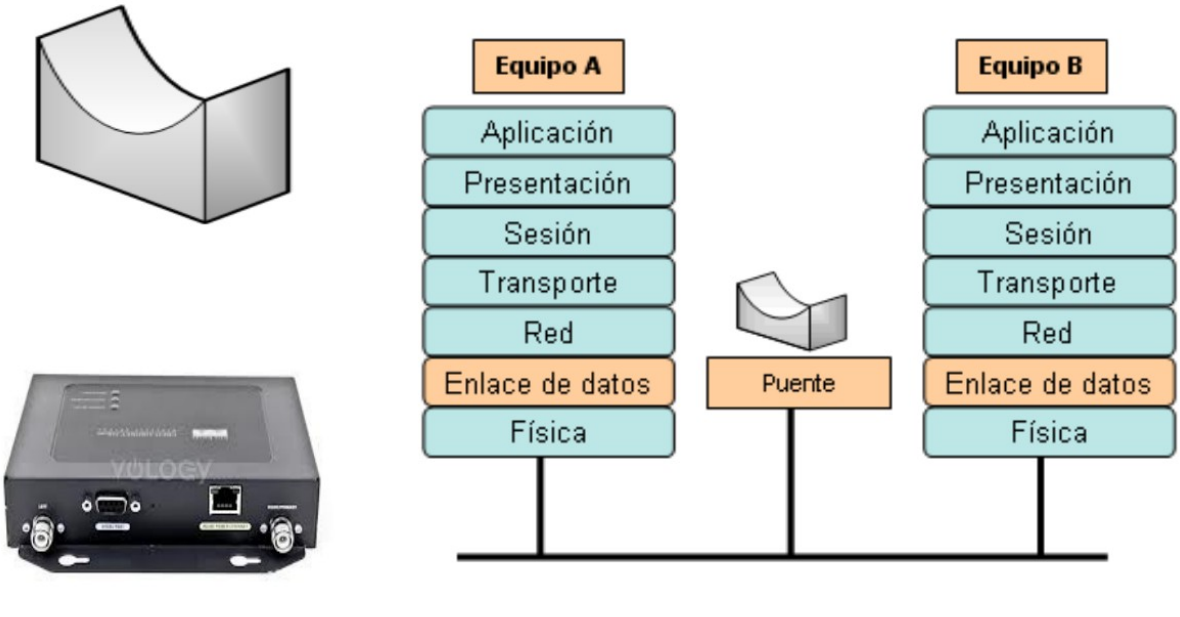
Puentes. Nivel 2

Un puente es un dispositivo de capa 2 diseñado para conectar dos segmentos LAN. El propósito de un puente es filtrar el tráfico de una LAN, para que el tráfico local siga siendo local, pero permitiendo la conectividad a otras partes (segmentos) de la LAN para enviar el tráfico dirigido a esas otras partes.

¿Pero que es un segmento? Es una definición muy variable, nosotros vamos a considerarlo como dos partes distintas de la red. Por ejemplo la red del piso 1 y la red del piso 2 que están conectadas. También podemos ampliarlo, por ejemplo una pequeña empresa que tiene dos oficinas en dos edificios y están conectadas entre si, podemos llamar también a cada una de esas partes segmento.

Vale pero ¿cómo puede detectar el puente cuál es el tráfico de un segmento y cuál no lo es? La respuesta es la misma que podría dar el servicio de correos cuando se le pregunta cómo sabe cuál es el correo local: verifica la dirección local. Cada dispositivo de networking tiene una dirección MAC exclusiva en la tarjeta de red, el puente rastrea cuáles son las direcciones MAC que están ubicadas a cada lado del puente y toma sus decisiones basándose en esta lista de direcciones MAC.

Si el tráfico está entre dos ordenadores del piso 1 el puente decide que no debe mandar ese tráfico al piso 2 porque sabe por las direcciones MAC que el destino está en el mismo piso. Lo mismo para el caso de los dos edificios: el puente conecta los dos segmentos, cuando un ordenador pide información a otro el puente sabe que equipo están conectados en cada lado y sabe si debe mandar el tráfico al otro lado. Tradicionalmente, el término puente se refiere a un dispositivo con dos puertos.



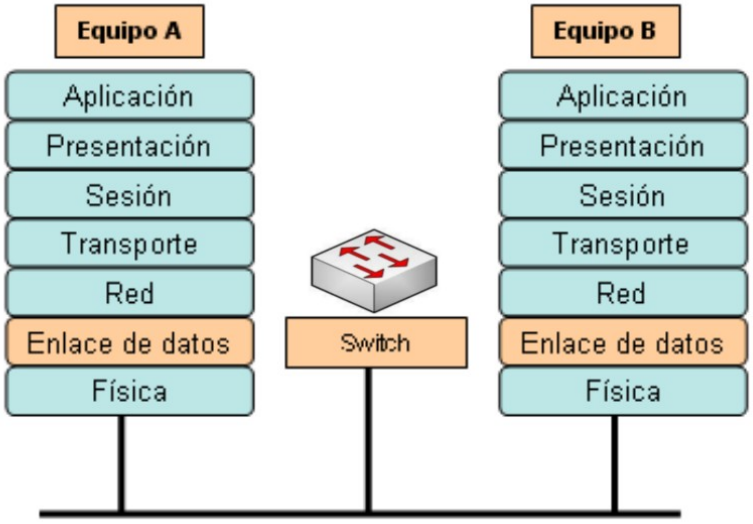
Puente (nivel 2)

Conmutadores o switches. Nivel 2

Un switch, al igual que un puente, es un dispositivo de capa 2. De hecho, el switch se denomina **puente multipuerto**, igual que antes cuando llamábamos al hub «repetidor multipuerto». La diferencia entre el hub y el switch es que los switches toman decisiones basándose en las direcciones MAC y los hubs no toman ninguna decisión. Como los switches son capaces de tomar decisiones, hacen que la LAN sea mucho más eficiente. Los switches hacen esto enviando los datos sólo hacia el puerto al que está conectado el host destino apropiado. Por el contrario, el hub envía datos desde todos los puertos, de modo que todos los hosts deban ver y procesar (aceptar o rechazar) todos los datos.

Como son mucho mejores y eficiente ten en cuenta siempre poner switches en tu red y no hubs, primera recomendación importante. Segunda recomendación: seguramente te parecerá una tontería y obviedad que te diga que si un coche es de buena marca es mejor que uno de marca mala: evidente. Pues aquí pasa lo mismo: hay marcas buenas y marcas malas y la diferencia va a estar evidentemente en las prestaciones y en las posibilidades de configuración. Así que segunda recomendación: invierte un poco de dinero en comprarlo de marca buena: son equipos para toda la vida y considéralo una inversión y no un gasto.

En el gráfico se indica el símbolo que corresponde al switch. Las flechas de la parte superior representan las rutas individuales que pueden tomar los datos en un switch, a diferencia del hub, donde los datos fluyen por todas las rutas



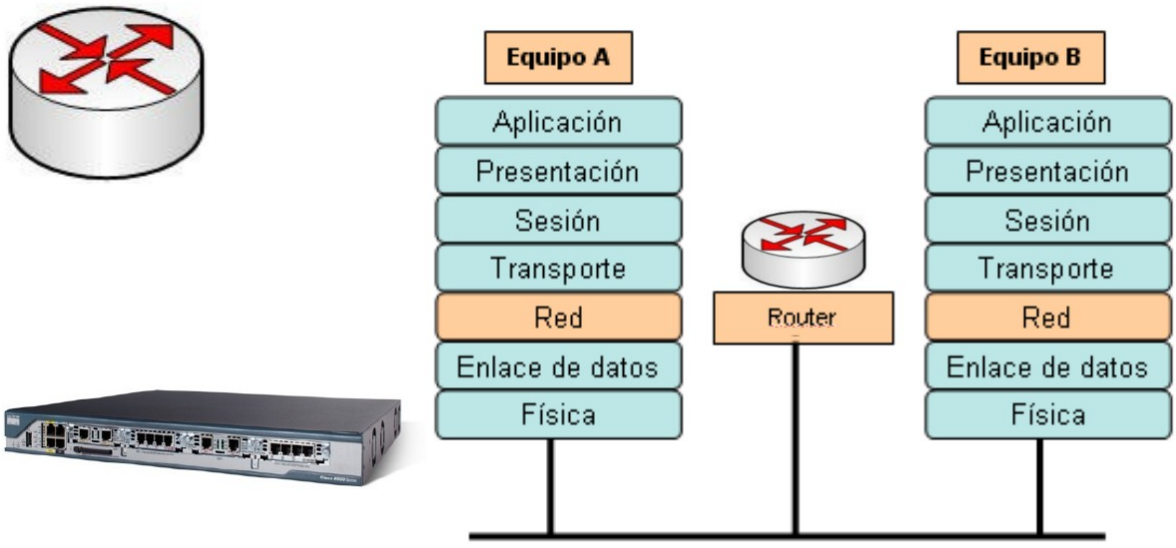
Conmutador o switch (nivel 2)

Encaminadores o routers. Nivel 3

El router es el primer dispositivo con que trabajaremos que pertenece a la capa de red del modelo OSI, o sea la Capa 3. Al trabajar en la Capa 3 el router puede tomar decisiones basadas en grupos de direcciones de red (la famosas direcciones IP) en contraposición con las direcciones MAC de Capa 2 individuales. Los routers también pueden conectar distintas tecnologías de Capa 2, como por ejemplo Ethernet, Token-ring y FDDI (fibra óptica). Sin embargo, dada su aptitud para enrutar paquetes basándose en la información de Capa 3, los routers se han transformado en el núcleo de Internet, ejecutando el protocolo IP.

El propósito de un router es examinar los paquetes entrantes (datos de capa 3), elegir cuál es la mejor ruta para ellos a través de la red y luego enviarlos hacia el puerto de salida adecuado. Los routers son los dispositivos de regulación de tráfico más importantes en las redes grandes. Permiten que prácticamente cualquier tipo de ordenador se pueda comunicar con otro en cualquier parte del mundo.

El símbolo correspondiente al router (observa las flechas que apuntan hacia adentro y hacia fuera) sugiere cuáles son sus dos propósitos principales: la selección de ruta y la transmisión de paquetes hacia la mejor ruta.



Encaminador o router (nivel 3)

2.4 Uso del medio en redes

La interconexión de los distintos nodos que forman una red puede realizarse de dos formas: **por conmutación o por difusión**.

2.4.1 Conmutación

Consisten en un conjunto de nodos interconectados entre sí, a través de medios de transmisión (cables), formando la mayoría de las veces una topología mallada o estrella, donde la información se transfiere encaminándola del nodo de origen al nodo destino mediante conmutación entre nodos intermedios.

Es típica de las WAN. Existe una línea dedicada para cada dos nodos. La conmutación a su vez puede ser de circuitos o de paquetes.

Conmutación de circuitos

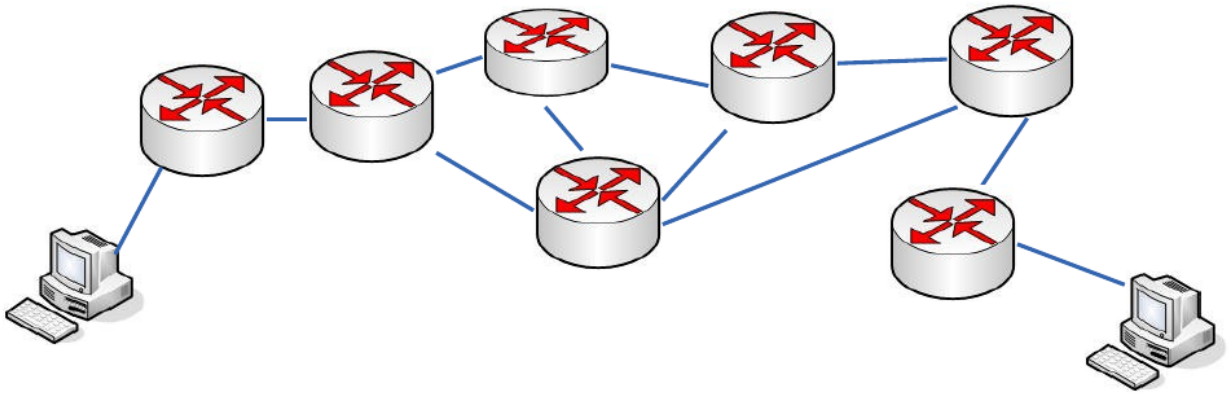
Se establece un único camino entre el origen y el destino para toda la comunicación.

Cuando un emisor quiere enviar un mensaje a un receptor a través de una red de conmutación de circuitos, lo primero que debe hacerse es el **establecimiento** del canal, es decir la conexión entre emisor y receptor, que se hace eligiendo un camino concreto de entre todos los posibles que existen. La ruta que sigue la información se establece al inicio de la comunicación y **se mantiene durante todo el proceso que dure la comunicación**, aunque existan algunos tramos de esa ruta que se comparten con otras rutas diferentes. Al finalizar la transmisión se produce la **liberación** del canal. La **red telefónica clásica** es un ejemplo de conmutación de circuitos.

Conmutación de paquetes

Se trata del procedimiento mediante el cual, cuando un nodo quiere enviar un mensaje a otro, lo divide en paquetes. Cada paquete es enviado por el medio con información de cabecera. En cada nodo intermedio por el que pasa el paquete se detiene el tiempo necesario para procesarlo y decidir el siguiente nodo al cual enviarlo. Así sucesivamente hasta el destino. Los paquetes pueden perderse o llegar en distinto orden.

Los distintos paquetes de un mismo mensaje pueden seguir caminos distintos hasta su destino. **Internet** es un ejemplo de conmutación de paquetes.

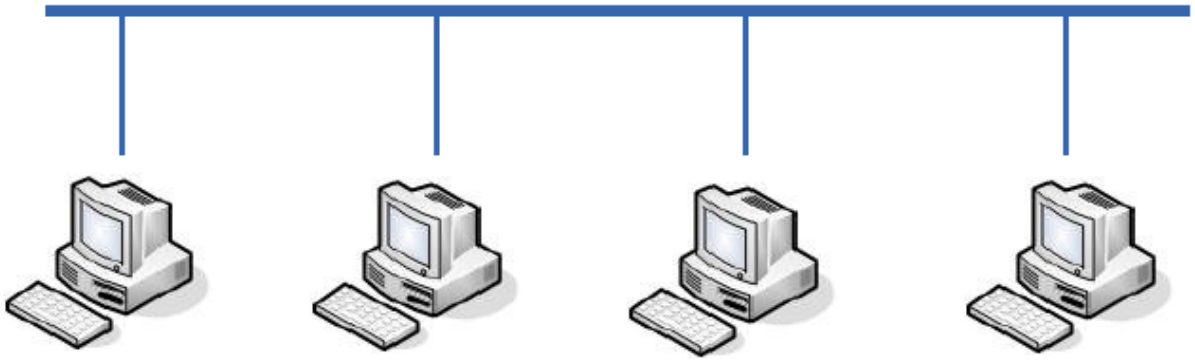


Ejemplo de red conmutada, cuyos equipos finales son ordenadores personales y los equipos intermedios son routers.

2.4.2 Difusión

En medio compartido el emisor envía a todos los nodos la información. El nodo receptor sabe que es para él y la recoge. Los otros nodos la dejan pasar. Las topologías que utilizan este tipo de redes son: bus, anillo y las basadas en ondas de radio.

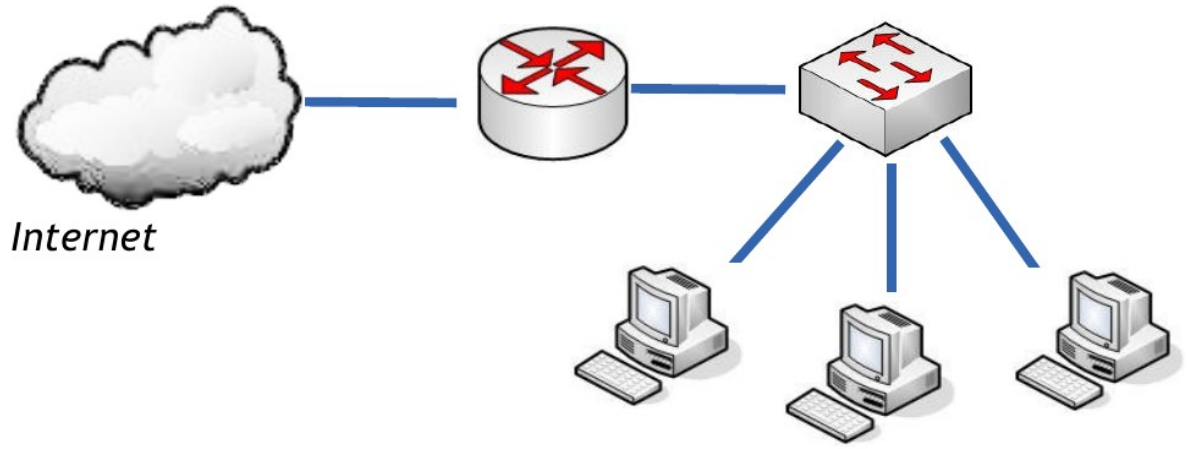
En este tipo de redes no existen nodos intermedios de conmutación. Todos los nodos comparten un medio de transmisión común, por el que la información transmitida por un nodo es conocida por todos los demás. En definitiva, es el destinatario el encargado de seleccionar y captar la información. Este uso del medio es propio de algunas **intranets** y de comunicaciones inalámbricas omnidireccionales.



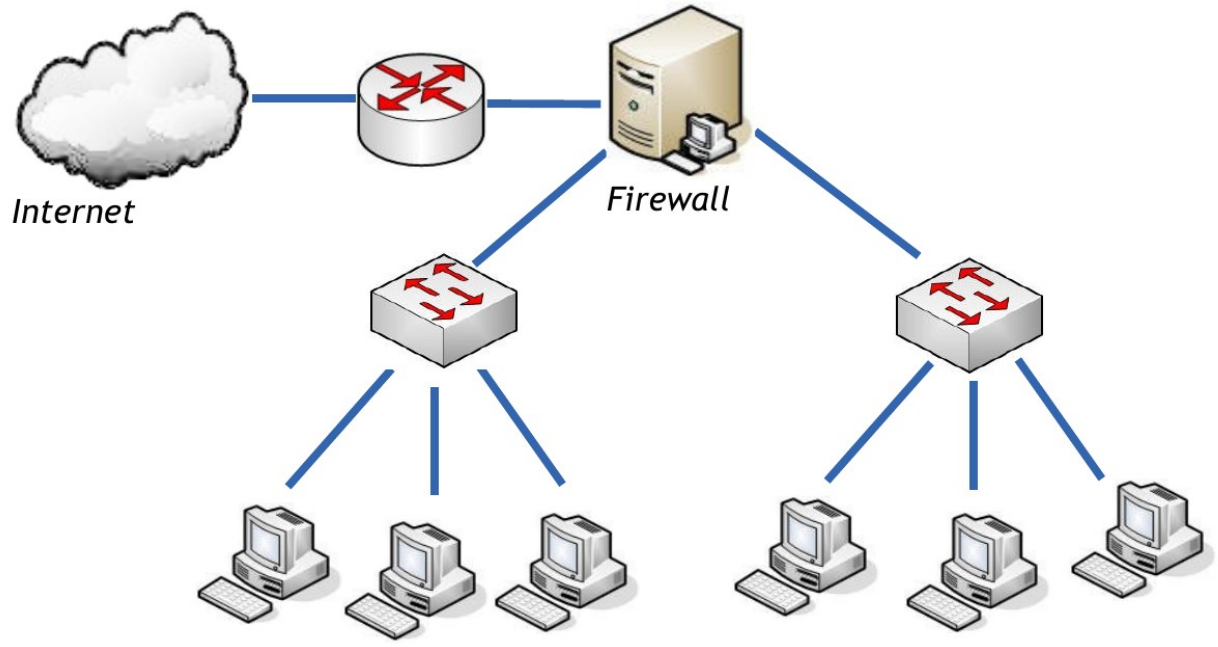
Ejemplo de red de difusión, cuyos equipos finales son ordenadores personales, el medio es un bus compartido y no existen nodos de conmutación.

2.5 Esquemas LAN

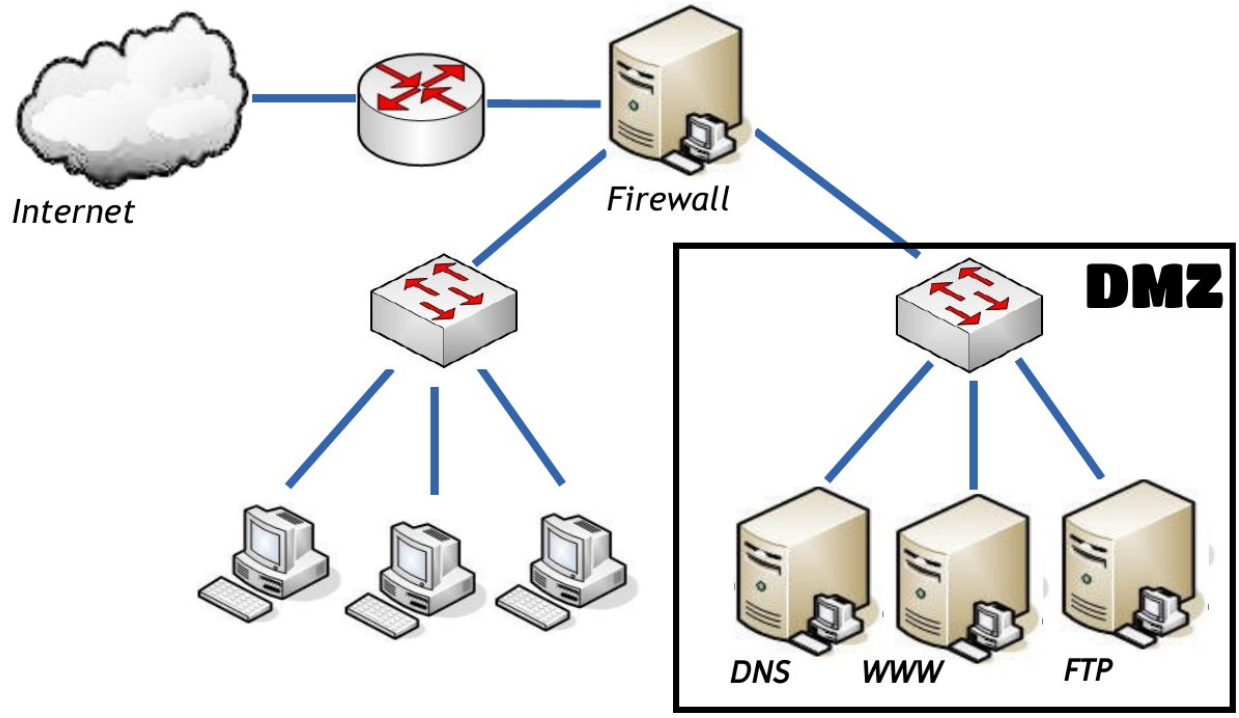
2.5.1 Red local simple



2.5.2 Red local organizada en 2 zonas



2.5.3 Red local con zona de usuarios y Zona DesMilitarizada



Una **DMZ** (del inglés Demilitarized zone) o **Zona DesMilitarizada**. En seguridad informática, una zona desmilitarizada (DMZ) o **red perimetral** es una red local (una subred) que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa – los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de e-mail, Web y DNS.

Las conexiones que se realizan desde la red externa hacia la DMZ se controlan generalmente utilizando port address translation (PAT).

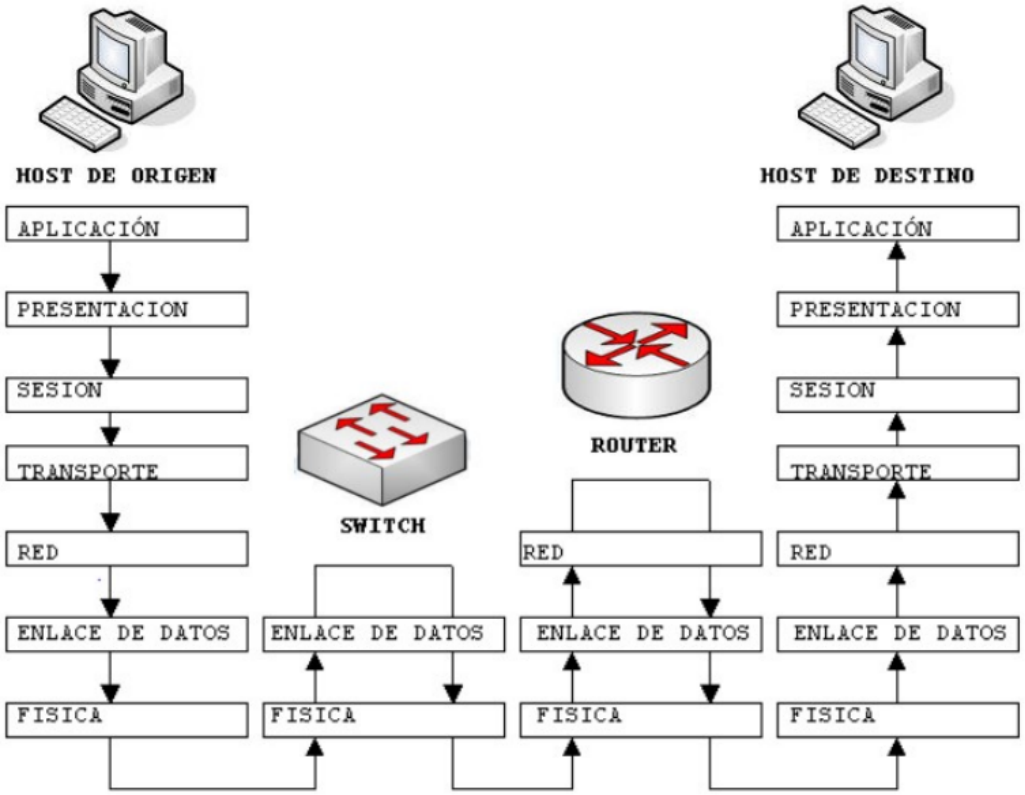
2.6 Referencias

- Planificación y Administración de Redes. Editorial Ra-ma.
- Redes Locales. Editorial Macmillan.

2.7 Actividades

1. Busca información acerca de las normas IEEE 802.3 y 802.11. Haz un breve resumen.
2. Busca información acerca de las normas TIA 568A y TIA 568B. Haz un breve resumen.

3. ¿En qué RFCs se hallan especificados los protocolos TCP e IP?. ¿Qué organismo los pública? ¿Se pueden obtener de forma gratuita?
4. Define protocolo. Nombra 3 protocolos de la capa de aplicación de TCP/IP.
5. Explica los siguientes términos:
   - Direccionamiento
   - Encaminamiento
   - Control de errores
   - Acceso al medio
   - Multiplexación
6. Realiza un esquema comparativo de las capas OSI y TCP/IP.
7. ¿Qué es una PDU? ¿Cómo se denominan en la arquitectura TCP/IP?
8. ¿Qué se entiende por encapsulación de los datos? ¿Y desencapsulación? ¿Cuál se produce cuando bajamos por la pila de protocolos y cuál cuando subimos?
9. Arquitecturas obsoletas. Haz un esquema de la arquitectura SNA. ¿Qué empresa la desarrolló?
10. Arquitecturas obsoletas. Haz un esquema de la arquitectura DECnet. ¿Qué empresa la desarrolló?
11. Arquitecturas obsoletas. Haz un esquema de la arquitectura SPX/IPX. ¿Qué empresa la desarrolló?
12. Arquitecturas obsoletas. Haz un esquema de la arquitectura X.25. ¿Qué organismo la desarrolló?
13. ¿Cómo se interpreta la siguiente imagen?



14. ¿Qué dispositivos trabajan en la capa 1 o física?
15. ¿Qué dispositivos trabajan en la capa 2 o de enlace?
16. ¿Qué dispositivos trabajan en la capa 3 o de red?
17. ¿En qué capa trabajo un host final?
18. ¿Qué diferencia existe entre la conmutación de circuitos y la conmutación de paquetes? Pon un ejemplo de cada una.
19. Nombra los dispositivos por los que pasa la información que un usuario envía desde una red local hacia Internet.
20. ¿Qué es una DMZ? ¿Cuál es su utilidad?

CAPÍTULO 3

LA CAPA FÍSICA

3.1 Concepto de capa física

La capa física se encarga de definir todos los aspectos relacionados con los elementos físicos de conexión de los dispositivos a la red, así como de establecer los procedimientos para transmitir la información sobre la serial física empleada. En este sentido, puede decirse que la capa física es la encargada de definir cuatro tipos de características de los elementos de interconexión:

- **Mecánicas**: se refiere a las características físicas del elemento de conexión con la red, es decir, a las propiedades de la interfaz física con el medio de comunicación. Por ejemplo, las dimensiones y forma del conector, el número de cables usados en la conexión, el número de pines del conector. el tamaño del cable, el tipo de antena, etc.
- **Eléctricas**: especifica las características eléctricas empleadas, por ejemplo, la tensión usada, velocidad de transmisión, intensidad en los pines. etc.
- **Funcionales**: define las funciones de cada uno de los circuitos del elemento de interconexión a la red, por ejemplo, pin X para transmitir, pin Y para recibir, etc.
- **De procedimiento**: establece los pasos a realizar para transmitir información a través del medio físico.

Esta capa ofrece a los niveles superiores un servicio de transmisión de datos, es decir, proporciona un mecanismo para enviar y recibir bits empleando el canal de comunicación. Es la capa de más bajo nivel.

Algunos protocolos y estándares que regulan aspectos de la capa física

- ANSI/TIA/EIA 568 A y B.
- ISO/IEC 11801.
- Parte de Ethernet y del estándar IEEE 802.3.

La transmisión de datos entre un emisor y un receptor siempre se realiza a través de un medio de transmisión. Los medios de transmisión se pueden clasificar como **guiados y no guiados**. En ambos casos, la comunicación se realiza **usando ondas electromagnéticas**. En los medios guiados, por ejemplo en pares trenzados, en cables coaxiales y en fibras ópticas, las ondas se transmiten confinándolas a lo largo de un camino físico. Por el contrario, los medios no guiados, también denominados inalámbricos, proporcionan un medio para transmitir las ondas electromagnéticas sin confinarlas, como por ejemplo en la propagación a través del aire, el mar o el vacío.

El término **enlace directo** se usa para designar un camino de transmisión entre dos dispositivos en el que la señal se propague directamente del emisor al receptor sin ningún otro dispositivo intermedio que no sea un **amplificador o repetidor**. Estos últimos se usan para incrementar la energía de la señal. Obsérvese que este término se puede aplicar tanto a medios guiados como no guiados.

Un medio de transmisión guiado es **punto a punto** si proporciona un enlace directo entre dos dispositivos que comparten el medio, no existiendo ningún otro dispositivo conectado. En una configuración guiada **multipunto**, el mismo medio es compartido por más de dos dispositivos.

Un medio de transmisión puede ser **simplex, half-duplex o full-duplex**. En la transmisión simplex, las señales se transmiten sólo en una única dirección; siendo una estación la emisora y otra la receptora. En half-duplex, ambas estaciones pueden transmitir, pero no simultáneamente. En fullduplex, ambas estaciones pueden igualmente transmitir y recibir, pero ahora simultáneamente. En este último caso, el medio transporta señales en ambos sentidos al mismo tiempo.

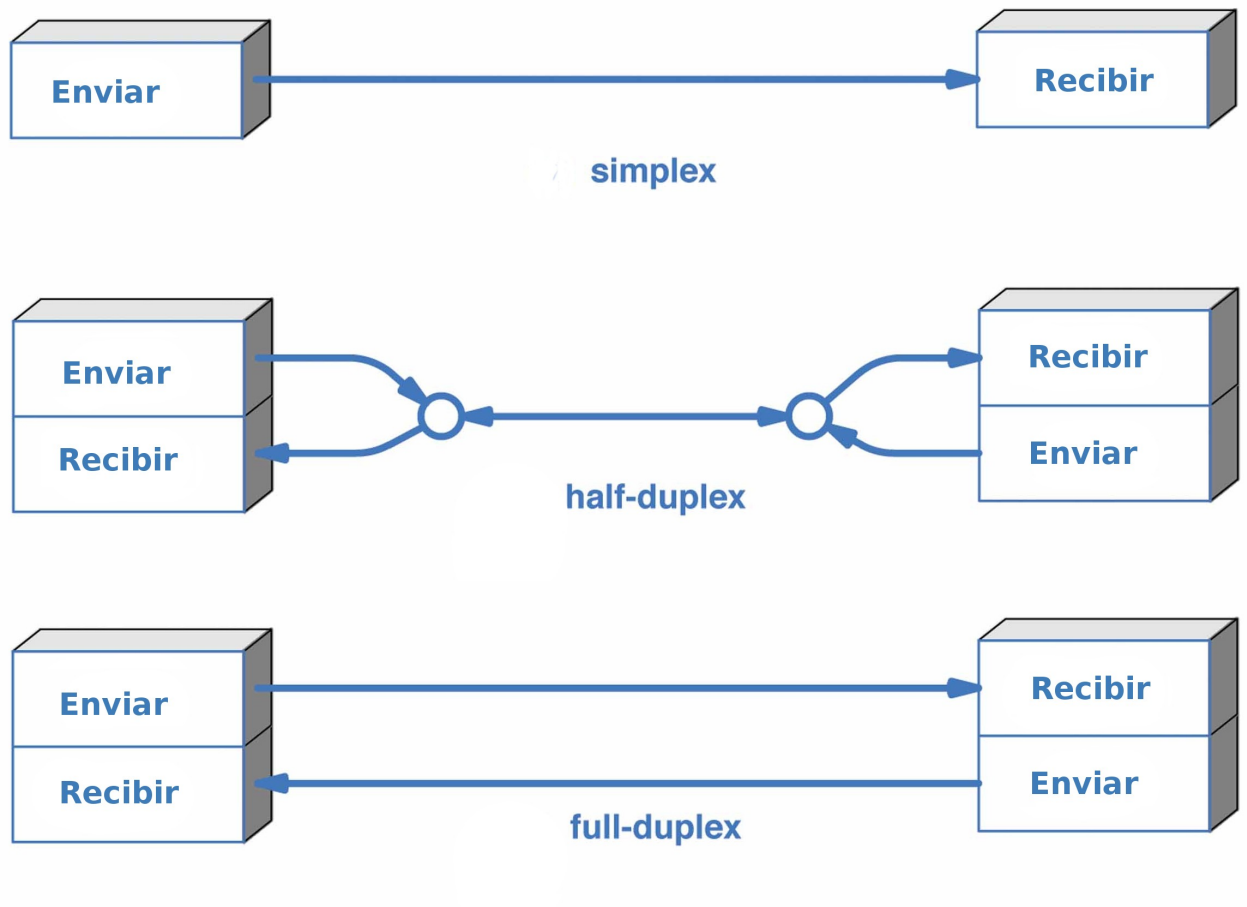


Figura 1: Tipos de transmisión

Toda señal electromagnética, considerada como función del tiempo, puede ser tanto analógica como digital.

- Una **señal analógica** es aquella en la que la intensidad de la señal varía suavemente en el tiempo. Es decir, no presenta saltos o discontinuidades.
- Una **señal digital** es aquella en la que la intensidad se mantiene constante durante un determinado intervalo de tiempo, tras el cual la señal cambia a otro valor constante. La señal continua puede corresponder a voz y la señal discreta puede representar valores binarios (0 y 1).

Cuando un medio o canal es compartido por varios emisores que desean transmitir a la vez, este debe multiplexarse.

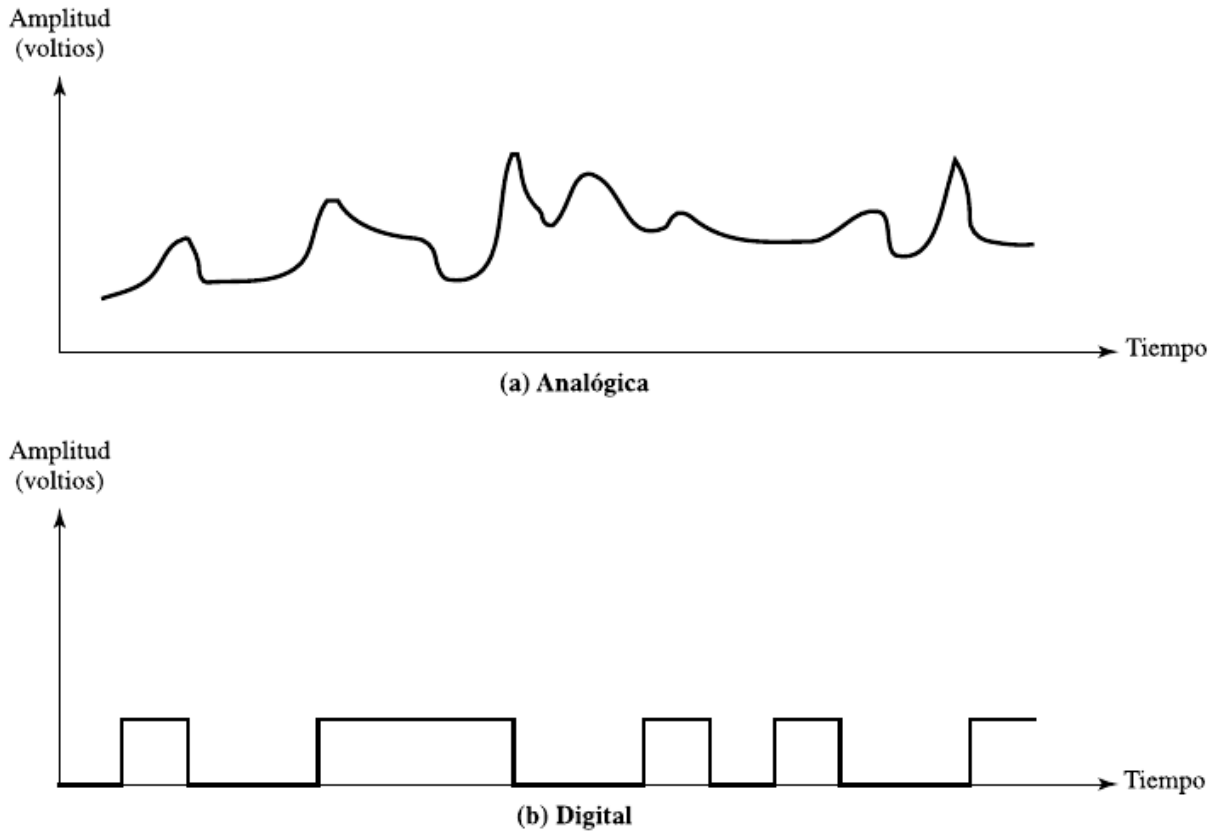


Figura 2: Señales analógicas y digitales

La **multiplexación** significa que se reserva parte del canal a cada emisor.

- En medios con transmisión analógica suele multiplexarse **por división de frecuencias** (Frequency-division multiplexing – FDM), asignandose a cada emisor una frencuencia distinta.
- En medios con transmisión digital suele multiplexarse **por división de tiempo** (Time division multiplexing -TDM), asignando a cada emisor una pequeña ranura de tiempo.

Para multiplexar un medio es necesario disponer de un dispositivo multiplexor en el origen y un dispositivo demultiplexor en el destino.

3.2 Perturbaciones en la transmisión

En cualquier sistema de comunicaciones se debe aceptar que la señal que se recibe diferirá de la señal transmitida debido a varias adversidades y dificultades sufridas en la transmisión. En las señales analógicas, estas dificultades pueden degradar la calidad de la señal. En las señales digitales, se generarán bits erróneos: un 1 binario se transformará en un 0 y viceversa.

Las dificultades más significativas son:

- La atenuación y la distorsión de atenuación.
- La distorsión de retardo.
- El ruido.

3.2.1 Atenuación

En cualquier medio de transmisión la energía de la señal decae con la distancia. En medios guiados, esta reducción de la energía es por lo general exponencial y, por tanto, se expresa generalmente como un número constante en decibelios por unidad de longitud. En medios no guiados, la atenuación es una función más compleja de la distancia y es dependiente, a su vez, de las condiciones atmosféricas.

La señal recibida debe tener suficiente energía para que la circuitería electrónica en el receptor pueda detectar la señal adecuadamente. En un enlace punto a punto, la energía de la señal en el transmisor debe ser lo suficientemente elevada como para que se reciba con inteligibilidad, pero no tan elevada que sature la circuitería del transmisor o del receptor, lo que generaría una señal distorsionada.

Para controlar la energía de la señal se usan amplificadores o repetidores. Hablamos de amplificadores cuando la señal es analógica y repetidores cuando la señal es digital.

3.2.2 Distorsión de retardo

La distorsión de retardo es un fenómeno debido a que la velocidad de propagación de una señal a través de un medio guiado varía con la frecuencia. Para una señal limitada en banda, la velocidad tiende a ser mayor cerca de la frecuencia central y disminuye al acercarse a los extremos de la banda. Por tanto, las distintas componentes en frecuencia de la señal llegarán al receptor en instantes diferentes de tiempo, dando lugar a desplazamientos de fase entre las diferentes frecuencias.

3.2.3 Ruido

Para cualquier dato transmitido, la señal recibida consistirá en la señal transmitida modificada por las distorsiones introducidas en la transmisión, además de señales no deseadas que se insertarán en algún punto entre el emisor y el

receptor. A estas últimas **señales no deseadas se les denomina ruido. El ruido es el factor de mayor importancia de entre los que limitan las prestaciones de un sistema de comunicación**.

La señal de ruido se puede clasificar en cuatro categorías:

- Ruido térmico.
- Ruido de intermodulación.
- Diafonía.
- Ruido impulsivo.

Ruido térmico

El ruido térmico se debe a la agitación térmica de los electrones. Está presente en todos los dispositivos electrónicos y medios de transmisión; como su nombre indica, es función de la temperatura.

El ruido térmico está uniformemente distribuido en el espectro de frecuencias usado en los sistemas de comunicación, es por esto por lo que a veces se denomina ruido blanco. **El ruido térmico no se puede eliminar** y, por tanto, impone un límite superior en las prestaciones de los sistemas de comunicación.

Ruido de intermodulación

Cuando señales de distintas frecuencias comparten el mismo medio de transmisión puede producirse ruido de intermodulación. El efecto del ruido de intermodulación es la aparición de señales a frecuencias que sean suma o diferencia de las dos frecuencias originales o múltiplos de éstas.

Diafonía

La diafonía la ha podido experimentar todo aquel que al usar un teléfono haya oído otra conversación; se trata, en realidad, de un **acoplamiento no deseado entre las líneas** que transportan las señales. Esto puede ocurrir por el acoplamiento eléctrico entre cables de pares cercanos o, en raras ocasiones, en líneas de cable coaxial que transporten varias señales.

Ruido impulsivo

Los ruidos antes descritos son de magnitud constante y razonablemente predecibles. Así pues, es posible idear un sistema de transmisión que les haga frente. Por el contrario, el ruido impulsivo es no continuo y **está constituido por pulsos o picos irregulares de corta duración y de amplitud relativamente grande**. Se generan por una gran diversidad de causas, por ejemplo, por perturbaciones electromagnéticas exteriores producidas por tormentas atmosféricas o por fallos y defectos en los sistemas de comunicación.

Generalmente, el ruido impulsivo no tiene mucha transcendencia para los datos analógicos. Por ejemplo, la transmisión de voz se puede perturbar mediante chasquidos o crujidos cortos, sin que ello implique pérdida significativa de inteligibilidad. Sin embargo, el ruido impulsivo **es una de las fuentes principales de error en la comunicación digital de datos**. Por ejemplo, un pico de energía con duración de 0,01 s no inutilizaría datos de voz, pero podría corromper aproximadamente 560 bits si se transmitieran a 56 kbps.

3.3 Medios cableados

Los medios guiados son aquellos compuestos por un material físico sólido que se encarga de transportar la señal de información sin que ésta sobrepase las fronteras físicas del medio. Medios de este tipo pueden transportar señales

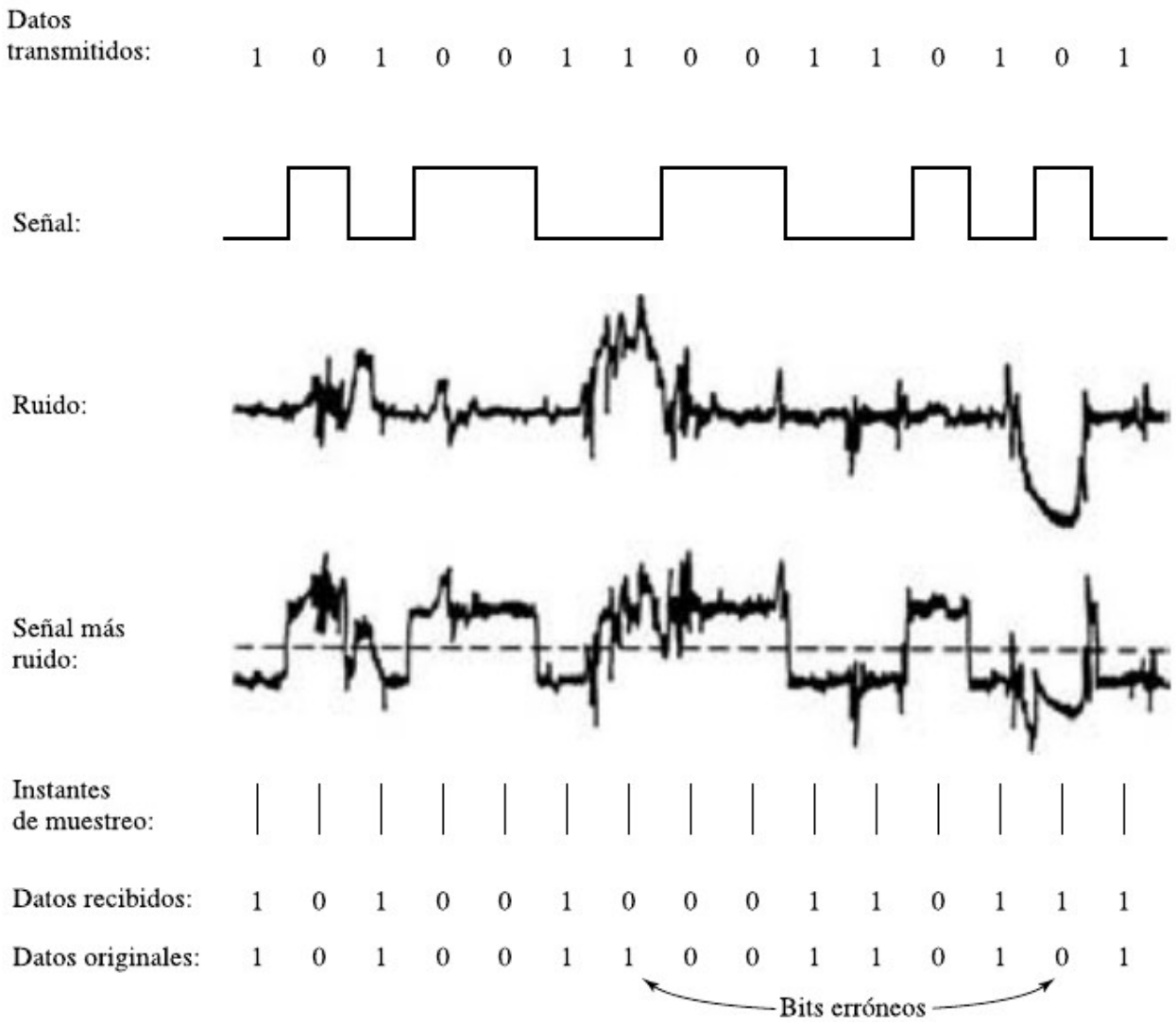


Figura 3: Efecto del ruido en una transmisión digital

formadas por ondas electromagnéticas como el par trenzado, el cable coaxial; o bien por señales ópticas, como la fibra óptica.

A continuación se detallan los medios cableados más importantes en el ámbito de las redes:

- Pares trenzados
- Cable coaxiales
- Fibra óptica

3.3.1 Pares trenzados

El cable de par trenzado consiste en dos alambres de cobre aislados que se trenzan de forma helicoidal, igual que una molécula de ADN. De esta forma el par trenzado constituye un circuito que puede transmitir datos. Esto se hace porque dos alambres paralelos constituyen una antena simple. Cuando se trenzan los alambres, las ondas de diferentes vueltas se cancelan, por lo que la radiación del cable es menos efectiva. Así la forma trenzada permite reducir la interferencia eléctrica tanto exterior como de pares cercanos. Un cable de par trenzado está formado por un grupo de pares trenzados, normalmente cuatro, recubiertos por un material aislante. Cada uno de estos pares se identifica mediante un color.

Según las protecciones frente a interferencias y a ruidos de la que dispongan, los cables de pares trenzados se clasifican en 4 tipos, de menor a mayor calidad y precio:

- **UTP**: No tiene protección.
- **FTP**: Tiene protección global.
- **STP**: Tiene protección por cada par.
- **S/FTP**: Tiene protección global y por cada par

Tipos de cables

UTP: Unshielded Twisted Pair

S/UTP o FTP : Screened Unshielded Twisted Pair o Foiled Twisted Pair

STP: Shielded Twisted Pair

S/STP o S/FTP: Screened Shielded Twisted Pair o Screened Foiled Twisted Pair

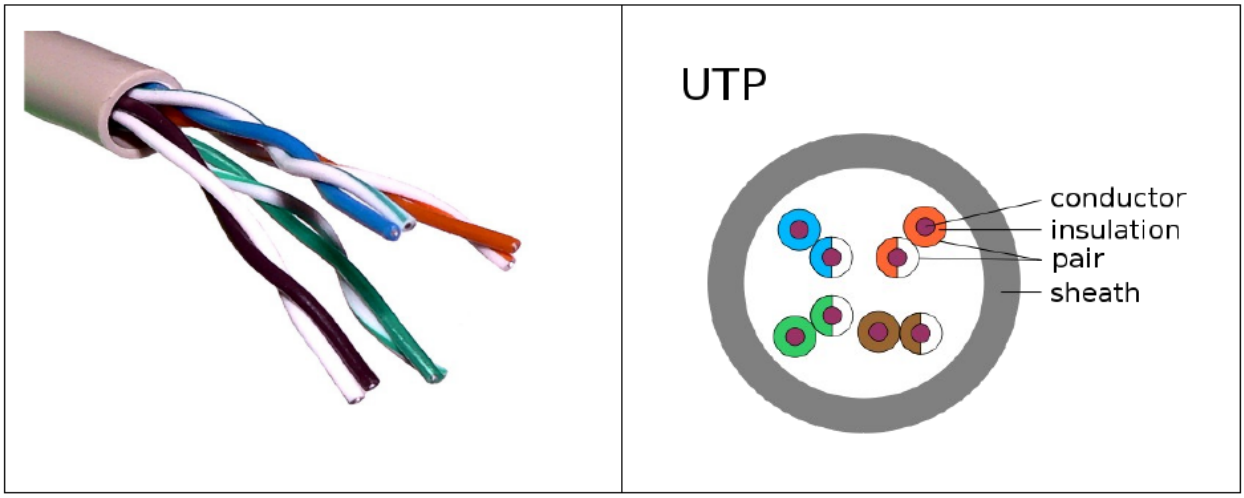


Figura 4: Pares trenzados sin apantallar

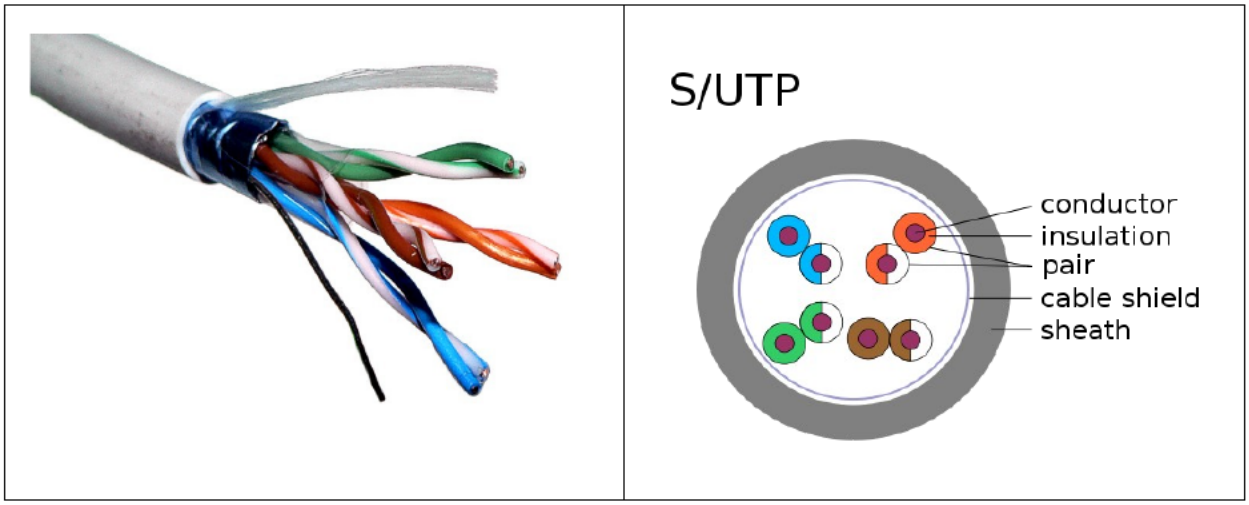


Figura 5: Pares trenzados con blindado global

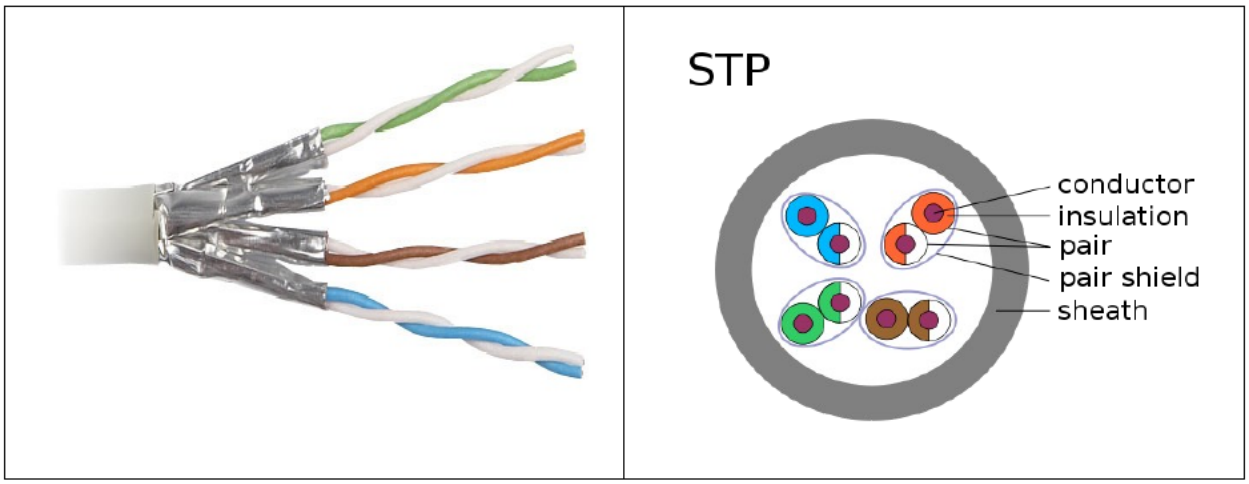


Figura 6: Pares trenzados apantallados

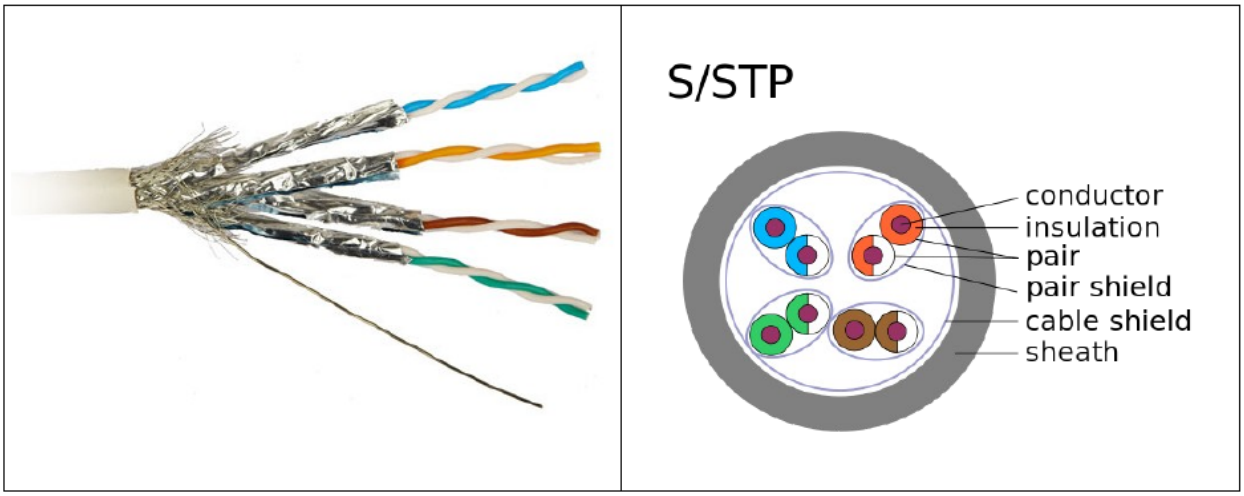


Figura 7: Pares trenzados apantallados con blindado global

Categorías y clases

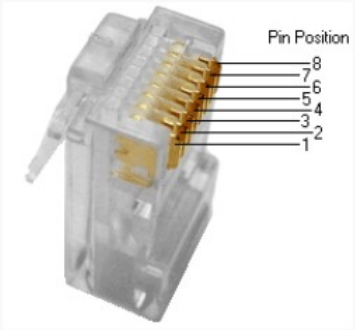
Según la norma **ISO/IEC 11801** los pares trenzados se pueden clasificar como:

Cat.	Clase	Ancho banda	Aplicaciones
1	A	0.4 MHz	Líneas telefónicas y módem. No descrito en las recomendaciones del EIA/TIA. No es adecuado para sistemas modernos.
2	B	4 MHz	Cable para conexión de antiguos terminales como el IBM 3270. No descrito en las recomendaciones del EIA/TIA. No es adecuado para sistemas modernos.
3	C	16 MHz	10BASE-T and 100BASE-T4 Ethernet. Descrito en la norma EIA/TIA-568. No es adecuado para transmisión de datos mayor a 16 Mbit/s.
4	▪	20 MHz	16 Mbit/s Token Ring. No usado comúnmente.
5	▪	100 MHz	100BASE-TX y 1000BASE-T Ethernet. Común en la mayoría de las LAN.
5e	D	100 MHz	100BASE-TX y 1000BASE-T Ethernet. Mejora del cable de Categoría 5. En la práctica es como la categoría anterior pero con mejores normas de prueba. Es adecuado para Gigabit Ethernet
6	E	250 MHz	10GBASE-T Ethernet. Cable más comúnmente instalado en Finlandia según la norma SFS-EN 50173-1.
6a	EA	500 MHz	10GBASE-T Ethernet. ISO/IEC 11801:2002 Enmienda 2.
7	F	600 MHz	Para servicios de telefonía, Videovigilancia por cable y Ethernet 1000BASE-T en el mismo cable. 10GBASE-T Ethernet. Cable S/FTP (pares blindados, cable blindado trenzado de 4 pares). Norma ISO/IEC 11801 2ª Ed.
7a	FA	1000 MHz	Para servicios de telefonía, Televisión por cable y Ethernet 1000BASE-T en el mismo cable. 10GBASE-T Ethernet. Cable S/FTP (pares blindados, cable blindado

Nota:

- Los circuitos de videovigilancia se conocen como **CCTV** - Closed Circuit TeleVision
- La televisión por cable se conoce como **CATV** - Community Antenna TeleVision

Conector RJ45

Pin	T568A Par	T568B Par	Cable	T568A Color	T568B Color	Pins en la cara del enchufe (el socket se invierte)
1	3	2	tip	blanco/linea verde	blanco/linea naranja	
2	3	2	ring	verde	naranja	
3	2	3	tip	blanco/linea naranja	blanco/linea verde	
4	1	1	ring	azul	azul	
5	1	1	tip	blanco/linea azul	blanco/linea azul	
6	2	3	ring	naranja	verde	
7	4	4	tip	blanco/linea marron	blanco/linea marron	
8	4	4	ring	marron	marron	

Nota: RJ son las siglas de Registered Jack.

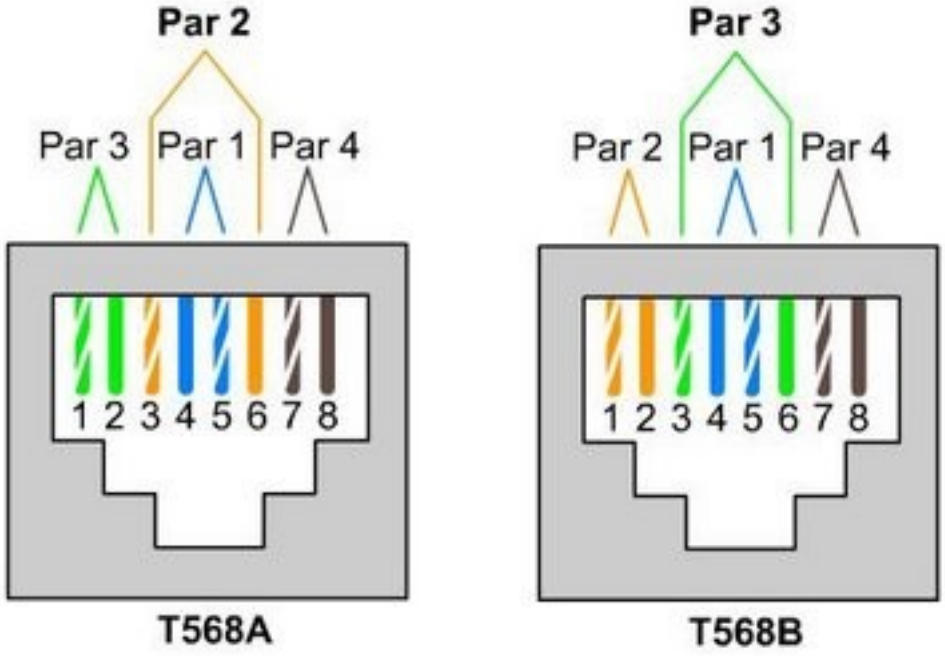
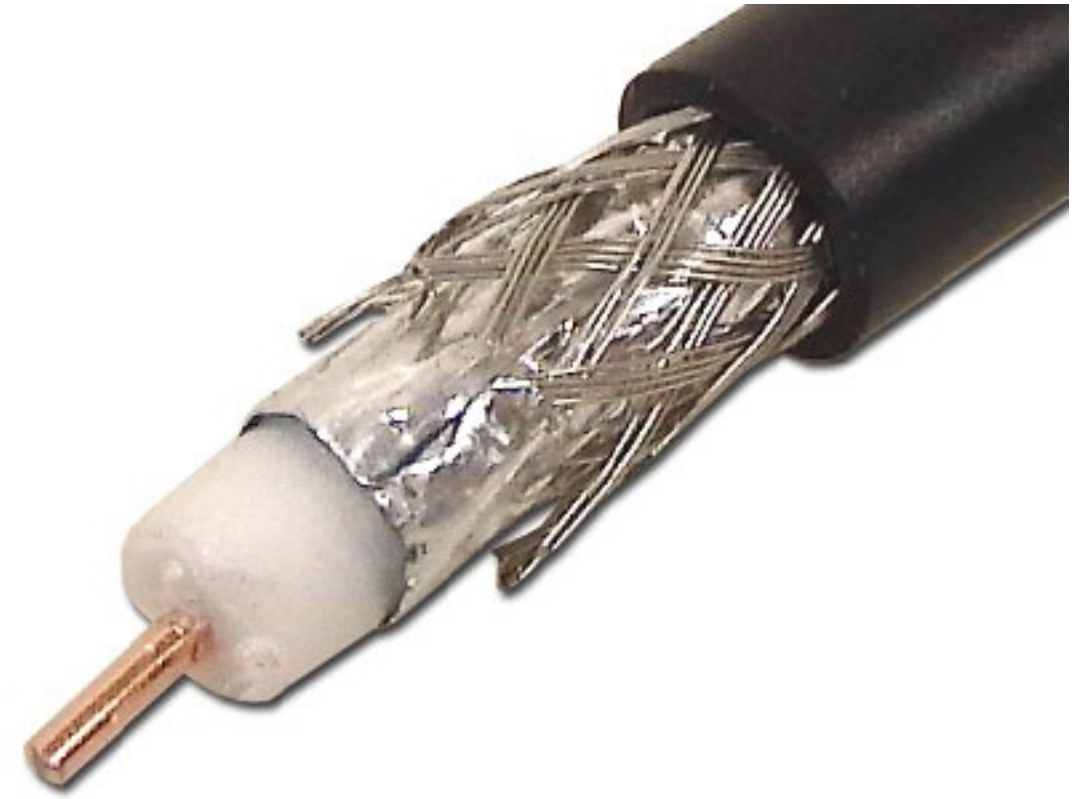


Figura 8: Normas de crimpado TIA 568A y 568B

3.3.2 Cable coaxial



El cable coaxial fue creado en la década de los 30, y es un cable utilizado para transportar señales eléctricas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado vivo, encargado de llevar la información, y uno exterior, de aspecto tubular, llamado malla, blindaje o trenza, que sirve como referencia de tierra y retorno de las corrientes. Entre ambos se encuentra una capa aislante llamada dieléctrico, de cuyas características dependerá principalmente la calidad del cable. Todo el conjunto suele estar protegido por una cubierta aislante (también denominada chaqueta exterior).

Debido a la necesidad de manejar frecuencias cada vez más altas y a la digitalización de las transmisiones, en años recientes se ha sustituido paulatinamente el uso del cable coaxial por el de fibra óptica, en particular para distancias superiores a varios kilómetros, porque el ancho de banda de esta última es muy superior.

El cable coaxial es quizá el medio de transmisión más versátil, por lo que se está utilizando cada vez más en una gran variedad de aplicaciones. Las más importantes son:

- La distribución de televisión.
- La telefonía a larga distancia.
- Los enlaces en computadores a corta distancia.
- Las redes de área local.

Tipos de cables

Existen dos tipos de cable coaxial:

- Cable coaxial de **banda base** Normalmente empleado en redes de computadoras, con resistencia de 50 Ω, por el que fluyen **señales digitales**. El tipo de conector es el RG58. Es el cable que **se utilizó inicialmente para las primeras redes locales, como Ethernet**, IBM PC-NET y ARCNET.

  - Grueso (Coaxial amarillo de 50 Ω). Su capacidad en términos de velocidad y distancia es grande, pero el coste del cableado es alto y su grosor no permite su utilización en canalizaciones con demasiados cables. Utilizado en la norma Ethernet 10Base-5.
  - Fino (Coaxial RG58 de 50 Ω) con terminaciones BNC. Es más barato y fino y, por tanto, solventa algunas de las desventajas del cable grueso; aunque obtiene peores rendimientos que el cable amarillo. Utilizado en la norma Ethernet 10Base-2.

- Cable coaxial de **banda ancha** Normalmente mueve **señales analógicas**, con resistencia de 75 Ω, posibilitando la transmisión de gran cantidad de información por varias frecuencias, y su uso más común es la **televisión por cable**. Esto ha permitido que muchos usuarios de Internet tengan un nuevo tipo de acceso a la red, para lo cual existe en el mercado una gran cantidad de dispositivos, incluyendo también módem para CATV.

Se puede encontrar un cable coaxial:

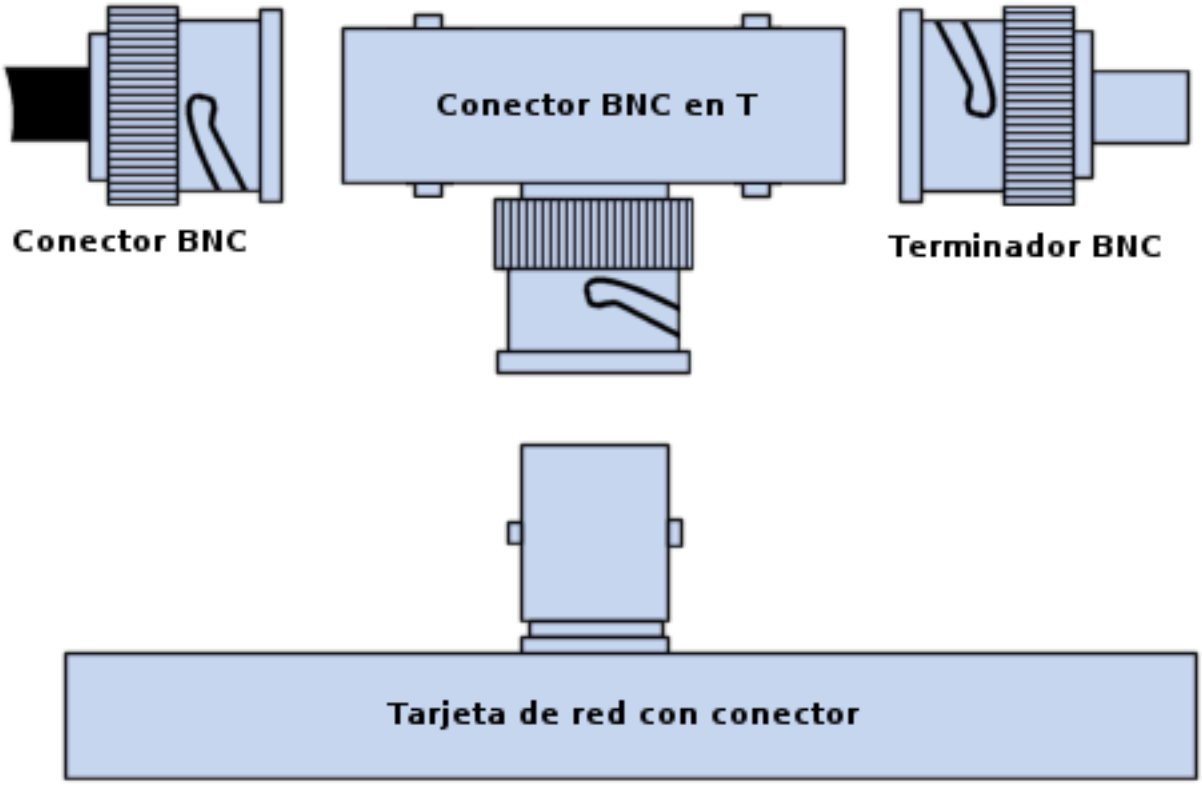
- entre la antena y el televisor;
- en las redes urbanas de televisión por cable (CATV) e Internet;
- entre un emisor y su antena de emisión (equipos de radioaficionados);
- en las líneas de distribución de señal de vídeo (se suele usar el RG-59);
- en las redes de transmisión de datos como Ethernet en sus antiguas versiones 10BASE2 y 10BASE5;
- en las redes telefónicas interurbanas y en los cables submarinos.

Antes de la utilización masiva de la fibra óptica en las redes de telecomunicaciones, tanto terrestres como submarinas, el cable coaxial era ampliamente utilizado en sistemas de transmisión de telefonía analógica basados en la multiplexación por división de frecuencia (FDM), donde se alcanzaban capacidades de transmisión de más de 10.000 circuitos de voz.

Asimismo, en sistemas de transmisión digital, basados en la multiplexación por división de tiempo (TDM), se conseguía la transmisión de más de 7.000 canales de 64 kbps.

Conectores

La conexión de cable coaxial requiere la utilización de unos conectores especiales. Los más utilizados son los denominados conectores **BNC** (Bayonet, Neill-Concelman).



Conector BNC

Figura 9: Este conector tiene un centro circular conectado al conductor del cable central y un tubo metálico conectado en el parte exterior del cable. Un anillo que rota en la parte exterior del conector asegura el cable mediante un mecanismo de bayoneta y permite la conexión.

Conector BNC en T

Extensor BNC o barrilete

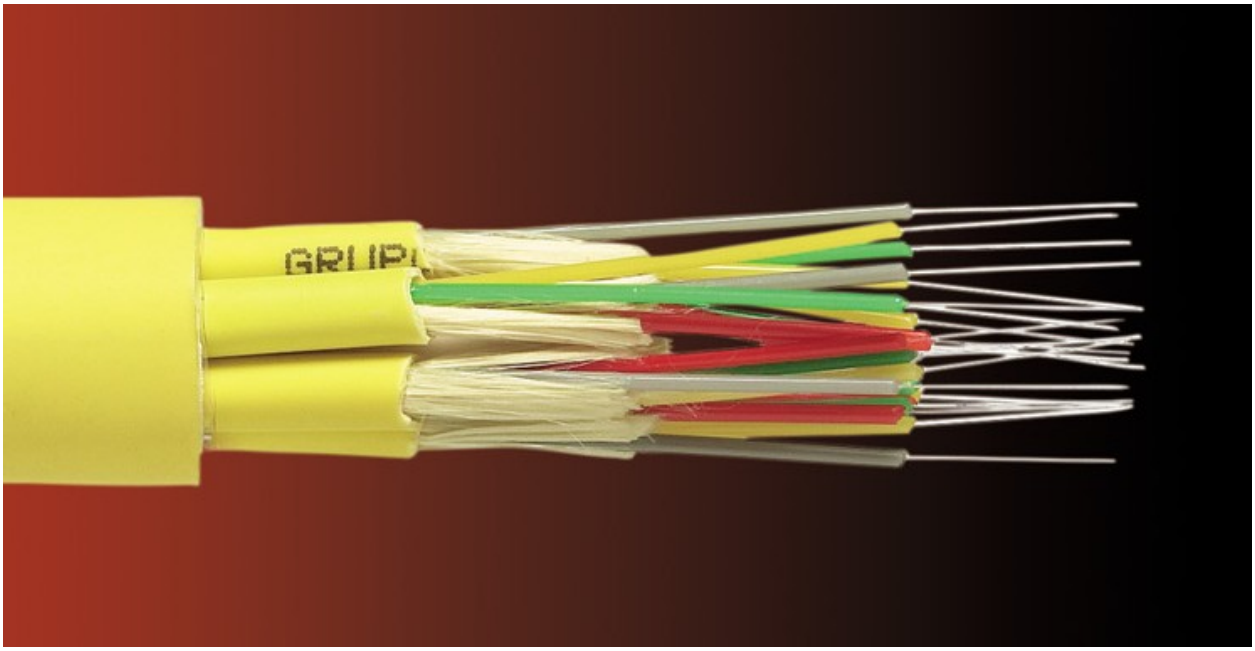
Terminador BNC

Figura 10: Consiste en dos conectores hembras y uno macho que le dan una forma similar a la letra "T". Los conectores hembra se conectan a cables coaxiales en la red y el macho va directamente conectado al adaptador de red del ordenador.

Figura 11: Este tipo de conector permite conectar un cable coaxial al extremo de otro, y así aumentar la longitud total de alcance.

Figura 12: Es un conector BNC que se utiliza para cerrar el extremo del bus del cable y evitar que las señales perdidas ocasionen interferencias. Una red montada con coaxial no podría funcionar sin ellos.

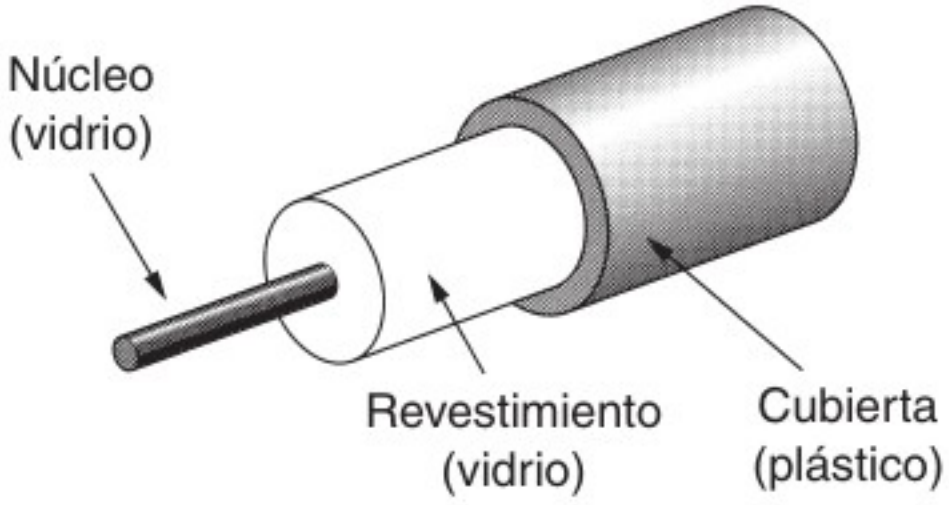
3.3.3 Fibra óptica



La fibra óptica es un medio flexible y delgado (de 2 a 125 μm) capaz de confinar un haz de naturaleza óptica. Para construir la fibra se pueden usar diversos tipos de cristales y plásticos. Las pérdidas menores se han conseguido con la utilización de fibras de silicio ultrapuro fundido.

Las fibras ultrapuras son muy difíciles de fabricar; las fibras de cristal multicomponente son más económicas y, aunque sufren mayores pérdidas, proporcionan unas prestaciones suficientes. La fibra de plástico tiene todavía un coste menor, pudiendo ser utilizada en enlaces de distancias más cortas, en los que sean aceptables pérdidas moderadamente altas.

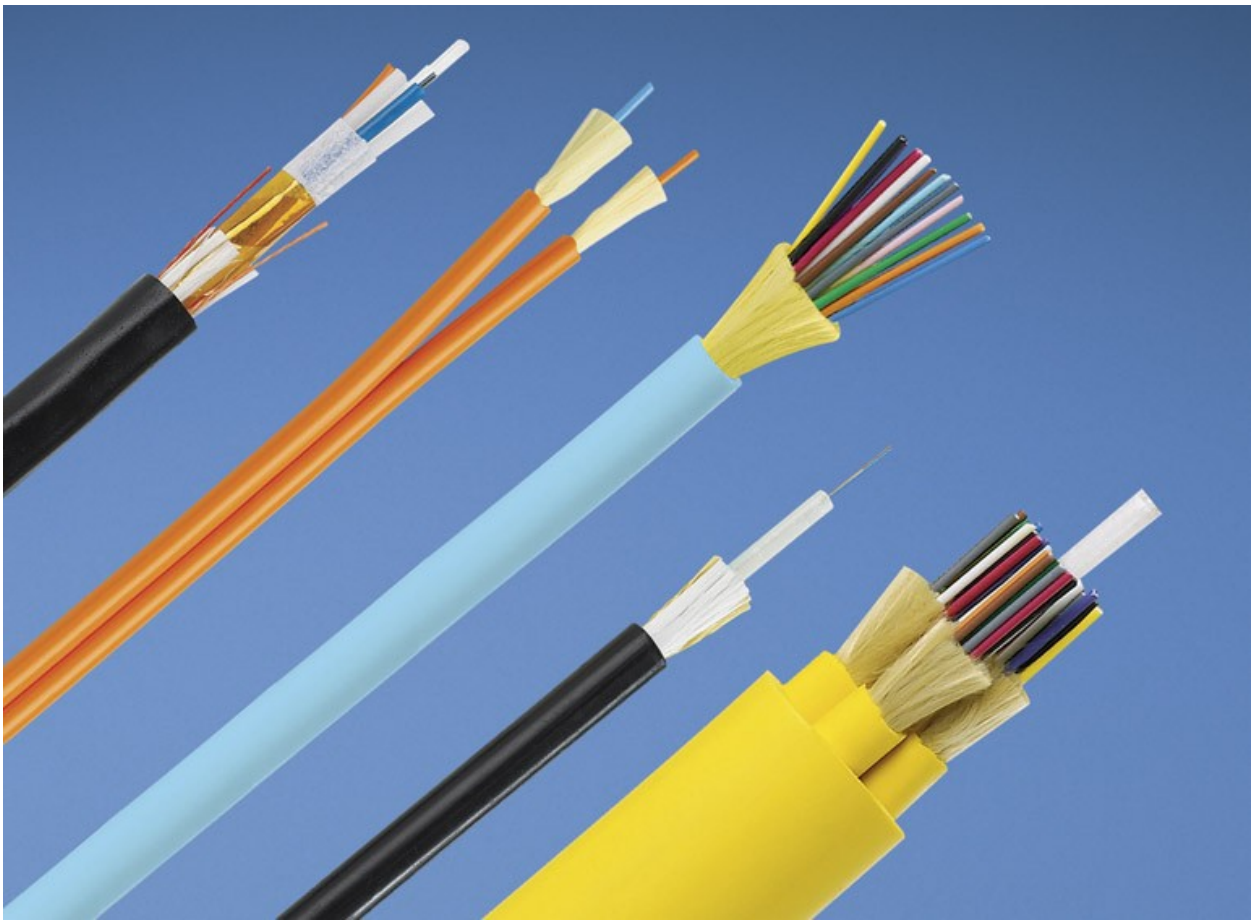
Un cable de fibra óptica tiene forma cilíndrica y está formado por tres secciones concéntricas: el núcleo, el revestimiento y la cubierta. El núcleo es la sección más interna; está constituido por una o varias fibras de cristal o plástico, con un diámetro entre 8 y 100 μm.



Cada fibra está rodeada por su propio revestimiento, que no es sino otro cristal o plástico con propiedades ópticas distintas a las del núcleo. La separación entre el núcleo y el revestimiento actúa como un reflector, confinando así el

haz de luz, ya que de otra manera escaparía del núcleo. La capa más exterior que envuelve a uno o varios revestimientos es la cubierta. La cubierta está hecha de plástico y otros materiales dispuestos en capas para proporcionar protección contra la humedad, la abrasión, posibles aplastamientos y otros peligros.

Uno de los avances tecnológicos más significativos y rompedores en la transmisión de datos ha sido el desarrollo de los sistemas de comunicación de fibra óptica. No en vano, la fibra disfruta de una gran aceptación para las telecomunicaciones a larga distancia y, cada vez, está siendo más utilizada en aplicaciones militares. Las mejoras constantes en las prestaciones a precios cada vez inferiores, junto con sus ventajas inherentes, han contribuido decisivamente para que la fibra sea un medio atractivo en los entornos de red de área local.



Las características diferenciales de la fibra óptica frente al cable coaxial y al par trenzado son:

- **Mayor capacidad**: el ancho de banda potencial y, por tanto, la velocidad de transmisión, en las fibras es enorme. Experimentalmente se ha demostrado que se pueden conseguir velocidades de transmisión de cientos de Gbps para decenas de kilómetros de distancia. Compárese con el máximo que se puede conseguir en el cable coaxial de cientos de Mbps sobre aproximadamente 1 km, o con los escasos Mbps que se pueden obtener para la misma distancia, o compárese con los 100 Mbps o incluso 1 Gbps para pocas decenas de metros que se consiguen en los pares trenzados.
- **Menor tamaño y peso**: las fibras ópticas son apreciablemente más finas que el cable coaxial o que los pares trenzados embutidos, por lo menos en un orden de magnitud para capacidades de transmisión comparables. En las conducciones o tubos de vacío previstos para el Comunicaciones y redes de computadores cableado en las edificaciones, así como en las conducciones públicas subterráneas, la utilización de tamaños pequeños tiene unas ventajas evidentes. La reducción en tamaño lleva a su vez aparejada una reducción en peso que disminuye, a su vez, la infraestructura necesaria.
- **Atenuación menor**: la atenuación es significativamente menor en las fibras ópticas que en los cables coaxiales

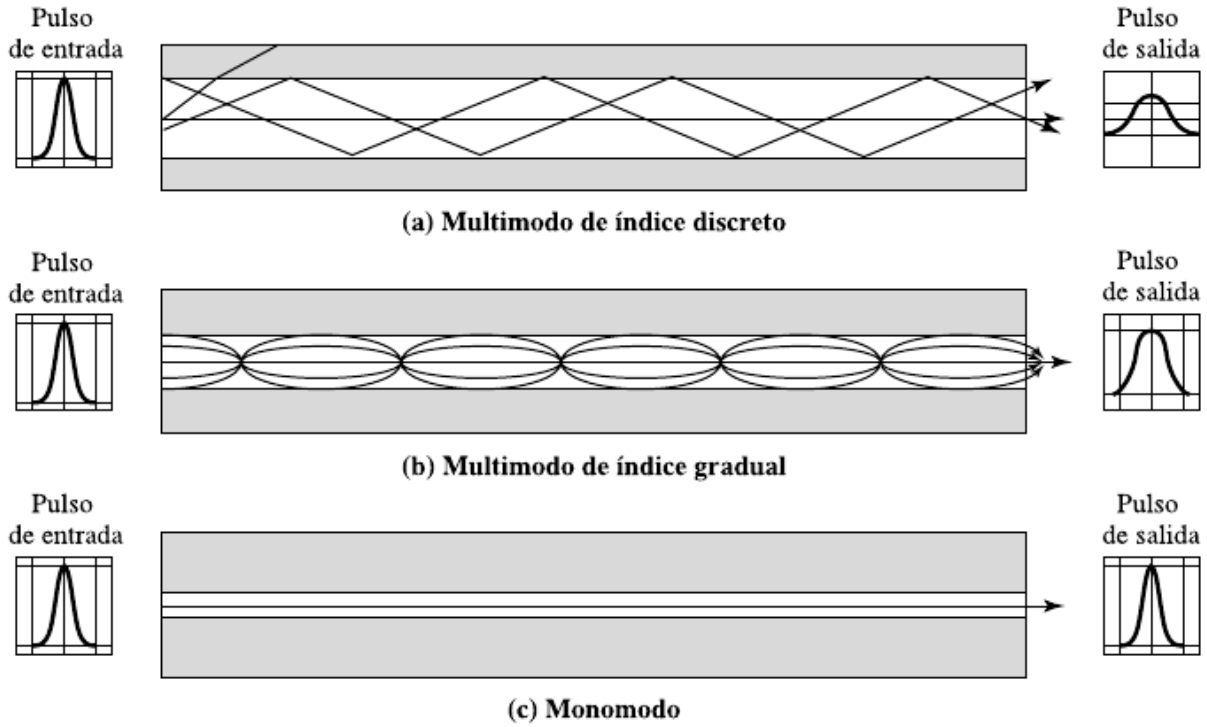
y pares trenzados, además, es constante a lo largo de un gran intervalo.

- **Aislamiento electromagnético**: los sistemas de fibra óptica no se ven afectados por los efectos de campos electromagnéticos exteriores. Estos sistemas no son vulnerables a interferencias, ruido impulsivo o diafonía. Por la misma razón, las fibras no radian energía, produciendo interferencias despreciables con otros equipos que proporcionan, a la vez, un alto grado de privacidad; además, relacionado con esto, la fibra es por construcción difícil de «pinchar».
- **Mayor separación entre repetidores**: cuantos menos repetidores haya el coste será menor, además de haber menos fuentes de error. Desde este punto de vista, las prestaciones de los sistemas de fibra óptica han sido mejoradas de manera constante y progresiva. Para la fibra es práctica habitual necesitar repetidores separados entre sí del orden de decenas de kilómetros e, incluso, se han demostrado experimentalmente sistemas con separación de cientos de kilómetros. Por el contrario, los sistemas basados en coaxial y en pares trenzados requieren repetidores cada pocos kilómetros.

Las cinco aplicaciones básicas en las que la fibra óptica es importante son:

- Transmisiones a larga distancia.
- Transmisiones metropolitanas.
- Acceso a áreas rurales.
- Bucles de abonado.
- Redes de área local.

Tipos de fibras



Un sistema de transmisión óptico tiene tres componentes: la fuente de luz, el medio de transmisión y el detector. Convencionalmente, un pulso de luz indica un bit 1 y la ausencia de luz indica un bit 0. El medio de transmisión es una fibra de vidrio ultradelgada. El detector genera un pulso eléctrico cuando la luz incide en él. Al agregar una fuente de luz en un extremo de una fibra óptica y un detector en el otro, se tiene un sistema de transmisión de datos

unidireccional que acepta una señal eléctrica, la convierte y transmite mediante pulsos de luz y, luego, reconvierte la salida a una señal eléctrica en el extremo receptor.

Puesto que cualquier rayo de luz que incida en la frontera con un ángulo mayor que el crítico se reflejará internamente, muchos rayos estarán rebotando con ángulos diferentes. Se dice que cada rayo tiene un modo diferente, por lo que una fibra que tiene esta propiedad se denomina **fibra multimodo**. Este tipo de fibra es más adecuada para la transmisión a distancias cortas.

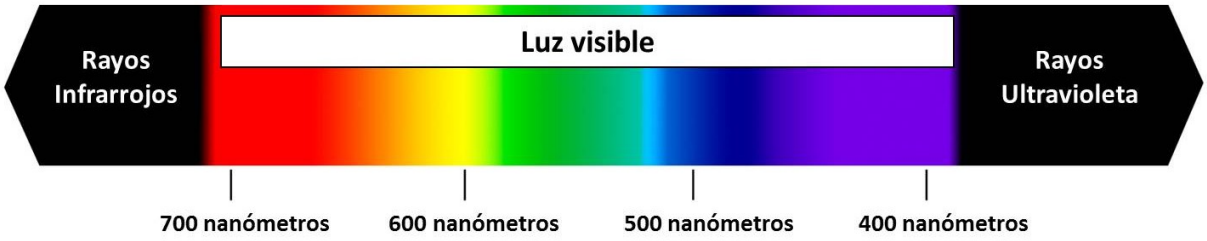
Por otro lado, si el diámetro de la fibra se reduce a unas cuantas longitudes de onda de luz, la fibra actúa como una guía de ondas y la luz se puede propagar sólo en línea recta, sin rebotar, lo cual da como resultado una **fibra monomodo**. Las fibras monomodo son más caras, pero se pueden utilizar en distancias más grandes. Las fibras monomodo disponibles en la actualidad pueden transmitir datos a 50 Gbps a una distancia de 100 km sin amplificación. En el laboratorio se han logrado tasas de datos todavía mayores a distancias más cortas.

Existe un tercer modo de transmisión variando gradualmente el índice de refracción del núcleo, este modo se denomina **multimodo de índice gradual**. Las características de este último modo están entre las de los otros dos modos comentados. En lugar de describir un zig-zag, la luz en el núcleo describe curvas helicoidales debido a la variación gradual del índice de refracción, reduciendo así la longitud recorrida. El efecto de tener una mayor velocidad de propagación y una longitud inferior posibilita que la luz periférica llegue al receptor al mismo tiempo que los rayos axiales del núcleo. Las fibras de índice gradual se utilizan frecuentemente en las redes de área local.

¿LED o láser?

Tanto el LED como el láser tienen ciertas características que los hacen apropiados para determinados propósitos. A continuación se muestra una tabla con dichas características.

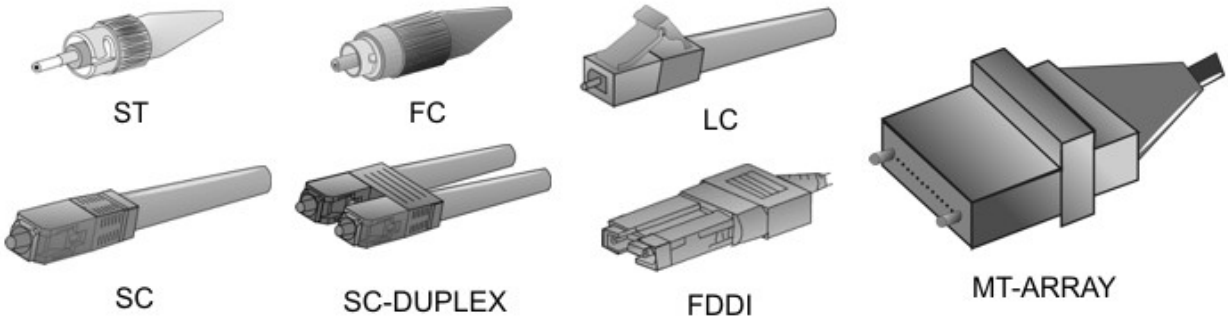
Elemento	LED	Láser semiconductor
Tasa de datos	Baja	Alta
Tipo de fibra	Multimodo	Multimodo o monomodo
Distancia	Corta	Larga
Tiempo de vida	Largo	Corto
Sensibilidad a la temperatura	Menor	Considerable
Costo	Bajo	Elevado



Para las comunicaciones se utilizan **tres bandas** de longitud de onda, las cuales se centran en **850, 1300 y 1550 nm**, respectivamente, es decir se hallan en el **infrarrojo**. Las últimas dos tienen buenas propiedades de atenuación (una pérdida de menos de 5 % por kilómetro). La banda de 850 nm tiene una atenuación más alta, pero a esa longitud de onda, los láseres y los componentes electrónicos se pueden fabricar con el mismo material (arseniuro de galio).

Conectores

Estos elementos se encargan de conectar las líneas de fibra a un elemento, ya puede ser un transmisor o un receptor. Los tipos de conectores disponibles son muy variados, entre los que podemos encontrar se hallan los siguientes:



3.4 Medios inalámbricos

Los medios inalámbricos son medios no guiados que basan su funcionamiento en la radiación de energía electromagnética. Esa energía es transmitida por un emisor y recibida por un receptor.

Existen dos configuraciones para la emisión y recepción de la energía:

- **Direccional**: en este tipo de transmisión, toda la energía se concentra en un haz que es emitido en una cierta dirección, por lo que se exige que el emisor y el receptor se encuentren alineados.

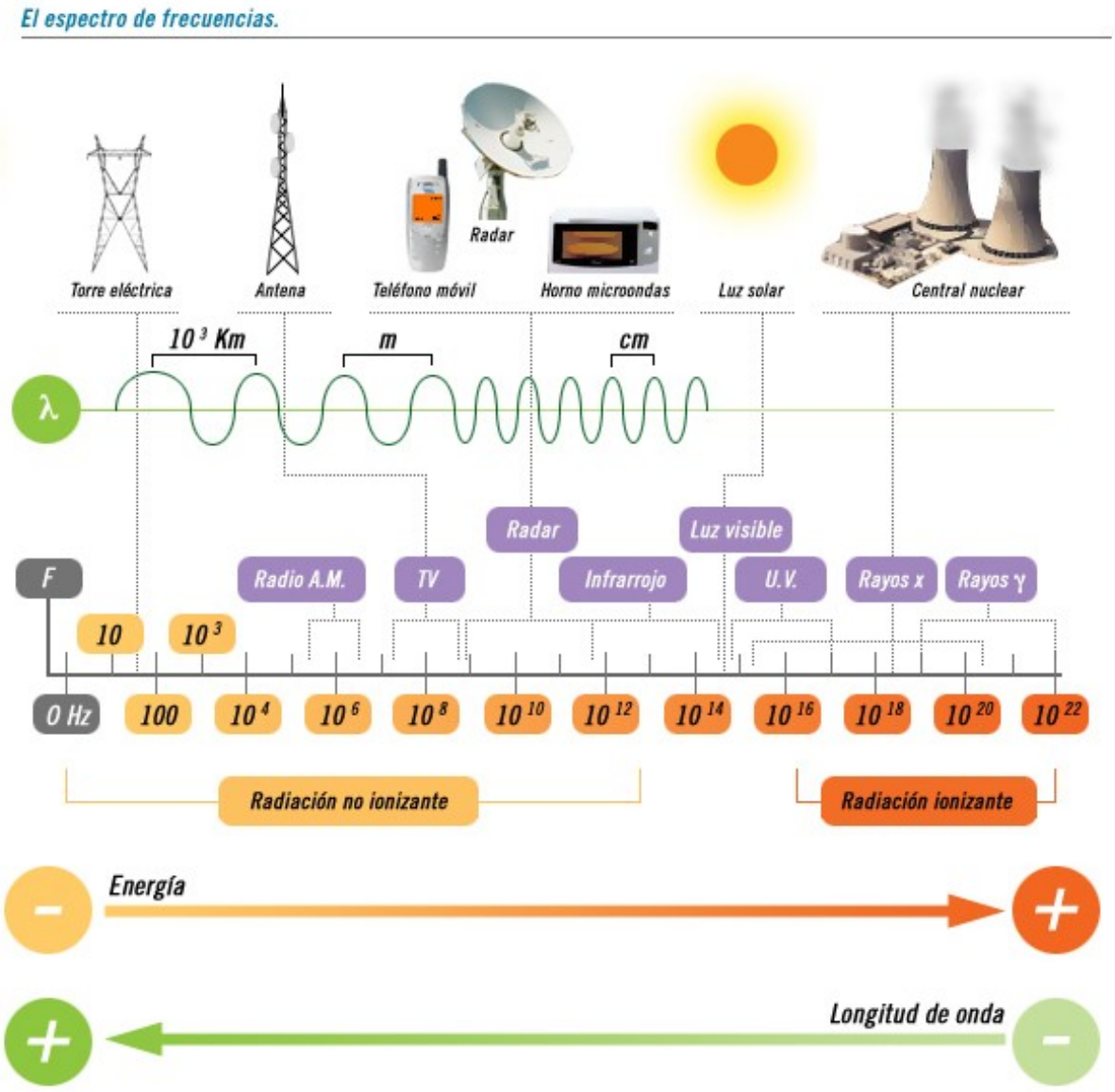
- **Omnidireccional**: en este caso la energía es dispersada en todas las direcciones, por lo que varias antenas pueden captarlas.

Tipos

Se podría hacer una clasificación de las comunicaciones que utilizan el medio inalámbrico atendiendo a la frecuencia que se utiliza. Aunque no existe una separación frecuencia clara, se pueden considerar cuatro tecnologías:

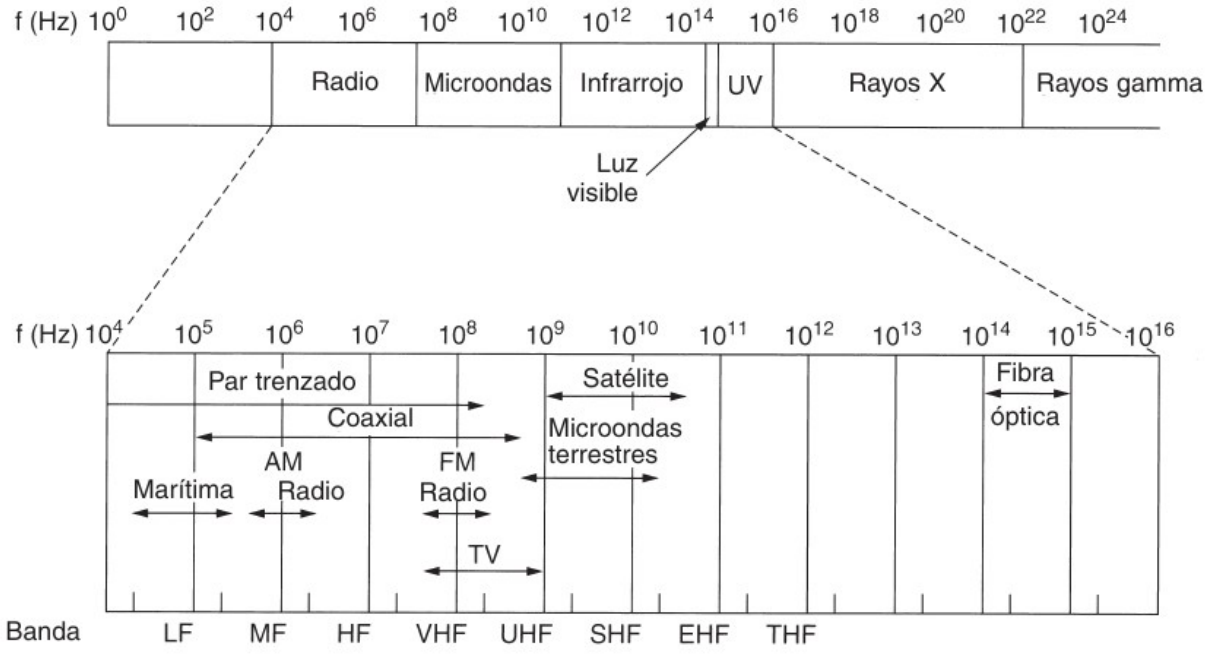
- Ondas de radio
- Microondas
- Infrarrojos
- Luz visible

3.4.1 Espectro electromagnético



■	Longitud de onda (m)	Frecuencia (Hz)
Radio	1000 km – 1 mm	300 Hz - 300Gz
Luz	1 mm – 10 nm	300 GHz – 30 PHz
Rayos X	10 nm – 10 pm	30 PHz – 30 EHz
Rayos gamma	10 pm -	30 Ehz -

Frecuencias y medios empleados



Nota: Las ondas en las frecuencias del **ultravioleta, rayos x y rayos gamma** son ionizantes, es decir tienen repercusiones perjudiciales sobre los tejidos de los seres vivos, por lo que **NO se utilizan para la transmisión**.

Rango de frecuencia	Longitud de onda	Banda (frecuencia)	Tipo de propagación	Aplicaciones
300 Hz – 3 KHz	1000-100 km	ELF (extrem. baja)	Superficie	Comunicaciones submarinas
3 KHz – 30 KHz	100-10 km	VLF (muy baja)	Superficie	Comunicaciones maritimas
30 KHz – 300 KHz	10-1 km	LF (baja) LW = (Onda larga)	Superficie	Difusión AM
300 KHz – 3 MHz	1000-100 m	MF (media) = MW (Onda media)	Troposférica	Difusión AM
3 MHz – 30 MHz	100-10 m	HF (alta) = SW (Onda corta)	Ionosférica	Difusión AM, radioaficionados
30 MHz – 300 MHz	10-1 m	VHF (muy alta)	Visión directa	Difusión FM, TV VHF
300 MHz – 3 GHz	1000-100 mm	UHF (ultra alta)	Visión directa	TV UHF, teléfonos móviles
3 GHz – 30 GHz	100-10 mm	SHF (super alta)	Visión directa y espacio	Microondas terrestres, satélites
30 GHz – 300 GHz	10-1 mm	EHF (extrema. alta)	Espacio	Satélites, radar y comunicaciones experimentales
300 GHz – 6 THz	1 mm – 50 µm	Infrarrojo Lejano		
6 THz – 120 THz	50 µm – 2,5 µm	Infrarrojo Medio		
120 THz - 384 THz	2,5 µm – 780 nm	Infrarrojo Cercano		
384 THz – 789 THz	780 nm – 380 nm	Luz Visible		
789 THz – 1.5 PHz	380 nm – 200 nm	Ultravioleta Cercano		
1.5 PHz – 30 PHz	200 nm -10 nm	Ultravioleta Extremo		

3.4.2 Microondas

Se denomina microondas a las ondas electromagnéticas definidas en un rango de frecuencias determinado generalmente de **entre 300 MHz y 300 GHz**, que supone una longitud de onda en el **rango de 1 m a 1 mm**.

Importante: Otras definiciones, por ejemplo las de los estándares IEC 60050 y IEEE 100 sitúan su rango de frecuencias entre 1 GHz y 300 GHz, es decir, longitudes de onda de entre 30 centímetros a 1 milímetro.

El rango de las microondas está incluido en las bandas de radiofrecuencia, concretamente en las de **UHF** (ultra-high frequency - frecuencia ultra alta) 0,3–3 GHz, **SHF** (super-high frequency - frecuencia super alta) 3–30 GHz y **EHF** (extremely-high frequency - frecuencia extremadamente alta) 30–300 GHz. Otras bandas de radiofrecuencia incluyen ondas de menor frecuencia y mayor longitud de onda que las microondas. Las microondas de mayor frecuencia y menor longitud de onda —en el orden de milímetros— se denominan ondas milimétricas.

Bandas ISM

ISM (Industrial, Scientific and Medical) son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica. En la actualidad estas bandas han sido popularizadas por su uso en comunicaciones WLAN (e.g. Wi-Fi) o WPAN (e.g. Bluetooth).

Conviene destacar que el Reglamento de Radiocomunicaciones de UIT ha destinado a nivel mundial (y en algún caso, regional) bandas para uso primario para las aplicaciones Industriales, Científicas y Médicas (ICM). La Nota de Pie 5.150 dice:

> "Las bandas:
>
> - 13.553-13.567 kHz (frecuencia central 13.560 kHz),
> - 26.957-27.283 kHz (frecuencia central 27.120 kHz),
> - 40,66-40,70 MHz (frecuencia central 40,68 MHz),
> - 902-928 MHz en la Región 2 (frecuencia central 915 MHz),
> - **2.400-2.500 MHz (frecuencia central 2.450 MHz)**,
> - 5.725-5.875 MHz (frecuencia central 5.800 MHz) y
> - 24-24,25 GHz (frecuencia central 24,125 GHz),
>
> están designadas para aplicaciones industriales, científicas y médicas (ICM). Los servicios de radiocomunicación que funcionan en estas bandas deben aceptar la interferencia perjudicial resultante de estas aplicaciones. "

El uso de estas bandas de frecuencia está abierto a todo el mundo sin necesidad de licencia, respetando las regulaciones que limitan los niveles de potencia transmitida. Este hecho fuerza a que este tipo de comunicaciones tengan cierta tolerancia frente a errores y que utilicen mecanismos de protección contra interferencias, como técnicas de ensanchado de espectro.

Algunos aparatos que usan la frecuencia de 2,4 GHz son los microondas, teléfonos inalámbricos, monitores de bebés, IEEE 802.15.1 (WPAN - Bluetooth) e IEEE 802.11 (WLAN)...

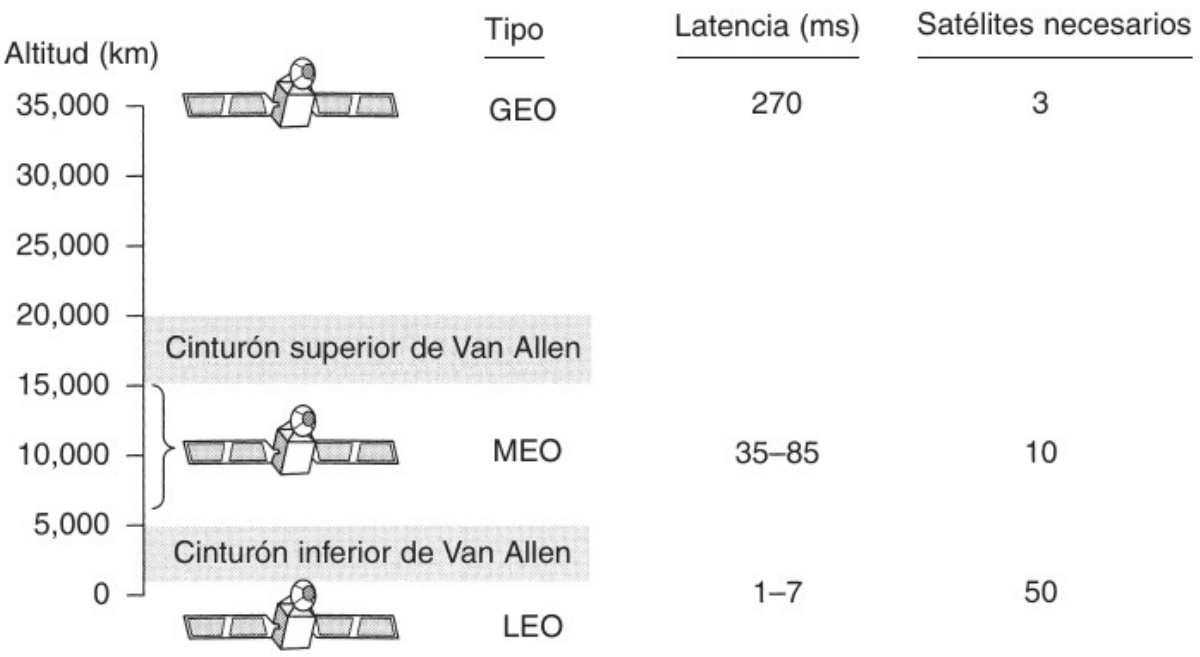
Transmisiones por satélite

Las comunicaciones por satélite han sido una revolución tecnológica de igual magnitud que la desencadenada por la fibra óptica. Entre las aplicaciones más importantes de los satélites cabe destacar:

- La difusión de televisión.
- La transmisión telefónica a larga distancia.
- Las redes privadas.

El rango de frecuencias óptimo para la transmisión vía satélite está en el intervalo comprendido entre 1 y 10 GHz. Por debajo de 1 GHZ, el ruido producido por causas naturales es apreciable, incluyendo el ruido galáctico, el solar, el atmosférico y el producido por interferencias con otros dispositivos electrónicos. Por encima de los 10 GHz, la señal se ve severamente afectada por la absorción atmosférica y por las precipitaciones.

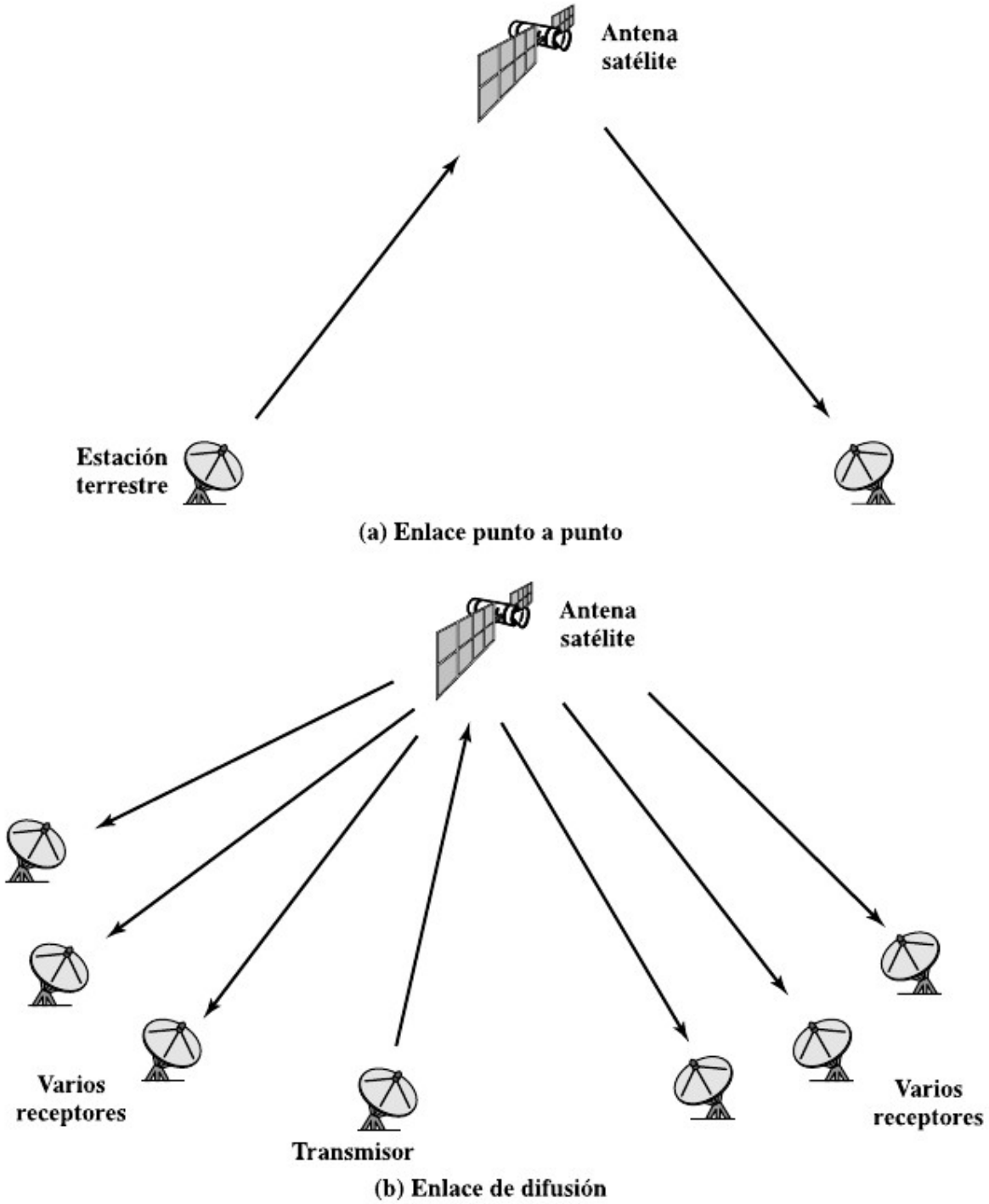
Según la altura a la que se sitúen los satélites, existen 3 tipos:



- En 1945, el escritor de ciencia-ficción Arthur C. Clarke calculó que un satélite a una altitud de 35.800 km en una órbita ecuatorial circular aparentaría permanecer inmóvil en el cielo, por lo que no sería necesario rastrearlo (Clarke, 1945). Con la tecnología disponible en esa época no era factible el envío y mantenimiento de dichos satélites. La invención del transistor cambió las cosas, y el primer satélite de comunicaciones artificial, Telstar, fue lanzado en julio de 1962. Desde entonces, los satélites de comunicaciones se han convertido en un negocio multimillonario y en el único aspecto del espacio exterior altamente rentable. Con frecuencia, a estos satélites que vuelan a grandes alturas se les llama **satélites GEO (Órbita Terrestre Geoestacionaria)**.
- Los **satélites MEO (Órbita Terrestre Media)** se encuentran a altitudes mucho más bajas, entre los dos cinturones de Van Allen. Vistos desde la Tierra, estos satélites se desplazan lentamente y tardan alrededor de seis horas para dar la vuelta a la Tierra. Por consiguiente, es necesario rastrearlos conforme se desplazan. Puesto que son menores que los GEO, tienen una huella más pequeña y se requieren transmisores menos potentes para alcanzarlos. Hoy en día no se utilizan para telecomunicaciones, por lo cual no los examinaremos aquí. Los 24 satélites **GPS (Sistema de Posicionamiento Global)** que orbitan a cerca de 18,000 km son ejemplos de satélites MEO.
- En una altitud más baja encontramos a los **satélites LEO (Órbita Terrestre Baja)**. Debido a la rapidez de su movimiento, se requieren grandes cantidades de ellos para conformar un sistema completo. Por otro lado, como los satélites se encuentran tan cercanos a la Tierra, las estaciones terrestres no necesitan mucha potencia, y el retardo del viaje de ida y vuelta es de tan sólo algunos milisegundos. En esta sección examinaremos tres ejemplos, dos sobre las comunicaciones de voz y uno sobre el servicio de Internet.

Existen 2 configuraciones para la transmisión por satélite:

- enlace punto a punto
- enlace de difusión



3.5 Datos y codificaciones

Tanto la información analógica como la digital pueden ser codificadas mediante señales analógicas o digitales. La elección de un tipo particular de codificación dependerá de los requisitos exigidos, del medio de transmisión, así como

de los recursos disponibles para la comunicación.

Existen 4 combinaciones posibles:

- **Datos digitales, señales digitales**: la forma más sencilla de codificar digitalmente datos digitales es asignar un nivel de tensión al uno binario y otro nivel distinto para el cero. Para mejorar las prestaciones hay que utilizar códigos distintos al anterior, alterando el espectro de la señal y proporcionando capacidad de sincronización.
- **Datos digitales, señales analógicas**: los módem convierten los datos digitales en señales analógicas de tal manera que se puedan transmitir a través de líneas analógicas. Las técnicas básicas son la modulación por desplazamiento de amplitud (ASK), modulación por desplazamiento de frecuencia (FSK) y modulación por desplazamiento de fase (PSK). En todas ellas, para representar los datos digitales, se modifican uno o más parámetros característicos de la señal portadora.
- **Datos analógicos, señales digitales**: los datos analógicos, como por ejemplo la voz y el vídeo, frecuentemente, se digitalizan para ser transmitidos en sistemas digitales. La técnica más sencilla es la modulación por impulsos codificados (PCM) la cual implica un muestreo periódico de los datos analógicos y una cuantización de las muestras.
- **Datos analógicos, señales analógicas**: los datos analógicos se modulan mediante una portadora para generar una señal analógica en una banda de frecuencias diferente, la cual se puede utilizar en un sistema de transmisión analógico. Las técnicas básicas son la modulación de amplitud (AM), la modulación de frecuencia (FM) y la modulación de fase (PM).

3.5.1 Datos digitales, señales digitales

La forma más frecuente y fácil de transmitir señales digitales es mediante la utilización de un nivel diferente de tensión para cada uno de los dos dígitos binarios. Los códigos que siguen esta estrategia comparten la propiedad de que el nivel de tensión se mantiene constante durante la duración del bit; es decir, no hay transiciones (no hay retorno al nivel cero de tensión). Por ejemplo, la ausencia de tensión se puede usar para representar un 0 binario, mientras que un nivel constante y positivo de tensión puede representar al 1. Este código se denomina no retorno a cero (NRZ, Non-return to Zero). Sin embargo, es más habitual usar un nivel negativo para representar un valor binario y una tensión positiva para representar al otro. Este último código se denomina **código no retorno a nivel cero** (NRZ-L, Nonreturn to Zero-Level). **NRZ-L** se usa generalmente para generar o interpretar los datos binarios en terminales y otros dispositivos.

Una variante del NRZ se denomina **NRZI (Noreturn to Zero, invert on ones)**. Al igual que NRZ-L, NRZI mantiene constante el nivel de tensión durante la duración de un bit. Los datos se codifican mediante la presencia o ausencia de una transición de la señal al principio del intervalo de duración del bit. Un 1 se codifica mediante la transición (bajo a alto o alto a bajo) al principio del intervalo de señalización, mientras que un cero se representa por la ausencia de transición.

Sus limitaciones (tanto NRZ-L como NRZI) hacen que estos códigos no sean atractivos para aplicaciones de transmisión de señales.

En el caso del esquema **bipolar-AMI**, un 0 binario se representa por ausencia de señal y 1 binario se representa como un pulso positivo o negativo. Los pulsos correspondientes a los deben tener una polaridad alternante. Este tipo de esquema tiene las siguientes ventajas. En primer lugar, no habrá problemas de sincronización en el caso de que haya una cadena larga de unos. Cada 1 fuerza una transición, por lo que el receptor se puede sincronizar en dicha transición. Una cadena larga de ceros sigue siendo un problema.

Los comentarios del párrafo anterior son también trasladables al código **pseudoternario**. En este caso, el bit 1 se representa por la ausencia de señal y el 0 mediante pulsos de polaridad alternante. No hay ninguna ventaja particular de esta codificación respecto de la anterior, siendo base de muchas aplicaciones.

La **codificación Manchester** es un método de codificación eléctrica de una señal binaria en el que en cada tiempo de bit hay una transición entre dos niveles de señal. Siempre hay una transición en mitad del intervalo de duración del bit.

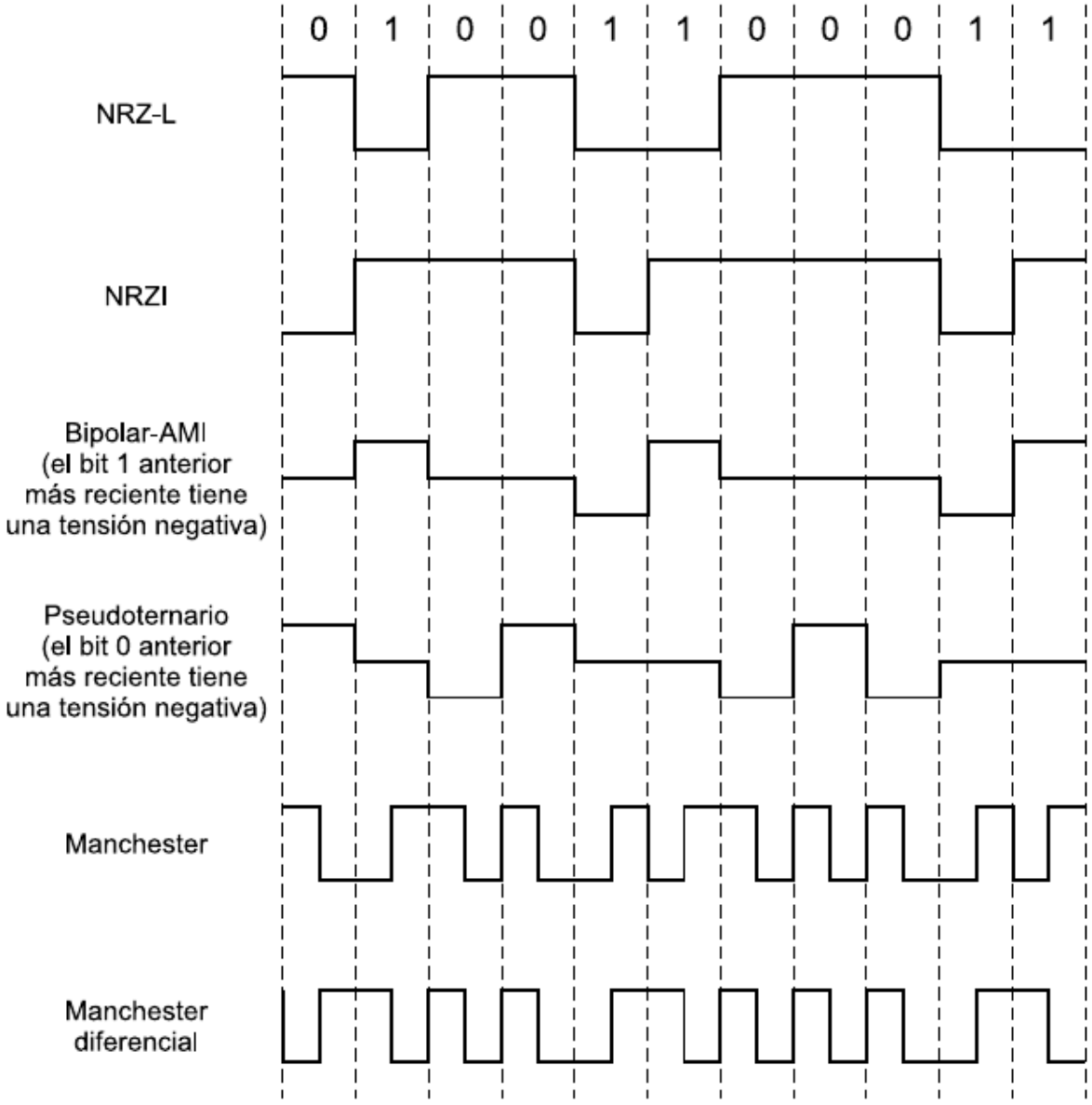


Figura 13: Datos digitales -> Señales digitales

Esta transición en la mitad del bit sirve como procedimiento de sincronización, a la vez que sirve para transmitir los datos: una transición de bajo a alto representa un 1 y una transición de alto a bajo representa un 0.

En **Manchester diferencial**, la transición a mitad del intervalo se utiliza tan sólo para proporcionar sincronización. La codificación de un 0 se representa por la presencia de una transición al principio del intervalo del bit, y un 1 se representa mediante la ausencia de una transición al principio del intervalo. El código Manchester diferencial tiene como ventajas adicionales las derivadas de la utilización de una aproximación diferencial.

Estos dos códigos se usan con frecuencia en los esquemas de transmisión de datos. Uno de los más conocidos es el código Manchester, elegido como parte de la especificación de la norma **IEEE 802.3 (Ethernet)** para la transmisión en redes LAN de cable coaxial en banda base o par trenzado con bus CSMA/CD. El Manchester diferencial se ha elegido en la norma **IEEE 802.5** para redes **LAN en anillo con paso de testigo**, en las que se usan pares trenzados apantallados.

3.5.2 Datos digitales, señales analógicas

La **modulación por desplazamiento de amplitud**, en inglés **Amplitude-Shift Keying (ASK)**, es una forma de modulación en la cual se representan los datos digitales como variaciones de amplitud de la onda portadora en función de los datos a enviar.

Tanto los procesos de modulación ASK como los procesos de demodulación son relativamente baratos. La técnica ASK es **usada comúnmente para transmitir datos digitales sobre la fibra óptica**. Para los transmisores LED, el valor binario 1 es representado por un pulso corto de luz y el valor binario 0 por la ausencia de luz. Los transmisores de láser normalmente tienen una corriente «de tendencia» fija que hace que el dispositivo emita un nivel bajo de luz. Este nivel bajo representa el valor 0, mientras una onda luminosa de amplitud más alta representa el valor binario 1.

La **modulación por desplazamiento de frecuencia o FSK (Frequency Shift Keying)** es una técnica de transmisión digital de información binaria (ceros y unos) utilizando dos frecuencias diferentes. La señal moduladora solo varía entre dos valores de tensión discretos formando un tren de pulsos donde un cero representa un «1» o «marca» y el otro representa el «0» o «espacio»

La **modulación por desplazamiento de fase o PSK (Phase Shift Keying)** es una forma de modulación angular que consiste en hacer variar la fase de la portadora entre un número de valores discretos.

3.5.3 Datos analógicos, señales digitales

A menudo tenemos datos analógicos (por ejemplo, la voz o cualquier tipo de audio) que es necesario digitalizar. Una de las primeras técnicas y de las más conocidas es la PCM.

La **modulación por impulsos codificados** (**PCM** por sus siglas inglesas de Pulse Code Modulation) es un procedimiento de modulación utilizado para transformar una señal analógica en una secuencia de bits (señal digital), este método fue inventado por Alec Reeves en 1937. Una trama o stream PCM es una representación digital de una señal analógica en donde la magnitud de la onda analógica es tomada en intervalos uniformes (muestras), cada muestra puede tomar un conjunto finito de valores, los cuales se encuentran codificados

El proceso de convertir una señal analógica en digital se lleva en 3 pasos:

- **Muestreo**: tomamos muestras de la señal cada cierto tiempo de forma periódica. Cuantas más muestras tomemos por segundo mayor calidad en sonido digital obtendremos. Por ejemplo, la musica almacenada en un CD de audio ha sido muestreada a 44,1 kHz, es decir se tomaron 44100 muestras en un segundo.
- **Cuantización**: cada muestra debe evaluarse dentro de una escala. Cuanto más valores tenga dicha escala, más calidad tendrán las muestras digitalizadas. En un CD las muestras se cuantifican en una escala de 65536 valores (16 bits)
- **Codificación**: El último paso es representar cada muestra en un bloque de bits. En el caso del CD, cada muestra está representada con 16 bits.

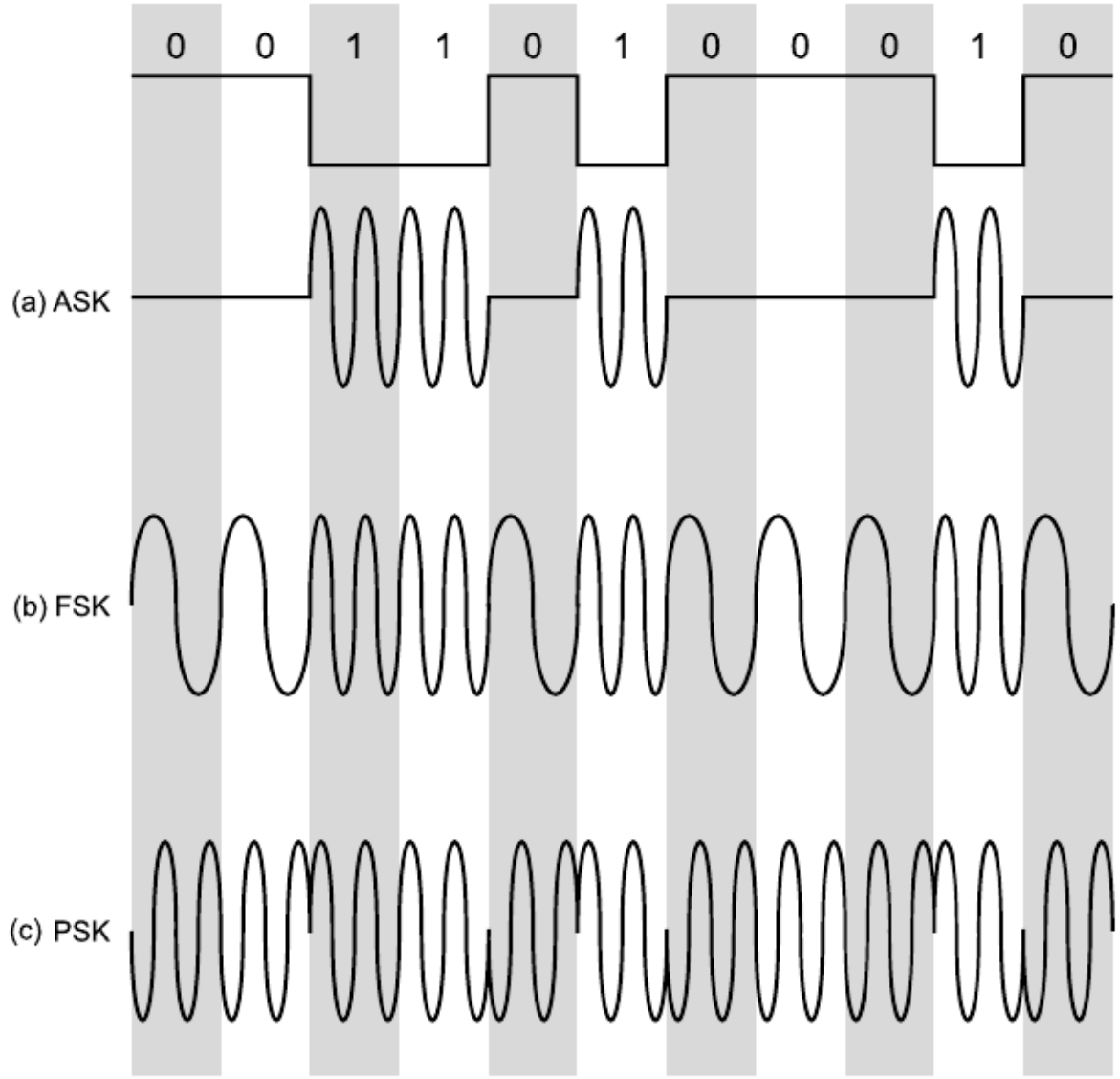


Figura 14: Datos digitales -> señales analógicas

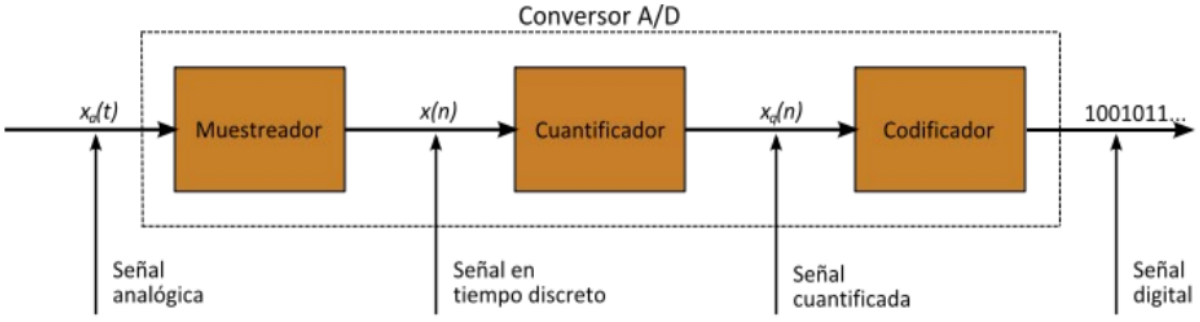


Figura 15: Conversor Analógico a Digital

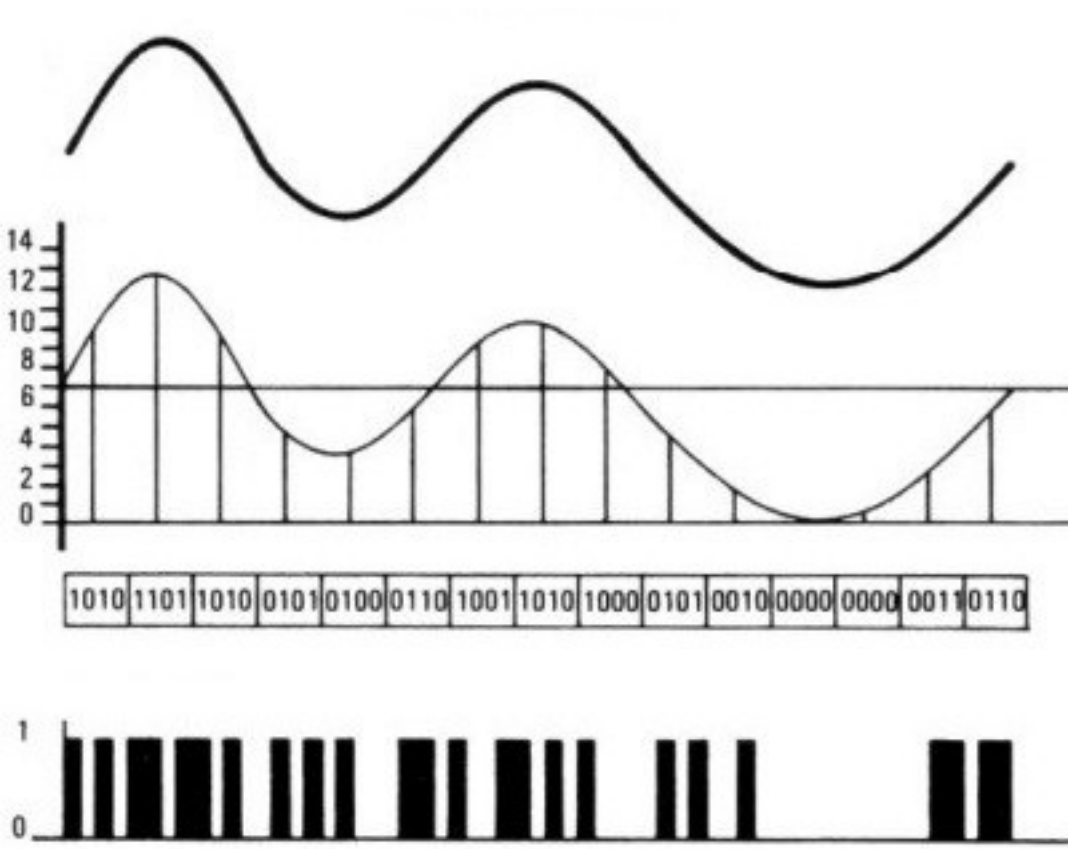


Figura 16: Proceso de digitalización de una onda analógica

En el gráfico superior, el muestreo esta indicado por las líneas verticales. Cada línea vertical indica el momento en el que tomamos la muestra. Si tuviesemos más líneas verticales más juntas, el número de muestras por cantidad de tiempo sería superior y la digitalización tendría mayor calidad.

La escala vertical indica los valores que pueden tomar las muestras. Si alguna muestra no coincide exactamente con un valor de la escala, entonces se aproxima al valor más cercano de la escala. Por ejemplo la primera muestra se ha redondeado a valor 10.

Por último, se codifica en binario dicho valor.

Suponiendo que el gráfico se refiera a una escala temporal de 1 segundo, en dicha digitalización hemos realizado un muestreo de 15Hz (15 muestras en un segundo) y una cuantización de 14 valores (aprox. 4 bits). Estos son valores tremendamente bajos para ser utilizados en casos reales pero el modelo está simplificado por motivos didácticos.

3.5.4 Datos analógicos, señales analógicas

La **modulación de amplitud (AM)** es una técnica utilizada en la comunicación electrónica, más comúnmente para la transmisión de información a través de una onda portadora de radio. La modulación en amplitud (AM) funciona mediante la variación de la amplitud de la señal transmitida en relación con la información que se envía.

Una gran ventaja de AM es que su demodulación es muy simple y, por consiguiente, los receptores son sencillos y baratos.

La AM es usada en la radiofonía, en las ondas medias, ondas cortas, e incluso en la VHF: es utilizada en las comunicaciones radiales entre los aviones y las torres de control de los aeropuertos.

La **frecuencia modulada (FM)** o modulación de frecuencia es una modulación angular que transmite información a través de una onda portadora variando su frecuencia. En aplicaciones analógicas, la frecuencia instantánea de la señal modulada es proporcional al valor instantáneo de la señal moduladora.

La frecuencia modulada es usada comúnmente en las radiofrecuencias de muy alta frecuencia por la alta fidelidad de la radiodifusión de la música y el habla (p. ej. Radio FM). El sonido de la televisión analógica también es difundido por medio de FM.

La **modulación de fase (PM)** que se caracteriza porque la fase de la onda portadora varía en forma directamente proporcional de acuerdo con la señal modulante. La modulación de fase no suele ser muy utilizada porque se requieren equipos de recepción más complejos que los de frecuencia modulada. El aspecto de las señales FM y PM es muy parecido. De hecho, es imposible diferenciarlas sin tener un conocimiento previo de la función de modulación.

3.6 Referencias

- Comunicaciones y redes de computadores. 7ª ed. Editorial Pearson-Prentice-Hall.
- Redes de computadoras. 4ª ed. Editorial Pearson-Prentice-Hall.

3.7 Actividades

1. ¿Qué diferencia hay entre un amplificador y un repetidor?
2. Según los sentido que pueda tomar una transmisión, ésta se clasifica en . . .
3. ¿En qué consiste la multiplexación y que tipos existen?
4. **Define los siguientes términos:**
    - Atenuación

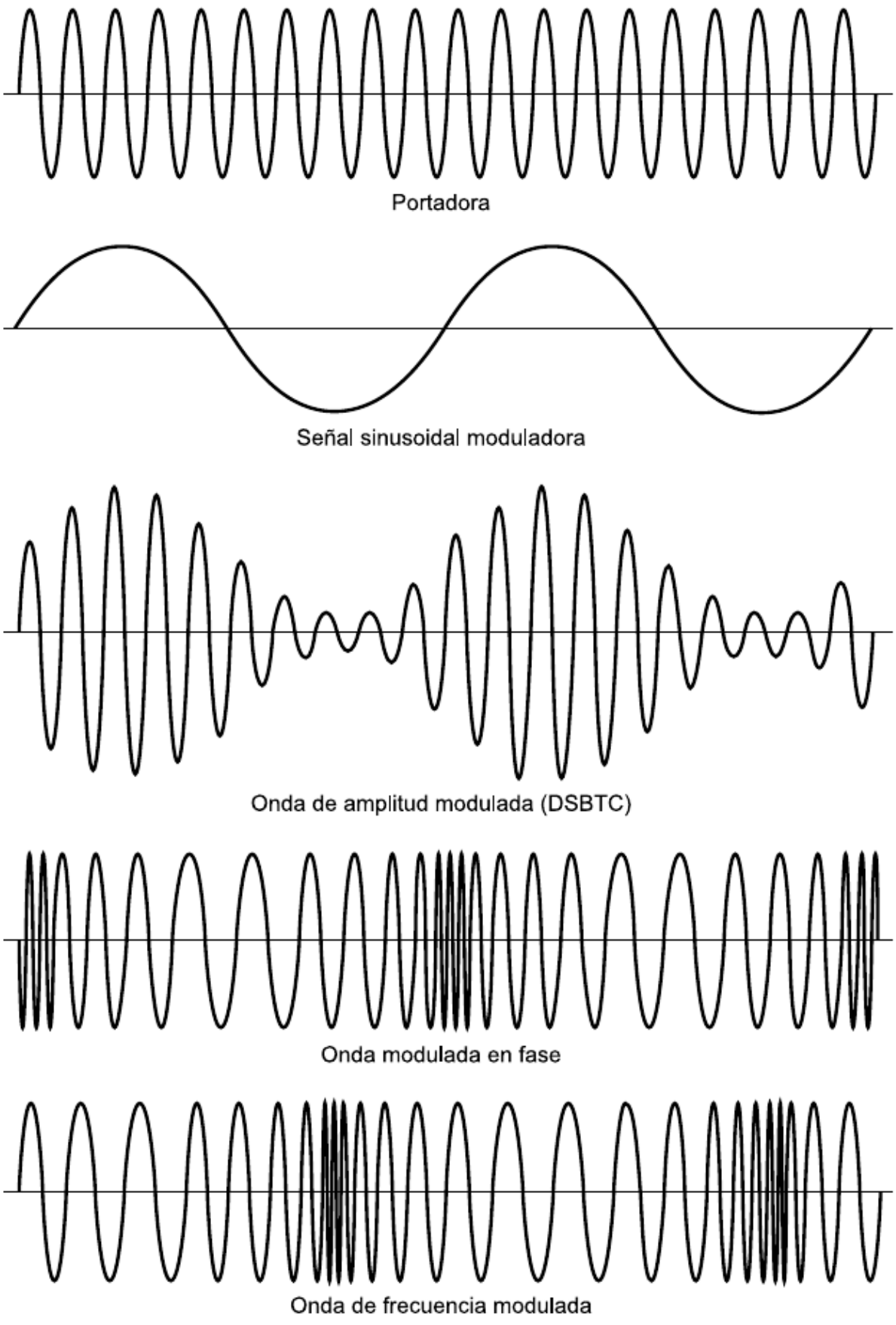


Figura 17: Datos analógicos -> Señales analógicas

- Diafonía
- Ruido térmico
- Ruido impulsivo

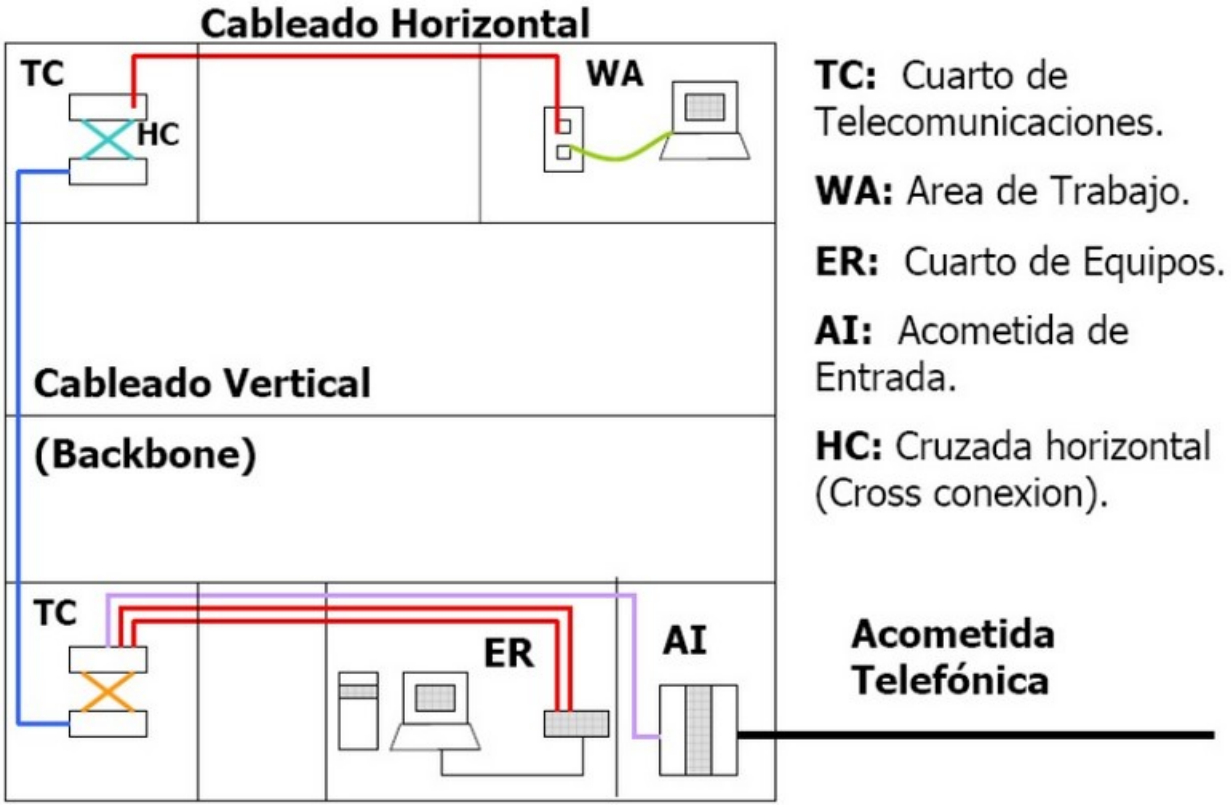
5. ¿Qué tipos de cables de pares trenzados existen atendiendo a su protección frente a interferencias y ruido?
6. Haz una tabla donde se indique la clase, categoría y ancho de banda para los pares trenzados desde la categoría 3 en adelante.
7. ¿Qué código de colores se utilizan en las normas T568A y T568B?
8. Busca información acerca de los distintos conectores RJ ((Registered Jack) que podemos encontrarnos.
9. ¿Qué tipo de cable utilizan las redes 10BASE2 y 10BASE5? ¿Qué otro nombre reciben estas redes?
10. ¿Qué ventajas tiene la fibra óptica sobre el par trenzado y el coaxial?
11. Indica los 3 tipos de fibras ópticas que existen y resume las características de cada una de ellas.
12. Además de la fibra óptica de vidrio existe también una fibra óptica de plástico (**POF**, en sus siglas en inglés). Busca información acerca de sus características y aplicaciones. Busca además 2 empresas que trabajen con ella.
13. Entra en la web submarinecablemap y encuentra
    - un cable que conecte la península ibérica con sudamérica
    - un cable que conecte Reino Unido con Japón
    - un cable que conecte Reino Unido con Alaska

    Para cada uno indica el nombre que recibe y su longitud.
14. ¿Qué se entiende por microondas?
15. ¿Qué se entiende por transmisión direccional y omnidireccional?
16. ¿Qué frecuencias utiliza la comunicaciones Wifi y Bluetooth?
17. ¿Cómo se denominan las órbitas donde se sitúan los satélite de comunicaciones?
18. ¿Qué órbitas utilizan los satélites de Hispasat e Iridium?
19. ¿En qué redes se usaba la codificación Manchester y Manchester diferencial?
20. En fibra óptica, ¿qué codificación se utiliza?

CAPÍTULO 4

SISTEMAS DE CABLEADO ESTRUCTURADO

4.1 Introducción



Un **Sistema de Cableado estructurado** (**SCE**. En inglés, Structured Cabling System - SCS) es un conjunto de productos de cableado, conectores, y equipos de comunicación que integran los servicios de voz, datos y video en conjunto

con sistema de administración dentro de una edificación tales como los sistemas de alarmas, seguridad de acceso y sistemas de energía, etc). En resumen **es un cableado para todos los servicios que implican información y control en una edificación**.

SCE es una metodología, basada en estándares, de diseñar e instalar un sistema de cableado que integra la transmisión de voz, datos y vídeo. Un SCE propiamente diseñado e instalado proporciona una infraestructura de cableado que suministra un desempeño predefinido y la flexibilidad de acomodar futuros crecimientos por un período extendido de tiempo.

En definitiva, Cableado Estructurado es el cableado de un edificio o una serie de edificios que permite interconectar equipos activos, de diferentes o igual tecnología permitiendo la integración de los diferentes servicios que dependen del tendido de cables como datos, telefonía , control, etc.

El objetivo fundamental es cubrir las necesidades de los usuarios durante la vida útil del edificio sin necesidad de realizar más tendido de cables.

Problemas que resuelve:

- Cambios en los edificios, en la distribución de puestos de trabajo, etc.
- No solamente servicios de datos y telefonía, sino video, alarmas, climatización, control de acceso, etc.
- Unificar tendido de cables.
- Cambios en la tecnología de los equipos de Telecomunicaciones

4.1.1 Espacios

- Acometida de red
- Cuartos de telecomunicaciones o cuartos de equipamiento
- Áreas de trabajo

4.1.2 Elementos pasivos

- Cableado
- Rosetas (TO – Telecommunications Outlets)
- Paneles de parcheo (Patch panels)
- Armarios (Racks)

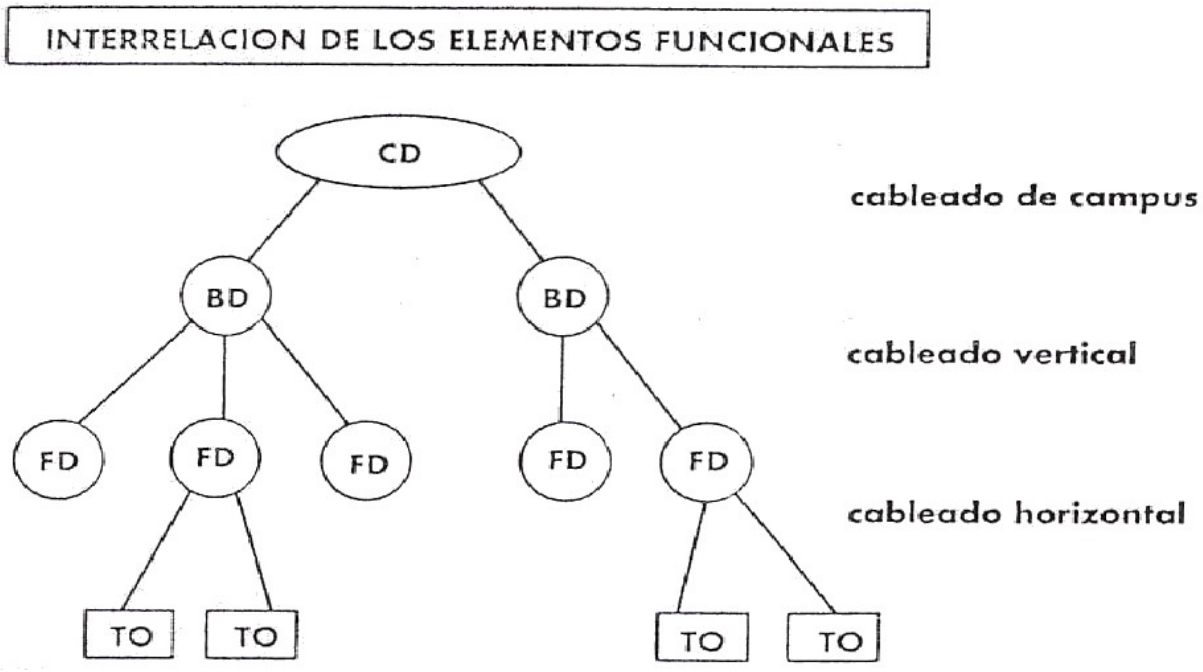
4.1.3 Elementos activos

- Puntos de acceso inalámbricos
- Conmutadores (switches)
- Enrutadores (routers)
- Cortafuegos (firewalls)
- Servidores (servers)

4.1.4 Distribuidores

- Distribuidor de Campus (CD – Campus Distributor)
- Distribuidor de Edificio (BD – Building Distributor)
- Distribuidor de Planta (FD – Floor Distributor)

4.1.5 Subsistemas de cableado



- Subsistema de cableado troncal de campus
- Subsistema de cableado troncal vertical
- Subsistema de cableado horizontal

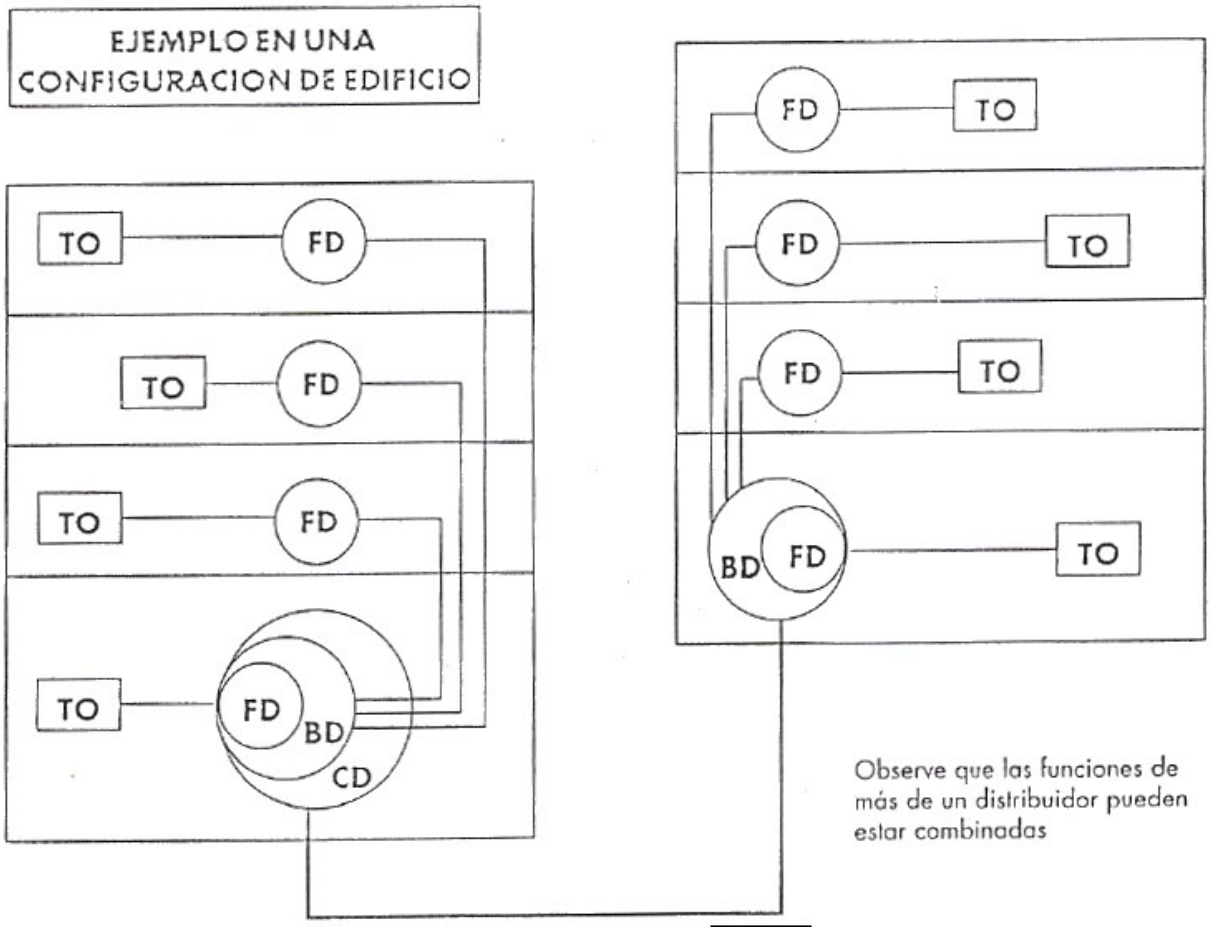
Otro cableado es:

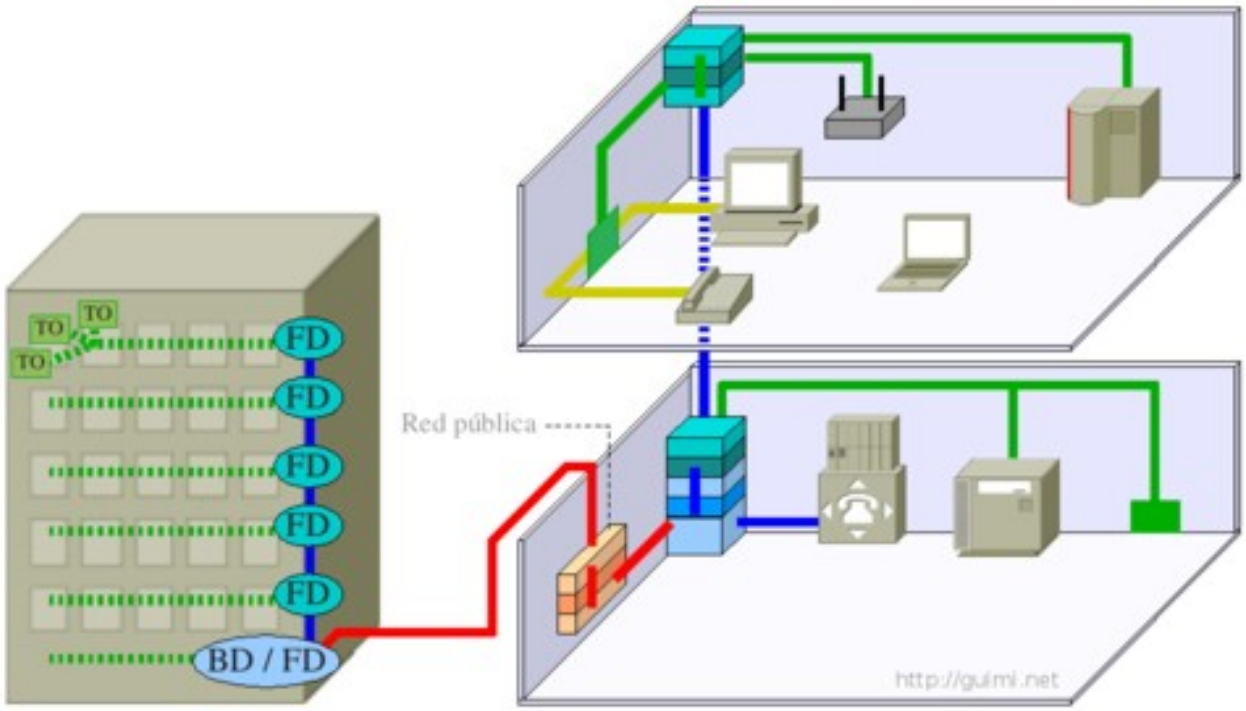
- Cables de usuario
- Cables de interconexión
- Cables o latiguillos de parcheo (patch cords)

4.1.6 Normativa

Para edificios de oficinas existen unas normas que establecen la forma de hacer el cableado. El cableado realizado según esas normas se denomina cableado estructurado, y permite integrar distintas tecnologías y servicios de red (voz, audio, vídeo, datos). Las ventajas de seguir estas normas están en la sencillez de gestión y mantenimiento, robustez y flexibilidad ya que la mayoría de las tecnologías de red local funcionan sobre cableado estructurado. Esas normas son la **TIA/EIA-568, la ISO/IEC 11801, la EN 50173 y la UNE EN 50173**

La norma **TIA/EIA-568B** es de ámbito estadounidense y clasifica componentes en **categorías** (cables, conectores, repartidores, módulos, tendidos, interfaces, etc.). La norma **ISO/IEC 11801** es de ámbito internacional y clasifica


EJEMPLO EN UNA
CONFIGURACION DE EDIFICIO
TO
FD
BD
CD
Observe que las funciones de
más de un distribuidor pueden
estar combinadas


TO
FD
BD / FD
Red pública
http://guimi.net

enlaces permanentes en **clases**, para los componentes individuales se basa en la norma TIA/EIA. En el año 2002 se publicaron las últimas versiones de ambas normas. Las dos normativas (TIA/EIA-568B e ISO/IEC 11801) coinciden bastante en la clasificación de las diversas categorías de cableado.

La norma europea **EN 50173 1** (la versión española es la UNE-EN 50173) se basa en la norma ISO 11801.

Cuando se diseña un cableado es conveniente cumplir todas las normativas simultáneamente, instalando componentes según su categoría y certificando los enlaces realizados según su clase, ya que de esta forma se asegura una máxima compatibilidad con todos los fabricantes y sistemas. Hay que tener en cuenta que por un lado una mala instalación realizada con buenos componentes quizá no pueda certificarse, y por otro lado es más fácil asegurar la calidad de una instalación utilizando componentes certificados.

EPHOS 2 (European Procurement Handbook for Open Systems - Phase 2) recuerda que desde 1986 se "obliga a todos los responsables de contrataciones públicas (...) a hacer referencia a estándares o preestándares europeos o internacionales". Es decir se obliga a cumplir las normas EN 50173 1, ISO 11801, ISO 802.x... y cumplir una serie de requisitos de Compatibilidad Electromagnética (CEM), protección de incendios, número de zócalos...

Nota: ISO 11801 está orientada a distancias de hasta 3.000 m., espacios de hasta 1.000.000 m^2 y entre 50 y 50.000 usuarios.

Una instalación de cableado estructurado debe servir a largo plazo, por diez años o más.

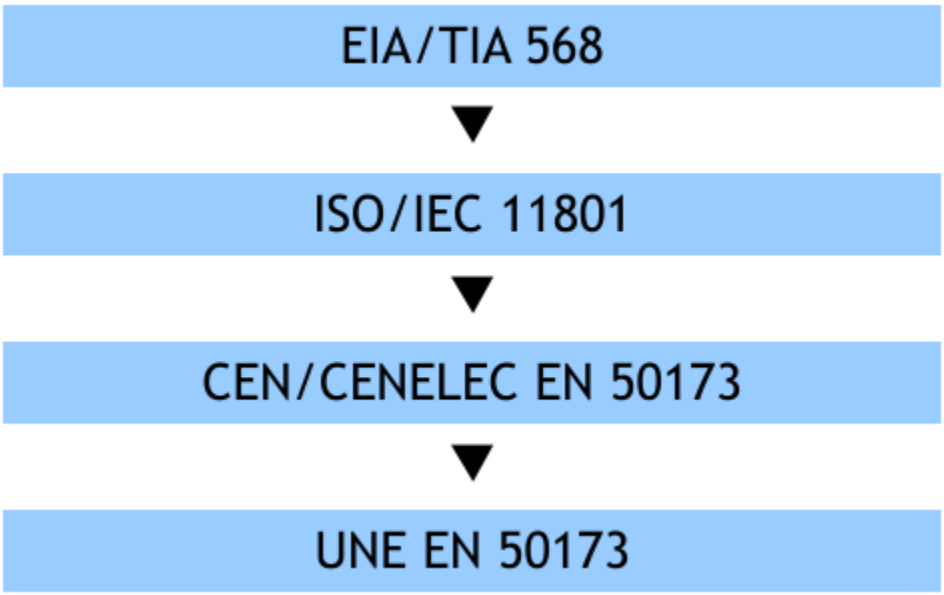


Figura 1: Evolución de la normativa de los SCE

Normativa estadounidense

Los estadounidenses fueron los primeros en publicar un estándar para la estructuración y diseño de los SCE. Las organizaciones encargadas de llevar a cabo esta tarea fueron la TIA y la EIA. El estándar se publicó en 1991 bajo el nombre de **EIA/TIA 568** (Commercial building wiring standard) y su propósito era definir y especificar los tipos de cables y conectores, las arquitecturas técnicas básicas y los métodos de verificación de cables, conectores e instalaciones para los SCE de los edificios comerciales**.

Con el tiempo el estándar fue mejorado, actualizado y ratificado por la ANSI, dando lugar, en 1995, al **ANSI/TIA/EIA 568-A**. Este a su vez, fue reemplazado en 2001 por el **ANSI/TIA/EIA 568-B**, vigente en la actualidad aunque ya está

empezando a ser reemplazado en parte por el nuevo estándar en desarrollo **ANSI/TIA 568-C**.

La normativa aplicable a SCE es:

- ANSI/TIA/EIA 568-B

  Cableado de Telecomunicaciones en Edificios Comerciales. (Cómo instalar el Cableado)

  - TIA/EIA 568-B1 Requerimientos generales
  - TIA/EIA 568-B2 Componentes de cableado mediante par trenzado balanceado
  - TIA/EIA 568-B3 Componentes de cableado, Fibra óptica

- ANSI/TIA/EIA 569-A y B

  Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales (Cómo disponer el cableado)

- ANSI/TIA/EIA 570-A y B

  Normas de Infraestructura Residencial de Telecomunicaciones

- ANSI/TIA/EIA 598-A

  Define los códigos de colores para la fibra óptica.

- ANSI/TIA/EIA 606-A

  Normas de Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales

- ANSI/TIA/EIA 607

  Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales.

- ANSI/TIA/EIA 758

  Norma Cliente-Propietario de cableado de Planta Externa de Telecomunicaciones.

Normativa internacional

El principal organismo internacional encargado de desarrollar estándares para el cableado estructurado es la organización ISO/IEC, que en 1994 publicó su estándar ISO/IEC 11801 (Information technology. Generic cabling for customer premises), basado en el EIA/TIA 568 pero con algunas diferencias, como la clasificación y definición de los tipos de cables y de los elementos funcionales de los SCE. Este estándar se revisa constantemente para introducir actualizaciones y mejoras; actualmente se encuentra en la versión 2.2.

Aunque el ISO/IEC 11801 es el estándar internacional más importante relacionado con los SCE, existen muchos más que regulan diferentes aspectos relacionados con los SCE que no aparecen en el ISO/IEC 11801. Es de destacar, por su relación con este módulo, el **ISO/IEC 14763** (Information technology. Implementation and operation of customer premises cabling), que se divide en 3 partes:

- 14763-1: administración de redes locales.
- 14763-2: planificación e instalación
- 14763-3: pruebas a realizar en el cableado de fibra óptica.

Normativa europea

La normativa europea para el cableado estructurado la desarrolla, principalmente, la organización CEN/CENELEC y está basada en los estandares internacionales.

La adaptación del estándar ISO/IEC 11801 a la normativa europea es el estándar **EN 50173** (Information technology. Perfomance requirements of generic cabling schemes), actualmente dividido en 5 partes:

- 50173-1: requisitos generales de las instalaciones locales.
- 50173-2: requisitos generales de las instalaciones de oficinas.
- 50173-3: requisitos generales de las instalaciones industriales.
- 50173-4: requisitos generales de las viviendas.
- 50173-5: requisitos generales de los centros de datos.

Otros estándares europeos importantes sobre el cableado estructurado son:

- EN 50174

  Procedimientos de especificación y aseguramiento de la calidad (50174-1) Planificación y prácticas de instalación en el interior (50174-2) Planificación y prácticas de instalación en el exterior (50174-3)

- EN 50346

  Prueba del cableado instalado

- EN 50310

  Aplicación de la unión equipotencial y de la puesta a tierra.

La normativa europea sobre los SCE es de obligado cumplimiento en todos los países de la Unión Europea.

Normativa española

La normativa española se basa en los estándares europeos EN publicados por la CEN/CENELEC. La adaptación de los estándares EN a la normativa española la lleva a cabo AENOR y su resultado son los estándares UNE EN.

Normativa aplicable:

4.1.7 Cableado

Las principales diferencias de rendimiento entre los distintos tipos de cables radican en la anchura de banda permitida (y consecuentemente en el rendimiento máximo de transmisión), su grado de inmunidad frente a interferencias electromagnéticas y la relación entre la pérdida de la señal y la distancia recorrida (atenuación).

En la actualidad existen básicamente tres tipos de cables factibles de ser utilizados para el cableado en el interior de edificios o entre edificios:

- Par Trenzado
- Coaxial (No se recomienda para instalaciones nuevas, excepto redes de TV y CATV)
- Fibra Óptica

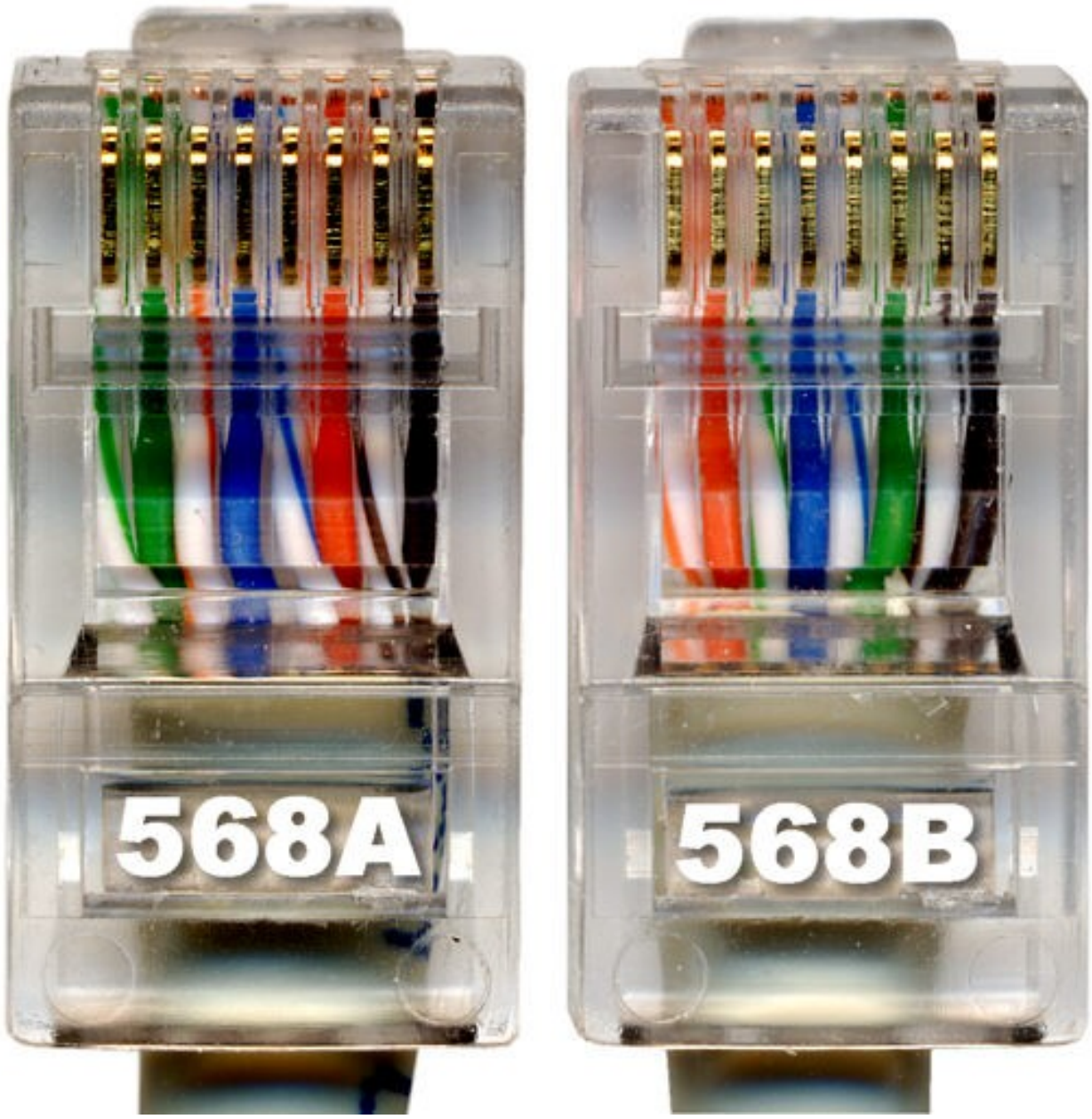
Par trenzado

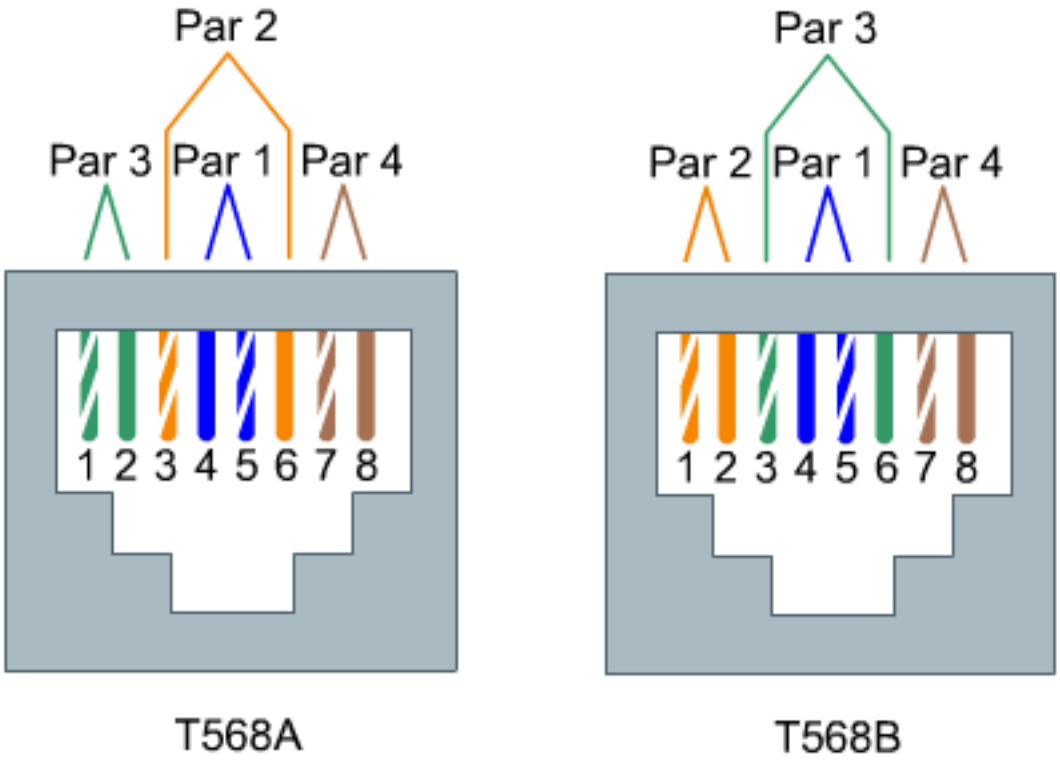
Es actualmente el tipo de cable más común en redes de área local.

La clasificación en categorías, además de aplicarse a un cable aislado se aplica a instalaciones ya hechas. Algunos errores comunes son por ejemplo destrenzar una longitud excesiva en los conectores, apretar demasiado las bridas o doblar excesivamente el cable.

Este tipo de cable soporta: Redes de Área Local ISO 8802.3 (Ethernet) e ISO 8802.5 (Token Ring); Telefonía analógica y digital; Líneas de control y alarmas; Alimentación eléctrica (PoE: Power over Ethernet)...


Diseño del edificio
UNE EN 50310
Diseño del SCE
UNE EN 50173-1
Planificación del SCE
UNE EN 50174-1
UNE EN 50174-2
UNE EN 50174-3
UNE EN 50310
Implementación del SCE
UNE EN 50174-1
UNE EN 50174-2
UNE EN 50174-3
UNE EN 50310
UNE EN 50346
Gestión del SCE en funcionamiento
UNE EN 50174-1


568A
568B


Par 2
Par 3
Par 1
Par 4
1 2 3 4 5 6 7 8
T568A
Par 3
Par 2
Par 1
Par 4
1 2 3 4 5 6 7 8
T568B

En telefonía se usa el par 1; Ethernet (10/100) pares 2 y 3; Gigabit Ethernet todos; Token Ring pares 1 y 3; FDDI, ATM y TP-PMD pares 2 y 4.Ethernet es compatible con el uso para alimentar eléctricamente aparatos (PoE: Power over Ethernet).

- Cable paralelo Ethernet: usar la misma normativa en los dos extremos.
- Cable cruzado Ethernet (10/100): usar una normativa en cada extremo.
- Cable cruzado Gigabit Ethernet (10/100/1000): usar una normativa en un extremo y en el otro extremo usar la otra normativa pero cruzando además los pares 1 y 4.

Cable cruzado Gigabit Ethernet (10/100/1000) Opción 1

T568A	T568B mod.
1-	1-
2-	2-
3-	3-
4-	4-
5-	5-
6-	6-
7-	7-
8-	8-

Cable cruzado Gigabit Ethernet (10/100/1000) Opción 2

T568B	T568A mod.
1-	1-
2-	2-
3-	3-
4-	4-
5-	5-
6-	6-
7-	7-
8-	8-

El estándar ISO/IEC 11801, en su edición del año 2002, define varias clases de interconexiones de par trenzado de cobre, que difieren en la frecuencia máxima para la que se requiere un cierto rendimiento de canal :

- **Clase A** : hasta 100 kHz utilizando elementos de la categoría 1
- **Clase B** : hasta 1 MHz utilizando elementos de la categoría 2
- **Clase C** : hasta 16 MHz usando elementos de la categoría 3
- **Clase D** : hasta 100 MHz utilizando elementos de categoría 5e
- **Clase E** : hasta 250 MHz utilizando elementos de la categoría 6
- **Clase E :sub:A** : hasta 500 MHz utilizando elementos categoría 6A (enmienda 1 y 2 de la norma ISO / IEC 11801, 2 ª ed .)
- **Clase F** : hasta 600 MHz con categoría de elementos 7
- **Clase F :sub:A** : hasta 1000 MHz utilizando elementos categoría 7A (enmienda 1 y 2 de la norma ISO / IEC 11801 , 2 ª Ed.)

La impedancia de enlace estándar es de 100 Ω .

Conectores

- **8P8C: RJ-45 (UTP), RJ-49 (FTP, STP, SSTP)**
- GG45

- TERA

Figura 2: 8P8C: RJ-45 y RJ-49

La clase F se puede terminar ya sea con conectores eléctricos GG45 compatibles con 8P8C que incorporan el estándar 8P8C o con conectores TERA. En noviembre de 2010, todos los fabricantes de equipos activos han optado por apoyar el 8P8C para sus productos 10 Gigabit Ethernet sobre cobre y no el GG45 o TERA.

Los conectores GG45, estandarizados en 2001 como IEC 60603-7-7, proporcionan compatibilidad con versiones anteriores para conectores con el estándar 8P8C en una interfaz de cable de categoría 6 (modo 1), donde se utilizan ocho conductores para la operación en categoría 6 (100/ 250 MHz).

Además, el GG45 tiene cuatro conductores adicionales en las esquinas extremas que soportan la interfaz de alta velocidad de categoría 7 (600 MHz) y Cat 7a (1000MHz) . Los 4 conductores adicionales están conectados a 2 pares mientras que los otros 2 pares trenzados permanecen conectados a los pines más distantes del conector original de 8P8C : 1 y 2 , y 7 y 8. Un conector de categoría 6 o 6A utiliza las posiciones de contacto originales , pero un conector de categoría 7 o 7A en su lugar utiliza los contactos situados en las cuatro esquinas y tiene un saliente que activa un interruptor dentro de la toma de las posiciones de contacto alternativas. Esto reduce la diafonía dentro del conector a la que el aumento de la velocidad de datos es sensible.

TERA es un conector para su uso con cables de datos de par trenzado blindado de categoría 7, desarrollado por la compañia Siemen y estandarizado en 2003 por la Comisión Electrotécnica Internacional (IEC) 61076-3-104. La revisión de la norma de 2006 amplió el desempeño caracterizado hasta 1000 MHz. El conector tiene un tamaño diferente del conector 8P8C más común.

TERA es también una interfaz útil para la tecnología de las comunicaciones broadcast. Este conector permite el uso compartido de cable, lo que permite a los usuarios integrar servicios de video, voz y datos a través de un único enlace de cableado.

Recomendaciones con el par trenzado

Cable coaxial

Originalmente fue el cable más utilizado en las redes locales debido a su alta capacidad y resistencia a las interferencias, pero en la actualidad su uso está en declive.

Figura 3: GG45

Figura 4: TERA

- Cuando se desenrolle el cable se procurará no cortarlo demasiado justo, y deberá utilizarse el cable desenrollado

Desenrolle el cable en un stand o soporte

No desenrolle sin soporte

El diámetro interior del enrollado deberá ser como mínimo 1 m

- Evite someter el cable a excesivas torsiones

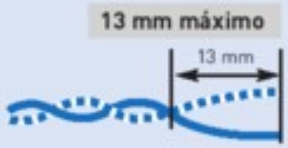
- Cuando fije el cable coloque los collarines sin apretarlos, evite que el cable se comprima

Asegúrese permitiendo un leve movimiento de los cables

Si lo asegura con fuerza, el cable queda aplastado

- Nunca pise los cables o coloque objetos pesados encima

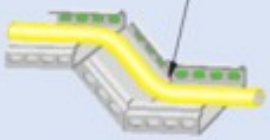
- Es necesario limitar el destrenzado de los conductores a 13 mm como máximo para evitar el fenómeno de la paradiafonía



Destrenzado de los conductores

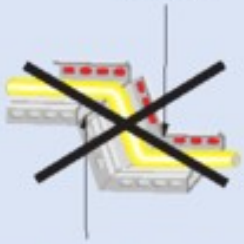
- El radio de curvatura mínimo es 8 veces el diámetro exterior del cable en FTP y 4 veces en UTP

Radio de curvatura adecuado



Cable instalado con un adecuado radio de curvatura

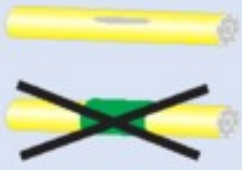
Radio de curvatura pequeño



Evitar apretar en las esquinas

Radio de curvatura pequeño: no protegido contra objetos cortantes

- Si la cubierta del cable está deteriorada, no lo repare; reemplace el cable

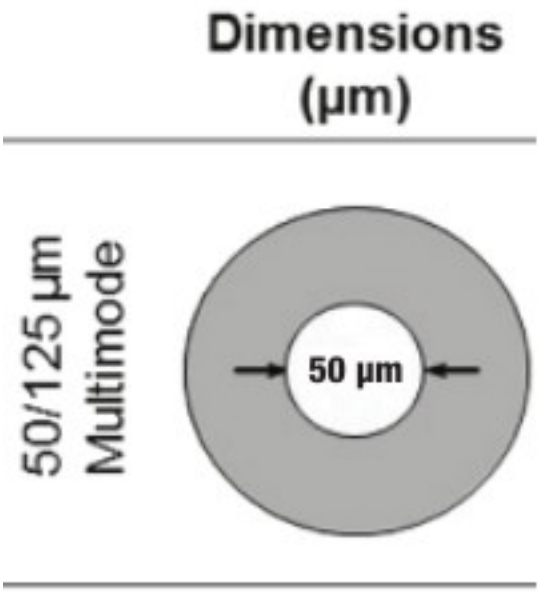


Fibra óptica

La fibra óptica es un medio excelente para la transmisión de información por sus **características**: gran ancho de banda, baja atenuación de la señal que permite cubrir grandes distancias sin repetidores, integridad -proporción de errores baja (BER: Bit Error Rate)-, inmunidad a interferencias electromagnéticas, alta seguridad y larga duración -resistente a la corrosión y altas temperaturas-.

Sus mayores **desventajas** son su coste de producción -superior al resto de los tipos de cable- y su fragilidad durante el manejo en producción.

La terminación de los cables de fibra óptica requiere un tratamiento especial para convertir la señal óptica en eléctrica que ocasiona un aumento de los costes de instalación ("**optoelectrónica**").



La luz normalmente es emitida por un diodo de inyección láser (ILD: Injection Laser Diode) o un diodo de emisión de luz (LED: Light-Emitting Diode). Los ILDs emiten luz coherente, es decir un único rayo de luz, por tanto cada pulso de luz se propaga a través de la fibra en un solo modo, sin dispersión, y se utilizan con fibras monomodo.

Los **LEDs** generan luz normal no coherente, es decir cada pulso de luz genera múltiples rayos de luz que se propagan en diferentes modos con dispersión -por lo que **no se puede usar en grandes distancias**- y se utilizan con fibras multimodo.

El equipamiento basado en fibra monomodo e **ILDs** proporciona un gran ancho de banda y una baja atenuación con la distancia, por lo que se utiliza para transmitir a grandes velocidades y/o **a grandes distancias**. En cambio el equipamiento basado en fibra multimodo y LEDs resulta más económico y sencillo de implantar.

El vidrio no absorbe igual todas las longitudes de onda, es decir

no es igual de "transparente" a todos los colores. En particular las longitudes de onda de menor atenuación se encuentran situadas alrededor de los 850 (multimodo), 1310 (multimodo y monomodo) y 1550 (monomodo) nm y se conocen como **primera, segunda y tercera ventana**, respectivamente. Todas las ventanas se encuentran en la zona infrarroja del espectro (la parte visible se encuentra entre 400 y 760 nm). Las ventanas que se encuentran a mayores longitudes de onda tienen menor atenuación; sin embargo la menor atenuación va acompañada de un mayor costo de la optoelectrónica necesaria.

La transmisión por una fibra óptica normalmente es simplex; **para conseguir comunicación full-duplex es necesario instalar dos fibras, una para cada sentido**.

En redes locales se utilizan principalmente fibras multimodo con emisores LED de primera o segunda ventana. Estos equipos son más baratos que los láser, tienen una vida más larga, son menos sensibles a los cambios de temperatura y más seguros. A muy altas velocidades es necesario utilizar emisores láser ya que los emisores de luz normal no pueden reaccionar con la rapidez suficiente, por eso en algunas redes locales (Gigabit Ethernet, Fibre Channel y ATM) se utilizan emisores láser de primera ventana cuando se quiere gran velocidad pero no se requiere gran alcance.

Dado que los cableados de red local no disponen normalmente de fibra monomodo se ha extendido en los últimos años el uso de emisores láser en fibra multimodo, principalmente para Fibre Channel y Gigabit Ethernet.

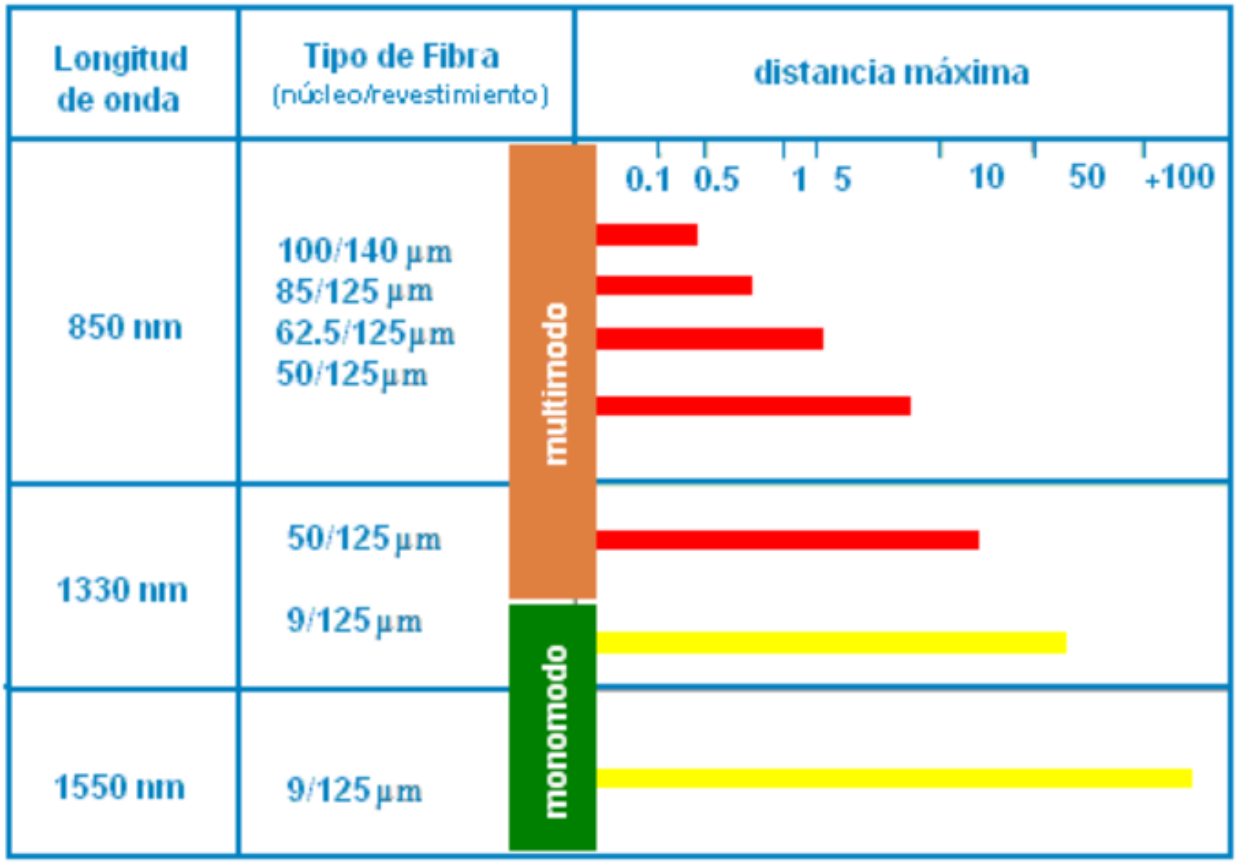
En redes de área extensa siempre se utiliza fibra monomodo y emisores láser. Actualmente en segunda ventana se puede llegar a distancias de 40 Km y en tercera hasta 160 Km sin amplificadores intermedios. El mayor costo de los emisores se ve en este caso sobradamente compensado por la reducción en equipos intermedios (amplificadores y regeneradores de la señal).

En las fibras se especifican indicando el diámetro del núcleo y el de la cubierta; las fibras multimodo típicas son de 50/125 µm y 62,5/125 µm; las fibras monomodo suelen ser de 9/125 µm, es decir el núcleo es mucho más estrecho puesto que el haz no se dispersa.

El estándar ISO/IEC 11801, en su edición del año 2002, define varias clases de interconexión de fibra óptica :

- **OM1** : multimodo con núcleo de 62.5 µm; ancho de banda modal mínimo de 200 MHz * km a 850 nm
- **OM2** : multimodo con núcleo de 50 µm; ancho de banda modal mínimo de 500 MHz * km a 850 nm
- **OM3** : multimodo con núcleo de 50 µm; el ancho de banda modal mínimo de 2000 MHz * km a 850 nm
- **OM4** : multimodo con núcleo de 50 µm; ancho de banda modal mínimo de 4700 MHz * km a 850 nm
- **OS1** : monomodo con atenuación de 1db/km
- **OS2** : monomodo con atenuación de 0.4db/km

Distancias soportadas



Código de colores de los cables de fibra local

Tipo de fibra / Clase	Diámetro (µm)	Color del revestimiento
Multimodo 1a	50/125	Naranja
Multimodo 1a	62.5/125	Pizarra
Multimodo 1a	85/125	Azul
Multimodo 1a	100/140	Verde
Monomodo IVa	Todo	Amarillo
Monomodo IVb	Todo	Rojo

Código de colores para cables multi-fibra

Las fibras individuales en un cable de múltiples fibras a menudo se distinguen una de otra por cubiertas con código de color o tampones en cada fibra. EIA/TIA-598 define esquemas de identificación de fibras, fibras tamponadas, unidades de fibra, y los grupos de unidades de fibra dentro de la planta exterior y cables de fibras ópticas locales. Esta norma permite a las unidades de fibra que se identifiquen por medio de una leyenda impresa. Este método se puede utilizar para la identificación de cintas de fibra y subunidades de fibra. La leyenda contendrá un número correspondiente impreso numérica posición y / o el color para su uso en la identificación.

Interconexión de fibra óptica

Código de color de la fibra óptica para Cubiertas (TIA/EIA-598)

MaxCap-BB-OM3/OM4
400, 800, LSZH, 525, 825, LSZH25, todas las series de interconexión, riser, plenum y LSZH

MMF - 62.5/50µm, OM1/OM2+
400, 800, LSZH, 525, 825, LSZH25, todas las series de interconexión, riser, plenum y LSZH

Monomodo mejorado incluyendo BB-XS
400, 800, LSZH, 525, 825, LSZH25, todas las series de interconexión, riser, plenum y LSZH

Híbrido
400, 800, LSZH, 525, 825, LSZH25, todas las cables interiores-exteriores y cables de planta exterior independientemente del tipo de fibra

Posición	Color de la cubierta	Posición	Color de la cubierta
1	azul	13	azul / negro
2	naranja	14	naranja / negro
3	verde	15	verde / negro
4	marrón	16	marrón / negro
5	pizarra	17	pizarra / negro
6	blanco	18	blanco / negro
7	rojo	19	rojo / negro
8	negro	20	negro / amarillo
9	amarillo	21	amarillo / negro
10	violeta	22	violeta / negro
11	rosa	23	rosa / negro
12	agua	24	agua / negro


Código de color de la fibra óptica para
Tubo holgado, Tubo estrecho(TIA/EIA-598)
Posición
Colores
1
Azul
2
Anaranjado
3
Verde
4
Café
5
Plateado (Gris)
6
Blanco
7
Rojo
8
Negro
9
Amarillo
10
Violeta
11
Rosa (Rosado)
12
Aqua (Celeste)

Para la interconexión de fibras ópticas se utilizan conectores, adaptadores y soldaduras. Los conectores y adaptadores ofrecen máxima versatilidad pero introducen una pérdida de la señal de 0,5 a 0,75 dB aproximadamente (un 10 %). La soldadura o fusión tiene una pérdida de señal muy pequeña, pero ha de llevarla a cabo un técnico especializado con equipo altamente sofisticado.

Adaptadores

FC-FC

ST-ST

SC-SC

LC a FC

SC a ST

Un adaptador es básicamente un puente, es decir una transición mecánica necesaria para dar continuidad al paso de luz del extremo de un cable de fibra óptica a otro. Existen adaptadores "híbridos"", que permiten acoplar dos diseños distintos de conector.

Conectores

En el pasado el conector ST se ha utilizado habitualmente en redes de datos con fibras multimodo. Actualmente el estándar ISO 11801 impone para las nuevas instalaciones el uso de SC Duplex (SC-D) -usado habitualmente en telefonía- pues mantiene la polaridad. Otro conector que se ha utilizado bastante en telefonía es el FC.

Conector FC

El conector FC se utiliza ampliamente en el mercado de las telecomunicaciones, donde los **cables de fibra óptica monomodo largos** pueden funcionarmás de 50 kilómetros. En estas situaciones extremas, el conector necesita tener pérdidas muy bajas y la geometría precisa.

Conector ST

Estructura:

1. **Ferrule**, debe albergar la fibra y alienarla. La calidad del ferrule es determinante para lograr que la fibra esté correctamente centrada y se logre la mejor conexión posible. El ferrule en conectores ST tiene un diámetro


AMP

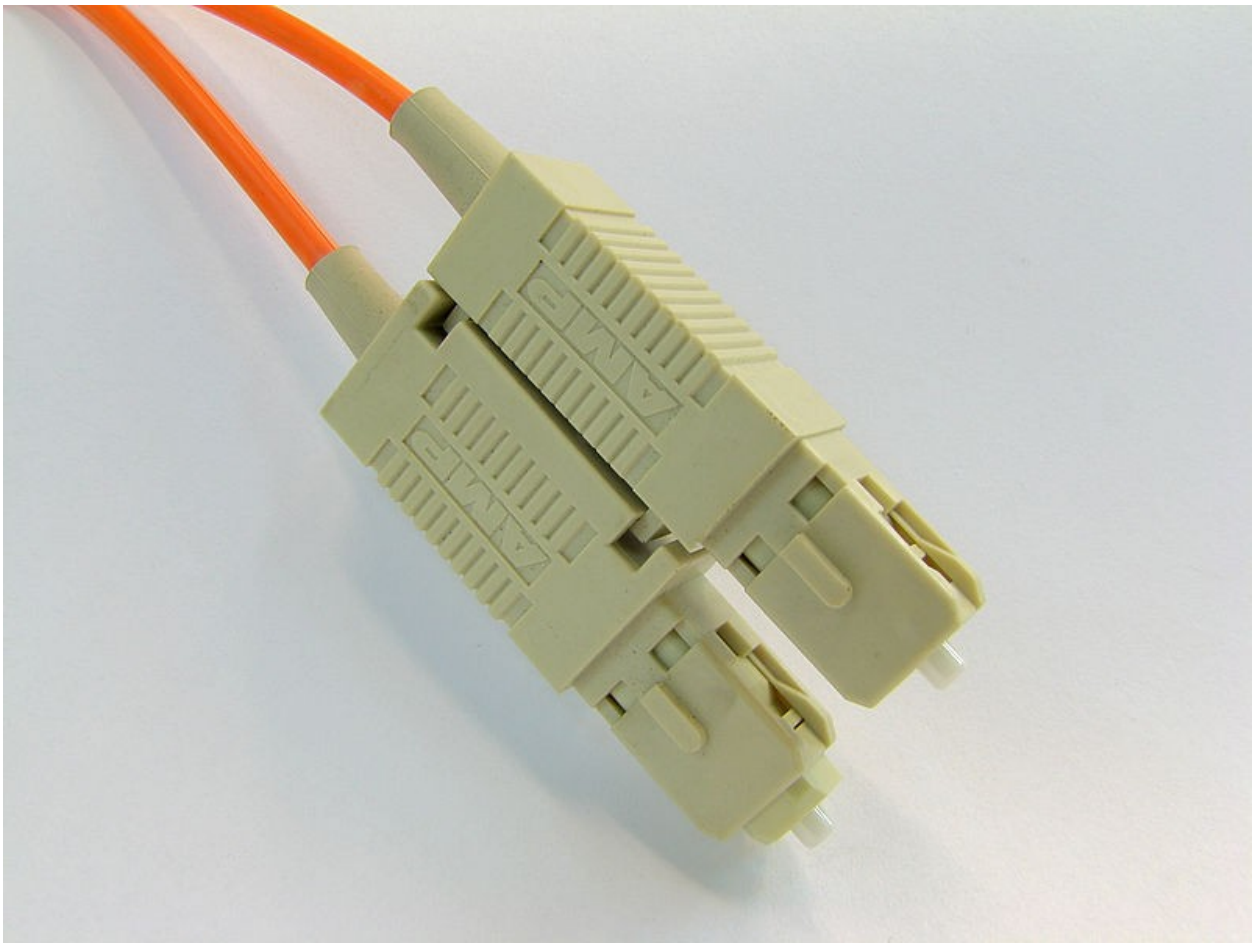


Figura 5: Conector FC

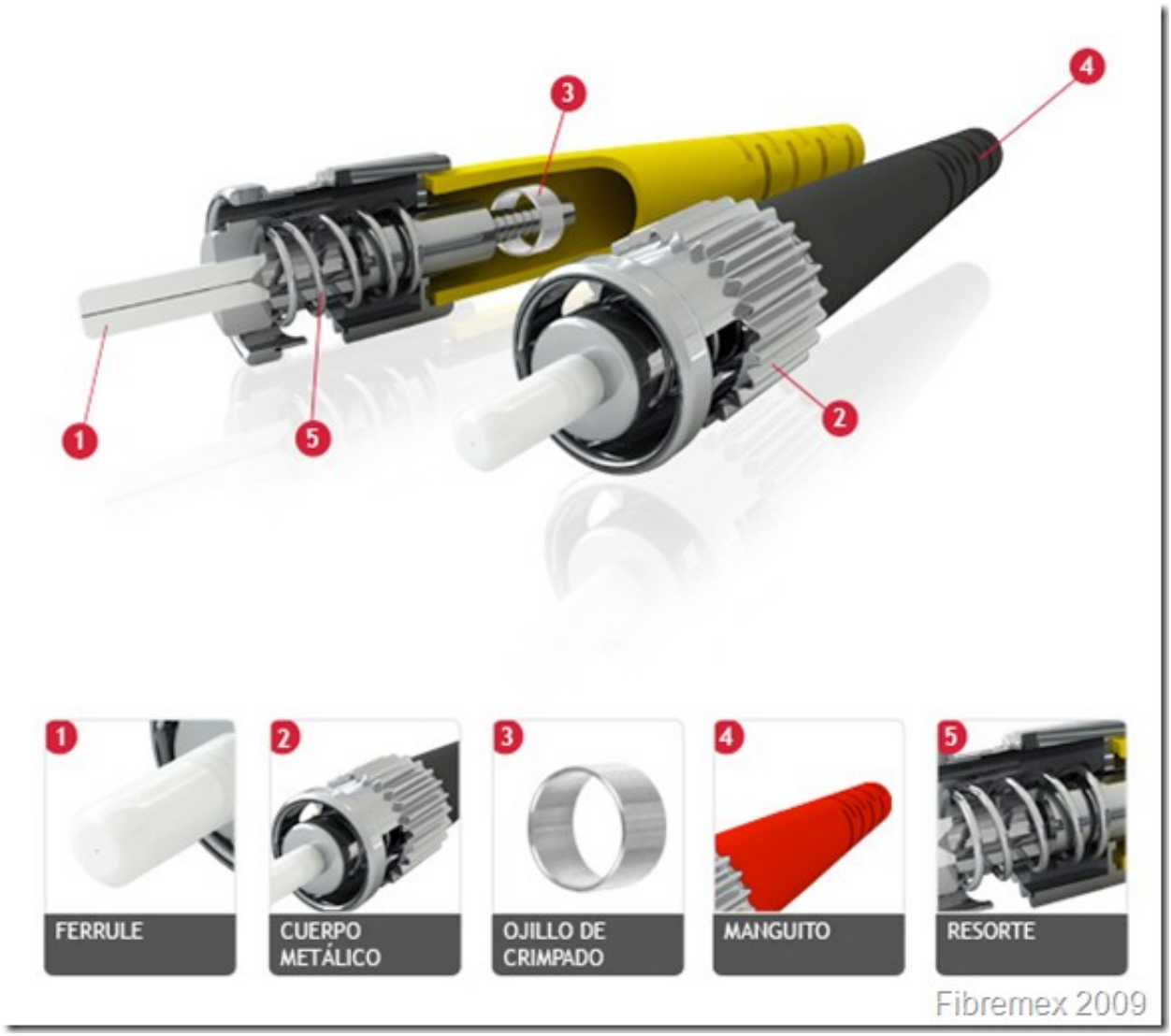


Figura 6: Conector ST

exterior de 2,5 mm, siendo el orificio interior de 127 um para las FMM. Los ferrule pueden ser de metal, cerámica o plástico.

2. **Cuerpo metálico**, con una marca que sólo permite su inserción en una posición, una vez introducido se gira un cuarto de vuelta y queda fijado por un resorte con mecanismo de bayoneta.
3. **Anillo de crimpado**
4. **Manguito**, imprescindible para dar rigidez mecánica al conjunto y evitar la rotura de la fibra.
5. **Resorte** que permite cerrar o liberar el mecanismo de bayoneta.

Este veterano conector ha sido durante mucho tiempo el más empleado para finalizar **fibras ópticas multimodo** (FMM), hoy en día está en desuso, no obstante sigue muy presente en multitud de instalaciones. Su diseño se inspira en los conectores para cables coaxiales, tiene un sistema de anclaje por bayoneta que hace de este conector un modelo muy resistente a las vibraciones por lo que es especialmente indicado para entornos exigentes.

ST se considera como un conector óptico de **segunda generación**.

Principales características:

- Pérdidas típicas de inserción FMM < 0,3 dB, FSM < 0,2 dB
- Pérdidas típicas de retorno FMM > 25 dB, FSM > 55 dB

Conector SC (suscriber connector)

Estructura:

1. **Ferrule**, generalmente de cerámica con un diámetro exterior de 2,5 mm, siendo el orificio interior de 127 um para las FMM y 125,5 para las FSM.
2. **Cuerpo**, de plástico con un sistema de acople "Push Pull" que impide la desconexión si se tira del cable, también bloque posibles rotaciones indeseadas del conector.
3. **Anillo de crimpado**
4. **Manguito**, imprescindible para dar rigidez mecánica al conjunto y evitar la rotura de la fibra.

Para este conector se emplea una regla nemotécnica según la cual SC significa square connector (conector cuadrado) . Esta diferencia de forma es lo primero que a simple vista se observa respecto al conector ST. Los conectores SC han ido sustituyendo al los ST sobre todo en cableados estructurados, fundamentalmente por ser más fáciles de conectorizar, lograr mayor densidad de integración y por permitir su variedad-duplex en la que los dos canales de transmisión/recepción Tx/Rx se pueden tener en el mismo modular.

SC se considera un conector óptico de **tercera generación**, mejorando en tamaño, resistencia y facilidad de uso con respecto a la anterior.

Principales características:

- Pérdidas típicas de inserción FMM < 0,1 dB, FSM < 0,1 dB
- Pérdidas típicas de retorno FMM > 30 dB, FSM > 55 dB

Conector LC (Lucent technologies connector)

Estructura:

1. **Ferrule**, de cerámica con un diámetro exterior de 1,25 mm, la mitad que sus precedentes SC o ST.
2. **Cuerpo**, de plástico con un sistema de acople RJ "Push Pull" que impide la desconexión si se tira del cable, también bloquea posibles rotaciones indeseadas del conector.
3. **Anillo de crimpado**
4. **Manguito**, imprescindible para dar rigidez mecánica al conjunto y evitar la rotura de la fibra.

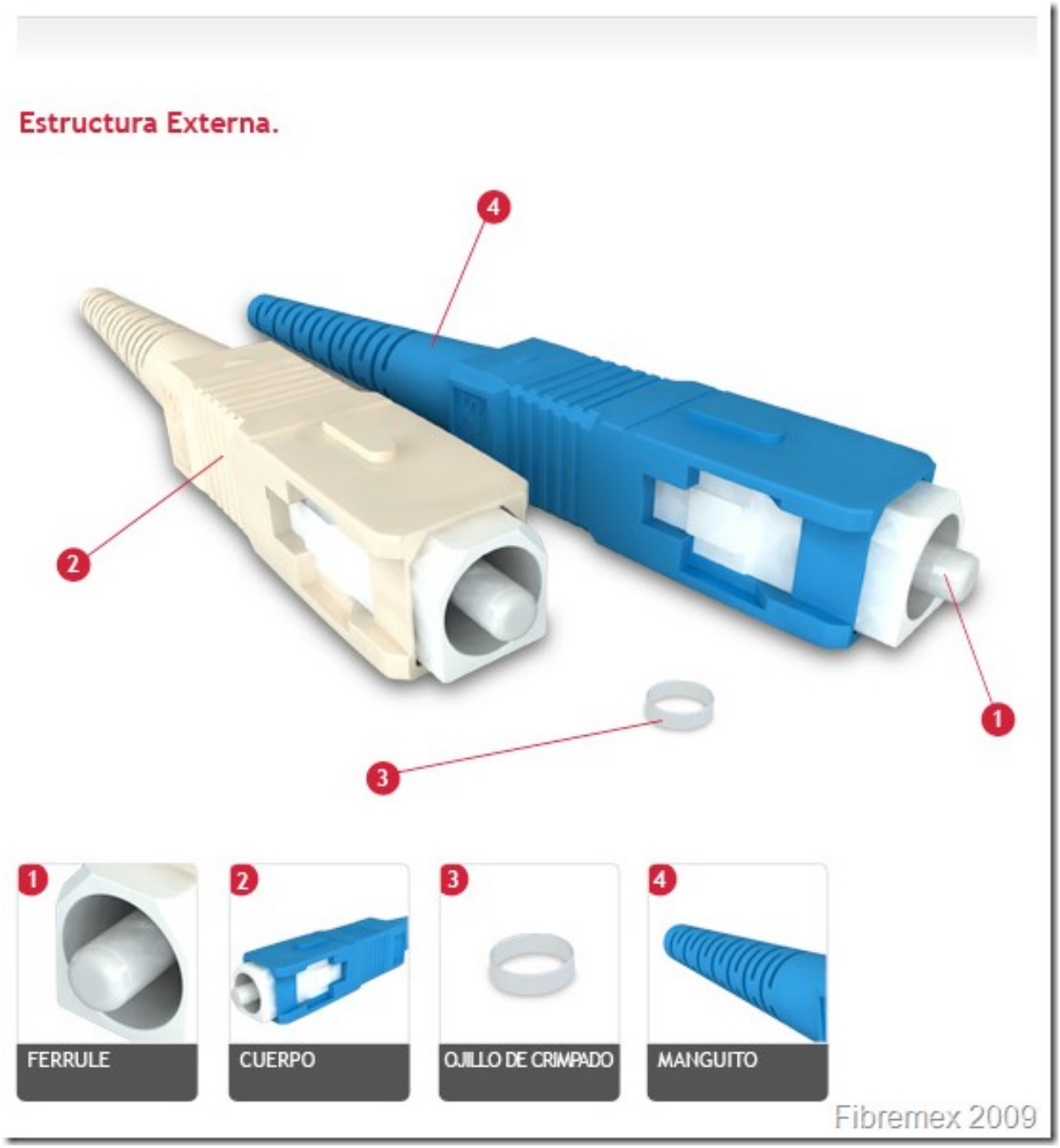


Figura 7: Conector SC

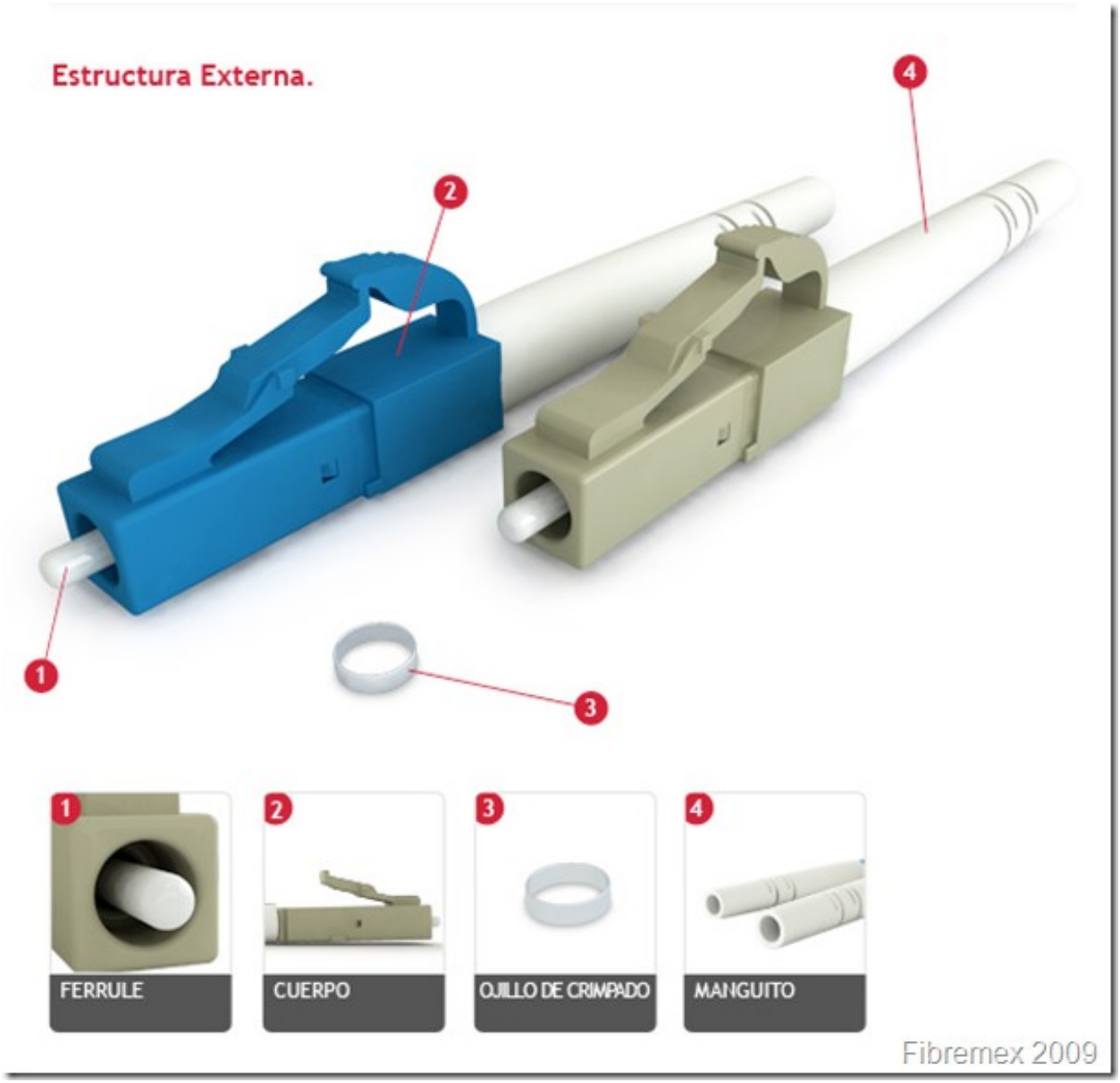


Figura 8: Conector LC

Aquí tenemos un conector óptico que reduce a la mitad el tamaño de un conector SC, esto hace que su escala de integración sea muy alta, por ello cada vez es más frecuente ver en los switch que tienen puertos de fibra para conectores LC duplex integrados en módulos mini GBIC o SFP. El sistema de anclaje es muy parecido al de los conectores RJ hay que presionar sobre la pestaña superior para introducirlos o liberarlos, esta pestaña es tan pequeña que esto se hace con un destornillador plano de punta fina.

LC se considera un conector óptico de **cuarta generación**, mejora en tamaño, resistencia y facilidad de uso con respecto a las generaciones anteriores.

Principales características:

- Pérdidas típicas de inserción FMM < 0,1 dB, FSM < 0,1 dB
- Pérdidas típicas de retorno FMM > 30 dB, FSM > 55 dB

Comparativa de cables

En el siguiente cuadro se presenta una comparativa de los distintos tipos de cables descritos.

▪	Par Trenzado	Par Trenzado Blindado	Coaxial	Fibra Óptica
Tecnología probada	Sí	Sí	Sí	Sí
Ancho de banda	Medio	Medio	Alto	Muy Alto
Full Duplex	Sí	Sí	Sí	Sí por pares
Distancias medias	100 m - 65 Mhz	100 m - 67 Mhz	500 m - (Ethernet)	2 km (Multi.) 100 km (Mono.)
Inmunidad Electromagnética	Limitada	Media	Media	Alta
Seguridad	Baja	Baja	Media	Alta
Coste	Bajo	Medio	Medio	Alto

Selección del tipo de cableado

Cuando se instalen cables de cobre o de fibra óptica en canalizaciones subterráneas, éstos deben tener protección adicional contra roedores, humedad y agua, radiación ultravioleta, campos magnéticos y tensión de instalación.

Si la distancia o el ancho de banda demandado lo exige será necesario utilizar fibra óptica. Además se recomienda utilizar fibra cuando se da alguna de las siguientes circunstancias:

- El cableado une edificios diferentes; en este caso el uso de cable de cobre podría causar problemas debido a posibles diferencias de potencial entre las tierras de los edificios que podrían provocar corrientes inducidas en el cable. Además se podría ver muy afectado por fenómenos atmosféricos.
- Se desea máxima seguridad en la red (el cobre es más fácil de interceptar que la fibra).
- Se atraviesan atmósferas que pueden resultar corrosivas para los metales.
- Se sospecha que puede haber problemas de interferencia eléctrica por proximidad de motores, luces fluorescentes, equipos de alta tensión, etc.

Cuando no se dé alguna de las razones que aconsejan utilizar fibra es recomendable utilizar cobre, ya que es más barato el material, la instalación y las interfaces de conexión de los equipos; además es más fácil realizar modificaciones en los paneles de conexión, empalmes, etc.

En general en una instalación grande se utiliza fibra para los tendidos principales (uniones entre edificios y cableado vertical para distribución por plantas dentro del edificio) y cobre para el cableado horizontal y quizá también para el cableado vertical (junto con la fibra) si las distancias entre los armarios así lo aconsejan.

Es recomendable que los cables de cobre y fibra óptica dentro de un edificio sean **resistentes al fuego, generen poco humo y cero halógenos** y sean retardantes de la llama, de acuerdo al estándar IEC 332-1, o equivalente.

La gran mayoría de los cables UTP tienen una cubierta construida con **PVC (Policloruro de vinilo)**, que se presenta normalmente en color gris. El PVC resiste relativamente bien las altas temperaturas, es un buen aislante eléctrico, es flexible y sobre todo es barato, por todo ello es un material muy empleado en las construcción de cubiertas de cables.

Pero las cubiertas de PVC de los cables tienen un punto importante en contra, el PVC contiene en su composición halógenos y además al quemarse emite dioxinas, estas dioxinas suspendidas en el humo pueden desplazarse a grandes distancias, depositarse en la tierra y terminar en las plantas llegando a contaminar la cadena alimenticia. De ahí que el PVC este considerado por muchos como una material potencialmente contaminante y tóxico.

En el interior de edificios y por motivos de seguridad se tiende a que los cables tengan cubiertas que en caso de incendio emitan poco humo al quemarse (Low Smoke) y por lo dicho antes se busca que estas cubiertas no contengan halógenos (Zero Halogen) esto se puede conseguir gracias al polipropileno (PP) un plástico con bastante mejor fama que el PVC.

Hay que recordar que cuando se produce fuego en un edificio la mayoría de las víctimas sucumben intoxicadas por el humo no por quemaduras. Los edificios están plagados de cables, en un hotel o en un hospital se habla normalmente de kilómetros de cableados tendidos. No es de extrañar por tanto que en muchos pliegos de condiciones de proyectos de cableado estructurado se exija además de la categoría del cable el que la cubierta del mismo sea **LSZH (Low Smoke Zero Halogen)**.

Un cable UTP de CAT-6 con cubierta LSZH es bastante más caro que otro de la misma categoría con cubierta en PVC. Los cables UTP con cubierta LSZH suelen ser de colores muy llamativos como el naranja o el amarillo, y tienen inscrito en la cubierta el acrónimo LSZH.

4.1.8 Canalizaciones

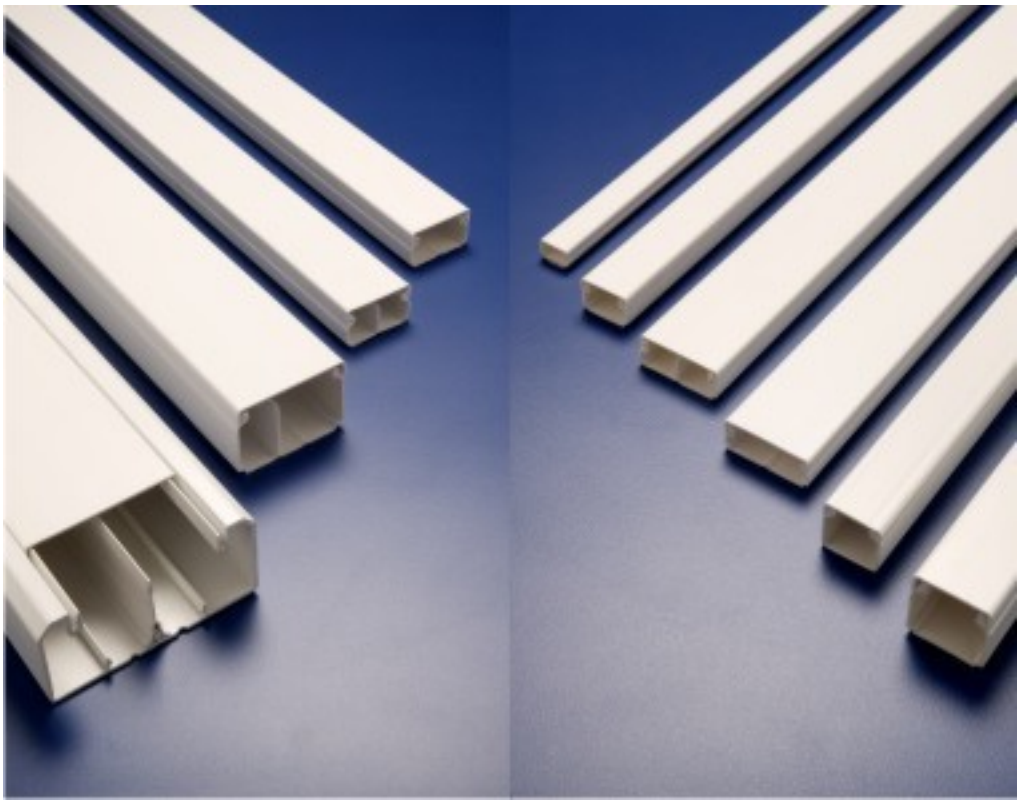
Las canalizaciones son utilizadas para distribuir y soportar el cable y conectar equipamiento entre la salida del área de trabajo y el cuarto de telecomunicaciones. Los cables deben ir fijados en capas mediante abrazaderas colocadas a intervalos de 4 metros.

Para evitar interferencias electromagnéticas la canalización de las corrientes débiles (cables de datos) debe mantenerse separada de corrientes fuertes (cables eléctricos y dispositivos electromagnéticos). Además en caso de cruzarse deben hacerlo perpendicularmente.

Fuente de campo (se supone una tensión inferior a 480 voltios)	Separación mínima según la potencia (KVA)		
▪	< 2	[2, 5]	> 5
Líneas de corriente o equipos eléctricos no apantallados	13 cm	30 cm	60 cm
Líneas o equipos no apantallados próximos a cables de tierra	6 cm	15 cm	30 cm
Líneas apantalladas	0 cm	15 cm	30 cm
Transformadores, motores eléctricos, aires acondicionados…	100 - 120 cm	100 - 120 cm	100 - 120 cm
Tubos fluorescentes y balastros	12 - 30 cm	12 - 30 cm	12 - 30 cm

Canaletas

Se pueden usar canaletas de telecomunicaciones que podrán ir a la altura del suelo, por el rodapié, o por las paredes.



Falso suelo

Consiste en hacer una tarima levantando unos centímetros el suelo de la habitación, y pasar el cableado por debajo de ésta.

Falso techo

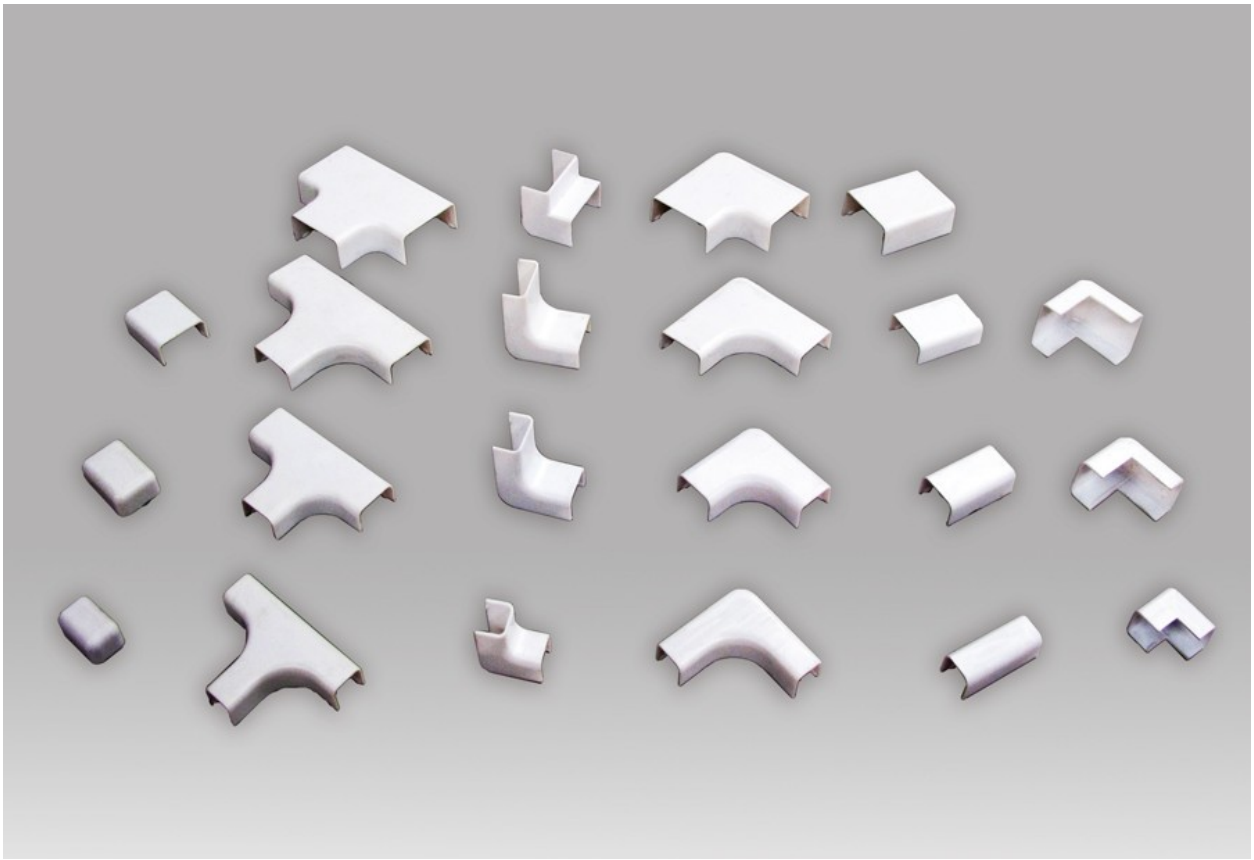
Para instalaciones de este tipo no es necesario instalar prácticamente ningún elemento adicional, salvo en algunos casos que no tengamos las suficientes verticales dentro de la sala para acceder a algunos lugares, pudiéndose instalar columnas metálicas para descender hasta el puesto de trabajo.

Bandejas colgantes

4.2 Instalación de cableado estructurado

4.2.1 Estructura

El cableado genérico es una estructura jerárquica en forma de estrella. Este sistema permite generar otras distribuciones, como anillo o bus, utilizando interconectores en los terminadores. Conexiones directas entre FDs o BDs son deseables y permitidas, pero no pueden sustituir a las conexiones jerárquicas. El número y tipo de subsistemas que



incluye una implementación depende de diversos factores. Por ejemplo un campus con un solo edificio puede no necesitar de subsistema de cableado de campus. Además se pueden agrupar múltiples distribuidores, por ejemplo es habitual combinar en un solo distribuidor el CD con uno de los BD, o un BD con uno de los FD.

Para comunicar cualquier FD y el CD solo debe ser necesario atravesar un BD -como máximo-.

Acometidas de red

Las acometidas de redes son necesarias tanto para los cables que constituyen el subsistema troncal o espinazo de campus, como para los cables de redes públicas y privadas (por ejemplo, líneas de comunicación de datos como X.25, Frame-Relay, RDSI, etc.) que entran en el edificio y con los que se realiza una transición para distribuirlos luego a través del sistema interno de cableado.

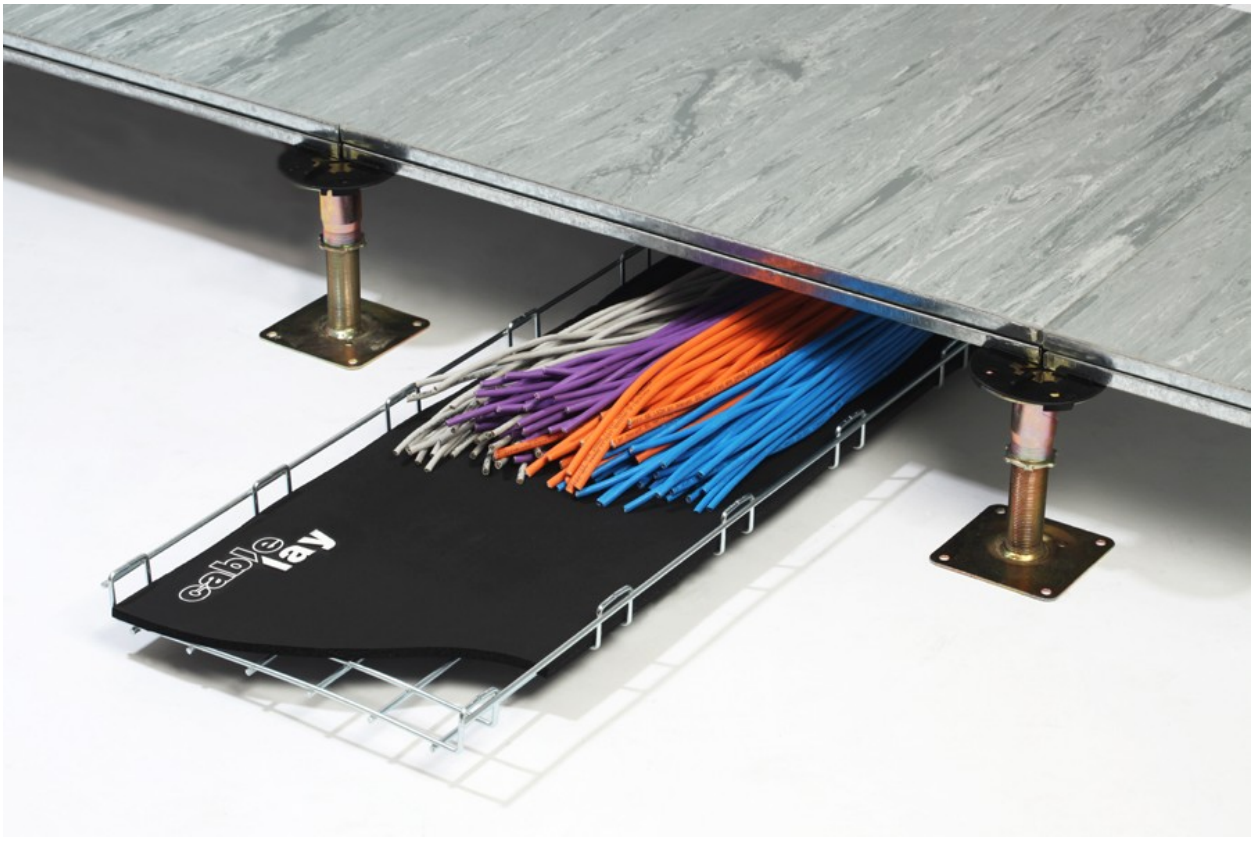
Comprende desde el punto de entrada en la pared del edificio hasta el tendido del cable que le hace llegar al armario distribuidor de planta o de campus.

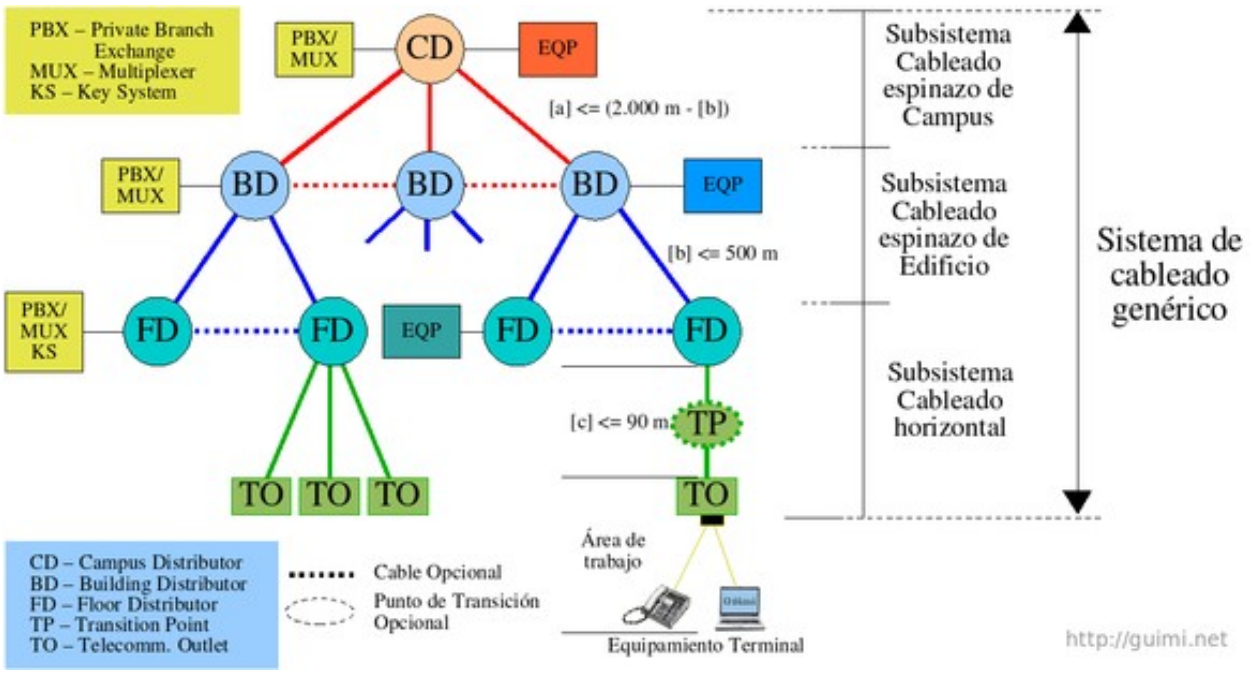
En España se utiliza el reglamento de Infraestructuras Comunes de Telecomunicación en edificios.

Cuartos de telecomunicaciones / Cuartos de equipamiento

Un **cuarto o sala de telecomunicaciones** (**TC**: Telecommunications Closet) es un espacio cerrado de un edificio utilizado para el uso exclusivo de cableado de telecomunicaciones y sistemas auxiliares: bastidores (racks), concentradores, aire acondicionado propio...

Un **cuarto o sala de equipamiento** es un tipo más complejo de sala de comunicaciones donde se ubican, además de telecomunicaciones otros equipos de red. Cada cuarto debe tener acceso directo al ca-


cable
lay


PBX – Private Branch Exchange
MUX – Multiplexer
KS – Key System
PBX/ MUX
CD
EQP
[a] <= (2.000 m - [b])
PBX/ MUX
BD
BD
BD
EQP
[b] <= 500 m
PBX/ MUX KS
FD
FD
EQP
FD
FD
[c] <= 90 m
TP
TO
TO
TO
TO
Área de trabajo
Equipamiento Terminal
CD – Campus Distributor
BD – Building Distributor
FD – Floor Distributor
TP – Transition Point
TO – Telecomm. Outlet
Cable Opcional
Punto de Transición Opcional
Subsistema Cableado espinazo de Campus
Subsistema Cableado espinazo de Edificio
Subsistema Cableado horizontal
Sistema de cableado genérico
http://guimi.net

ble espinazo. Un cuarto de equipamiento (**ER**: Equipment Room) es un espacio cerrado de uso específico para equipamiento de datos y telecomunicaciones que puede contener o no distribuidores (haciendo la función de TC). Todo espacio que contenga más de un distribuidor se considera un ER.

Los cuartos de telecomunicaciones deben considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad o audio. No debe contener otras instalaciones eléctricas que no sean del equipamiento propio del cuarto.

Un cuarto de equipamiento puede incluir espacio de trabajo para el personal correspondiente.

Los **armarios** (bastidores o **racks**) deben de contar con al menos 82 cm de espacio libre por delante y detrás, medidos a partir de la superficie más sobresaliente del armario.

Deben disponer de acometida eléctrica diferenciada, apantallamiento frente a interferencias electromagnéticas, sistemas de alimentación interrumpida, sistema de luz de emergencia y ventilación adecuada.

Todo edificio debe contener al menos un cuarto de telecomunicaciones o un cuarto de equipo; no hay un límite máximo.

En los TC la temperatura debe mantenerse permanentemente entre 10 y 35 grados centígrados y la humedad relativa debe mantenerse por debajo del 85 %, realizándose un cambio completo de aire por hora.

En los ER la temperatura debe mantenerse permanentemente entre 18 y 24 grados centígrados y la humedad relativa debe mantenerse entre el 30 % y el 55 %, realizándose un cambio completo de aire por hora.

Por esto a veces los **TC y ER** son también llamados "**salas frías**".

Área de trabajo

Se define como la **zona donde están los distintos puestos de trabajo** de la red. En cada uno de ellos habrá una roseta de conexión que permita conectar el equipo o equipos que se quieran integrar en la red.

El área de trabajo comprende todo lo que se conecta a partir de la roseta de conexión hasta los propios dispositivos a conectar (ordenadores e impresoras fundamentalmente). Están también incluidos cualquier filtro, adaptador, etc., que se necesite. Estos irán siempre conectados en el exterior de la roseta. La instalación se utiliza para transmitir voz, datos u otros servicios, cada uno de ellos deberá tener un conector diferente de la propia roseta de conexión.

Al cable que va desde la roseta hasta el dispositivo a conectar se le llama latiguillo y no puede superar los 3 metros de longitud.

Subsistema de Cableado de Campus (Cableado troncal)

Este subsistema, en inglés "Campus Backbone Cabling Subsystem", incluye [longitud máxima]:

1. Distribuidor de Campus (CD: Campus Distributor)
2. Latiguillos del CD [20 m, mayores distancias deben descontarse del Cable Espinazo]
3. Latiguillos entre los paneles y el equipamiento de CD -incluyendo PBX- [30 m [1]]

4. **Cable Espinazo de Campus -Cable Troncal-** (Campus Backbone Cable) [Sumado al cable espinazo de edificio no debe superar los **2.000 m**. Con fibra monomodo puede aumentarse, pero distancias mayores que 3.000 m quedan fuera del propósito de la norma]. Incluye terminadores.

Subsistema de Cableado de Edificio (Cableado vertical)

Este subsistema, en inglés "Building Backbone Cabling Subsystem", incluye:

1. Distribuidor de Edificio (BD: Building Distributor)
2. Latiguillos del BD [20 m, mayores distancias deben descontarse del Cable Espinazo]
3. Latiguillos entre los paneles y el equipamiento de BD -incluyendo PBX- [30 m [1]]
4. **Cable Espinazo de Edificio -Cable Vertical-** (Building Backbone Cable) [**500 m**]. Incluye terminadores.

Subsistema de Cableado Horizontal

Este subsistema, en inglés "Horizontal Cabling Subsystem", incluye:

1. Distribuidor de Planta (FD: Floor Distributor)
2. Latiguillos del FD [6 m]
3. Latiguillos entre los paneles y el equipamiento de FD
4. **Cable Horizontal** [**90 m**, independientemente del medio] (Horizontal Cable). Incluye terminadores.
5. Punto de Transición (Opcional) [No incrementa la longitud del cable horizontal] (TP: Transition Point)
6. Salida de Telecomunicaciones -Roseta- (TO: Telecommunications Outlet)

La roseta (TO) forma parte del área de trabajo.

Nota: No es obligatorio, pero se recomienda fuertemente que la suma de longitudes de los latiguillos sea menor o igual que 10 m: (2) + (3) + (cable del área de trabajo <=3 m) <= 10 m

---

Distribuidores

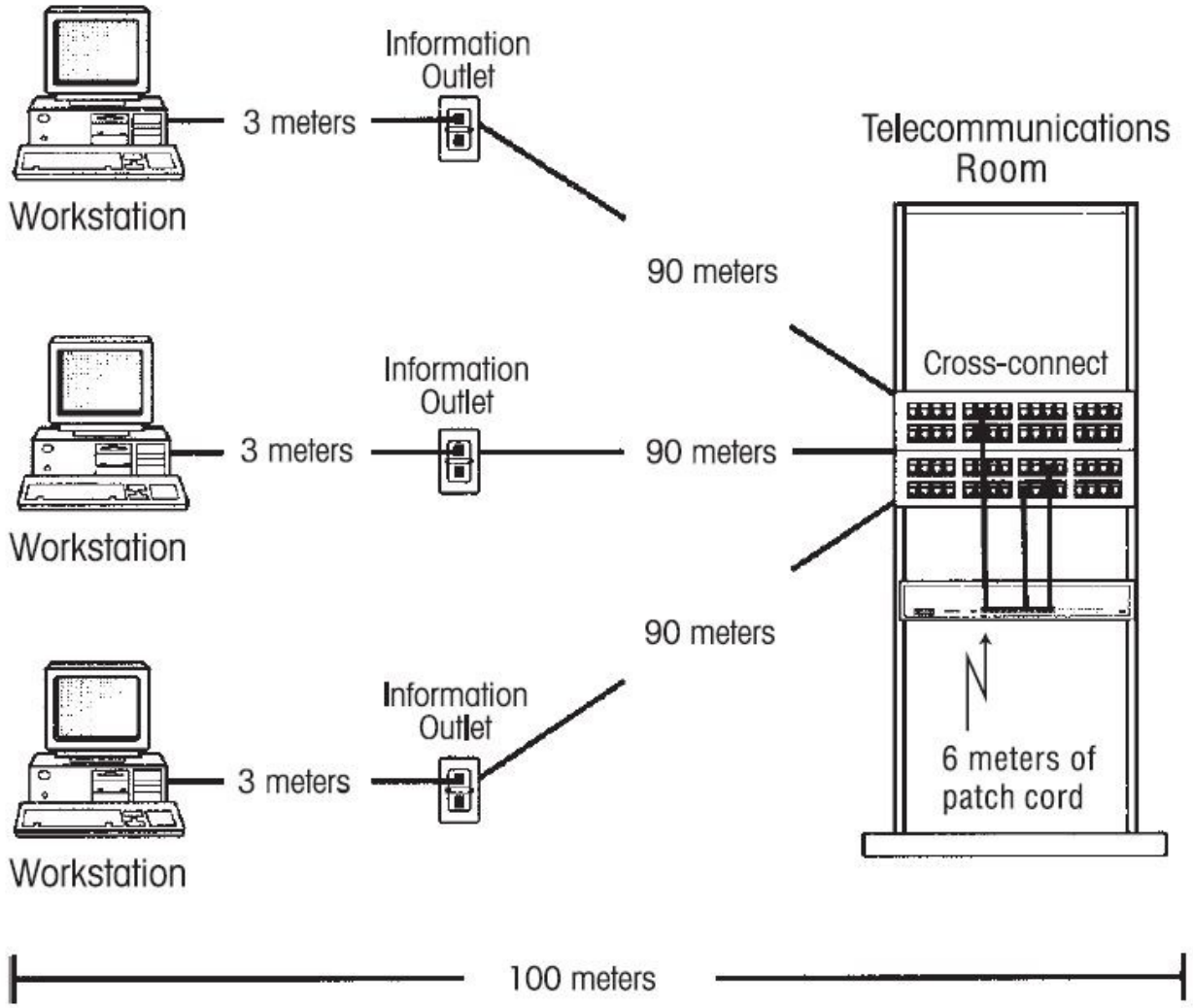
La distribución se organiza en **racks**. Un rack es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están normalizadas para que sean compatibles con equipamiento de cualquier fabricante. **También son llamados bastidores, cabinas, cabinets o armarios**.

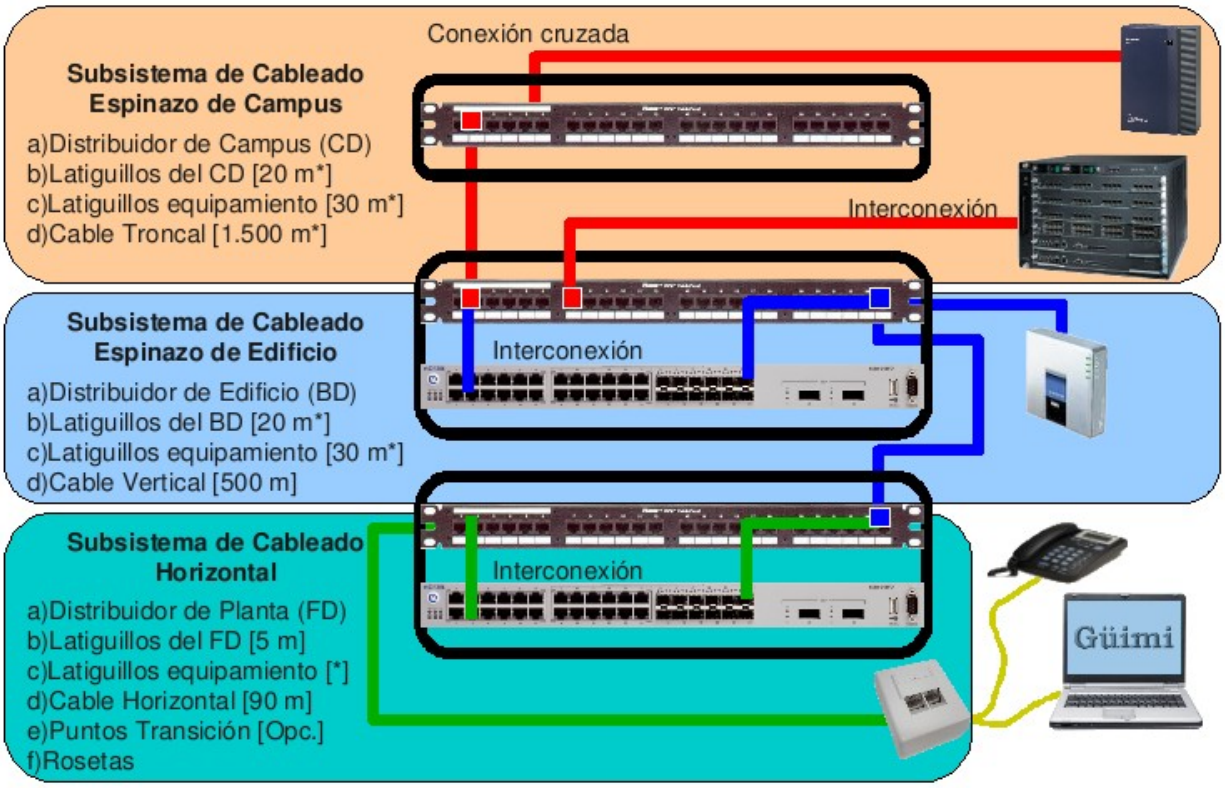
Externamente, los racks para montaje de servidores tienen una **anchura estándar de 600 mm** y un **fondo de 600, 800, 900, 1000** y ahora incluso 1200mm. La anchura de 600 mm para racks de servidores coincide con el tamaño estándar de las losetas en los centros de datos. De esta manera es muy sencillo hacer distribuciones de espacios en centros de datos (CPD). Para el cableado de datos se utilizan también racks de 800 mm de ancho, cuando es necesario disponer de suficiente espacio lateral para el guiado de cables.

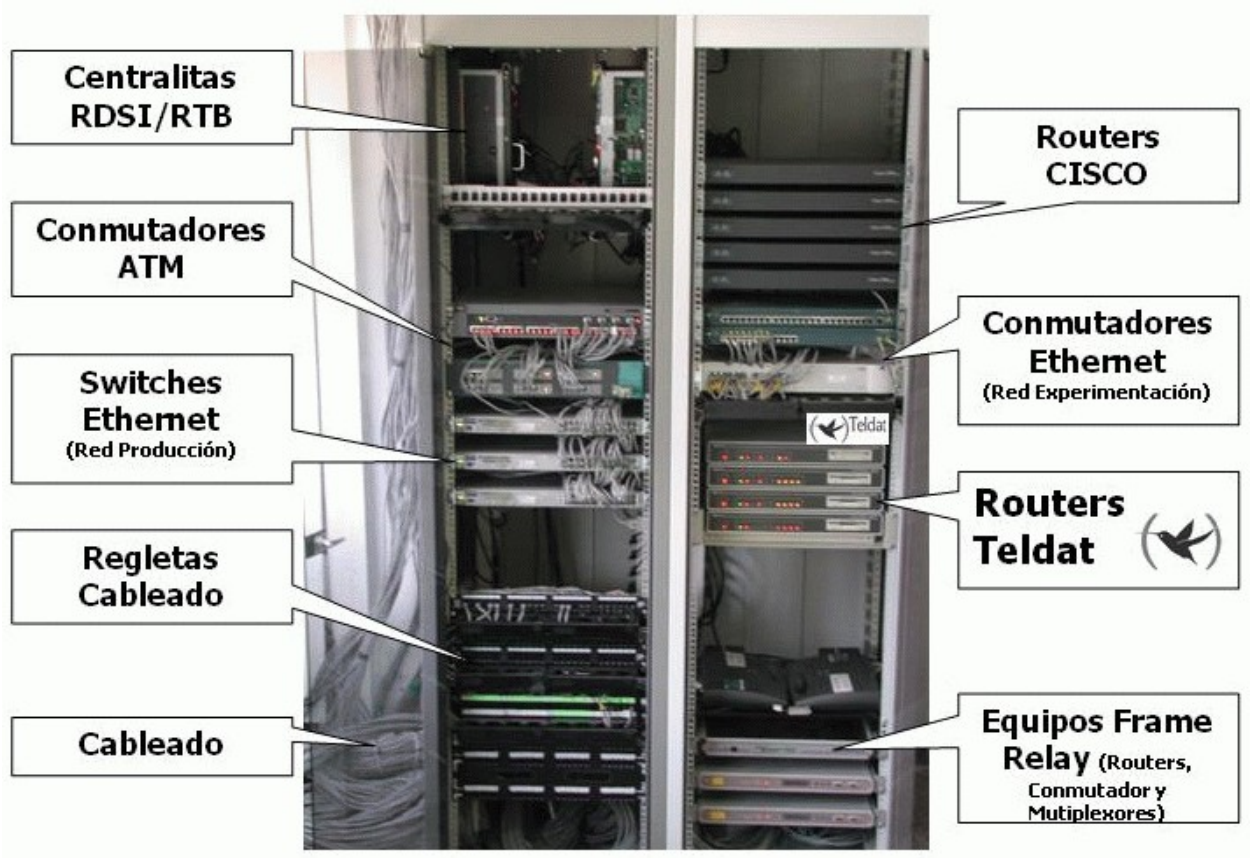
Conjunto de racks

Los racks son útiles en un centro de proceso de datos, donde el espacio es escaso y se necesita alojar un gran número de dispositivos. Estos dispositivos suelen ser:

- Servidores cuya carcasa ha sido diseñada para adaptarse al bastidor. Existen servidores de 1, 2 y 4 unidades rack; y servidores blade que permiten compactar más compartiendo fuentes de alimentación y cableado.
- Conmutadores y enrutadores de comunicaciones.


Information
Outlet
3 meters
Workstation
Telecommunications
Room
90 meters
Cross-connect
Information
Outlet
3 meters
90 meters
Workstation
90 meters
Information
Outlet
3 meters
6 meters of
patch cord
Workstation
100 meters

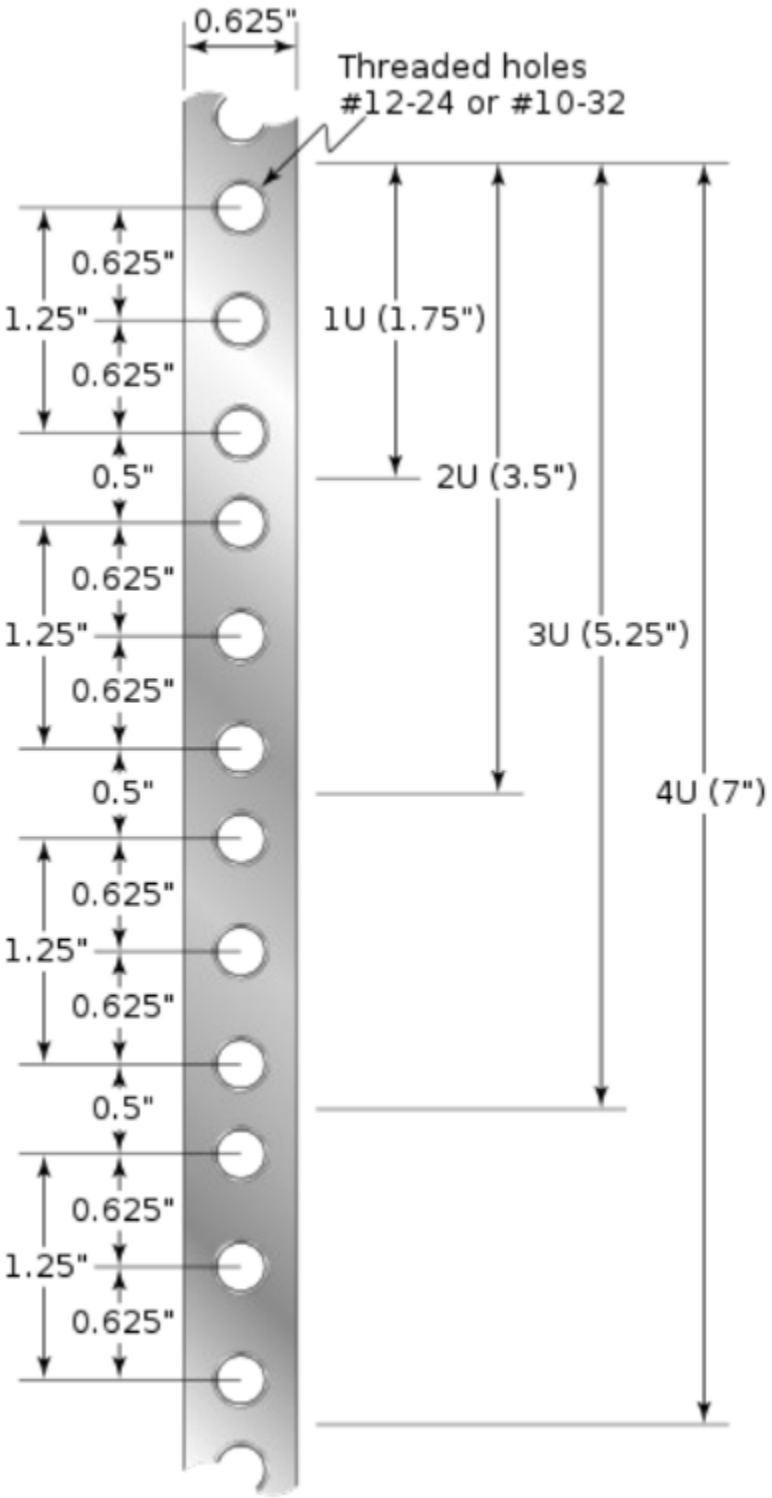

Conexión cruzada
Subsistema de Cableado
Espinazo de Campus
a)Distribuidor de Campus (CD)
b)Latiguillos del CD [20 m*]
c)Latiguillos equipamiento [30 m*]
d)Cable Troncal [1.500 m*]
Interconexión
Subsistema de Cableado
Espinazo de Edificio
a)Distribuidor de Edificio (BD)
b)Latiguillos del BD [20 m*]
c)Latiguillos equipamiento [30 m*]
d)Cable Vertical [500 m]
Interconexión
Subsistema de Cableado
Horizontal
a)Distribuidor de Planta (FD)
b)Latiguillos del FD [5 m]
c)Latiguillos equipamiento [*]
d)Cable Horizontal [90 m]
e)Puntos Transición [Opc.]
f)Rosetas
Interconexión
Güimi


Centralitas RDSI/RTB
Conmutadores ATM
Switches Ethernet (Red Producción)
Regletas Cableado
Cableado
Routers CISCO
Conmutadores Ethernet (Red Experimentación)
Routers Teldat
Equipos Frame Relay (Routers, Conmutador y Mutiplexores)
Teldat

- Paneles de parcheo, que centralizan todo el cableado de la planta.
- Cortafuegos.

El equipamiento simplemente se desliza sobre un raíl horizontal y se fija con tornillos. También existen bandejas que permiten apoyar equipamiento no normalizado. Por ejemplo, un monitor o un teclado.

Estándar de rack



Las especificaciones de un rack estándar se encuentran bajo las normas equivalentes DIN 41494 parte 1 y 7, UNE-20539 parte 1 y parte 2 e IEC 297 parte 1 y 2, EIA 310-D y tienen que cumplir la normativa medioambiental RoHS.

La anchura del bastidor está estandarizada y es de 19 pulgadas. Las columnas verticales a ambos lados miden 15,875 milímetros de ancho cada una formando un total de 31,75 milímetros (5/4 pulgadas).* Están separadas por 450,85 milímetros (17 3/4 pulgadas) haciendo un total de 482,6 milímetros (**exactamente 19"**). Cada columna tiene agujeros a intervalos regulares, que se agrupan de 3 en 3 para formar lo que se conoce como unidad rack (U). Verticalmente, los racks se dividen en regiones de **1,75 pulgadas de altura (= 1U**).

La altura de los racks está normalizada y sus dimensiones externas de 200 mm en 200 mm. Siendo lo normal que existan **desde 4U de altura hasta 46U de altura**.

Las alturas disponibles normalmente según normativa sería 1000, 1200, 1400, 1600, 1800, 2000 y 2200 mm.

La profundidad del bastidor no está normalizada, ya que así se otorga cierta flexibilidad al equipamiento. No obstante, suele ser de 600, 800, 900, 1000 incluso 1200 milímetros.

Existen también racks de pared que cumplen el formato 19" y cuenta con fondos de 300, 400, 450, 500, 500 y 600 mm totales, siendo muy útiles para pequeñas instalaciones.

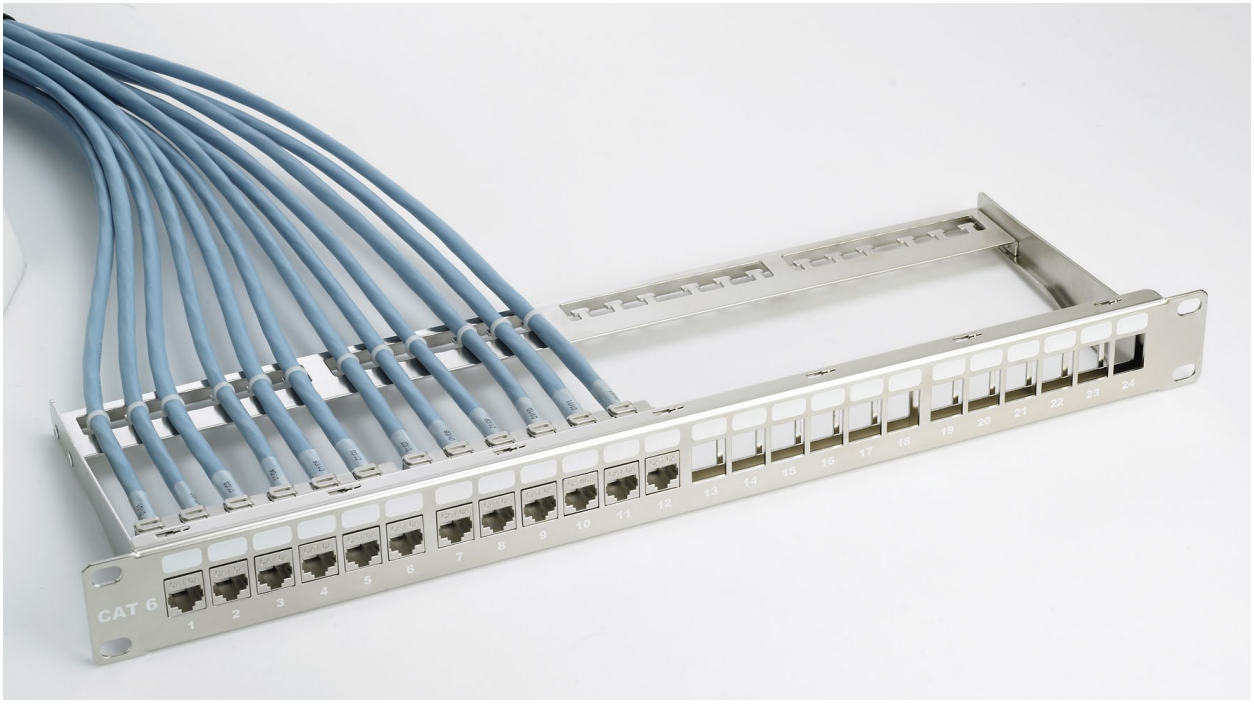
Debería haber un mínimo de un armario distribuidor de planta (FD) por cada 1.000m^2 de espacio reservado para oficinas, con un mínimo de un FD por

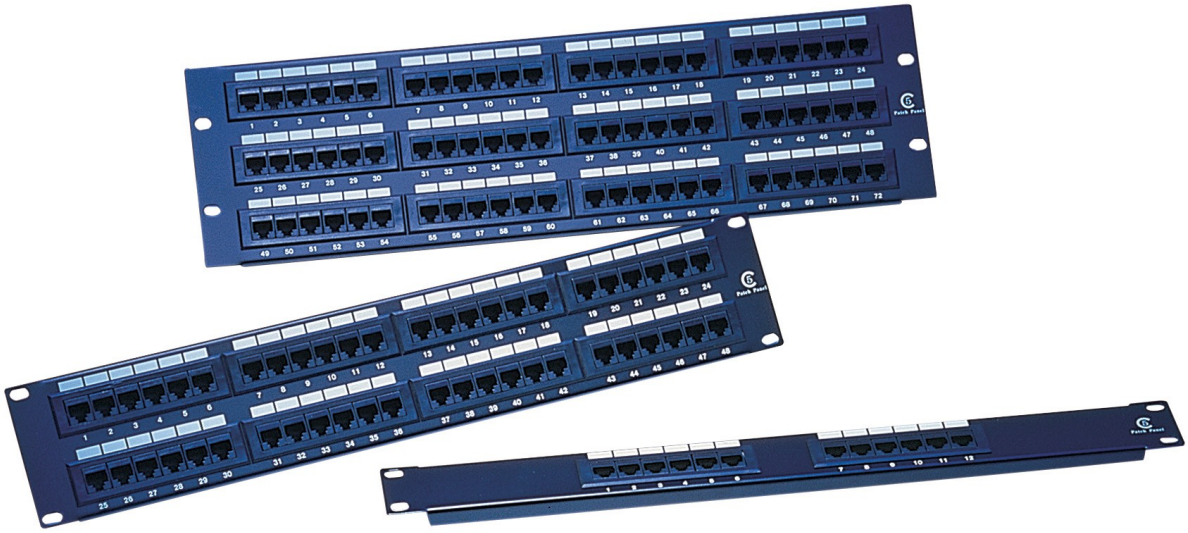
planta. Si una planta se utiliza poco para oficinas (como un vestíbulo) puede atenderse desde un FD de una planta adyacente.

Todo distribuidor (CD, BD, FD) debe estar en un cuarto de telecomunicaciones o en un cuarto de equipamiento.

Paneles de parcheo

Un panel de parcheo es un elemento pasivo que se atornilla en el rack y a donde van a parar los cables de las distintas rosetas.

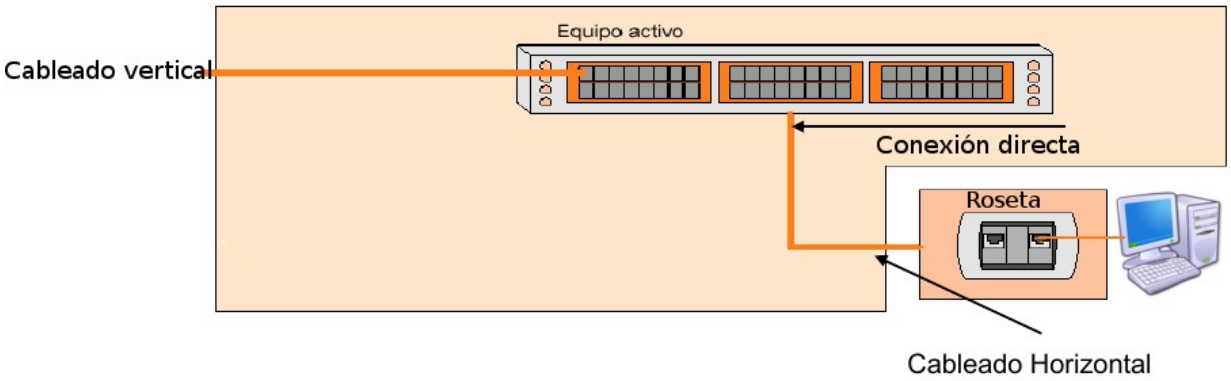




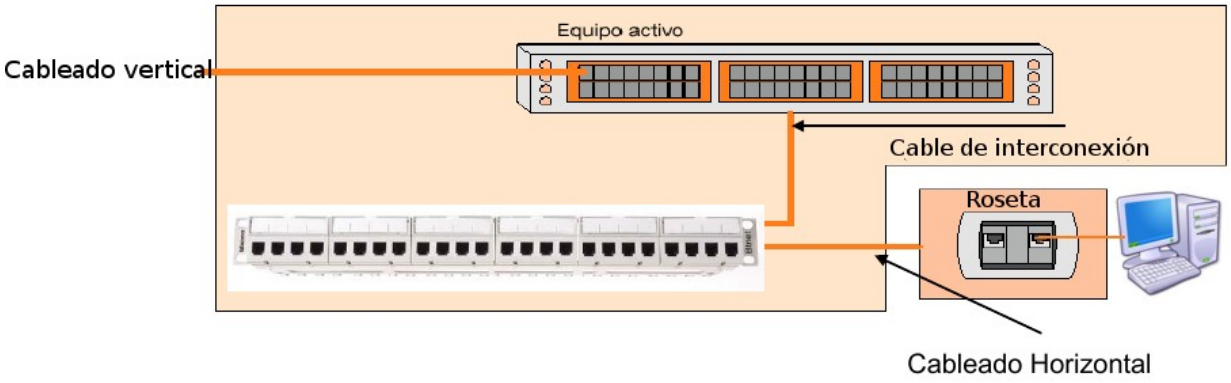
Existen 3 tipos de conexiones que podemos realizar:

- **Conexión directa**
- **Interconexión**
- **Conexión cruzada**

En la **conexión directa no hacemos uso de paneles de parcheo**. En el centro de datos, la conexión directa no es una opción acertada porque cuando se producen cambios, los operadores están obligados a localizar cables y moverlos con cuidado hacia una nueva ubicación: un esfuerzo impertinente, costoso, poco confiable y que requiere tiempo. Los centros de datos que cumplen con la norma TIA-942 no conectan los equipos en forma directa.



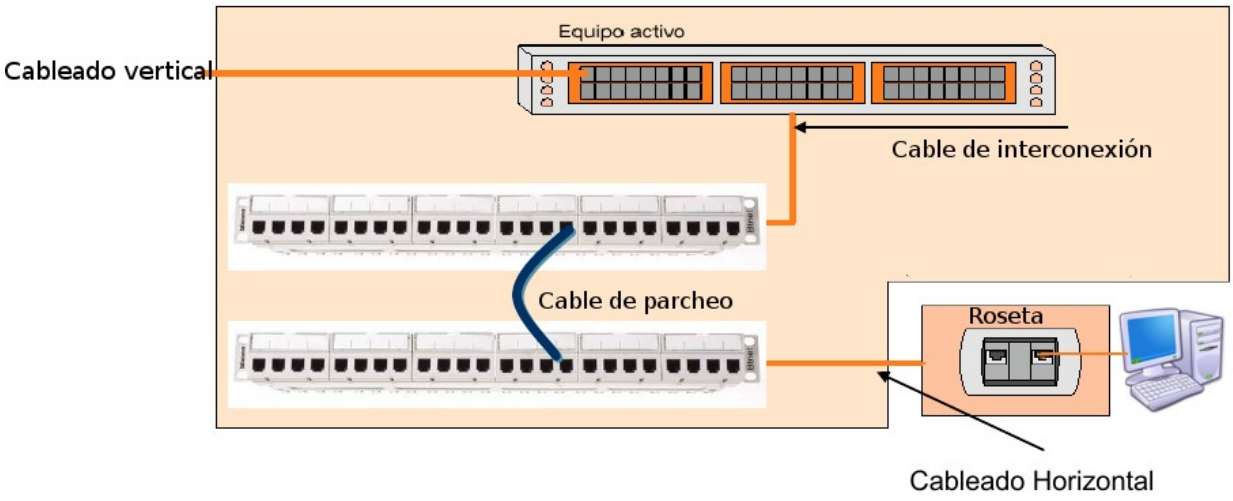
En la **interconexión hacemos uso de un panel de parcheo intermedio**. Cuando se produce algún cambio en una interconexión, los operadores vuelven a tender los cables del sistema final para volver a tender el circuito. Este método es mucho más eficaz que la conexión directa, pero no es tan sencillo o fiable como el método de conexión cruzada.



En la **conexión cruzada hacemos uso de dos paneles de parcheo intermedios**. Con un sistema de parcheo de conexión cruzada centralizada, se pueden alcanzar los requisitos de bajo costo y un servicio muy confiable. En esta estructura simplificada, todos los elementos de la red tienen conexiones de cables de equipos permanentes que se terminan una vez y no se vuelven a manejar nunca más. Los técnicos aíslan elementos, conectan nuevos elementos, rastrean problemas y realizan el mantenimiento y otras funciones usando conexiones de cable de parcheo semipermanentes en el frente de un sistema de conexión cruzada.

A continuación se enumeran algunas ventajas clave que brinda un sistema de conexión cruzada bien diseñado:

- Costos de operación más bajos: Comparada con otras propuestas, la conexión cruzada reduce enormemente el tiempo que lleva agregar tarjetas, trasladar circuitos, modernizar software y realizar mantenimiento.



- Confiabilidad y disponibilidad mejoradas: Las conexiones permanentes protegen los cables de los equipos de la actividad cotidiana que puede deteriorarlos. Como los movimientos, adiciones y cambios se realizan en campos de parcheo, en lugar de en los paneles de conexión de equipos sensibles de ruteo y conmutación, los cambios en la red se pueden realizar sin afectar el servicio. Con la capacidad para aislar los segmentos de red para reparar averías y volver a tender circuitos mediante un simple parcheo, el personal del centro de datos gana tiempo para realizar las reparaciones adecuadas durante horas normales en lugar de hacerlas durante la noche o en turnos de fin de semana.
- Ventaja Competitiva: Un sistema de conexión cruzada permite hacer cambios rápidos a la red. El activar nuevos servicios se logra al conectar un cordón de parcheo y no requiere de una intensa mano de obra. Como resultado, las tarjetas se añaden a la red en minutos, en lugar de horas reduciendo el tiempo, lo que permite obtener mayores ingresos y ofrecer una ventaja competitiva – disponibilidad del servicio en forma más rápida.

Resumiendo, cuando los equipos activos (enrutadores, conmutadores…) se cablean directamente a paneles de algún subsistema de cableado, se denomina **interconexión (interconnect)**, y cuando lo hacen a paneles independientes se denomina **conexión cruzada (cross connect)**.

Cableado y equipamiento de área de trabajo

El cableado y equipamiento del área de trabajo no es parte del sistema de cableado genérico y la norma no impone requisitos al respecto, salvo las indicadas respecto a longitud y tipo de cable. Incluye:

1. Cable del área de trabajo o de usuario
2. Equipamiento terminal

TO, MUTO y PT - Salidas de telecomunicaciones y Puntos de transición

Una alta densidad de TOs aporta flexibilidad al cableado para permitir cambios. En muchos países se utilizan dos TOs para un máximo de $10m^2$. Pueden presentarse individualmente, por parejas o en grupo, pero cada área de trabajo debe cubrirse con al menos dos.

Cada TO debe estar identificado con una etiqueta permanente y visible. Si uno de ellos está conectado con cable de par trenzado y utiliza menos de 4 pares debe ser claramente marcado.

La configuración mínima consiste en:

1. Un TO con cable balanceado de 100, preferentemente cable de 4 pares, categoría 3 o superior.

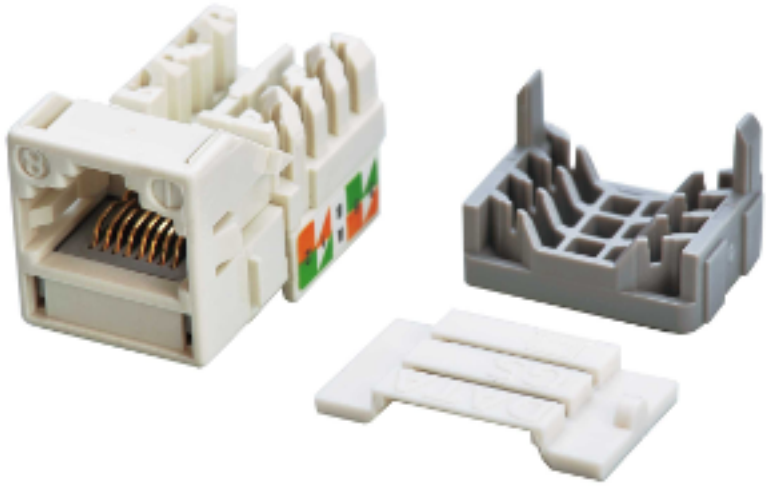
2. Otro(s) TO con dos hilos de fibra óptica multimodo (50/125 o 62,5/125) o cable balanceado (categoría 3 o superior).

Se conocen como MUTO (Muti-User TO) las rosetas multiusuario, que pueden dar servicio a 12 áreas de trabajo como máximo (24 TOs). Deben ser fácilmente accesibles y su instalación debe ser permanente, es decir, no pueden estar localizadas en un techo o piso falso, en un armario... El cable desde el FD hasta un PT o un MUTO debe tener mínimo 15 m.

Un TP sirve para cambiar entre distintas formas del mismo tipo de cable (p.e. de cable plano a cable redondo) o como punto de consolidación. No puede ser utilizado como distribuidor ni se pueden conectar a él equipos activos. Las características de los cables deben ser mantenidas en la entrada y la salida.

Los puntos de consolidación son una interconexión en el cableado horizontal que permite reconfiguraciones más sencillas en oficinas cambiantes y se permiten para un máximo de 12 áreas de trabajo (24 TOs).

La diferencia más visible entre un TP y una MUTO es que el TP requiere una conexión adicional (una TO) para cada cable horizontal. Las TP se utilizan en oficinas cambiantes donde las TO se irán moviendo de un sitio a otro y las MUTO en oficinas que necesitan concentrar sus TO.



4.2.2 Tipo de cableado

Los tipos de cable permitidos por la norma vigente son:

- **Cable de pares trenzados con o sin blindaje**.
- **Cable de fibra óptica multimodo de 62.5/125 µm**.
- **Cable de fibra óptica multimodo de 50/125 µm**.
- Cable de fibra óptica monomodo 8-10/125 µm (para largas distancias).

Se usarán preferentemente los tres primeros tipos de cable.

4.2.3 Administración

La administración es un aspecto esencial del cableado genérico. La administración incluye la identificación exacta y el registro de todos los componentes del sistema, así como las canalizaciones y los espacios (TC y ER). Un buen registro puede incluir diagramas de cableado, mapas de conectividad, localización de TOs...

Deben registrarse todos los cambios que se realicen y cuando se han realizado, preferentemente por ordenador, y preparar procedimientos adecuados de actualización.

Si se realizan test de aceptación deberían registrarse también sus resultados.

Cada elemento, canalización y espacio debe tener su identificación claramente visible. A cada elemento, canalización y espacio se le asignará una identificación (mediante colores, números o cadenas alfanuméricas) unívoca.

Cada TO debe etiquetarse de modo que referencie la impedancia del cable, su categoría y número de pares o bien el diseño de fibra óptica utilizado.

Los cables deben marcarse en ambos extremos.

La norma 606 es vital para el buen funcionamiento de su cableado estructurado ya que habla sobre la identificación de cada uno de los subsistemas basado en etiquetas, códigos y colores, con la finalidad de que se puedan identificar cada uno de los servicios que en algún momento se tengan que habilitar o deshabilitar. Esto es muy importante, ya que en la documentación que se debe entregar al usuario final, la norma dice que se tendrá que especificar la forma en que está distribuida la red, por dónde viaja, qué puntos conecta y los medios que utiliza (tipos de cables y derivaciones).

La norma **TIA/EIA 606** proporciona una guía que puede ser utilizada para la ejecución de la administración de los sistemas de cableado.

Resulta fundamental para lograr una cotización adecuada suministrar a los oferentes la mayor cantidad de información posible. En particular, es muy importante proveerlos de planos de todos los pisos, en los que se detallen:

1. Ubicación de los gabinetes de telecomunicaciones
2. Ubicación de ductos a utilizar para cableado vertical
3. Disposición detallada de los puestos de trabajo
4. Ubicación de los tableros eléctricos en caso de ser requeridos
5. Ubicación de pisoductos si existen y pueden ser utilizados

Para proveer un **esquema de información** sobre la administración del camino para el cableado de telecomunicación, espacios y medios independientes. Marcando con un código de color y grabando en estos los datos para la administración de los cables de telecomunicaciones para su debida identificación. La siguiente tabla muestra el código de color en los cables.

> NARANJA Terminación central de oficina VERDE Conexión de red / circuito auxiliar PURPURA Conexión mayor / equipo de dato BLANCO Terminación de cable MC a IC GRIS Terminación de cable IC a MC AZUL Terminación de cable horizontal CAFÉ Terminación del cable del campus AMARILLO Mantenimiento auxiliar, alarmas y seguridad ROJO Sistema de teléfono

Para el etiquetado del cableado, rosetas y otros elementos se sigue la norma 606-A o 606-B (siendo esta última la más moderna).

A continuación se muestra un ejemplo de etiquetado:

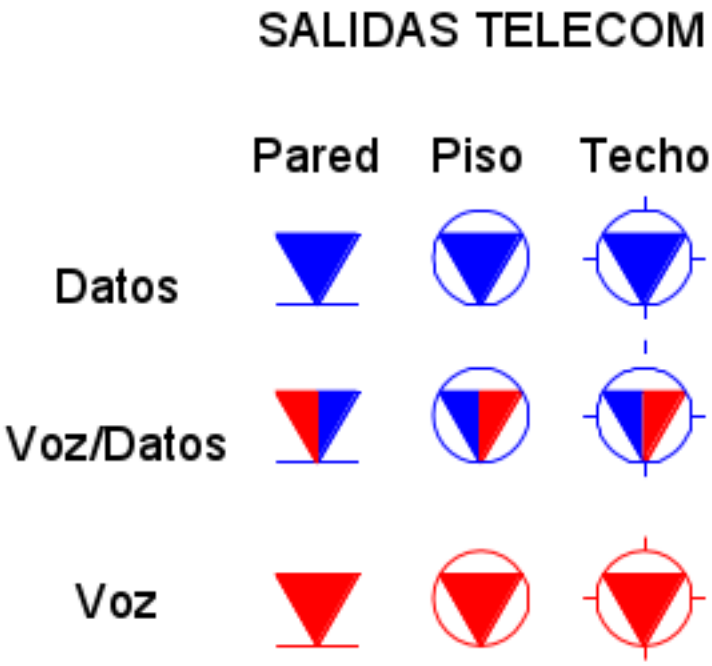
Esta imagen se corresponde con la etiqueta que identifica uno de los troncales en cobre de la red de cableado estructurado de un centro educativo.

El código que ves se ajusta a las especificaciones descritas por la norma americana TIA/EIA 606-A que aunque no es de obligado cumplimiento aquí, es de lejos la que mejor explica la gestión de un cableado estructurado. ¿Pero qué información contiene este código?

[E2-0A]/[E3-0A]-23

> Nuestra red se extiende por cuatro edificios que identificamos individualmente con dos dígitos (Ex). De tal manera que E1 significa Edificio 1 y E2, por ejemplo, Edificio 2. La norma 606-A se aplica en este caso dentro de la clase o categoría tres.

[E2-0A]


SALIDAS TELECOM
Pared
Piso
Techo
Datos
Voz/Datos
Voz


(E3-0A)-24
(E2-0A)/(E3-0A)-23
© 2012 EMTT

Es uno de lo extremos del troncal que empieza en el armario A de la planta baja (0) del Edificio 2. Esta filosofía es típica de la norma americana, se referencian los recintos, armarios y envolventes no los nombres de las salas, despachos o aulas. ¿La razón? pues es bien simple, lo primero cambia más difícilmente de nombre que lo segundo.

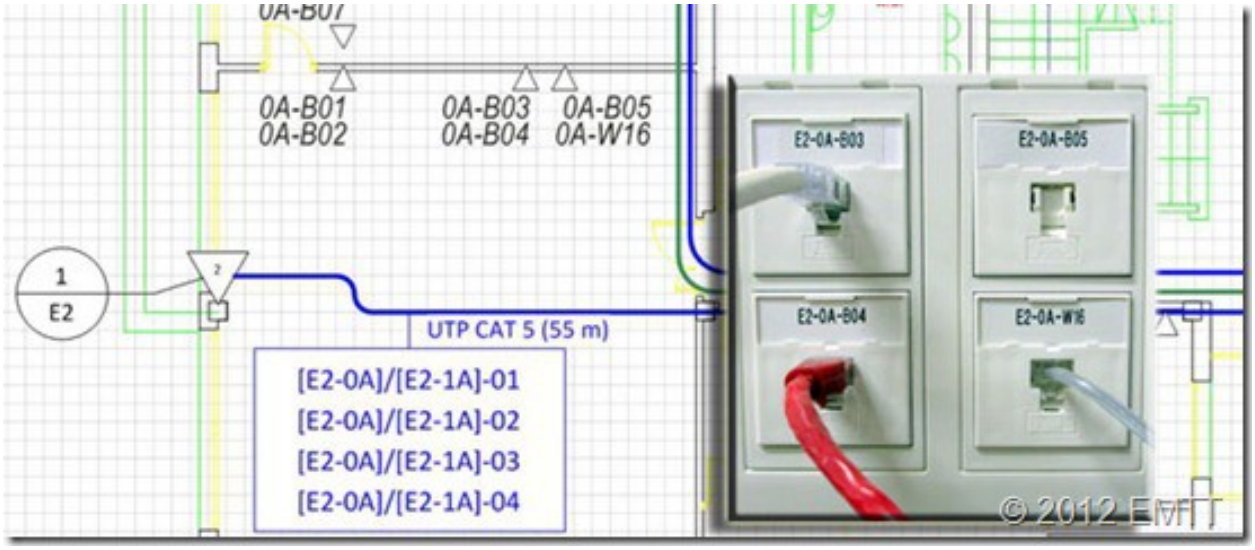
[E3-0A]

Es el otro extremo del troncal ubicado en el armario A de la planta baja del Edificio 3. La barra inclinada nos informa de que se trata de un troncal.

23

Identifica el número del troncal establecido entre ambos edificios.

La norma permite añadir más códigos, para diferenciar por ejemplo fibra de cobre aunque las etiquetas resultantes pueden llegar a ser bastante largas así que nosotros hemos optado por simplificar al máximo y basarnos en el complemento que aportan los planos de la instalación.



Vemos en esta otra imagen como quedan cuatro tomas de un puesto de trabajo en la distribución horizontal. Al trabajar en clase 3 se debe indicar siempre el edificio. En las tomas lo hacemos pues este modelo de Cima Box ofrece un buen espacio para poner bellas etiquetas, en el plano nos hemos tomado la licencia de no incluir el código de los edificios por ser obvio y con el fin de ganar en claridad.

E2-0A-B03

Nos informa de que esta toma viene del Edificio 2, planta baja, rack A. Dentro del armario se ubica en el panel de patcheo B, boca 03.

E2-0A-W16

Viene del mismo sitio pero de otro panel de patcheo diferente. En concreto se trata de telefonía así que la letra W pretende diferenciar esta cuestión directamente. Esta práctica no es obligada pero si aconsejada por la propia norma.

El nivel de detalle en el proyecto y la instalación al que se puede llegar aplicando esta norma es muy alto. Abarca tomas de tierra, recintos, canalizaciones, simbología, códigos de colores, planos y mucho más. Si te dedicas a esto y te gusta cuidar los detalles merece la pena leerse todo el documento. Un buen proyecto en manos de un buen instalador es algo que no puede terminar mal.

Cada elemento de la infraestructura se codifica y organiza en una base de datos donde pasa a denominarse registro. La imagen superior muestra parte de la información de uno de estos registros que incluimos al certificar.

4.3 Verificación y comprobación

Se puede hacer comprobaciones sobre el enlace permanente (lo más habitual, sirve para certificar una instalación) o sobre el canal completo.

Los procedimientos de verificación y comprobación se dividen en tres partes: rendimiento de enlace (sobre el cableado), transmisión (sobre los componentes del cableado) y medidas de los componentes.

4.3.1 Pruebas de rendimiento de los enlaces

En la norma se describe qué debe ser medido no cómo debe ser medido. Estas medidas suelen necesitar ser realizadas por expertos con maquinaria especializada.

Las pruebas de cables apantallados deben realizarse conectando la medida de toma de tierra.

Se comprueba las terminaciones, la calibración, la perdida de conversión longitudinal, la pérdida por retorno y el retardo de propagación.

Para fibra óptica se mide la atenuación, retardo de la propagación y pérdida óptica por retorno.

Las pruebas pueden usarse para:

- conformidad
- localización de errores
- aceptación (sobre cableado conforme)

Equipos de medida

Son equipos portátiles que se encargan de medir los parámetros para certificar los enlaces. Consta de 2 equipos. Uno principal donde se manejan y presentan los datos y otro remoto en el otro extremo con el que se comunica éste.

Disponen de latiguillos especiales certificados para que el latiguillo no sea fuente de posibles problemas. Normalmente tienen una conexión RS-232 o USB para pasar los datos a un PC.

Deben cumplir la normativa TSB67 y ser calibrados periódicamente.

Se les indica la clase de cableado que se pretende certificar y el tipo de cable que se utiliza y se realiza un “autotest”.

Los equipos indican si se pasa la certificación o no y qué parámetro queda fuera de los márgenes del estándar.

También comprueba el mapa de cableado por si se hubiera cruzado o conectado mal algún hilo.

Los principales parámetros que afectan la longitud máxima del enlace/canal son:

- atenuación,
- diafonía (crosstalk) -se mide su atenuación- (en cables de pares balanceados),
- ancho de banda (para fibra óptica),
- pérdida de retorno,
- retardo de propagación.

4.3.2 Cableado de par trenzado

Cartografía de las conexiones

Permite verificar las conexiones del cableado:

- Continuidad de los 8 hilos desde la pantalla o blindaje en su caso

- Ausencia de cortocircuitos entre los hilos
- Correcto emparejado de RJ45

Atenuación

La atenuación mide la disminución de la intensidad de la señal a lo largo de un cable (expresada en dB) debido a la impedancia y a la pérdida por radiación al ambiente. Es medida en cada par a diferentes frecuencias según la clase considerada. Es una medida crítica de la calidad del cable. Se mide en dB.

Algunos factores que la incrementan son la frecuencia, la distancia, la temperatura o la humedad. La reduce el apantallamiento.

No debe superar un máximo (deberá ser lo más bajo posible).

Atenuación diafónica

La diafonía es un tipo de interferencia (crosstalk) -acoplamiento electromagnético- entre pares de un mismo cable. La señal de un par induce una señal en los otros pares que se propaga en ambos sentidos. Se mide en dB.

La atenuación diafónica es la capacidad de un par para resistir una perturbación provocada por otro par (diafonía) medida para cada par del mismo lado del cable (6 mediciones para un cable de 4 pares), a diferentes frecuencias según la clase considerada. Permite medir la calidad del tendido del cable y de las conexiones.

Se mide en los dos extremos del cable:

- **NEXT** (Near-End Crosstalk) o paradiafónica en el extremo emisor.
- **FEXT** (Far-End Crosstalk) o telediafónica en el receptor.

El NEXT suele ser mayor que el FEXT y añade ruido a los datos de vuelta.

Como lo que se mide es la "pérdida" de la señal inducida, el valor de la atenuación paradiafónica deberá ser lo más alto posible -debe superar un mínimo-.

Es necesario limitar el destrenzado de los conductores a 13 mm como máximo para evitar el fenómeno de la paradiafonía. Es interesante anotar que la tecnología de procesamiento de señales digitales (DSP) puede realizar una cancelación de la paradiafonía.

Relación atenuación-diafonía (ACR: Attenuation/Crosstalk Ratio)

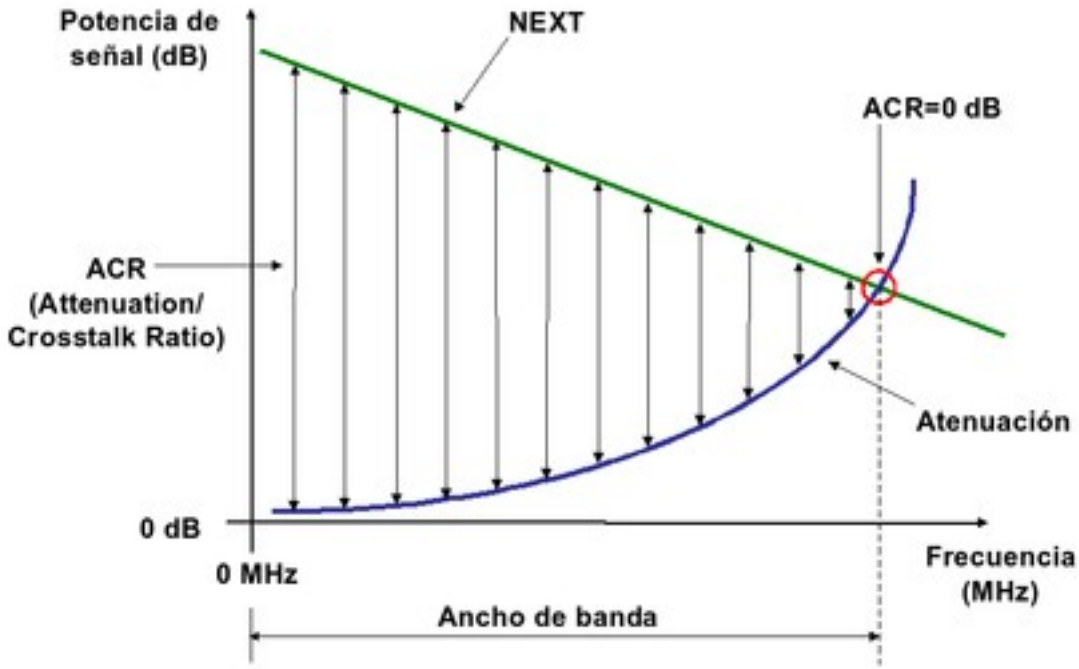
Determina la calidad de la transmisión en el cableado y es la relación entre la atenuación y NEXT (la atenuación de la diafonía del extremo cercano o paradiafonía):

ACR (dB) = NEXT (dB) - Atenuación (dB)

El valor de ACR ha de ser lo mayor posible -debe superar un mínimo-, ya que eso implica una NEXT elevada y una baja atenuación.

El ACR ayuda a definir el ancho de banda de una señal al establecer la máxima frecuencia útil donde la relación señal/ruido es suficiente para soportar ciertas aplicaciones (aquella en que ACR=0).

Se alcanza (aproximadamente) para Cat.3 con 16 MHz, para Cat. 5e con 100 MHz, para Cat. 6 con 250 MHz y para Cat.7 con 600 MHz.



Pérdida de retorno (Return loss)

Es la relación entre lo que se emite por un par y lo que vuelve por el mismo par, debido a rebotes en los empalmes. Esta pérdida debe ser lo más alta posible -debe superar un mínimo-. Se mide en dB.

Algunas aplicaciones como Gigabit Ethernet utilizan un esquema de codificación de transmisión full-duplex en que las señales de transmisión y recepción están superpuestas en el mismo par conductor. Este tipo de aplicaciones son más sensibles a errores resultantes por el retorno de la señal.

Otras pruebas y medidas

- Retardo de propagación: El tiempo que tarda la señal en llegar al otro extremo. Se espera que no supere un máximo.
- Variación del retardo (Delay Skew): Es la diferencia de retardo de propagación de la señal que hay de un par a otro. Comienza a medirse a partir de Cat. 5e para redes Gigabit. Se espera que no supere un máximo.
- Resistencia en continua: Resistencia ante el paso de corriente continua. Se espera que no supere un máximo.
- Paradiafonía en modo suma de potencias (PSNEXT: Power Sum NEXT): Es el acoplamiento provocado por la suma de las señales de 3 de los pares en el cuarto y medido en el extremo emisor. Como mide pérdidas, se espera que supere un mínimo.
- Relación Paradiafonía/Atenuación en modo suma de potencia (PSACR: Power Sum ACR): Es la diferencia PSNEXT - Atenuación (en decibelios). Se espera que supere un mínimo.
- Relación Telediafonía/Atenuación (ELFEXT): Es la diferencia FEXT - Atenuación (en decibelios). Se espera que supere un mínimo.
- Relación Telediafonía/Atenuación en modo suma de potencias (PSELFEXT: Power Sum ELFEXT): En este caso el acoplo que mide el FEXT será producto de la señal de los tres cables en el cuarto. Se espera que supere un mínimo.

Valores esperables

Los datos se calculan en base a fórmulas cuyos resultados dependen de la frecuencia. A continuación se muestra una tabla con valores límites a las máximas frecuencias de las principales clases de cable, calculados para 90 m de cable rígido y 10 m de cable flexible con 4 conectores.

▪	Atenuac dB	NEXT dB	ACR dB	Pérd.Ret dB	Ret.Pro µs	Var.Ret µs	PSNEXT dB	PSACR dB	ELFEXT dB	PSELFEXT dB
D 100 MHz	24,0	30,1	6,1	10,0	0,55	0,05	27,1	3,1	17,4	14,4
E 250 MHz	35,9	33,1	-2,8	8,0	0,55	0,05	30,2	-5,8	15,3	12,3
F 600 MHz	54,6	51,2	-3,4	8,0	0,55	0,05	48,2	-6,4	21,1	18,1

4.3.3 Cableado de fibra óptica

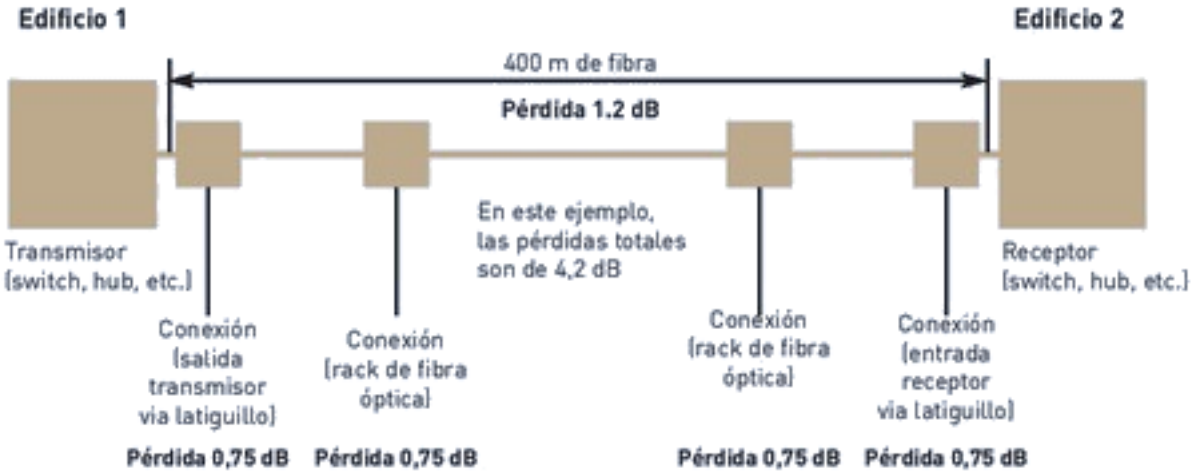
Los parámetros dependen de la ventana de transmisión que se mida: 850 (multimodo), 1310 (multimodo y monomodo) y 1550 (monomodo) nm.

Atenuación óptica

Pérdida de señal en el otro extremo debido al comportamiento del medio físico. Se mide en dB/Km.

Aumenta con la distancia, los empalmes y soldaduras, las curvas, la suciedad, la temperatura y el envejecimiento de la instalación.

Se espera que no supere un máximo. La atenuación máxima es del orden de 0,3 dB por cada 100 m de fibra y de 0,75 dB por conexión (par de conectores).



Ancho de banda modal

Es una medida de la capacidad de frecuencia de transmisión -ensanchamiento del pulso- en fibras multimodo. Es importante en conexiones de alta velocidad (Gigabit). Se mide en MHz*Km y debe superar un mínimo.

Pérdida de retorno (Return Loss)

Es la relación entre lo que se emite por una fibra y lo que vuelve por ella, debido a rebotes en los empalmes. Esta pérdida debe ser lo más alta posible -debe superar un mínimo-. Se mide en dB.

Se considera un fenómeno de eco. Indica la compatibilidad entre unos componentes de la instalación.

Retardo de propagación

Es el tiempo que tarda la señal en llegar al otro extremo. Se espera que no supere un máximo.

Valores esperables

Los datos se calculan en base a fórmulas cuyos resultados dependen de la ventana de transmisión y la distancia. A continuación se muestra una tabla con valores límites de las principales clases de cable, calculados para 300 m de fibra.

▪	Multi 850 nm	Multi 1300 nm	Mono 1310 nm	Mono 1550 nm
Atenuación dB / Km	3,5	1,50	1,00	1,00
Ancho de banda Mhz - Km	200	500	N/A	N/A

4.4 Referencias

- Redes locales. Ed. Macmillan Profesional
- Proyecto de Cableado Estructurado del Ayto. de Alhama de Murcia (PDF)
- Proyecto de Cableado Estructurado de Centro Cívico de Arona, Islas Canarias (PDF)
- Proyecto de Cableado Estructurado de Casa Consistorial de Archez, Málaga (PDF)
- Tutorial de Comunicaciones Ópticas
- Catálogos en PDF de FibreFab para fibra óptica
- Catálogo completo on-line de Hyperline
- Productos de Hyperline
- Productos de FlukeNetworks para certificación
- Blog marismas-emtt sobre redes y comunicaciones
- Blog guimi.net con recursos muy variados
- Vídeo: Timelapse de presentación
- Vídeo: Ejemplo virtual con Sketchup
- Vídeo: Preparación de rosetas y panel de parcheo (en inglés)

4.5 Actividades

4.5.1 Enunciado

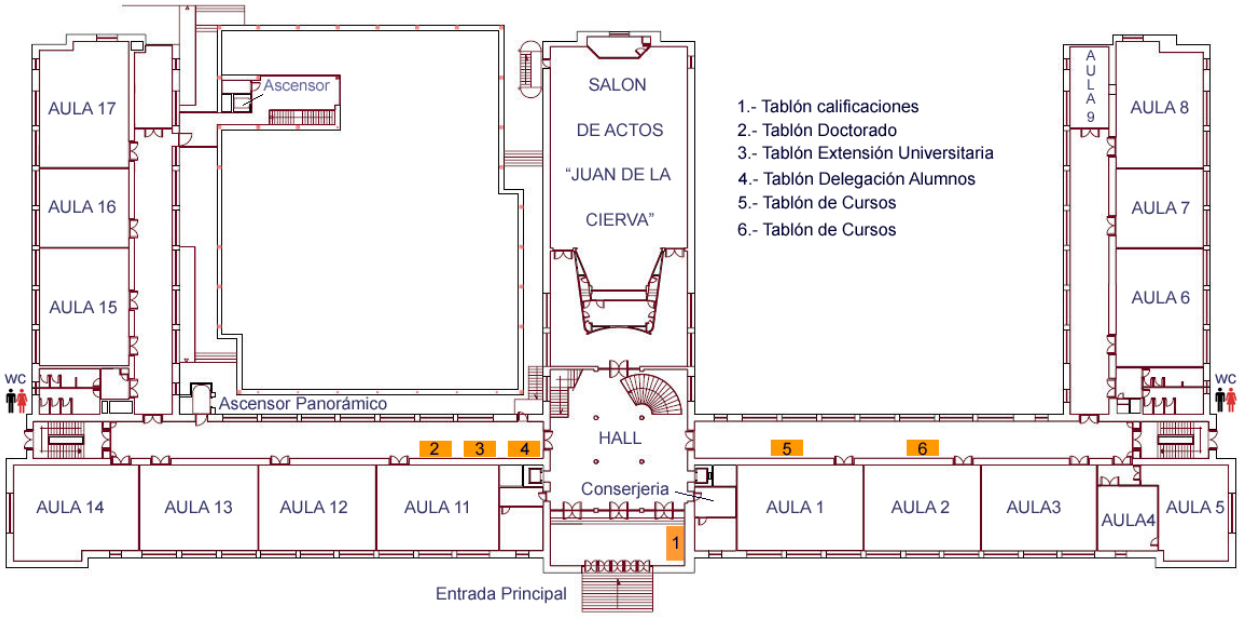
Tenemos una empresa de servicios informáticos y nos han contratado para desplegar el cableado estructurado de una universidad. El campus está compuesto por 2 edificios separados 700 metros entre si. La acometida telefónica se sitúa en la planta baja del primer edificio (Junto al aula 4). Tenemos libertad para elegir los espacios donde se pondrán los cuartos de comunicaciones o equipos. Y no tenemos limitación en el presupuesto.

Los planos son los siguientes:

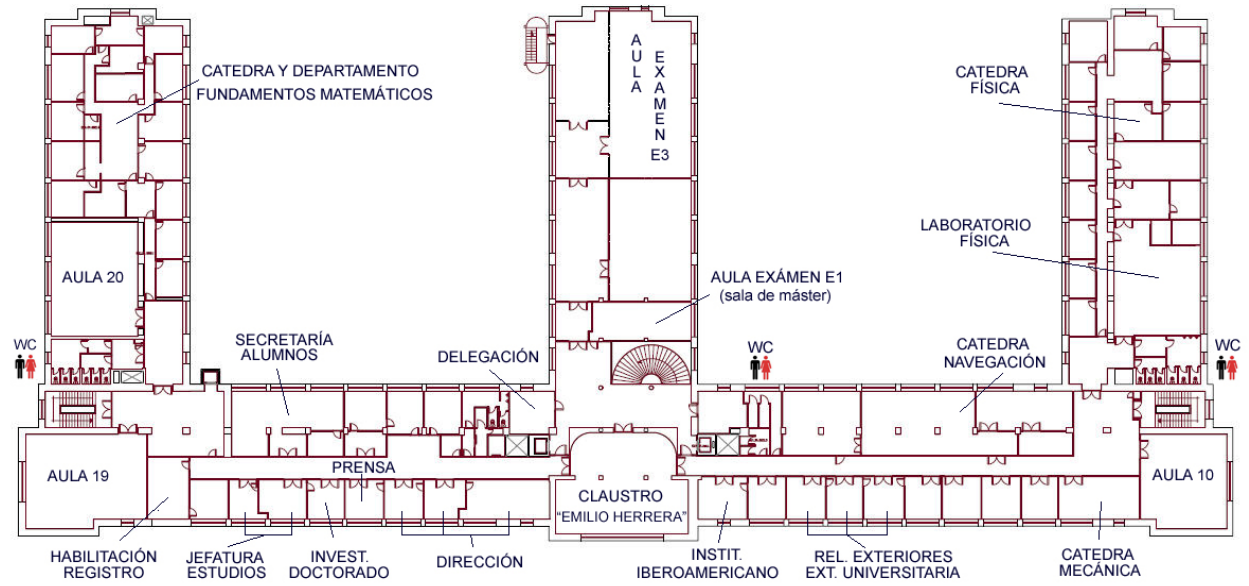
Primer edificio

- Fachada: 120 metros
- Profundidad: 60 metros

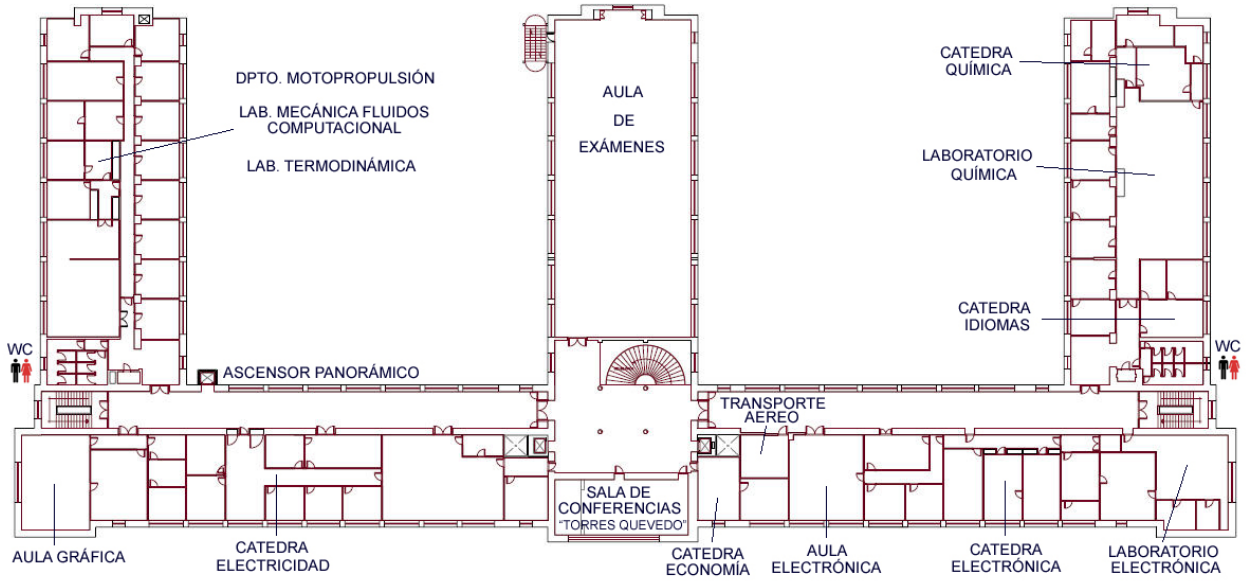
Planta baja



Planta primera



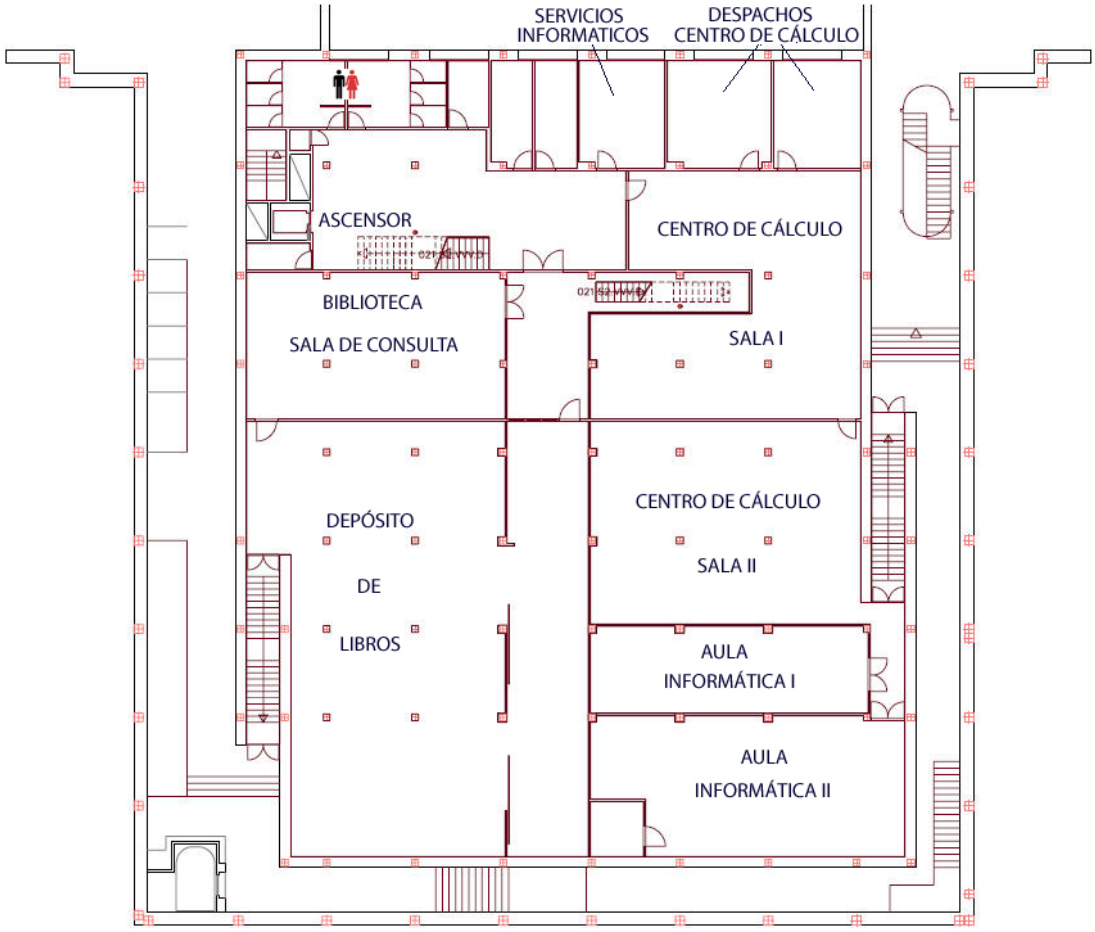
Planta segunda



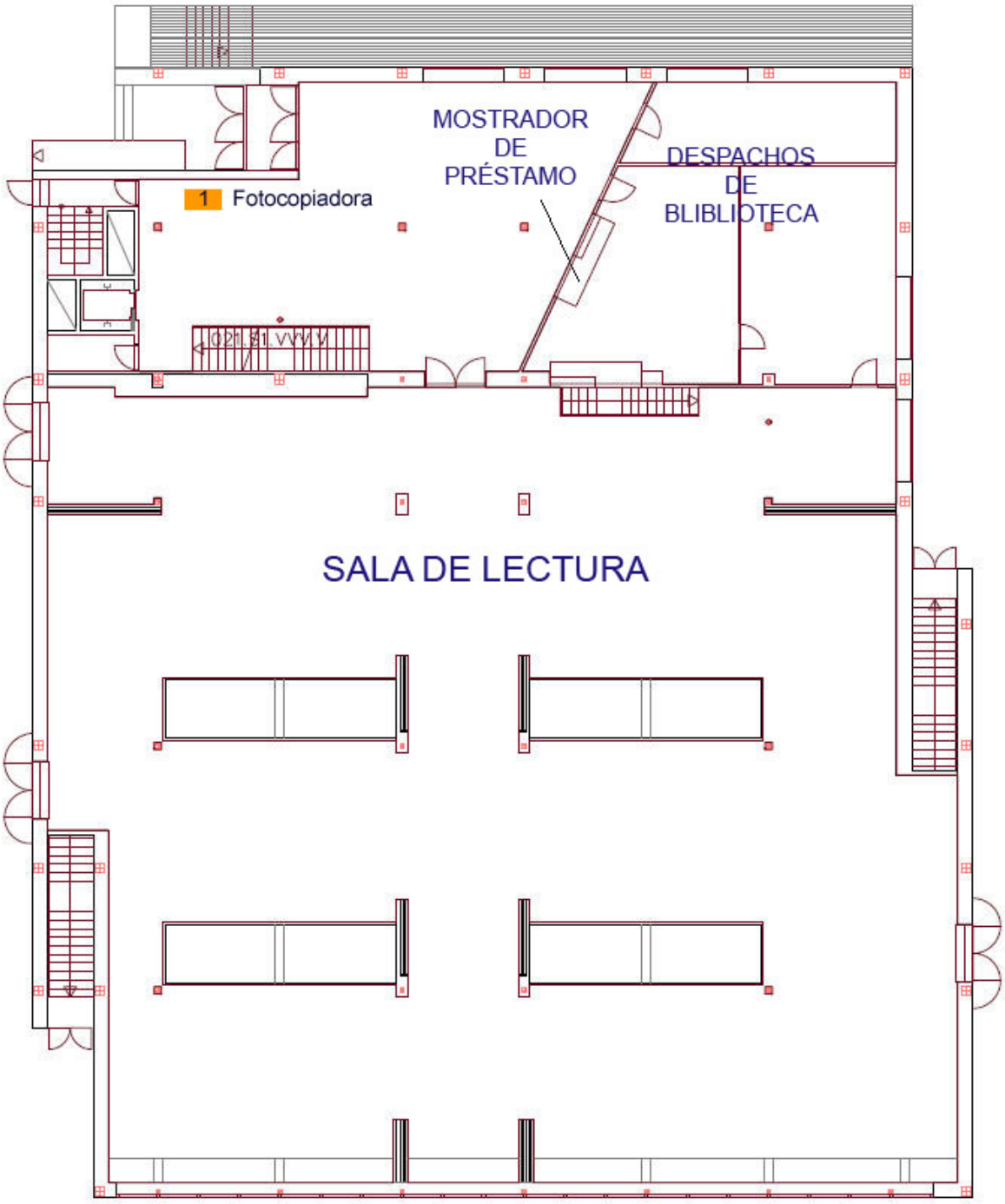
Segundo edificio

- Fachada: 50 metros.
- Profundidad: 60 metros.

Planta baja



Planta primera



4.5.2 Ejercicios

1. Indica qué dependencias serán los cuartos de comunicaciones.
2. Indica qué áreas de trabajo dispondrán de cableado de datos y para cuantos equipos.
3. Indica cuánto material necesitarás.

- Armarios

- Cables trenzados y fibra óptica
- Conectores
- Routers
- Switches
- Puntos de acceso inalámbricos
- Rosetas
- Canaletas
- Paneles de parcheo
- Cualquier otro material que necesites.

4. Haz un presupuesto (sólo para material, sin incluir mano de obra ni herramientas necesarias). Para ello consulta precios en las siguientes webs:

- http://www.cablematic.es
- http://www.cablecom.es
- http://www.senetic.es
- http://esp.hyperlinesystems.com
- http://www.universalnetworks.co.uk

CAPÍTULO 5

SEGURIDAD Y PROTECCIÓN MEDIOAMBIENTAL

5.1 Seguridad y salud laboral

La **seguridad y salud laboral** (denominada anteriormente como «seguridad e higiene en el trabajo») tiene por objeto la aplicación de medidas y el desarrollo de las actividades necesarias para la prevención de riesgos derivados del trabajo.

El concepto de **salud** es definido por la Constitución de 1946 de la Organización Mundial de la Salud como el caso de **completo bienestar físico, mental y social**, y no solamente la ausencia de afecciones o enfermedades. También puede definirse como el nivel de eficacia funcional o metabólica de un organismo tanto a nivel micro (celular) como en el macro (social).

Para prevenir los daños a la salud ocasionados por el trabajo está constituida la **Organización Internacional del Trabajo (OIT)**; es un organismo especializado de las Naciones Unidas de composición tripartita que reúne a gobiernos, empleadores y trabajadores de sus estados miembros con el fin de emprender acciones conjuntas destinadas a promover el trabajo decente en el mundo.

5.1.1 Marco internacional

- La **convención de 1981 de la OIT sobre la Seguridad y Salud nº 155** y sus recomendaciones nº 164, dispone que se adopten medidas políticas nacionales de seguridad y salud en el trabajo y estipula las actuaciones necesarias tanto a nivel nacional como a nivel empresarial para impulsar la seguridad y salud en el trabajo y la mejora del medioambiente.
- **La convención de 1985 de la OIT sobre Seguridad y Salud, nº 161** y sus recomendaciones nº 171, dispone la creación de servicios de salud laboral que contribuyan a la implantación de las medidas políticas de seguridad y salud en el trabajo.
- 1998, instrucciones técnicas y éticas para la vigilancia de la salud de los trabajadores.

Unión Europea

A nivel de la Unión Europea existen los siguientes organismos relacionados con la Seguridad y la Salud en el Trabajo.

- El Comité Consultivo para la Seguridad, la Higiene y la Protección de la Salud en el Centro de Trabajo.
- Agencia Europea para la Seguridad y Salud en el Trabajo, con sede en Bilbao (España).
- Fundación Europea para la Mejora de las Condiciones de Vida y de Trabajo, con sede en Dublín (Irlanda).
- La Comisión Internacional de Salud Laboral (ICOH)
- La Asociación Internacional de la Seguridad Social (ISSA)

5.1.2 Riesgo laboral

Se denomina «riesgo laboral» a **todo aquel aspecto del trabajo que tiene la potencialidad de causar un daño**. La prevención de riesgos laborales es la disciplina que busca promover la seguridad y salud de los trabajadores mediante la identificación, evaluación y control de los peligros y riesgos asociados a un proceso productivo, además de fomentar el desarrollo de actividades y medidas necesarias para prevenir los riesgos derivados del trabajo.

5.1.3 Planificación y acción preventiva

En España, por ejemplo la **Ley 31/1995, de 8 de noviembre de Prevención de Riesgos Laborales** (que desarrolla el artículo 40.2 de la Constitución Española), en la exposición de motivos, expone entre otros argumentos los siguientes:

> La protección del trabajador frente a los riesgos laborales exige una actuación en la empresa que desborda el mero cumplimiento formal de un conjunto predeterminado, más o menos amplio, de deberes y obligaciones empresariales y, más aún, la simple corrección a posteriores situaciones de riesgo ya manifestadas. La planificación de la prevención desde el momento mismo del diseño del proyecto empresarial, la inicial evaluación de los riesgos laborales y su actualización periódica a medida que se alteren las circunstancias, la ordenación de un conjunto coherente y globalizador de medidas de acción preventiva adecuadas a la naturaleza de los riesgos detectados y el control de la efectividad de dichas medidas constituyen los elementos básicos del nuevo enfoque en la prevención de riesgos laborales. Y, junto a ello, se completa con la información y la formación de los trabajadores dirigidas a un mejor conocimiento tanto del alcance real de los riesgos derivados del trabajo como de la forma de prevenirlos y evitarlos, de manera adaptada a las peculiaridades de cada centro de trabajo, a las características de las personas que en él desarrollan su prestación laboral y a la actividad concreta que realizan.
>
> Ley de prevención de riesgos laborales España

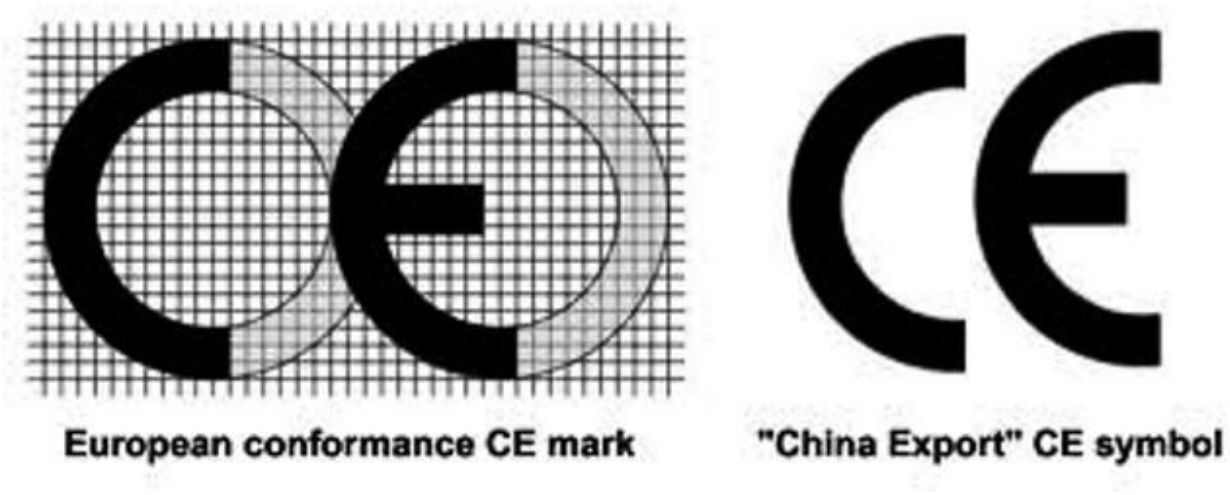
Maquinaria, equipos, productos y útiles de trabajo

No sólo el empresario que tiene un trabajador queda obligado por la normativa de prevención de riesgos laborales, sino que **se suelen establecer también obligaciones que afectan a los fabricantes, importadores y suministradores de maquinaria, equipos, productos y útiles de trabajo**. Un logotipo para este fin es el CE mark.

Nota: Aunque se parece al anterior, **el símbolo CE de "China Export" no conlleva el cumplimiento de ningún tipo de normativa específica**. Únicamente es utilizado para indicar que el producto proviene de China.

5.1.4 Evaluación de riesgos laborales

La evaluación de los riesgos laborales es el **proceso dirigido a estimar la magnitud de aquellos riesgos que no hayan podido evitarse**, obteniendo la información necesaria para que el empresario esté en condiciones de tomar una decisión apropiada sobre la necesidad de adoptar medidas preventivas y, en tal caso, sobre el tipo de medidas que deben adoptarse. Pueden ser necesarias medidas tales como:



- **Eliminar o reducir el riesgo, mediante medidas de prevención** en el origen, organizativas, de protección colectiva, de protección individual, o de formación e información a los trabajadores.
- **Controlar periódicamente las condiciones**, la organización y los métodos de trabajo y el estado de salud de los trabajadores.

El 28 de abril se celebra el Día Mundial de la Seguridad y Salud en el Trabajo. Para la evaluación de la magnitud de los riesgos existe un método que basa la estimación de riesgos para cada peligro, en la determinación de la potencial severidad del daño (consecuencias) y la probabilidad de que ocurra el hecho. De esta forma, en el ámbito de la **severidad del daño**, se clasifican en:

- **ligeramente dañino**, como los daños superficiales y las molestias e irritación;
- **dañino**, cuando se trata de quemaduras, conmociones, fracturas menores, sordera, dermatitis, asma, etc.; y
- **extremadamente dañino**, en casos de amputaciones, fracturas mayores, envenenamientos, cáncer o enfermedades agudas y que acorten severamente la vida.

En cuanto a la **probabilidad** de que el daño ocurra, se manejan tres categorías:

- **baja**, cuando el daño ocurrirá raras veces;
- **media**, si ocurrirá algunas veces, y
- **alta**, cuando ocurrirá siempre o casi siempre.

5.1.5 Grupos y especialidades

A efectos de determinación de las capacidades y aptitudes necesarias para la evaluación de los riesgos y el desarrollo de la actividad preventiva, las funciones a realizar se clasifican en los siguientes grupos :

1. Funciones de nivel básico.
2. Funciones de nivel intermedio.
3. Funciones de nivel superior, correspondientes a las **especialidades y disciplinas preventivas de**:
    - **medicina del trabajo**
    - **seguridad en el trabajo**
    - **higiene industrial**

- **ergonomía y psicosociología aplicada**.

Higiene Industrial

La higiene industrial conforma un conjunto de conocimientos y técnicas dedicados a reconocer, evaluar y controlar aquellos factores del ambiente, psicológicos o tensionales, que provienen, del trabajo y pueden causar enfermedades o deteriorar la salud.

La Higiene industrial está conformada por un conjunto de normas y procedimientos tendientes a la protección de la integridad física y mental del trabajador, preservándolo de los riesgos de salud inherentes a las tareas del cargo y al ambiente físico donde se ejecutan.

Está relacionada con el **diagnóstico y la prevención de enfermedades ocupacionales** a partir del estudio y control de dos variables: el hombre y su ambiente de trabajo.

Posee un **carácter eminentemente preventivo**, ya que se dirige a la salud y a la comodidad del empleado, evitando que éste enferme o se ausente de manera provisional o definitiva del trabajo.

Objetivos de la Higiene Industrial

- Reconocer los agentes del medio ambiente laboral que pueden causar enfermedad en los trabajadores.
- Evaluar los agentes del medio ambiente laboral para determinar el grado de riesgo a la salud.
- Eliminar las causas de las enfermedades profesionales.
- Reducir los efectos perjudiciales provocados por el trabajo en personas enfermas o portadoras de defectos físicos.
- Prevenir el empeoramiento de enfermedades y lesiones.
- Mantener la salud de los trabajadores.
- Aumentar la productividad por medio del control del ambiente de trabajo.
- Proponer medidas de control que permitan reducir el grado de riesgo a la salud de los trabajadores.
- Capacitar a los trabajadores sobre los riesgos presentes en el medio ambiente laboral y la manera de prevenir o minimizar los efectos indeseables.

Ergonomía en el trabajo

El diseño ergonómico del puesto de trabajo **intenta obtener un ajuste adecuado entre las aptitudes o habilidades del trabajador y los requerimientos o demandas del trabajo**. El objetivo final, es optimizar la productividad del trabajador y del sistema de producción, al mismo tiempo que garantizar la satisfacción, la seguridad y salud de los trabajadores.

El diseño ergonómico del puesto de trabajo debe tener en cuenta las características antropométricas de la población, la adaptación del espacio, las posturas de trabajo, el espacio libre, la interferencia de las partes del cuerpo, el campo visual, la fuerza del trabajador y el estrés biomecánico, entre otros aspectos. Los aspectos organizativos de la tarea también son tenidos en cuenta.

Para diseñar correctamente las condiciones que debe reunir un puesto de trabajo se tiene que tener en cuenta, entre otros, los siguientes factores:

- Los riesgos de carácter mecánico que puedan existir.
- Los riesgos causados por una postura de trabajo incorrecta fruto de un diseño incorrecto de asientos, taburetes, etc.

- Riesgos relacionados con la actividad del trabajador (por ejemplo, por las posturas de trabajo mantenidas, sobreesfuerzos o movimientos efectuados durante el trabajo de forma incorrecta o la sobrecarga sufrida de las capacidades de percepción y atención del trabajador).
- Riesgos relativos a la energía (la electricidad, el aire comprimido, los gases, la temperatura, los agentes químicos, etc.)

El diseño adecuado del puesto de trabajo debe servir para:

- Garantizar una correcta disposición del espacio de trabajo.
- Evitar los esfuerzos innecesarios. Los esfuerzos nunca deben sobrepasar la capacidad física del trabajador.
- Evitar movimientos que fuercen los sistemas articulares.
- Evitar los trabajos excesivamente repetitivos.

5.1.6 Prevención de riesgos laborales

Los siniestros laborales pueden deberse a condiciones medioambientales del centro de trabajo, condiciones físicas del trabajo, condiciones del puesto de trabajo y condiciones derivadas del sistema organizativo del trabajo. Cada riesgo laboral lleva conexo un plan preventivo para evitarlo o paliar su gravedad. Un siniestro puede ocasionarse:

- por **ignorancia de los riesgos** que se corren
- por una **actuación negligente**, es decir, no tomar las precauciones necesarias para ejecutar una tarea o
- por una **actitud temeraria** de rechazar los riesgos que están presentes en el área de trabajo.

Consejos básicos

- Proteger la vista de la radiación ultravioleta.
- Protegerse del aire acondicionado.
- Protección de las manos cuando se hace uso de productos químicos.
- Utilización de ropa adecuada contra el frío.
- Protección del riesgo solar.
- Correcto tratamiento de las posibles quemaduras.
- Plan de actuación en situaciones de emergencia.

Normas básicas de seguridad y salud

Las normas básicas de seguridad y salud en los centros de trabajo condicionan de forma significativa las condiciones generales de trabajo y son un conjunto de medidas destinadas a proteger la salud de los trabajadores, prevenir accidentes laborales y promover el cuidado de la maquinaria, herramientas y materiales con los que se trabaja. Las normas se concretan en un conjunto de prácticas de sentido común donde **el elemento clave es la actitud responsable y la concienciación de todas las personas a las que afecta**.

La eficacia de la norma se concreta en el siguiente principio:

> **Respételas y hágalas respetar**.

El cumplimiento de estos aspectos aumentará el sentido de seguridad y salud de los trabajadores y disminuirán los riesgos profesionales de accidentes y enfermedades en el trabajo. Las empresas deben llevar un registro en un libro adecuado y visado de todos los siniestros laborales que se producen indicando la fecha, hora, partes y personas afectadas y tipo de **gravedad del accidente: leve, grave, o mortal**. Con el registro de los accidentes de trabajo se establecen

las **estadísticas de siniestralidad laboral** a nivel de empresa y de otros ámbitos superiores territorialmente o sectorialmente. De acuerdo con las estadísticas de siniestralidad se establecen los planes, campañas o proyectos de prevención de accidentes laborales.

5.1.7 Riesgos laborales

Los riesgos laborales pueden clasificarse en 3 grandes grupos:

- De **carácter medioambiental**
- Relacionados con el **lugar de trabajo y los equipos o máquinas** que se manipulan
- Relacionados con la **ergonomía y la psicosociología aplicada**.

De carácter medioambiental

- Aspecto general del centro de trabajo
- Climatización
- Ventilación industrial
- Contaminantes biológicos
- Contaminantes químicos
- Iluminación
- Radiaciones
- Ruidos

Las condiciones ambientales pueden resultar nocivas tanto para la salud física como para la salud psíquica en función de una serie de perturbaciones; estas condiciones son las que se conocen como **riesgo higiénico**.

Aspecto general del centro de trabajo

El aspecto general de un centro de trabajo viene definido por la seguridad estructural que ofrezcan sus edificios, es decir, ausencia de riesgos de desprendimientos o hundimientos por ser excesivamente antiguos o estar sobrecargados; no estar afectado por el síndrome del edificio enfermo; ausencia de riesgos medioambientales tanto con emisión de contaminantes a la atmósfera como contaminación de aguas o tierras por residuos o emisiones en los desagües; control de los riesgos físicos que puedan sufrir los trabajadores en sus puestos de trabajo donde estén dotados de sus equipos de protección individual (EPI); señalización adecuada de los accesos al centro de trabajo; luminosidad y cuidado del entorno y tener señalizados y organizados planes de evacuación rápidos y seguros.

Climatización

Las condiciones de trabajo climáticas son la temperatura y la humedad en las que se desarrolla un trabajo. El trabajo físico genera calor en el cuerpo. Para regularlo, el organismo humano posee un sistema que permite mantener una temperatura corporal constante en torno a los 37 °C. La regulación térmica y sensación de confort térmico depende del calor producido por el cuerpo y de los intercambios con el medio ambiente. Todo ello está en función de:

- Temperatura del ambiente.
- Humedad del ambiente.
- Actividad física que se desarrolle.

- Clase de vestimenta.

Unas malas condiciones termohigrométricas pueden ocasionar efectos negativos en la salud que variarán en función de las características de cada persona y su capacidad de aclimatación, así **podemos encontrar resfriados, congelación, deshidratación, golpes de calor y aumento de la fatiga, lo que puede incidir en la aparición de accidentes**.

Se puede producir **riesgo de estrés térmico** por calor en ambientes con temperatura del aire alta (zonas de clima caluroso, verano), radiación térmica elevada (fundiciones, acerías, fábricas de ladrillos y de cerámica, plantas de cemento, hornos, panaderías, etc.), altos niveles de humedad (minas, lavanderías, fábricas de conservas, etc.), en lugares donde se realiza una actividad intensa o donde es necesario llevar prendas de protección que impiden la evaporación del sudor. En caso de la realización de tareas en el exterior hay que contemplar también otros factores climáticos como la exposición al sol, capaz de causar cáncer de piel.

Ventilación industrial

La ventilación industrial se refiere al conjunto de tecnologías que se utilizan para neutralizar y eliminar la presencia de calor, polvo, humo, gases, condensaciones, olores, etc. en los lugares de trabajo, que puedan resultar nocivos para la salud de los trabajadores. Muchas de estas partículas disueltas en la atmósfera no pueden ser evacuadas al exterior porque pueden dañar el medio ambiente.

En esos casos surge la necesidad, de reciclar estas partículas para disminuir las emisiones nocivas al exterior, o en su caso, proceder a su recuperación para reincorporarlas al proceso productivo. Ello se consigue mediante un equipo adecuado de captación y filtración. Según sean las partículas, sus componentes y las cantidades generadas exigen soluciones técnicas específicas.

Para evitar que los vapores y humos se disipen por todo el recinto de las naves industriales se realiza la instalación de campanas adaptadas al mismo foco de producción de residuos para su total captación. El caudal procedente de la zona de captación se conduce hacia el filtro correspondiente según el producto e instalación, donde se separan las partículas del aire limpio.

Los sistemas de ventilación industrial pueden ser:

- **Ventilación estática o natural**: mediante la colocación de extractores estáticos situados en las cubiertas de las plantas industriales aprovechan el aire exterior para ventilar el interior de las naves industriales y funcionan por el efecto Venturi (Principio de Bernoulli)
- **Ventilación dinámica o forzada**: se produce mediante ventiladores extractores colocados en lugares estratégicos de las cubiertas de las plantas industriales.

Cuando la concentración de un agente nocivo en el ambiente del puesto de trabajo supere el valor límite ambiental los trabajadores tienen que utilizar los equipos de protección individual adecuados para proteger las vías respiratorias.

Contaminantes biológicos

El concepto de agente biológico incluye, pero no está limitado, a bacterias, hongos, virus, protozoos, rickettsias, clamidias, endoparásitos humanos, productos de recombinación, cultivos celulares humanos o de animales y los agentes biológicos potencialmente infecciosos que estas células puedan contener, priones y otros agentes infecciosos.

Las principales vías de penetración en el cuerpo humano son:

- **Vía respiratoria**: a través de la inhalación.
- **Vía dérmica**: por contacto con la piel, en muchas ocasiones sin causar erupciones ni alteraciones notables.

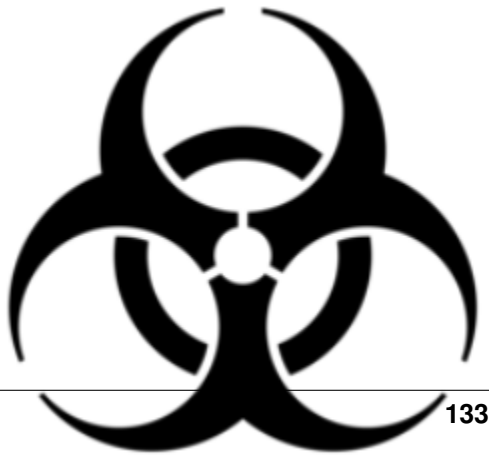


Figura 1: Símbolo de riesgo biológico

- **Vía digestiva**: a través de la boca, esófago, estómago y los intestinos, generalmente cuando existe el hábito de ingerir alimentos, bebidas o fumar en el puesto de trabajo.
- **Vía parenteral**: por contacto con heridas que no han sido protegidas debidamente.

Cuando las condiciones de trabajo puedan ocasionar que se introduzcan en el cuerpo humano, los contaminantes biológicos pueden provocar en el mismo **un daño de forma inmediata** (intoxicación aguda) **o a largo plazo** (enfermedad profesional al cabo de los años).

Contaminantes químicos

Se denomina contaminante químico al elemento o compuesto químico cuyas características de estado le permiten entrar en el organismo humano, pudiendo originar un efecto adverso para su salud.

Las principales vías de penetración en el cuerpo humano son:

- **Vía respiratoria**: a través de la inhalación.
- **Vía dérmica**: por absorción cutánea.
- **Vía digestiva**: por ingestión.

Los contaminantes químicos pueden provocar en el mismo **un daño de forma inmediata** (intoxicación aguda) **o a largo plazo** (enfermedad profesional al cabo de los años).

La **toxicidad** es uno de los factores que determinan el riesgo, pero éste responde además a otros varios factores, como la intensidad y la duración de la exposición, la volatilidad del compuesto y el tamaño de las partículas. El concepto de toxicidad se refiere a los efectos biológicos adversos que pueden aparecer tras la interacción de la sustancia con el cuerpo, mientras que el concepto del riesgo incluye además la probabilidad de que se produzca una interacción efectiva.

Figura 2: Símbolo de sustancia nociva o irritante

Iluminación

La fatiga visual se ocasiona si los lugares de trabajo y las vías de circulación no disponen de suficiente iluminación, ya sea natural o artificial, adecuada y suficiente durante la noche y cuando no sea suficiente la luz natural.

Las instalaciones de iluminación de los locales, de los puestos de trabajo y de las vías de circulación deberían estar colocadas de tal manera que el tipo de iluminación previsto no suponga riesgo de accidente para los trabajadores.

Los locales, los lugares de trabajo y las vías de circulación en los que los trabajadores estén particularmente expuestos a riesgos en caso de avería de la iluminación artificial deben poseer una iluminación de seguridad de intensidad suficiente.

La iluminación deficiente ocasiona fatiga visual en los ojos, perjudica el sistema nervioso, ayuda a la deficiente calidad de trabajo y es responsable de una buena parte de los accidentes de trabajo. Un sistema de iluminación debe cumplir los siguientes requisitos:

- La iluminación tiene que ser suficiente y la necesaria para cada tipo de trabajo.
- La iluminación tiene que ser constante y uniformemente distribuida para evitar la fatiga de los ojos, que deben acomodarse a la intensidad variable de la luz. Deben evitarse contrastes violentos de luz y sombra, y las oposiciones de claro y oscuro.
- Los focos luminosos tienen que estar colocados de manera que no deslumbren ni produzcan fatiga a la vista debido a las constantes acomodaciones.

Radiaciones

Las radiaciones **son ondas electromagnéticas** de energía o partículas cargadas que, al incidir sobre el organismo humano, pueden llegar a producir efectos dañinos para la salud de los trabajadores.

Los efectos para la salud dependen de la dosis absorbida por el organismo pudiendo afectar a distintos tejidos y órganos (médula ósea, órganos genitales ...) **provocando desde náuseas, vómitos o cefaleas hasta alteraciones cutáneas y cáncer**.

Para protegerse de las radiaciones se utilizan diversos medios, siendo los más eficaces: reducir al máximo la exposición a la radiación, añadir blindajes interpuestos entre las radiaciones y el trabajador y aumentar la distancia al foco de la radiación, ya que la intensidad de la radiación decrece con el cuadrado de la distancia.

Existen 2 tipos de radiaciones:

- **Ionizantes**
- **No ionizantes**

La **radiación ionizante** consiste en partículas, incluidos los fotones, que **causan la separación de electrones de átomos y moléculas**. Pero algunos tipos de radiación de energía relativamente baja, como la luz ultravioleta, sólo puede originar ionización en determinadas circunstancias. Para distinguir estos tipos de radiación de la radiación que siempre causa ionización, se establece un límite energético inferior arbitrario para la radiación ionizante, que se suele situar en torno a 10 kiloelectronvoltios (keV).

Figura 3: Símbolo de radiación ionizante

Se entiende por **radiación no ionizante** aquella onda o partícula que **no es capaz de arrancar electrones de la materia** que ilumina produciendo, como mucho, excitaciones electrónicas.

El término radiación no ionizante hace referencia a la interacción de ésta con la materia; al tratarse de frecuencias consideradas "bajas" y por lo tanto también energías bajas por fotón, en general, su efecto es potencialmente menos peligroso que las radiaciones ionizantes.

Las principales radiaciones no ionizantes son:

- Microondas
- Luz láser
- Rayos infrarrojos
- Luz visible

La frecuencia de la radiación no ionizante determinará en gran medida el efecto sobre la materia o tejido irradiado; por ejemplo, las microondas portan frecuencias próximas a los estados vibracionales de las moléculas del agua, grasa o azúcar, al "acoplarse" con las microondas se calientan. La región infrarroja también excita modos vibracionales; esta parte del espectro corresponde a la llamada radiación térmica. Por último la región visible del espectro por su frecuencia es capaz de excitar electrones, sin llegar a arrancarlos.

Figura 4: Símbolo de radiación no ionizante

Ruidos

Los trabajadores sometidos a altos niveles de ruido en su puesto de trabajo, **aparte de sufrir pérdidas de su capacidad auditiva pueden llegar a la sordera, acusan una fatiga nerviosa que es origen de una disminución de la eficiencia** humana tanto en el trabajo intelectual como en el manual.

Se puede definir al ruido como un sonido no deseado e intempestivo y por lo tanto molesto, desagradable y perturbador. **El nivel de ruido se mide en decibelios (dB)**. Hay un nivel de ruido a partir del cual se considera peligrosa y se hace necesario protegerse del mismo con los elementos de seguridad adecuados.

Disposiciones relativas a la exposición al ruido

Los riesgos derivados de la exposición al ruido deberán eliminarse en su origen o reducirse al nivel más bajo posible, teniendo en cuenta los avances técnicos y la disponibilidad de medidas de control del riesgo en su origen.

- Utilizar elementos de protección de ruido adecuados que amortigüen la mayor cantidad de ruido posible.
- Limitar la exposición al ruido.
- Adecuar la concepción y disposición de los lugares y puestos de trabajo.
- Ofrecer información y formación adecuadas para enseñar a los trabajadores a utilizar correctamente el equipo de trabajo con vistas a reducir al mínimo su exposición al ruido.

Para la reducción técnica del ruido deberá procederse a:

- Reducir el ruido aéreo, por ejemplo, por medio de pantallas, cerramientos, recubrimientos con material acústicamente absorbente.
- Reducir el ruido transmitido por cuerpos sólidos, por ejemplo mediante amortiguamiento o aislamiento.
- Establecer programas apropiados de mantenimiento de los equipos de trabajo, del lugar de trabajo y de los puestos de trabajo.
- Reducir del ruido mediante una nueva organización del trabajo.

Relacionados con el lugar de trabajo y los equipos o máquinas que se manipulan

- Sobreesfuerzo
- Manipulación de máquinas y herramientas peligrosas
- Espacios de trabajo y zonas peligrosas
- Puertas y portones
- Suelos, aberturas, desniveles y escaleras
- Prevención con vehículos de transporte y manipuleo de cargas

- Vibraciones mecánicas
- Riesgo eléctrico
- Riesgos de explosión por atmósfera explosiva
- Riesgos derivados de la inhalación de gases, vapores,líquidos y polvo
- Manipulación de sustancias tóxicas y/o corrosivas

Sobreesfuerzos

Los sobreesfuerzos son los trabajos físicos que se realizan por encima del esfuerzo normal que una persona pueda desarrollar en una tarea determinada.

Las patologías derivadas de los sobreesfuerzos son la primera causa de enfermedad en los profesionales. Los sobreesfuerzos suponen casi el 30 por ciento de la siniestralidad laboral de tipo leve y se eleva al 85 % en las enfermedades que padecen los profesionales.

Para evitar los trastornos musculoesqueléticos en los que deriva el sobreesfuerzo, es necesario analizar los riesgos laborales de las condiciones de trabajo, la evaluación de estos riesgos laborales, la formación, la vigilancia de la salud y la prevención de la fatiga.

Las condiciones de trabajo se ven seriamente alteradas cuando se requieren realizar esfuerzos físicos superiores a los límites de actividad normales. Además del esfuerzo físico debe considerarse también como elementos perturbadores el esfuerzo, mental, visual, auditivo y emocional.

Para evaluar el esfuerzo físico hay que tener en cuenta la naturaleza del esfuerzo, y las posturas que se adoptan en el puesto de trabajo, estar sentado o de pie, y la frecuencia de posiciones incómoda.

La mayoría de accidentes laborales ocasionados por sobreesfuerzos son lesiones musculares pueden ser por causadas por golpes, o por causas internas producidas por alteraciones propias del músculo. Estas lesiones se pueden dividir en distensiones, calambres, contracturas y las más graves, desgarros.

Los factores desencadenantes de lesiones por sobreesfuerzo son:

- Manipular cargas pesadas.
- Trabajar con posturas forzadas.
- Realizar movimientos repetitivos.
- Padecer con anterioridad alguna lesión muscular u ósea en la zona afectada.
- Reincorporación prematura al puesto de trabajo después de una lesión mal curada.

Para evitar las lesiones por sobreesfuerzo es necesario tomar las medidas preventivas adecuadas y utilizar los equipos de protección individual necesarios.

Manipulación de máquinas y herramientas peligrosas

Todas las personas que manipulen cualquier máquina, aparato, instrumento o instalación en el trabajo están obligadas a cumplir las normas de seguridad que concierna a las máquinas que manipulan. Antes de ordenar la manipulación de una máquina o herramienta peligrosa a un trabajador, se debe proceder a instruirlo bien previamente en el manejo de la máquina.

Los riesgos más frecuentes que se derivan de la manipulación de las máquinas-herramientas básicamente son:

- Contacto accidental con la herramienta o la pieza en movimiento
- Atrapamiento con los órganos de movimiento de la máquina.

- Proyección de la pieza o de la herramienta.
- Dermatitis por contacto con los fluidos de corte utilizados como refrigerantes.

Por este motivo los empresarios tendrán que adoptar las medidas necesarias para que las máquinas y equipos de trabajo que se pongan a disposición de los trabajadores sean adecuados al trabajo que deba realizarse, de forma que garanticen la seguridad y la salud de los trabajadores. Cuando no sea posible garantizar de este modo totalmente la seguridad y la salud de los trabajadores durante la utilización de los equipos de trabajo, el empresario tomará las medidas adecuadas para reducir tales riesgos al mínimo.

Espacios de trabajo y zonas peligrosas

Las condiciones de trabajo pueden verse seriamente perturbadas si las dimensiones de los locales de trabajo no permiten que los trabajadores tengan la superficie y el volumen adecuado para que realicen su trabajo sin riesgos para su seguridad y salud y en condiciones ergonómicas aceptables.

Deben preverse separaciones entre los elementos materiales existentes en el puesto de trabajo. Cuando, por razones inherentes al puesto de trabajo, el espacio libre disponible no permita que el trabajador tenga la libertad de movimientos necesaria para desarrollar su actividad, deberá disponer de espacio adicional suficiente en las proximidades del puesto de trabajo.

Sólo podrán acceder los trabajadores autorizados a las zonas donde la seguridad de los trabajadores pueda verse afectada por riesgos de caída, caída de objetos y contacto o exposición a elementos agresivos. Asimismo, deberá disponerse, en la medida de lo posible, de un sistema que impida que los trabajadores no autorizados puedan acceder a dichas zonas.

Las zonas de los lugares de trabajo en las que exista riesgo de caída, de caída de objetos o de contacto o exposición a elementos agresivos, deberán estar claramente señalizadas.

Puertas y portones

La necesidad de regular el uso y la señalización de puertas y portones en los lugares de trabajo es la de prevenir que no puedan ocurrir accidentes laborales cuando los trabajadores pasan mercancías o transitan dentro de las naves industriales. Las puertas deben ser diseñadas y fabricadas de acuerdo a su función y en torno a otros aspectos como lo son:

- **La frecuencia de uso**: considerando la cantidad de personas que comúnmente usaren la puerta cotidianamente
- **Anchura adecuada**: (por ejemplo para dar paso a una silla de ruedas o vehículos motorizados),
- **Sentido de apertura**: si la puerta debe de abrir hacia un lado solamente (y hacia que lado ha de abrir) o si es de vaivén. Si es de apertura eléctrica o manual.
- **Sistemas de aviso**: si la puerta debe tener una ventanilla de aviso.
- **Materiales constitutivos de la puerta**: las puertas pueden ser categorizadas de acuerdo con sus propiedades en relación con el tiempo o duración estimada en un incendio ya que unas puertas pueden resistir el paso del fuego menos o más tiempo que otras.

Suelos, aberturas, desniveles y escaleras

Con el fin de evitar accidentes laborales por caídas o resbalamiento, los suelos de los locales de trabajo deberán ser fijos, estables y no resbaladizos, sin irregularidades ni pendientes peligrosas.

Las aberturas o desniveles que supongan un riesgo de caída de personas se protegerán mediante barandillas u otros sistemas de protección de seguridad equivalente, que podrán tener partes móviles cuando sea necesario disponer de acceso a la abertura. Deberán protegerse, en particular:

- Las aberturas en los suelos.
- Las aberturas en paredes o tabiques, siempre que su situación y dimensiones suponga riesgo de caída de personas, y las plataformas, muelles o estructuras similares.

Prevención con vehículos de transporte y manipulación de cargas

Los aparatos de manipulación de cargas en el interior de los establecimientos industriales están compuestos por **grúas, puentes-grúa, polipastos, montacargas, carretillas elevadoras** y las propias cargas que se manipulan.

Los riesgos asociados a la manipulación de cargas son los siguientes:

- Caída de objetos por deficiente sujeción de la carga
- Caída de objetos desprendidos por rotura de los elementos de sujeción, (ganchos, cuerdas cables. . .)
- Choques contra objetos móviles por oscilación de la carga.
- Caída de personas a distinto nivel
- Atrapamiento por o entre objetos móviles de los aparatos de elevación.

Vibraciones mecánicas

Se llaman vibraciones a las oscilaciones de partículas alrededor de un punto en un medio físico equilibrado cualquiera y se pueden producir por efecto del propio funcionamiento de una máquina o un equipo.

A efectos de las condiciones de trabajo existen dos tipos de vibraciones nocivas:

1. Las vibraciones transmitidas al sistema mano-brazo que es una vibración mecánica que, cuando se transmite al sistema humano de mano y brazo, supone riesgos para la salud y la seguridad de los trabajadores, en particular, problemas vasculares, de huesos o de articulaciones, nerviosos o musculares.
2. Las vibraciones transmitidas al cuerpo entero: que es un tipo de vibración mecánica que, cuando se transmite a todo el cuerpo, conlleva riesgos para la salud y la seguridad de los trabajadores, en particular, lumbalgias y lesiones de la columna vertebral.

Medidas preventivas para reducir los efectos nocivos de las vibraciones mecánicas

- Establecer otros métodos de trabajo que reduzcan la necesidad de exponerse a vibraciones mecánicas.
- Elegir un equipo de trabajo adecuado, bien diseñado desde el punto de vista ergonómico y generador del menor nivel de vibraciones posible, habida cuenta del trabajo al que está destinado.
- Elegir el equipo de protección individual adecuado (EPI) al trabajo que se esté realizando con el fin de reducir los riesgos de lesión por vibraciones, por ejemplo, asientos, amortiguadores u otros sistemas que atenúen eficazmente las vibraciones transmitidas al cuerpo entero y asas, mangos o cubiertas que reduzcan las vibraciones transmitidas al sistema mano-brazo.
- Establecer programas apropiados de mantenimiento de los equipos de trabajo, del lugar de trabajo y de los puestos de trabajo.
- Información y formar adecuadamente a los trabajadores sobre el manejo correcto y en forma segura del equipo de trabajo, para así reducir al mínimo la exposición a vibraciones mecánicas.
- Reducir al máximo la duración e intensidad de la exposición.
- Tomar medidas necesarias para proteger del frío y de la humedad a los trabajadores expuestos, incluyendo el suministro de ropa adecuada.

Riesgo eléctrico

Se denomina riesgo eléctrico al riesgo originado por la energía eléctrica. Dentro de este tipo de riesgo se incluyen los siguientes:

- **Choque eléctrico** por contacto con elementos en tensión (contacto eléctrico directo), o con masas puestas accidentalmente en tensión (contacto eléctrico indirecto).
- **Quemaduras** por choque eléctrico, o por arco eléctrico.
- **Caídas o golpes** como consecuencia de choque o arco eléctrico.
- **Incendios o explosiones** originados por la electricidad.

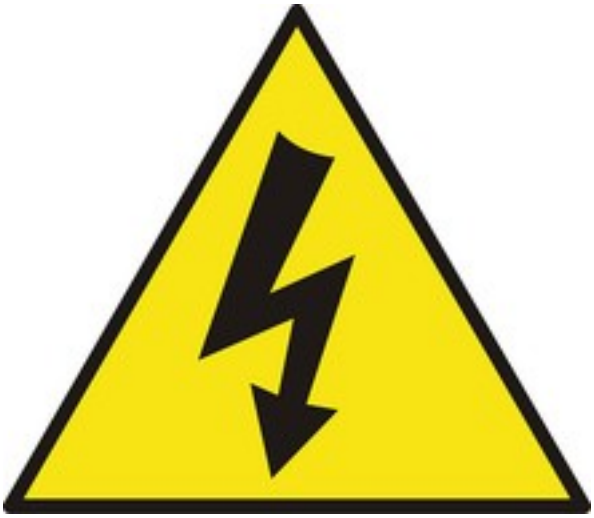


Figura 5: Símbolo de riesgo eléctrico

La corriente eléctrica puede causar efectos inmediatos como quemaduras, calambres o fibrilación, y efectos tardíos como trastornos mentales. Además puede causar efectos indirectos como caídas, golpes o cortes.

Los principales factores que influyen en el riesgo eléctrico son:

- La intensidad de corriente eléctrica.
- La duración del contacto eléctrico.
- La impedancia del contacto eléctrico, que depende fundamentalmente de la humedad, la superficie de contacto y la tensión y la frecuencia de la tensión aplicada.
- La tensión aplicada. En sí misma no es peligrosa pero, si la resistencia es baja, ocasiona el paso de una intensidad elevada y, por tanto, muy peligrosa. La relación entre la intensidad y la tensión no es lineal debido al hecho de que la impedancia del cuerpo humano varía con la tensión de contacto.
- Frecuencia de la corriente eléctrica. A mayor frecuencia, la impedancia del cuerpo es menor. Este efecto disminuye al aumentar la tensión eléctrica.
- Trayectoria de la corriente a través del cuerpo. Al atravesar órganos vitales, como el corazón pueden provocarse lesiones muy graves.

Los accidentes causados por la electricidad pueden ser leves, graves e incluso mortales. En caso de muerte del accidentado, recibe el nombre de **electrocución**.

Los trabajos en instalaciones eléctricas en emplazamientos con riesgo de incendio o explosión se realizarán siguiendo un procedimiento que reduzca al mínimo estos riesgos; para ello se limitará y controlará, en lo posible, la presencia de sustancias inflamables en la zona de trabajo y se evitará la aparición de focos de ignición, en particular, en caso de que exista, o pueda formarse, una atmósfera explosiva. En tal caso queda prohibida la realización de trabajos u operaciones (cambio de lámparas, fusibles, etc.) en tensión, salvo si se efectúan en instalaciones y con equipos concebidos para operar en esas condiciones, que cumplan la normativa específica aplicable.

Riesgos de explosión por atmósfera explosiva

Figura 6: Símbolo de sustancia explosiva

Se entiende por **atmósfera explosiva** la mezcla con el aire, en condiciones atmosféricas, de sustancias inflamables en forma de gases, vapores, nieblas o polvos, en la que, tras una ignición, la combustión se propaga a la totalidad de la mezcla no quemada.

Para prevenir las explosiones, en los lugares de trabajo, los empresarios han de proporcionar una protección contra ellas, de tipo técnico u organizativo en función del tipo de actividad, para impedir la formación de atmósferas explosivas o, cuando la naturaleza de la actividad no lo permita, evitar la ignición de atmósferas explosivas y atenuar los efectos perjudiciales de una explosión de forma que se garantice la salud y la seguridad de los trabajadores.

Medidas de protección contra las explosiones

- Los escapes o liberación, intencionada o no, de vapores, gases, nieblas inflamables o de polvos combustibles que pueda dar lugar a riesgos de explosión deberá ser desviado o evacuado a un lugar seguro.
- En caso de escapes de sustancias explosivas, los trabajadores deberán ser alertados mediante la emisión de señales ópticas o acústicas de alarma y desalojados en condiciones de seguridad antes de que se alcancen las condiciones de explosión.
- En caso de que un corte de energía pueda comportar nuevos peligros, hay que disponer de un sistema independiente para mantener el equipo y los sistemas de protección en situación de funcionamiento seguro

Figura 7: Símbolo de sustancia inflamable

independientemente del resto de la instalación si efectivamente se produjera un corte de energía.

- Deberá poder efectuarse la desconexión manual de los aparatos y sistemas de protección incluidos en procesos automáticos que se aparten de las condiciones de funcionamiento previstas, siempre que ello no comprometa la seguridad.

Prevención de emisiones de gases, vapores, líquidos y polvo

Entrar en contacto con emisión de gases, vapores, líquidos o polvo es un proceso bastante generalizado en máquinas y aparatos fijos y portátiles que manipulan los trabajadores.

En general, la emisión de la sustancia supone su posterior dispersión o difusión en el aire y, finalmente, su inhalación por el trabajador. La emisión puede provenir de diferentes operaciones o fuentes. La naturaleza de la sustancia condiciona su peligrosidad. Sus efectos sobre el organismo pueden ser muy diversos, pudiéndose distinguir, entre otros:

- Los irritantes del aparato respiratorio, por ejemplo: dióxido de azufre, cloro, etc.;
- Los sensibilizantes, por ejemplo: isocianatos;
- Los polvos fibrogénicos, por ejemplo: sílice cristalina;
- Los asfixiantes (químicos o "simples"), tales como el monóxido de carbono, el dióxido de carbono o los gases inertes;
- Los tóxicos que afectan a sistemas u órganos concretos, por ejemplo: mercurio (sistema nervioso, riñones) o plomo (sistema nervioso, sangre);
- Los carcinógenos (por ejemplo: amianto, benceno, cloruro de vinilo monómero), los mutágenos y los tóxicos para la reproducción;
- Los agentes infecciosos, etc.

Para evaluar los riesgos será necesario: Disponer de la información sobre las propiedades peligrosas de las sustancias y cualquier otra información necesaria para realizar dicha evaluación que, en su caso, deba facilitar el proveedor, o que pueda recabarse de éste o de cualquier otra fuente de información de fácil acceso. Hay que determinar la magnitud de la exposición del trabajador afectado.

Manipulación de sustancias tóxicas y/o corrosivas

El peligro de trabajar manipulando sustancias tóxicas **se deriva principalmente del desconocimiento** que puedan tener los trabajadores de los riesgos para la salud que tienen muchas sustancias químicas.

La **toxicidad** es la capacidad de cualquier sustancia química de producir efectos perjudiciales sobre un ser vivo, al entrar en contacto con él. Tóxico es cualquier sustancia, artificial o natural, que posea toxicidad (es decir, cualquier sustancia que produzca un efecto dañino sobre los seres vivos al entrar en contacto con ellos). El estudio de los tóxicos se conoce como toxicología. Ninguna sustancia química puede ser considerada no tóxica, puesto que cualquier sustancia (agua, oxígeno) es capaz de producir

un efecto tóxico si se administra la dosis suficiente. Esto queda representado en la famosa frase de Paracelso «sólo la dosis hace al veneno». Todas las sustancias poseen toxicidad; sin embargo unas tienen mayor toxicidad que otras. La intoxicación es el estado de un ser vivo en el que se encuentra bajo los efectos perjudiciales de un tóxico.

Una **sustancia corrosiva** es una sustancia que puede destruir o dañar irreversiblemente otra superficie o sustancia con la cual entra en contacto. Los principales peligros para las personas incluyen daño a los ojos, la piel y el tejido debajo de la piel; la inhalación o ingestión de una sustancia corrosiva **puede dañar las vías respiratorias y conductos gastrointestinales**. La quemadura a menudo puede conducir a vómitos y fuertes dolores de estómago. La exposición a la misma es denominada quemadura química.

Además de actuar directamente de manera destructiva si entran en contacto con la piel o las mucosas, algunas de las sustancia de esta clase son tóxicas o perjudiciales. Su ingestión o inhalación de sus vapores pueden dar por resultado un envenenamiento y algunas de ellas pueden incluso atravesar la piel.

Figura 9: Símbolo de sustancia corrosiva

El Parlamento Europeo aprobó en 2006 un reglamento que establece un sistema de registro, evaluación, autorización y restricción de sustancias químicas (REACH). Este reglamento obliga a los fabricantes de productos químicos peligrosos a demostrar que las sustancias que están comercializando son seguras para la salud pública y el medio ambiente.

Los objetivos generales del reglamento REACH son entre otros los siguientes:

- Acabar con la falta de conocimiento sobre la peligrosidad de las sustancias químicas.
- Proteger a las personas y al medio ambiente de los compuestos peligrosos.
- Detectar, limitar y, si fuera necesario, hacer desaparecer de la circulación a las sustancias de riesgo.
- Transferir la responsabilidad sobre las sustancias de las autoridades a los productores químicos.
- Permitir la entrada de sustancias en el mercado sólo si existe información específica disponible.
- Asegurar que existe información adecuada sobre todas las sustancias químicas y que esa información es transferida a todos los trabajadores que van a estar en contacto con ella.
- Fomentar la innovación para conseguir nuevas sustancias más seguras.
- Simplificar la reglamentación sobre productos químicos.

Ergonomía y Psicosociología Aplicada

En el entorno de exigencia elevada y competitividad así como las condiciones precarias en las que se desenvuelven muchos trabajadores está ocasionando una aparición creciente de trastornos psicológicos derivados de esas circunstancias. Los elementos potenciales que ocasionan estos trastornos son los siguientes:

- Precariedad laboral
- Trabajo estresante
- Trabajo monótono y rutinario
- Trabajo con esfuerzo mental
- Acoso laboral
- Síndrome de trabajador quemado (burn-out)

Precariedad laboral

Se denomina **precariedad laboral** a la situación que viven las personas trabajadoras que, por unas razones u otras sufren unas condiciones de trabajo por debajo del límite considerado como normal. La precariedad laboral tiene especial incidencia cuando los ingresos económicos que se perciben por el trabajo no cubren las necesidades básicas de una persona, ya que es la economía el factor con el que se cuenta para cubrir las necesidades de la gente.

Relaciones laborales precarias

- La temporalidad de los contratos de trabajo es uno de los factores que más contribuyen a la precariedad laboral. Otra percepción de precariedad es la retribución salarial que se obtenga por el trabajo realizado y que muchas veces resulta insuficiente para cubrir las necesidades mínimas vitales que permitan a una persona poder vivir de forma autónoma. La jornada de trabajo que se tenga y el calendario anual laboral también puede ser percibido como síntoma de precariedad cuando muchas personas tienen que trabajar a tiempo parcial diario lo que les impide lograr la retribución necesaria o tener en cambio que trabajar jornadas de trabajo muy superior a la legal para poder conseguir el salario necesario como consecuencia de tener un sueldo muy bajo. También se considera precariedad la que sufren aquellos trabajadores que no son dados de alta en la Seguridad Social y por tanto carecen de las prestaciones que les da derecho a quienes están protegidos por la Seguridad Social.

Trastornos en la salud generados por la precariedad en el trabajo

La precariedad laboral puede producir un aumento del sufrimiento psicológico y un empeoramiento de la salud y calidad de vida de las personas que dependen del trabajo o de la carencia del mismo. La incertidumbre sobre el futuro, que presenta el trabajo precario altera el comportamiento social del individuo, porque aumenta las dificultades para conformar y afianzar identidades individuales y colectivas en torno al trabajo. Las estadísticas de siniestralidad laboral indican que la incidencia de accidentes de trabajo es más alta entre la población con trabajo precario que las que tienen empleo estable, por desconocimiento y aplicación de las normas de seguridad de los trabajadores precarios y la realización a cargo de éstos de las actividades más nocivas y peligrosas.

Grupos sociales afectados por precariedad laboral

La precariedad laboral es un conjunto de inactividad, desempleo, eventualidad, empleo forzoso a tiempo parcial, economía sumergida que afectan más a las mujeres que a los varones, a los jóvenes en mayor medida que a los mayores, e inciden más en unas regiones que en otras. Asimismo, hay que destacar la grave situación de algunos colectivos como los parados de larga duración mayores de 40 años, las minorías étnicas o de inmigrantes y las personas con discapacidad.

Trabajo estresante

Una definición del estrés que tiene gran aceptación es la de Mc Grath (1970): «El estrés es un desequilibrio sustancial (percibido) entre la demanda y la capacidad de respuesta (del individuo) bajo condiciones en la que el fracaso ante esta demanda posee importantes consecuencias (percibidas)».

Se define como **estrés** a la respuesta del cuerpo a condiciones externas que perturban el equilibrio emocional de la persona. En el ámbito laboral, se denomina estrés laboral a un **conjunto de reacciones nocivas tanto físicas como emocionales que concurren cuando las exigencias del trabajo superan a las capacidades, los recursos o las necesidades del trabajador**.

La existencia de gran número de dolencias psicosomáticas, producto de los constreñimientos y exigencias de la sociedad actual, y muy en especial en lo referido al ámbito laboral, sujeto a incesantes transformaciones en la organización y en las demandas del trabajo, ha facilitado la difusión y la popularización de un término con el que, de un modo genérico, se define esta situación: el estrés.

La exposición prolongada al estrés en el trabajo afecta el sistema nervioso disminuyendo la resistencia biológica y perturbando el balance fisiológico natural del organismo (homeostasis). Por todo ello el estrés puede ocasionar varios problemas somáticos y psíquicos.

Algunas de las consecuencias negativas que ocasiona el estrés en el ámbito laboral, son las siguientes:

- Se puede desarrollar como trastorno psicológico agudo.
- Puede originar un incremento de accidentes laborales.
- Aumenta la tasa de absentismo laboral o bajo rendimiento de los trabajadores que lo padecen.
- Puede conducir a la incapacidad laboral por alteraciones somáticas o psicológicas.
- Se puede crear un clima psicosocial enrarecido en los centros de trabajo.

Trabajo con esfuerzo mental

Las tareas que requieren gran exigencia intelectual provocan fatiga mental o nerviosa como consecuencia de una **exigencia excesiva de la capacidad de atención, análisis y control del trabajador**, por la cantidad de información que recibe y a la que, tras analizarla e interpretarla, debe dar respuesta.

El esfuerzo mental se define como la cantidad de esfuerzo intelectual que se debe realizar para conseguir un resultado concreto. Los sistemas modernos de producción y gestión aumentan de forma considerable las demandas de la persona porque a menudo se introducen nuevas tecnologías para aliviar unas exigencias muy elevadas o para dar respuesta a una elevada demanda de producción. Un exceso de automatización puede comportar la exclusión del ser humano del conjunto operativo, pero no reducir la carga de trabajo, sino que puede dar lugar a niveles de exigencia que van más allá de las capacidades humanas, en concreto, de las capacidades cognitivas y de toma de decisiones.

Los síntomas de fatiga mental son: dolores de cabeza, sensación de cansancio, alteraciones en la capacidad de atención, somnolencia, fallos de precisión en los movimientos, y se traduce en disminución del rendimiento, de la actividad, aumento de errores, etc.

Tareas usuales que requieren esfuerzo mental

- Operar con maquinaria más sofisticada.
- Vigilar permanentemente el buen funcionamiento del equipo.
- Manejar más información para ejecutar tareas.
- Necesidad de programación de los equipos.
- Manejar información sobre los resultados de la tarea.
- Memorización para tareas rutinarias.

- Tener que tomar decisiones rápidas en el proceso.
- Realizar respuestas rápidas a errores típicos.
- Tener que elegir entre opciones.
- Respuesta a errores no típicos.
- Tener que realizar cálculos numéricos de cierta complejidad.

Trabajo monótono y rutinario

La monotonía en el trabajo surge de realizar **tareas repetitivas sin apenas esfuerzo y de forma continuada en el tiempo**, así como la ausencia de iniciativa personal en la organización de la tarea que se realiza. El trabajo monótono y rutinario efectuado en un ambiente poco estimulante es propio de la producción en masa y determinadas tareas de oficina. También aparece la monotonía cuando se realizan tareas en lugares aislados faltos de contactos humanos.

La monotonía y el trabajo repetitivo dependen de:

- Número de operaciones encadenadas de que conste la tarea
- Número repetitivo de veces que la tarea se realiza durante la jornada de trabajo

Las actividades monótonas influyen negativamente en las facultades de la persona de forma unilateral, de lo que resulta una fatiga más rápida e incluso la aparición de depresiones psíquicas así como dolores musculares causados por posturas estáticas.

La realización de trabajos monótonos y repetitivos puede desencadenar trastornos músculo-esqueléticos si ellos se realizan con malas posturas o movimientos incómodos. Entre los factores físicos de riesgo cabe citar la manipulación manual, la aplicación de fuerza con las manos, la presión mecánica directa sobre tejidos del cuerpo, las vibraciones y los entornos de trabajos fríos.

En el trabajo monótono o rutinario la persona actúa mecánicamente, no presta atención a lo que hace y pierde concentración, se distrae y se despista. Para evitarlo, el trabajo puede ser repetitivo en cierto modo, pero no rutinario, es bueno que el trabajador conozca bien su secuencia de trabajo, pero sin llegar a aburrirse.

Acoso laboral

Acoso laboral, también conocido como **acoso psicológico** en el trabajo, hostigamiento laboral o **mobbing**, es un continuado y deliberado maltrato verbal o modal que recibe un trabajador por otro u otros que se comportan con él de manera cruel y que atenta contra el derecho fundamental de todo ser humano a la dignidad y a la integridad física y psicológica. Por tanto se produce de forma sistemática y recurrente, durante un período que puede llegar a durar meses e incluso años. Puede ser:

- por sus jefes (acoso descendente)
- compañeros (acoso horizontal)
- subordinados (acoso ascendente)

El acoso psicológico tiene como objetivo intimidar, reducir, aplanar, apocar, amedrentar y consumir emocional e intelectualmente a la víctima, con vistas a eliminarla de la organización o satisfacer la necesidad insaciable de agredir, controlar y destruir que suele presentar el hostigador, que aprovecha la situación que le brinda la situación organizativa particular para canalizar una serie de impulsos y tendencias psicopáticas.

El acoso laboral está considerado no tanto como una nueva enfermedad sino como un **riesgo laboral de tipo psicosocial**. El cuadro de daño psicológico más habitual en los casos de mobbing suele ser el síndrome de estrés postraumático en su forma cronificada. Un cuadro que muy frecuentemente se confunde con depresión y problemas de ansiedad y que suele ser muy mal identificado.

Síndrome de trabajador quemado (Burn-out)

Burn-out es traducido literalmente como «quemarse», se trata de un estado de vacío interior, de desgaste espiritual, de "infarto al alma", en el que la persona afectada no sólo ha gastado sus energías recargables, sino su sustancia ha sido atacada y dañada. El síndrome burn-out se debe a distintas causas múltiples, no necesariamente una sola, y se origina siempre en largos períodos. Se ha encontrado en múltiples investigaciones que el síndrome ataca especialmente cuando el trabajo supera las ocho horas, no se ha cambiado de ambiente laboral en largos períodos y en la paga mal remunerada, sin embargo en personas que trabajan en amplias jornadas pero bien remuneradas es poco común la presencia del síndrome.

Incluye:

- **Agotamiento emocional**, que se refiere a la disminución y pérdida de recursos emocionales.
- **Despersonalización o deshumanización**, consistente en el desarrollo de actitudes negativas, de insensibilidad y de cinismo hacia los receptores de servicio prestado.
- **Falta de realización personal**, con tendencias a evaluar el propio trabajo de forma negativa, con vivencias de insuficiencia profesional y baja autoestima personal.
- **Síntomas físicos de estrés**, como cansancio y malestar general.

5.1.8 Dispositivos legales para disminuir la gravedad de los siniestros laborales

- Dotaciones y local para primeros auxilios
- **Equipo de protección individual (EPI)**: cascos, gafas, . . .
- **Equipo de protección colectiva**: barandillas, redes, . . .
- Señalización de seguridad
- Servicios higiénicos y locales de descanso
- Protección contra incendios
- Vías y salidas de evacuación
- Alumbrado de emergencia
- Limpieza, orden y mantenimiento de los centros de trabajo

5.1.9 Servicios de Prevención de Riesgos Laborales

Según el Real Decreto 39/1997, de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención de Riesgos Laborales, se entenderá por servicio de prevención propio el conjunto de medios humanos y materiales de la empresa necesarios para la realización de las actividades de prevención, y por servicio de prevención ajeno el prestado por una entidad especializada que concierte con la empresa la realización de actividades de prevención, el asesoramiento y apoyo que precise en función de los tipos de riesgos o ambas actuaciones conjuntamente. **Los servicios de prevención tendrán carácter interdisciplinario**, entendiendo como tal la conjunción coordinada de dos o más disciplinas técnicas o científicas en materia de prevención de riesgos laborales (Medicina del Trabajo, Seguridad en el trabajo, Higiene Industrial, y Ergonomía y Psicosociología)

Equipamiento sanitario

De acuerdo con el Real Decreto 843/2011, de 17 de junio, por el que se establecen los criterios básicos sobre la organización de recursos para desarrollar la actividad sanitaria de los servicios de prevención, el equipamiento sanitario básico del servicio sanitario en las instalaciones fijas del servicio de prevención será el siguiente:

1. Audiómetro y cabina audiométrica homologados en todos los servicios de prevención ajenos. En el caso de los servicios de prevención propios únicamente en el caso de que en las empresas a las que dan servicio haya exposición a ruido.
2. Camilla de exploración.
3. Contenedores de residuos sanitarios
4. Electrocardiógrafo.
5. Equipo de radiodiagnóstico: propio o concertado.
6. Equipo para control visión homologado.
7. Esfigmomanómetro.
8. Espirómetro o neumotacógrafo homologados.
9. Fonendoscopio.
10. Laboratorio: propio o concertado.
11. Linterna o fuente de luz externa.
12. Martillo de reflejos.
13. Botiquín de medicación, material y equipo suficiente para atender urgencias y primeros auxilios.
14. Negatoscopio.
15. Nevera con termómetro de máximas y mínimas.
16. Oftalmoscopio
17. Otoscopio
18. Rinoscopio
19. Peso clínico.
20. Talla.

5.2 Protección medioambiental

5.2.1 Conservación medioambiental

Conservación ambiental, conservación de las especies, conservación de la naturaleza o protección de la naturaleza son algunos de los nombres que se conocen las distintas formas de proteger y preservar el futuro de la naturaleza, el medio ambiente, o específicamente algunas de **sus partes: la flora y la fauna, las distintas especies, los distintos ecosistemas, los valores paisajísticos, etc**. Con el nombre de **conservacionismo** se designa al movimiento social que propugna esa conservación. Una de sus vertientes es el **movimiento ecologista**.

La conservación de la naturaleza y de los recursos naturales se basa esencialmente en tres aspectos:

- Ordenar el espacio y permitir diversas opciones de uso de los recursos.
- Conservar el patrimonio natural, cultural e histórico de cada país.
- Conservar los recursos naturales, base de la producción.

5.2.2 Reciclaje de residuos

El reciclaje es un proceso cuyo objetivo es convertir materiales (desechos) en nuevos productos para prevenir el desuso de materiales potencialmente útiles, reducir el consumo de nueva materia prima, reducir el uso de energía, reducir la contaminación del aire (a través de la incineración) y contaminación del agua (a través de los vertederos) por medio de la reducción de la necesidad de los sistemas de desechos convencionales, como también disminuir las emisiones de gases de efecto invernadero en comparación con la producción de plásticos. El reciclaje es un componente clave en la reducción de desechos contemporáneos y es el tercer componente de las **3R (Reducir, Reutilizar, Reciclar)**.

Los materiales reciclables incluyen varios tipos de vidrio, papel, metal, plástico, telas y componentes electrónicos. En muchos casos no es posible llevar a cabo un reciclaje en el sentido estricto debido a la dificultad o precio del proceso, de modo que suele reutilizarse el material o los productos para producir otros materiales. También es posible realizar un salvamento de componentes de ciertos productos complejos, ya sea por su valor intrínseco o por su naturaleza peligrosa.

Cadena de reciclado

La cadena de reciclado consta de varias etapas:

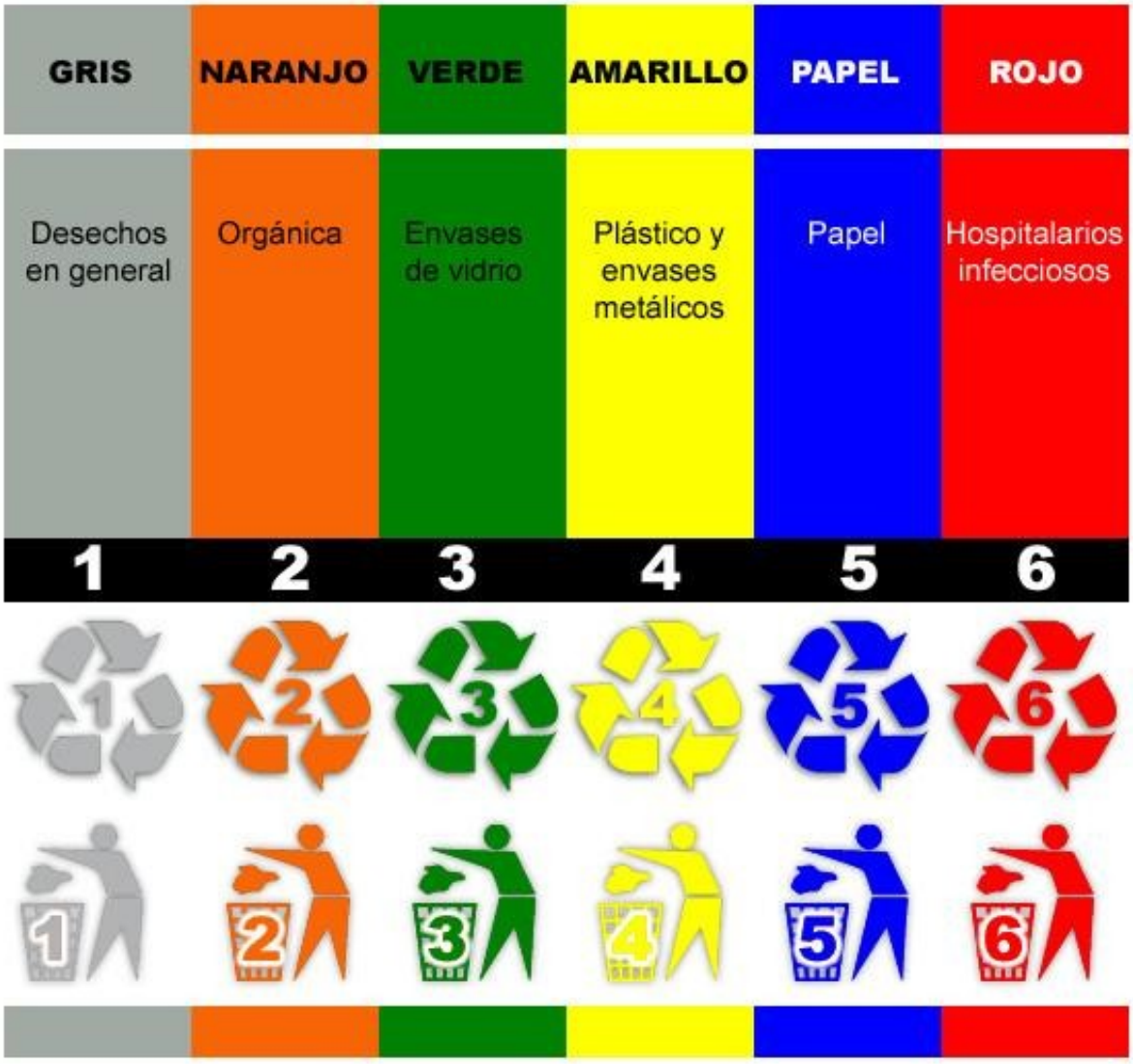
- **Origen**: que puede ser doméstico o industrial.
- **Recuperación**: que puede ser realizada por empresas públicas o privadas. Consiste únicamente en la recolección y transporte de los residuos hacia el siguiente eslabón de la cadena.
- **Plantas de transferencia**: se trata de un eslabón voluntario que no siempre se usa. Aquí se mezclan los residuos para realizar transportes mayores a menor costo (usando contenedores más grandes o compactadores más potentes).
- **Plantas de clasificación (o separación)**: donde se clasifican los residuos y se separan los valorizables.
- **Reciclador final (o planta de valoración)**: donde finalmente los residuos se reciclan (papeleras, plastiqueros, etc.), se almacenan (vertederos) o se usan para producción de energía (cementeras, biogás, etc.)

Para la separación en origen doméstico se usan **contenedores de distintos colores** ubicados en entornos urbanos o rurales:

- **Contenedor amarillo (envases)**: En este se deben depositar todo tipo de envases ligeros como los envases de plásticos (botellas, tarrinas, bolsas, bandejas, etc.), de latas (bebidas, conservas, etc.)
- **Contenedor azul (papel y cartón)**: En este contenedor se deben depositar los envases de cartón (cajas, bandejas, etc.), así como los periódicos, revistas, papeles de envolver, propaganda, etc. Es aconsejable plegar las cajas de manera que ocupen el mínimo espacio dentro del contenedor.
- **Contenedor verde (vidrio)**: En este contenedor se depositan envases de vidrio.
- **Color naranja (orgánico)**: Aunque es difícil encontrar un contenedor de color naranja, estos se utilizan exclusivamente para material orgánico. En caso de no disponer de este tipo de contenedor, como hemos comentado, utilizaríamos el gris.
- **Contenedor gris (orgánico)**: En él se depositan el resto de residuos que no tienen cabida en los grupos anteriores, fundamentalmente desechos orgánicos catalogados como materia biodegradable.
- **Contenedor rojo (desechos peligrosos)**: Como teléfonos móviles, insecticidas, pilas o baterías, aceite comestible o de vehículos, jeringas, latas de aerosol,etc.

Regla de las tres erres.

El reciclaje se inscribe en la estrategia de tratamiento de residuos de las tres erres:


GRIS
NARANJO
VERDE
AMARILLO
PAPEL
ROJO
Desechos en general
Orgánica
Envases de vidrio
Plástico y envases metálicos
Papel
Hospitalarios infecciosos
1
2
3
4
5
6

- **Reducir**, acciones para reducir la producción de objetos susceptibles de convertirse en residuos.
- **Reutilizar**, acciones que permiten el volver a usar un determinado producto para darle una segunda vida, con el mismo uso u otro diferente.
- **Reciclar**, el conjunto de operaciones de recogida y tratamiento de residuos que permiten reintroducirlos en un ciclo de vida.

Formas de reciclaje

- Reciclaje de hierro
- Reciclaje de aluminio
- Reciclaje del vidrio
- Reciclaje de pilas y baterías
- Reciclaje de cemento
- Reciclaje de papel y cartón
- Reciclaje de plástico
- Reciclaje de bolsas
- Reciclaje de tetra pak
- Reciclaje de computadoras y otros componentes electrónicos
- Reciclado mecánico
- Conversión en papel
- Conversión en composta para abono
- Derretimiento
- Fundición
- Revulcanizado
- Fermentación
- Recuperación

5.2.3 Desechos electrónicos

El tratamiento inadecuado de la chatarra electrónica, desechos electrónicos o basura tecnológica (en inglés: e-waste o WEEE) puede ocasionar graves impactos al medio ambiente y poner en riesgo la salud humana.

De acuerdo a la Organización para la Cooperación y el Desarrollo Económico (OCDE) un desecho electrónico es todo dispositivo alimentado por la energía eléctrica cuya vida útil haya culminado.

La convención de Basilea por su parte define la chatarra electrónica como todo equipo o componente electrónico incapaz de cumplir la tarea para la que originariamente fueron inventados y producidos.

Problemas ambientales asociados

Existen diversos daños para la salud y el medio ambiente generado por varios de los elementos contaminantes presentes en los desechos electrónicos, en especial

- el **mercurio**, que produce daños al cerebro y el sistema nervioso.
- el **plomo**, que potencia el deterioro intelectual, ya que tiene efectos perjudiciales en el cerebro y todo el sistema circulatorio.
- el **cadmio**, que produce fallas en la reproducción y posibilidad incluso de infertilidad, entre otras cosas.
- el **cromo**, que produce problemas en los riñones y los huesos.

Un celular móvil, por ejemplo, contiene entre 500 a 1000 compuestos diferentes. Estas sustancias peligrosas generan contaminación y exponen a los trabajadores en la fabricación de estos productos.

Mientras el celular, el monitor y el televisor estén en su casa no generan riesgos de contaminación. Pero cuando se mezclan con el resto de la basura y se rompen, esos metales tóxicos se desprenden y pueden resultar mortales. Adquirir un nuevo equipo informático es tan barato que abandonamos o almacenamos un ordenador cuando todavía no ha llegado al final de su vida útil, para comprar otro nuevo, desconociendo el enorme coste ecológico que comporta tanto la producción como el vertido de ordenadores.

Vertederos tecnológicos

Al día de hoy se sabe de la existencia de grandes vertederos donde los países occidentales vierten su basura electrónica. El mayor vertedero del mundo de ese tipo se encuentra en China, concretamente en la ciudad de Guiyu, información que el propio gobierno chino ha confirmado. Se calcula que en esa ciudad trabajan 150.000 personas para tratar la basura que llega, principalmente, de EE. UU., Canadá, Japón y Corea del Sur. Estas fuentes generadoras de toneladas de basura tecnológica eligen los países tercermundistas para depositar toda su chatarra.

Hoy en día se habla cada vez más de otro gigantesco punto para verter desechos localizado en Ghana, África.

Posibles soluciones

Algunas posibles soluciones consisten en:

- Reducir la generación de desechos electrónicos.
- Donar o vender los equipos electrónicos que todavía funcionen.
- Donar equipos rotos o viejos a organizaciones que los reparan y reutilizan con fines sociales.
- Reciclar los componentes que no puedan repararse. Hay empresas que acopian y reciclan estos aparatos sin costo para los dueños de los equipos en desuso.
- Promover la reducción de sustancias peligrosas que se usan en ciertos productos electrónicos que se venden en cada país.
- La responsabilidad extendida del productor en la cual luego de su uso por los consumidores el propio productor se lleva el producto, esto los impulsa a mejorar los diseños para que sean más sencillos de reciclar y reutilizar.
- En algunos países se piensa en todo el ciclo de vida de un producto. Se multa a la gente que no se comporta responsablemente luego de consumir. Incluso algunos productos tienen una tasa destinada a resolver la exposición final de esos materiales.

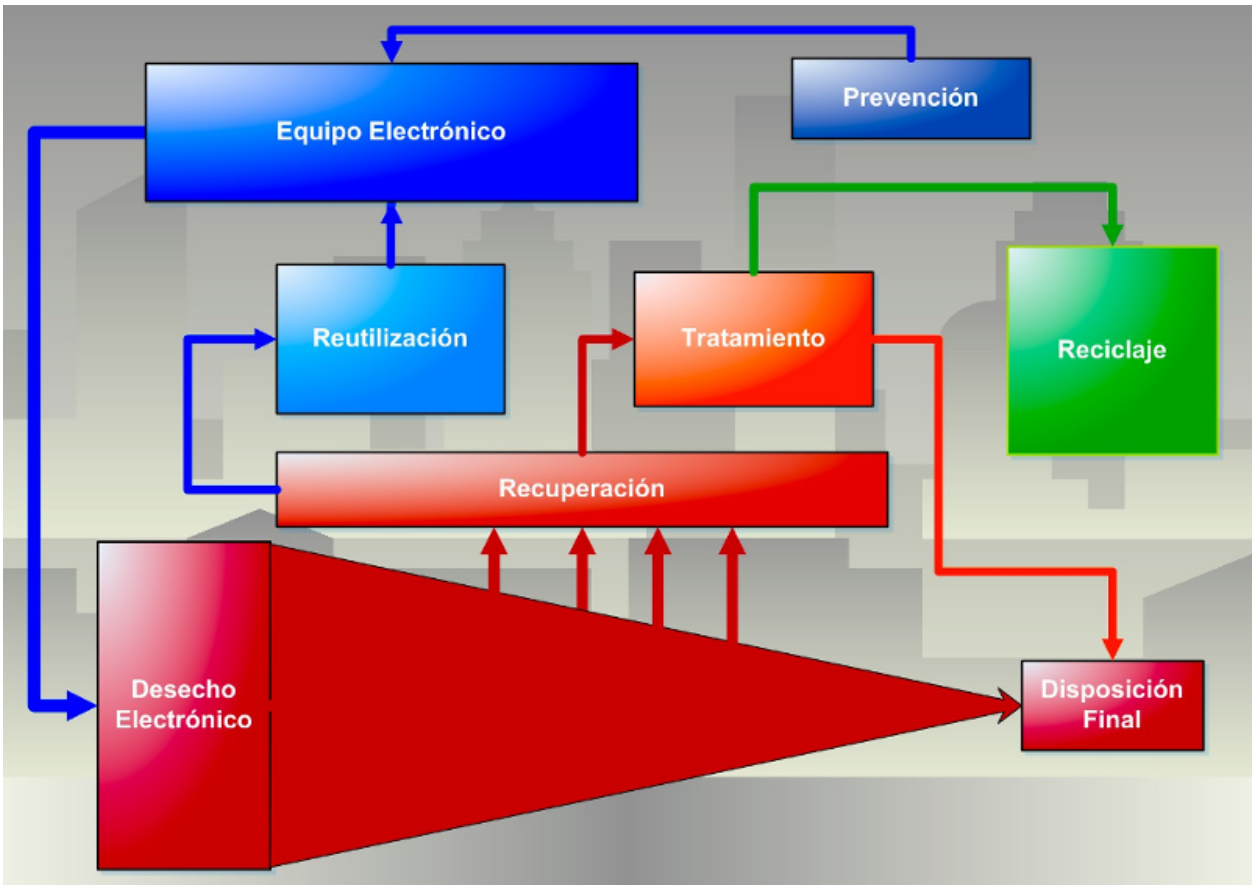


Figura 11: Esquema de como debería desarrollarse un manejo responsable de los desechos electrónicos.

5.3 Referencias

- Wikipedia

5.4 Actividades

1. Tenemos una empresa de servicios informáticos que se dedica a ofrecer soporte a empresas y usuarios en todo lo relacionado con la informática (hardware, redes, sistemas operativos, . . .). Elaborar un documento en el que se especifique:

- Tareas que se realizan y riesgos laborales asociados.
- Medidas de prevención
- Medidas de protección
- Residuos que se producen
- Medidas de reciclaje

CAPÍTULO 6

LA CAPA DE ENLACE

6.1 Conceptos generales

La capa de enlace de datos se sitúa en el **nivel 2** del modelo OSI. La misión de la capa de enlace es establecer una línea de comunicación libre de errores que pueda ser utilizada por la capa inmediatamente superior: la capa de red.

Como el nivel físico opera con bits, la capa de enlace tiene que montar bloques de información (llamados **tramas** en esta capa), dotarles de una dirección de capa de enlace (**Dirección MAC**), gestionar la detección o corrección de errores, y ocuparse del control de flujo entre equipos (para evitar que un equipo más rápido desborde a uno más lento).

En redes Ethernet esta capa se subdivide en dos subcapas:

- **Subcapa de enlace lógico** (**LLC** – Logical Link Control)
- **Subcapa de acceso al medio** (**MAC** - Medium Access Control)

La **subcapa de enlace lógico** se recoge en la norma IEEE 802.2 y es común para todos los demás tipos de redes (Ethernet o IEEE 802.3, IEEE 802.11 o Wi-Fi, IEEE 802.16 o WiMAX, etc.); todas ellas especifican un subcapa de acceso al medio así como una capa física distinta.

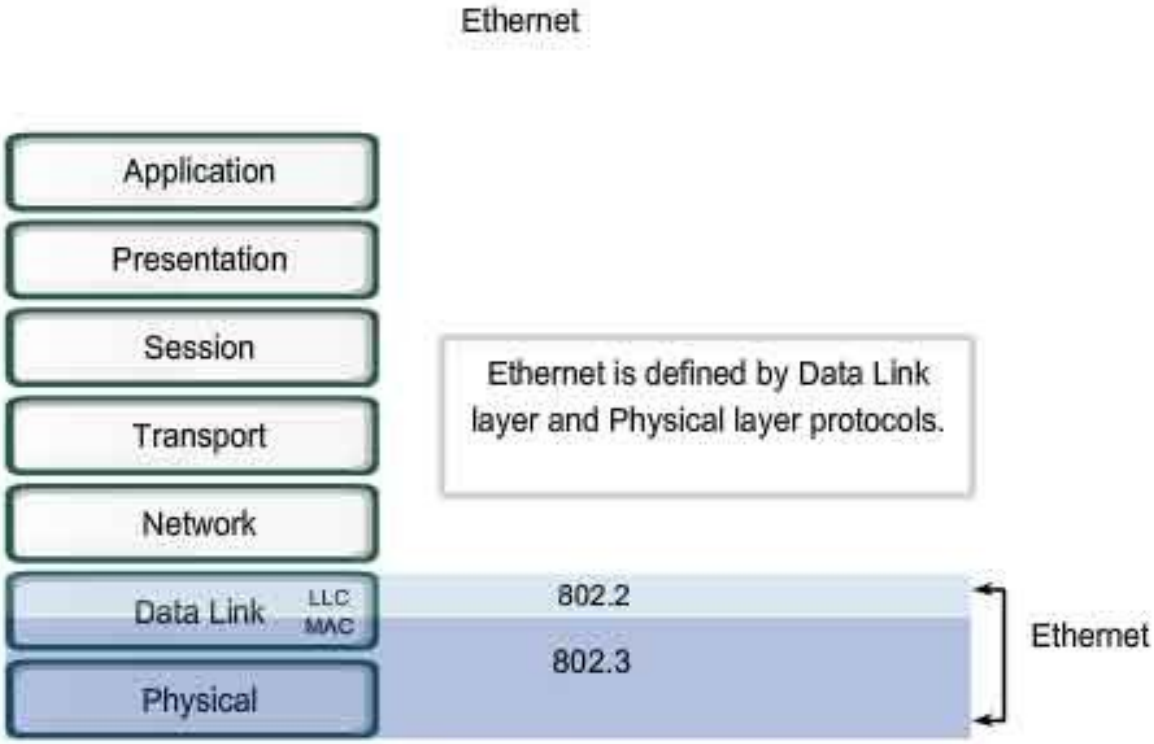
La **subcapa de control de acceso al medio** es la encargada de **arbitrar el uso del medio** de comunicación cuando este está compartido entre más de dos equipos como suele ser habitual en muchas LAN.

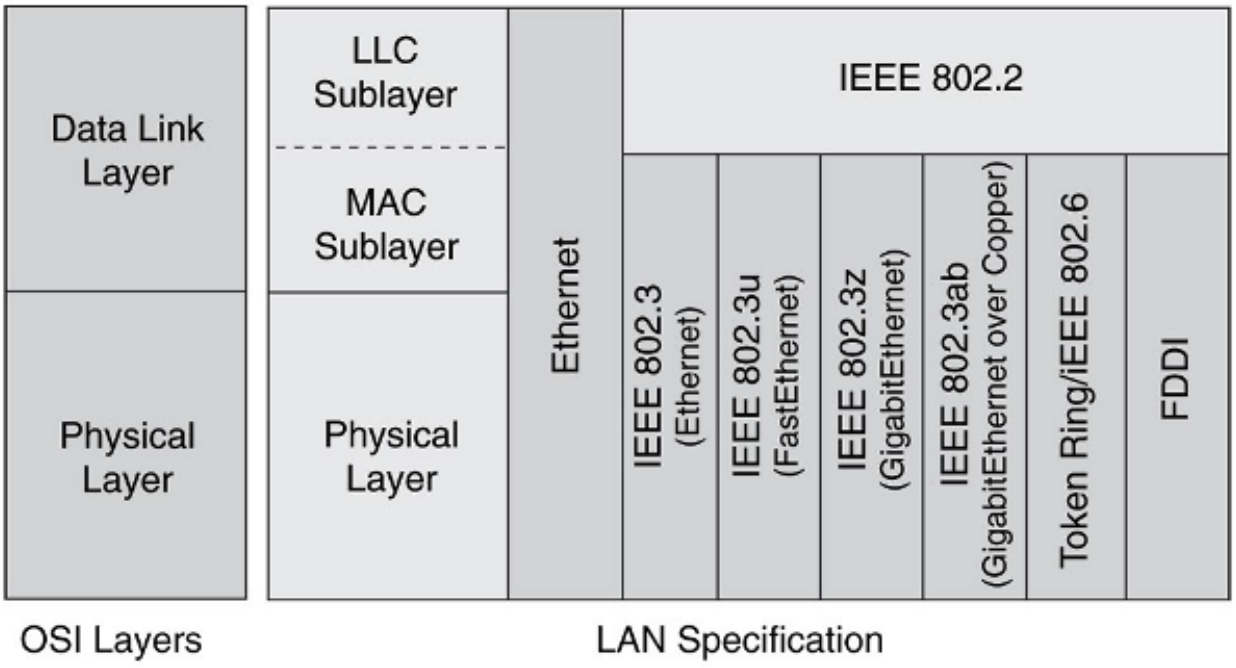
En la práctica la subcapa de acceso al medio suele formar parte de la propia tarjeta de comunicaciones, mientras que la subcapa de enlace lógico estaría en el programa adaptador de la tarjeta (*driver* en inglés).

Además de la **formación de tramas**, el nivel de enlace se ocupará del **tratamiento de los errores** que se produzcan en la recepción de las tramas, de eliminar tramas erróneas, solicitar retransmisiones, descartar tramas duplicadas, **adecuar el flujo de datos** entre emisores rápidos y receptores lentos, etc

Algunos protocolos y estándares que regulan aspectos de la capa de enlace

- Parte de la especificación de los protocolos **Ethernet y del estándar IEEE 802.3**.
- Parte de la especificación de la familia de estándares IEEE 802.11, para redes sin hilos.
- Point to point protocol (PPP).
- Parte de la especificación de tecnologías de enlace para WAN como HDLC, X.25, ATM, Frame Relay o xDSL.


Ethernet
Application
Presentation
Session
Transport
Network
Data Link
LLC
MAC
Physical
Ethernet is defined by Data Link layer and Physical layer protocols.
802.2
802.3
Ethernet


Data Link Layer
Physical Layer
LLC Sublayer
MAC Sublayer
Physical Layer
Ethernet
IEEE 802.2
IEEE 802.3 (Ethernet)
IEEE 802.3u (FastEthernet)
IEEE 802.3z (GigabitEthernet)
IEEE 802.3ab (GigabitEthernet over Copper)
Token Ring/IEEE 802.6
FDDI
OSI Layers
LAN Specification

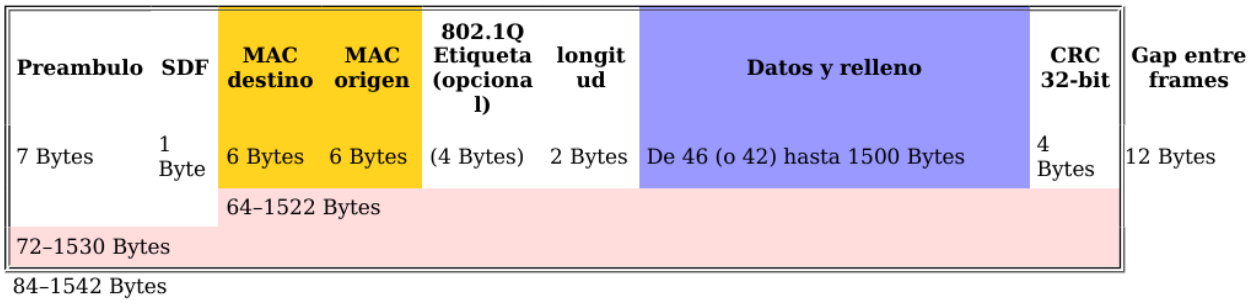
Protocolo	Denominación	Usado en
HDLC	High–level Data Link Control	ISO
SDLC	Synchronous Data Link Control	IBM SNA
LAPB	Link Access Procedure – Balanced	X.25
LAPD	Link Access Procedure – D-channel	RDSI
LAPF	Link Access Procedure for Frame-mode	Frame Relay
LLC	Logical Link Control	IEEE 802
SLIP	Serial Line Internet Protocol	
PPP	Point-to-Point Protocol	
ATM	Asynchronous Transfer Mode	

La capa de enlace se encarga de los siguientes aspectos:

- Delimitación de trama
- Segmentación y bloque
- Uso del medio compartido
- Control de flujo
- Control de errores

6.1.1 Delimitación de trama

Trama de 802.3 Ethernet



Nota: Al final de la trama hay un intervalo llamado IFG de 12 bytes que no se utiliza, se explica más adelante.

Campos de la trama:

- **Preámbulo**: Sincronización bit «10101010» (x7).
- **SDF**: Delimitador de comienzo de trama «10101011».
- **Direcciones MAC origen y destino**:
  - Notación (por ejemplo): F2:3E:C1:8A:B1:01
  - OUI: Identificador organización.(3 bytes primeros)
  - NIC: Id. Tarjeta interfaz de Red. (3 bytes últimos)
  - Dirección de difusión (broadcast) FF:FF:FF:FF:FF:FF. Este tipo de dirección se utiliza para que todos los equipos conectados en el mismo dominio de difusión recojan la trama.

- **Etiqueta**: es un campo opcional que indica la pertenencia a una VLAN o prioridad en IEEE P802.1p.
- **Longitud** (Valores < 1536).
- **Datos + Relleno**:
  - Trama mínima de 64 bytes (512 bits -> 51,2 μs).
  - Como Tx 2Tp: Datos+Relleno 46 bytes.
- **FCS** (Frame Check Sequence) -> CRC (CRC, Cyclic Redundancy Check):

  Secuencia de chequeo de trama. Es un CRC de un polinomio generador de orden 33:

  x32+x26+x23+x22+x16+x12+x11+x10+x8+x7+x5+x4+x2+x+1

Espacio mínimo entre tramas:

- **IFG**: «Inter-frame Gap» -> 12 bytes (96 bits) es un intervalo de espera que se realiza siempre antes de empezar a transmitir aún si el medio está libre.

CRC

La **comprobación de redundancia cíclica** (CRC) es un código de detección de errores usado frecuentemente en redes digitales y en dispositivos de almacenamiento para detectar cambios accidentales en los datos. Los bloques de datos ingresados en estos sistemas contiene un valor de verificación adjunto, basado en el residuo de una división de polinomios; el cálculo es repetido en el destino, y la acción de corrección puede tomarse en caso de que el valor de verificación no concuerde; por lo tanto se puede afirmar que este código es un tipo de función que recibe un flujo de datos de cualquier longitud como entrada y devuelve un valor de longitud fija como salida. El término suele ser usado para designar tanto a la función como a su resultado. Pueden ser usadas como suma de verificación para detectar la alteración de datos durante su transmisión o almacenamiento. Las CRC son populares porque su implementación en hardware binario es simple, son fáciles de analizar matemáticamente y son particularmente efectivas para detectar errores ocasionados por ruido en los canales de transmisión.

Ejemplo:

- Información a transmitir: 10110101101
- Polinomio generador: 10011
- Trama transmitida: `10110101101 0110`
- Resto (CRC-4): `0110`

6.1.2 Segmentación y bloque

La segmentación surge por la longitud de las tramas ya que si es muy extensa, se debe de realizar tramas más pequeñas con la información de esa trama excesivamente larga.

Si estas tramas son excesivamente cortas, se ha de implementar unas técnicas de bloque que mejoran la eficiencia y que consiste en concatenar varios mensajes cortos de nivel superior en una única trama de la capa de enlace más larga.

6.1.3 Uso del medio compartido

- División estática del canal
  - Técnicas de multiplexación (TDM, FDM o WDM, SDM, CDM)
- División dinámica del canal

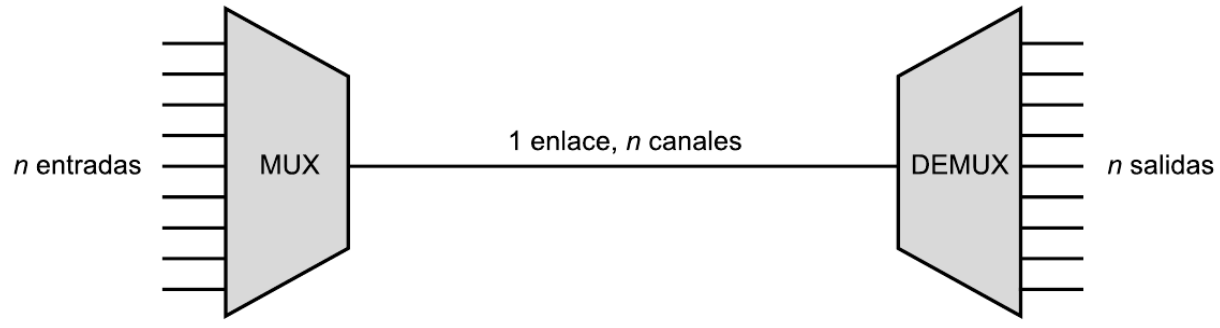
```
1011010110100000   |10011
10011              10101010010
 01011
 00000
  10110
  10011
   01011
   00000
    10111
    10011
     01000
     00000
      10001
      10011
       00100
       00000
        01000
        00000
         10000
         10011
          00110
          00000
           0110
```

$$x^{14} \quad x^{12}\,x^{11} \quad x^{9} \quad x^{7}\,x^{6} \quad x^{4} \quad |\,x^{4}+x+1$$
$$x^{14} \qquad x^{11}\,x^{10} \qquad\qquad x^{10}+x^{8}+x^{6}+x^{4}+x$$
$$x^{12} \quad x^{10}\,x^{9}$$
$$x^{12} \qquad x^{9}\,x^{8}$$
$$x^{10} \quad x^{8}\,x^{7}\,x^{6}$$
$$x^{10} \qquad x^{7}\,x^{6}$$
$$x^{8} \qquad x^{4}$$
$$x^{8} \qquad x^{5}\,x^{4}$$
$$x^{5}$$
$$x^{5} \qquad x^{2}\,x$$
$$x^{2}\,x$$

- Técnicas de contención (CSMA/CD)
- Protocolos libres de colisión (Paso de testigo, reserva)

División estática: Multiplexación

La multiplexación es la combinación de dos o más canales de información en un solo medio de transmisión usando un dispositivo llamado multiplexor. El proceso inverso se conoce como demultiplexación. Un concepto muy similar es el de control de acceso al medio.



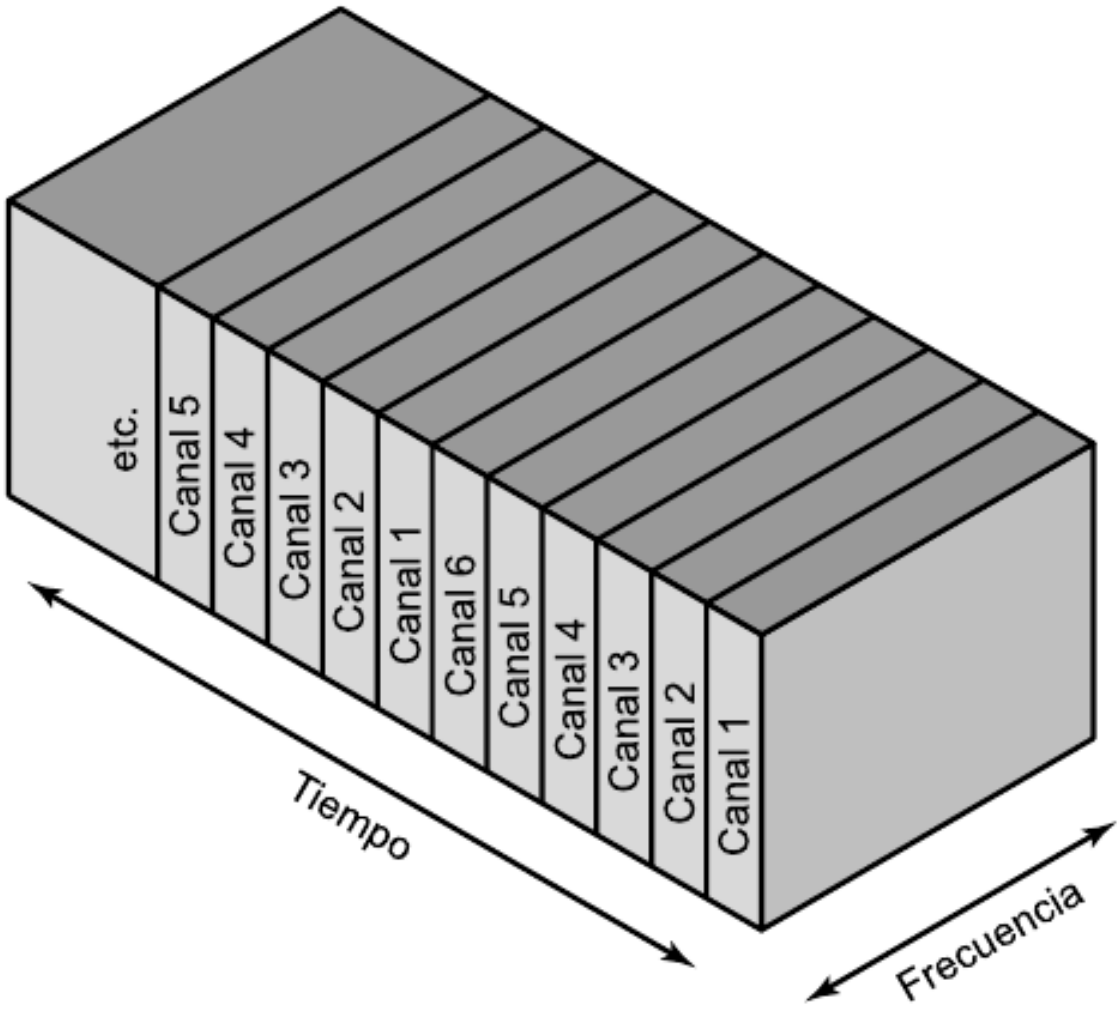
Una aplicación usual de la multiplexación son las comunicaciones de larga distancia. Los enlaces de las redes de larga distancia son líneas de alta capacidad de fibra, de cable coaxial o de microondas, de modo que pueden transportar simultáneamente varias transmisiones de voz y de datos haciendo uso de las técnicas de multiplexación.

Una analogía posible para el problema del acceso múltiple sería una habitación (que representaría el canal) en la que varias personas desean hablar al mismo tiempo. Si varias personas hablan a la vez, se producirán interferencias

y se hará difícil la comprensión. Para evitar o reducir el problema, podrían hablar por turnos (estrategia de división por tiempo - TDMA), hablar unos en tonos más agudos y otros más graves de forma que sus voces se distinguieran (división por frecuencia - FDMA), dirigir sus voces en distintas direcciones de la habitación (división espacial - SDMA) o hablar en idiomas distintos (división por código – CDMA), sólo las personas que conocen el código (es decir, el «idioma») pueden entenderlo.

TDMA (Acceso Múltiple por División de Tiempo)

Hace uso de multiplexación por división de tiempo o TDM (Time Division Multiplexing). En ella, el ancho de banda total del medio de transmisión es asignado a cada canal durante una fracción del tiempo total (intervalo de tiempo). Es decir se divide un único canal de frecuencia de radio en varias ranuras de tiempo. A cada persona que hace una llamada se le asigna una ranura de tiempo específica para la transmisión, lo que hace posible que varios usuarios utilicen un mismo canal simultáneamente sin interferir entre sí.



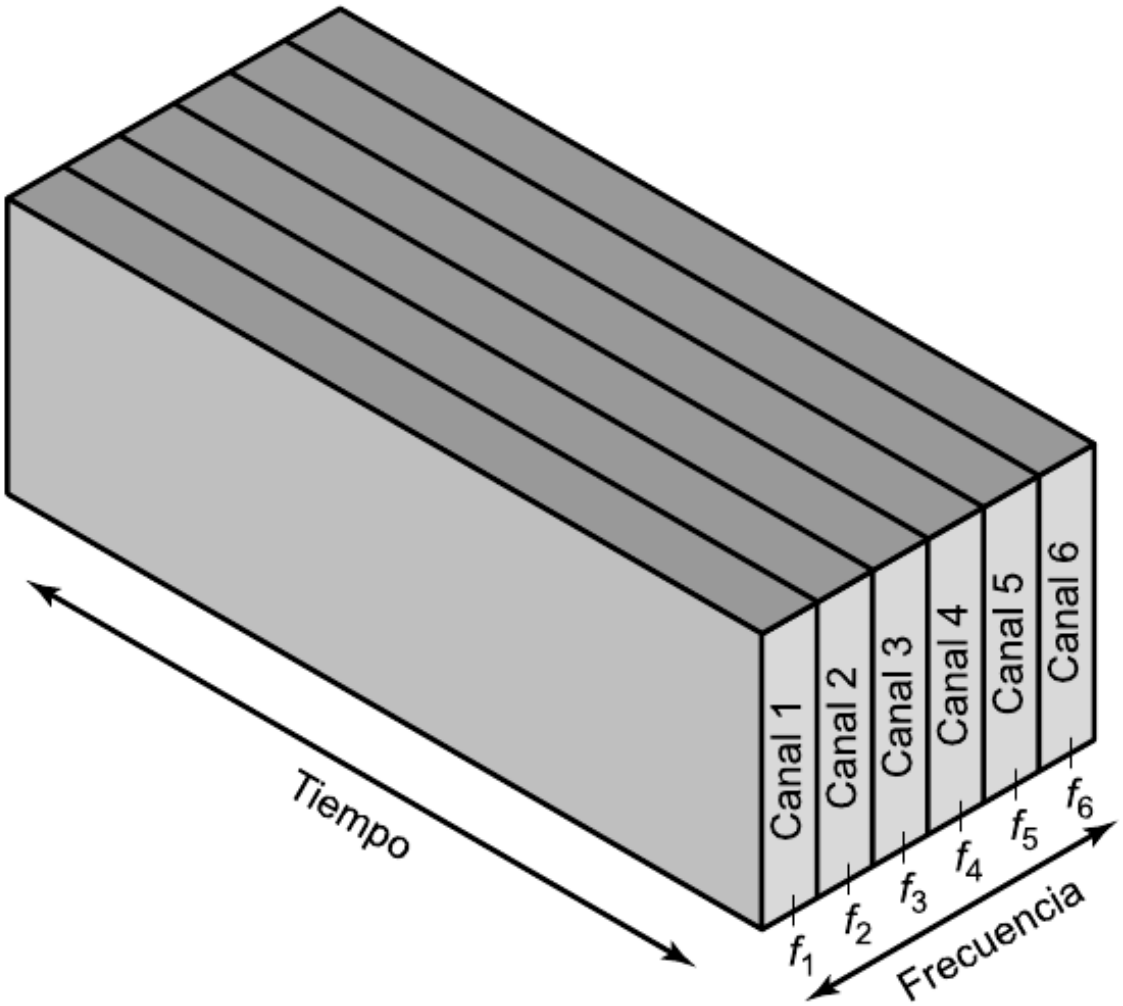
Multiplexación por división en el tiempo

Existen varios estándares digitales basados en TDMA, tal como TDMA D-**AMPS** (Digital-Advanced Mobile Phone System), TDMA D-AMPS-1900, PCS-1900 (Personal Communication Services), **GSM** (Global System for Mobi-

le Communication, en el que se emplea junto con saltos en frecuencia o frequency hopping), DCS-1800 (Digital Communications System) y PDC (Personal Digital Cellular).

FDMA (Acceso Múltiple por División de Frecuencia)

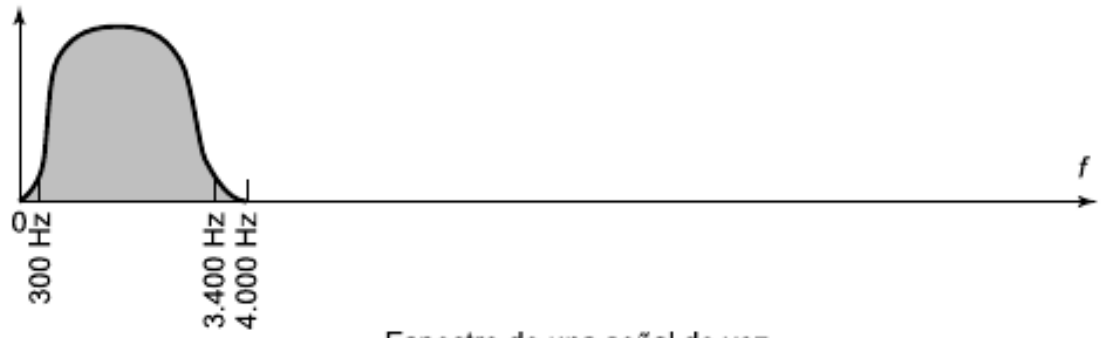
Hace uso de multiplexación por división de frecuencia o FDM (Frequency Division Multiplexing) y su equivalente para medios ópticos, por división de longitud de onda o WDM (Wavelength Division Multiplexing).



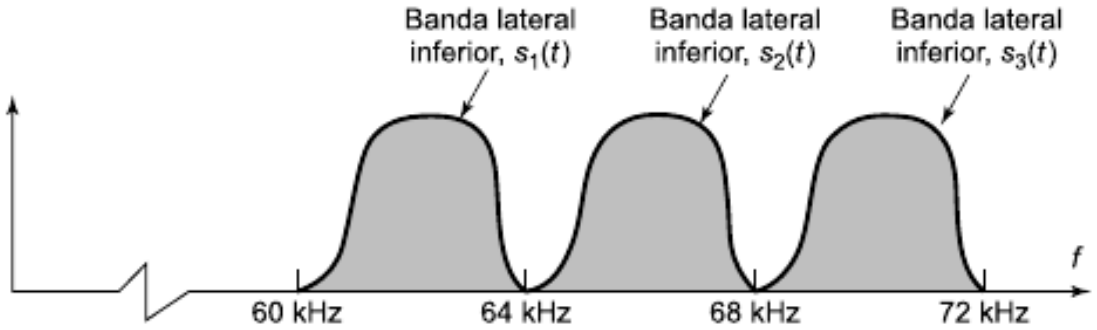
Multiplexación por división en frecuencias

FDM es un tipo de multiplexación utilizada generalmente en sistemas de transmisión analógicos. La forma de funcionamiento es la siguiente: se convierte cada fuente de varias que originalmente ocupaban el mismo espectro de frecuencias, a una banda distinta de frecuencias, y se transmite en forma simultánea por un solo medio de transmisión. Así se pueden transmitir muchos canales de banda relativamente angosta por un solo sistema de transmisión de banda ancha.

Hay muchas aplicaciones de FDM, por ejemplo, la **radio FM** comercial y las emisoras de **televisión analógica**, así como los sistemas de telecomunicaciones de alto volumen.



Espectro de una señal de voz



Espectro de la señal compuesta usando subportadoras de 64 kHz, 68 kHz y 72 kHZ

FDM de tres señales en la banda de voz.

Una variante de FDM es la utilizada en fibra óptica, donde se multiplexan señales, que pueden ser analógicas o digitales, y se transmiten mediante portadoras ópticas de diferente longitud de onda, dando lugar a la denominada multiplexación por división de longitud de onda, o **WDM** del inglés Wavelength Division Multiplexing.

SDMA (Acceso Múltiple por División de Espacio)

Hace uso de multiplexación por división de espacio o SDM (Space Division Multiplexing).

El Acceso múltiple por división de espacio es una tecnología que segmenta el espacio en sectores utilizando antenas unidireccionales. Se utiliza generalmente en **comunicaciones por satélite**, pero también en redes celulares para reducir el número de estaciones base.

CDMA (Acceso Múltiple por División de Código)

Hace uso de multiplexación por división en código o CDM (Code Division Multiplexing).

La división por código se emplea en múltiples sistemas de comunicación por radiofrecuencia, tanto de **telefonía móvil** (como IS-95, CDMA2000, FOMA o UMTS), transmisión de datos (**WiFi**) o navegación por satélite (**GPS**).

División dinámica: diversas técnicas

CSMA/CD (Acceso Múltiple con Escucha de Portadora y Detección de Colisiones)

CSMA/CD (del inglés Carrier Sense Multiple Access with Collision Detection) o, en español, acceso múltiple con escucha de portadora y detección de colisiones, es un protocolo de acceso al medio compartido. Su uso está especialmente extendido en **redes Ethernet** donde es empleado para mejorar sus prestaciones. En CSMA/CD, los dispositivos de red escuchan el medio antes de transmitir, es decir, es necesario determinar si el canal y sus recursos se encuentran disponibles para realizar una transmisión. Además, mejora el rendimiento de CSMA finalizando el envío cuando se ha detectado una **colisión**.

En CSMA/CD, cada estación que desea transmitir debe realizar una escucha del medio – escucha de portadora- para comprobar si éste se encuentra libre, es decir, para comprobar que ninguna otra estación está en ese instante transmitiendo un mensaje. Si el medio se encuentra libre entonces tiene lugar dicha transmisión. Aun así, puede ocurrir que varias estaciones tengan mensajes para enviar y que comiencen a transmitir una trama en el mismo instante. Cuando esto se sucede, se dice que ha ocurrido una colisión en la red. La estación que ha detectado la colisión procederá a enviar un mensaje de jam de 32 bits al resto de estaciones para notificar dicho evento. Una vez que todas las estaciones han sido notificadas, automáticamente se paran todas las transmisiones y se ejecuta un algoritmo de backoff (o de postergación) que consiste en esperar un tiempo aleatorio (backoff) antes de volver a intentar la transmisión.

Token Ring (Paso de testigo)

Esta técnica se basa en una pequeña **trama o testigo** que circula a lo largo del **anillo**. Un bit indica el estado del anillo (libre u ocupado) y cuando ninguna estación está transmitiendo, el testigo simplemente circula por el anillo pasando de una estación a la siguiente. Cuando una estación desea transmitir, espera a recibir el testigo modificando el bit de estado del anillo de libre a ocupado e inserta a continuación la información a enviar junto con su propia dirección y la de la estación destino. El paquete de datos circula por el anillo hasta llegar a la estación receptora que copia su contenido y lo vuelve a poner en circulación incluyendo una marca de recepción, de tal forma que, cuando vuelve a llegar a la estación emisora, ésta lo retira de la red y genera un nuevo testigo libre.

Este sistema es poco eficiente para cargas bajas, pero para cargas altas el sistema se comporta de manera muy eficiente y equitativo. Una desventaja seria es que se pierda el testigo, en cuyo caso toda la red se bloquearía. Los bits que

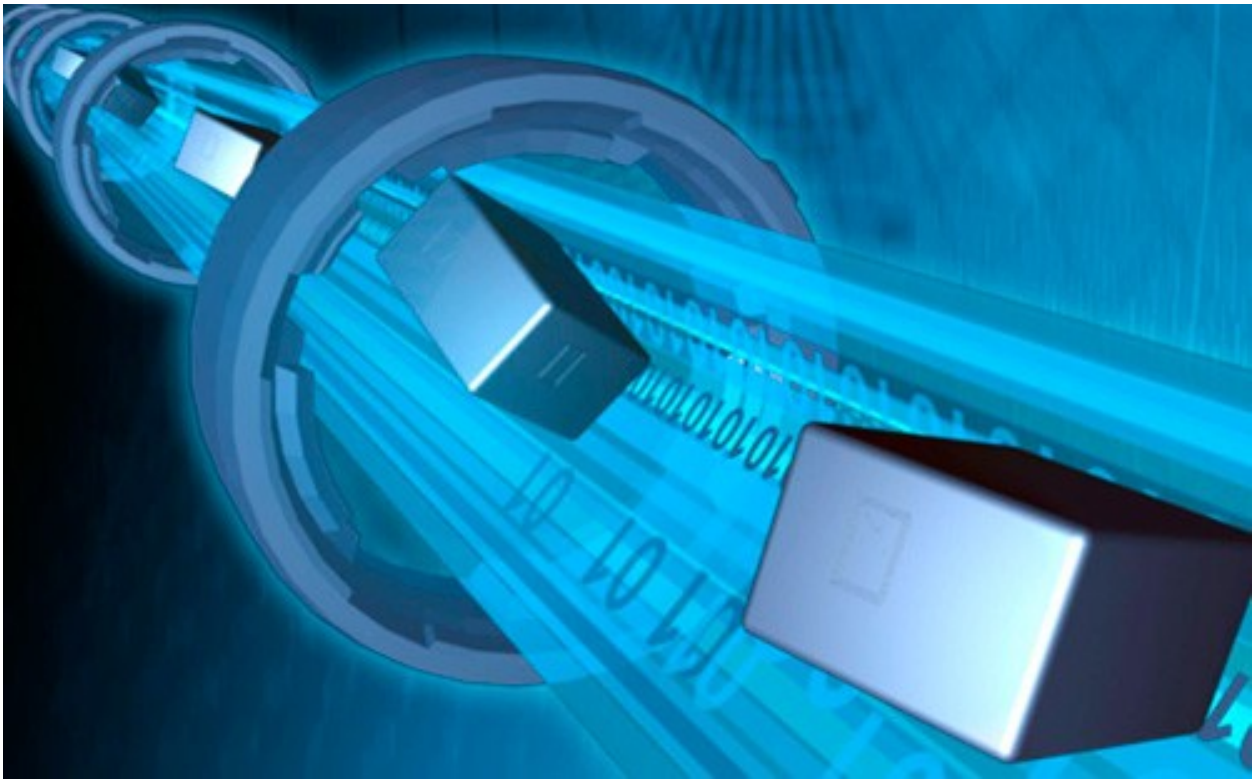
se modifican en el anillo indican si la trama que acompaña al anillo ha llegado a su destino, si no ha llegado o si ha llegado pero no se ha copiado. Esta información de control es muy importante para el funcionamiento del sistema.

Token Ring fue desarrollada por IBM en los años 1970 con topología física en anillo y técnica de acceso de paso de testigo, usando un frame de 3 bytes llamado token que viaja alrededor del anillo. Token Ring se recoge en el estándar IEEE 802.5. En desuso por la popularización de Ethernet.

Las características más destacadas de esta arquitectura son:

- Utiliza una topología lógica en anillo, aunque por medio de una unidad de acceso de estación múltiple (MSAU o **MAU** - Multistation access unit), la red puede verse como si fuera una estrella. Tiene **topología física estrella y topología lógica en anillo**.
- Cada equipo conectado a la red dispone de una interfaz de unidad adjunta (**AUI** - Attachment Unit Interface) que permite la conexión a la MAU.
- Utiliza cable especial apantallado, aunque el cableado también puede ser par trenzado.
- La longitud total de la red no puede superar los 366 metros.
- La distancia entre una computadora y el MAU no puede ser mayor que 100 metros (por la degradación de la señal después de esta distancia en un cable de par trenzado).
- A cada MAU se pueden conectar ocho computadoras.
- Estas redes alcanzan una velocidad máxima de transmisión que oscila entre los 4 y los 16 Mbps.
- Posteriormente el High Speed Token Ring (HSTR) elevó la velocidad a 110 Mbps pero la mayoría de redes no la soportan.

6.1.4 Control de flujo



El control de flujo es necesario para no saturar al receptor de uno a más emisores. Se realiza normalmente en la capa de transporte, y también a veces en la capa de enlace. Utiliza mecanismos de retroalimentación. El control de flujo conlleva dos acciones importantísimas que son la detección de errores y la corrección de errores.

Existen 2 técnicas:

- Control de flujo mediante parada y espera
- Control de flujo mediante ventana deslizante

Control de flujo mediante parada y espera

Nota: La numeración de tramas es 0 y 1.

Después se reinicia la numeración, lo que no significa que se vuelvan a enviar las tramas, sino que la numeración vuelve a iniciarse.

El procedimiento más sencillo para controlar el flujo, denominado control de flujo mediante parada y espera, funciona de la siguiente manera. Una entidad origen transmite una trama. Tras la recepción, la entidad destino indica su deseo de aceptar otra trama mediante el envío de una confirmación de la trama que acaba de recibir. **El origen debe esperar a recibir la confirmación antes de proceder a la transmisión de la trama siguiente**. De este modo, el destino puede parar el flujo de los datos sin más que retener las confirmaciones. Este procedimiento funciona adecuadamente y, de hecho, es difícil mejorar sus prestaciones cuando el mensaje se envía usando un número reducido de tramas de gran tamaño.

Sin embargo, en la práctica las tramas tienden a ser pequeñas puesto que así:

- el receptor necesita menor memoria temporal.
- se reduce el riesgo de errores.
- se evita la ocupación excesiva del medio por parte de una única estación transmisora.

Control de flujo mediante ventana deslizante

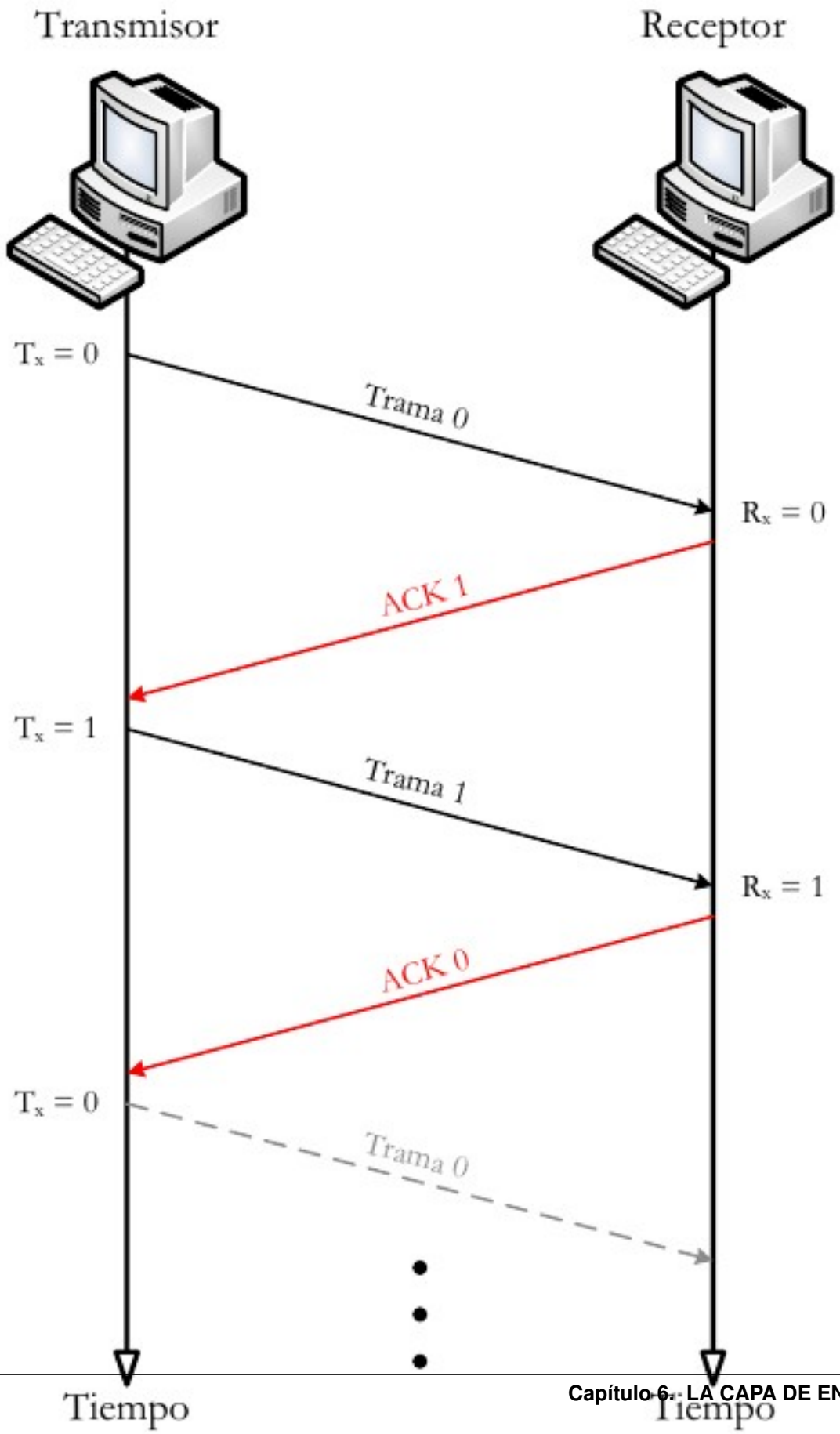
Con el procedimiento anterior solo puede haber en tránsito una trama a la vez. Si se permite que transiten **varias tramas al mismo tiempo sobre el enlace**, la eficiencia mejorará significativamente.

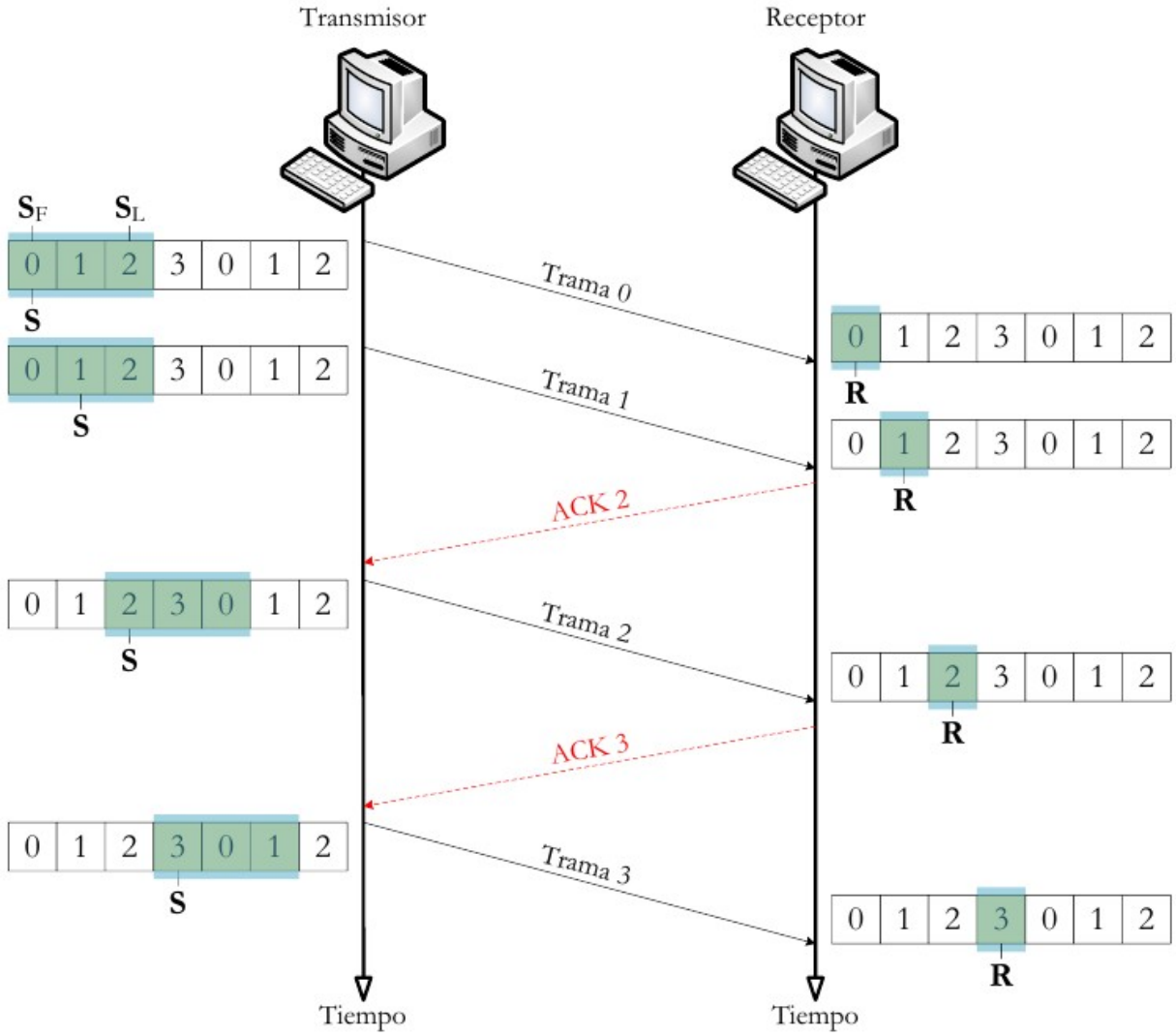
Veamos cómo funcionaría este procedimiento para dos estaciones, A y B, conectadas mediante un enlace full-duplex. La estación B reserva memoria temporal suficiente para almacenar 3 tramas. Por tanto, B puede aceptar 3 tramas, permitiéndosele a A enviar este mismo número de tramas sin tener que esperar ninguna confirmación. Para saber qué tramas se han confirmado, cada una de ellas se etiqueta con un número de secuencia. B confirma una trama mediante el envío de una confirmación que incluye el número de secuencia de la siguiente trama que se espera recibir. Esta confirmación informa también, implícitamente, acerca de que B está preparado para recibir las 3 tramas siguientes, comenzando por la de número especificado.

6.1.5 Control de errores

El control de errores hace referencia a los mecanismos necesarios para la detección y la corrección de errores que aparecen en una transmisión de tramas. Como se ha considerado hasta ahora, los datos se envían en base a una secuencia de tramas, las cuales se reciben en el mismo orden en que fueron enviadas y cada una de ellas, con carácter previo a su recepción, sufre un retardo arbitrario y posiblemente variable. Se contemplan dos tipos de errores potenciales:

- **Tramas perdidas**: se produce cuando una trama enviada no llega al otro extremo. Así, por ejemplo, una ráfaga de ruido puede dañar una trama de manera que el receptor no se percate siquiera de su transmisión.


Transmisor
Receptor
Tx = 0
Trama 0
Rx = 0
ACK 1
Tx = 1
Trama 1
Rx = 1
ACK 0
Tx = 0
Trama 0
Tiempo
Tiempo


Transmisor
Receptor
S_F
S_L
S
R
Trama 0
Trama 1
ACK 2
Trama 2
ACK 3
Trama 3
Tiempo
Tiempo

- **Tramas dañadas**: ocurre cuando una trama se recibe con algunos bits erróneos (modificados durante la transmisión).

Las técnicas más usuales para el control de errores se basan en algunas o todas las siguientes aproximaciones:

- **Detección de errores**: haciendo uso de códigos de comprobación de redundancia cíclica (CRC, Cyclic Redundancy Check).
- **Confirmaciones positivas**: el destino devuelve una confirmación positiva por cada trama recibida con éxito, libre de errores.
- **Retransmisión tras la expiración de un temporizador**: la fuente retransmite las tramas que no se han confirmado tras un periodo de tiempo predeterminado.
- **Confirmación negativa y retransmisión**: el destino devuelve una confirmación negativa para aquellas tramas en las que se detecta la ocurrencia de errores. El origen retransmitirá de nuevo dichas tramas.

Estos mecanismos se denominan genéricamente solicitud de repetición automática (**ARQ, Automatic Repeat reQuest**); el objetivo de un esquema ARQ es convertir un enlace de datos no fiable en fiable. Hay tres variantes ARQ estandarizadas:

- ARQ con parada y espera.
- ARQ con vuelta atrás N.
- ARQ con rechazo selectivo.

ARQ con parada y espera

Si existe un error en el envío de la trama (por que llegue dañada -CRC no coincidente- o se pierda -expire el temporizador-), se vuelve a transmitir.

ARQ con vuelta atrás N

El emisor va enviando las tramas que tiene en su ventana deslizante. Si existe un error en el envío de la trama (por que llegue dañada -CRC no coincidente- o se pierda -expire el temporizador-) se vuelve a transmitir esa trama y todas las siguientes aunque ya hayan sido enviadas previamente.

ARQ con rechazo selectivo

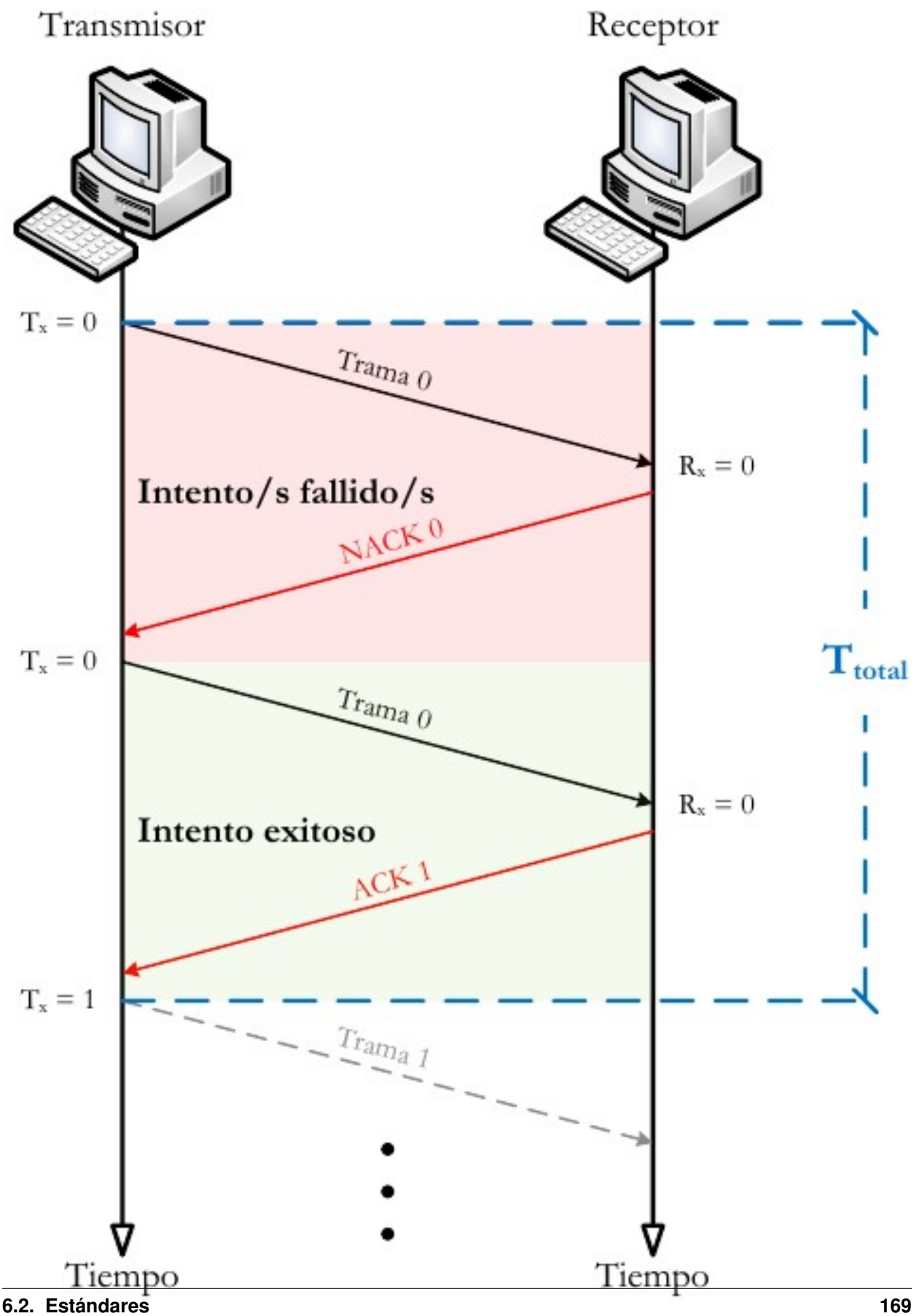
El emisor va enviando las tramas que tiene en su ventana deslizante. Si existe un error en el envío de una trama (por que llegue dañada o su temporizador expire), se vuelve a transmitir sólo esa trama.

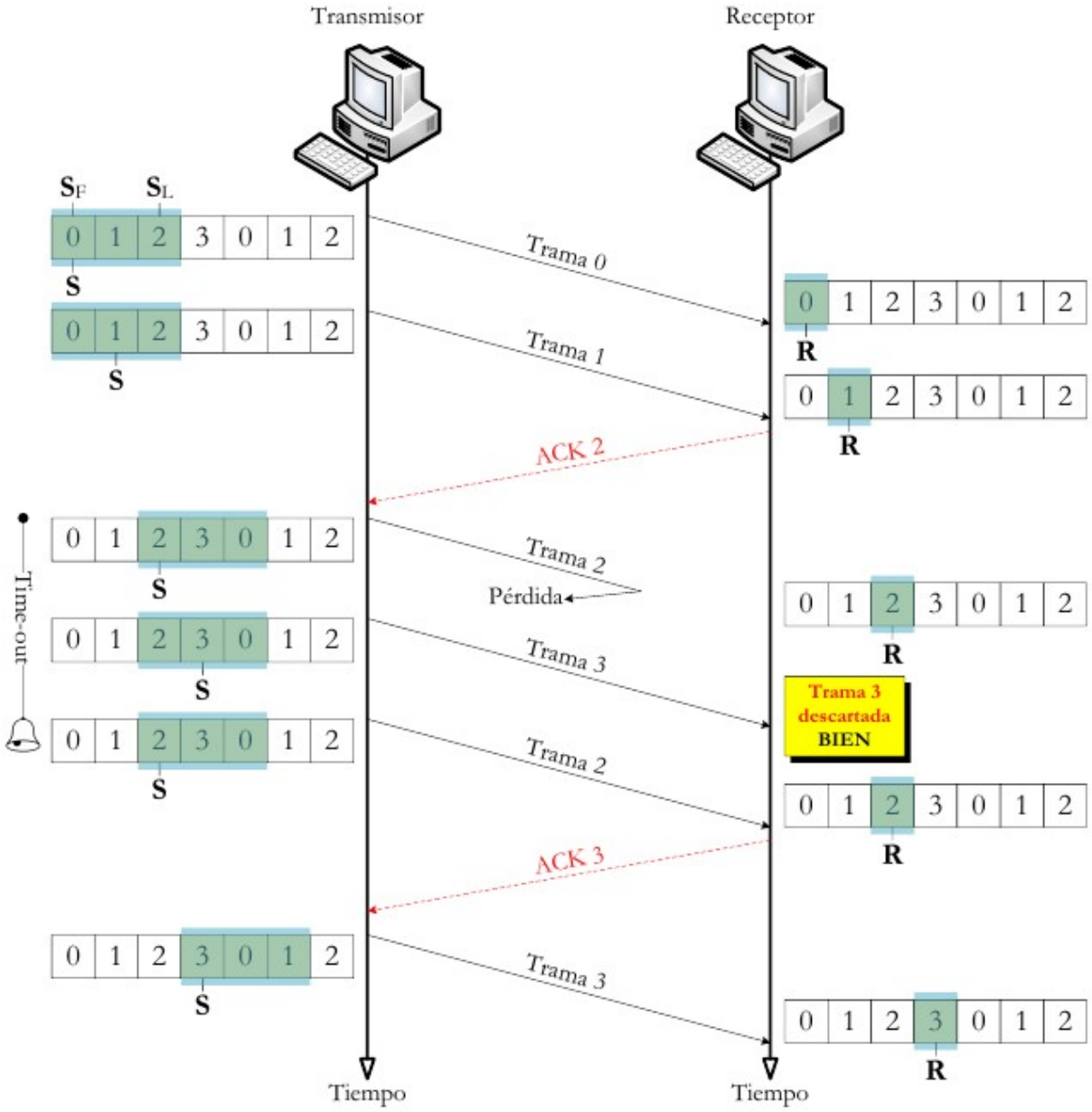
6.2 Estándares

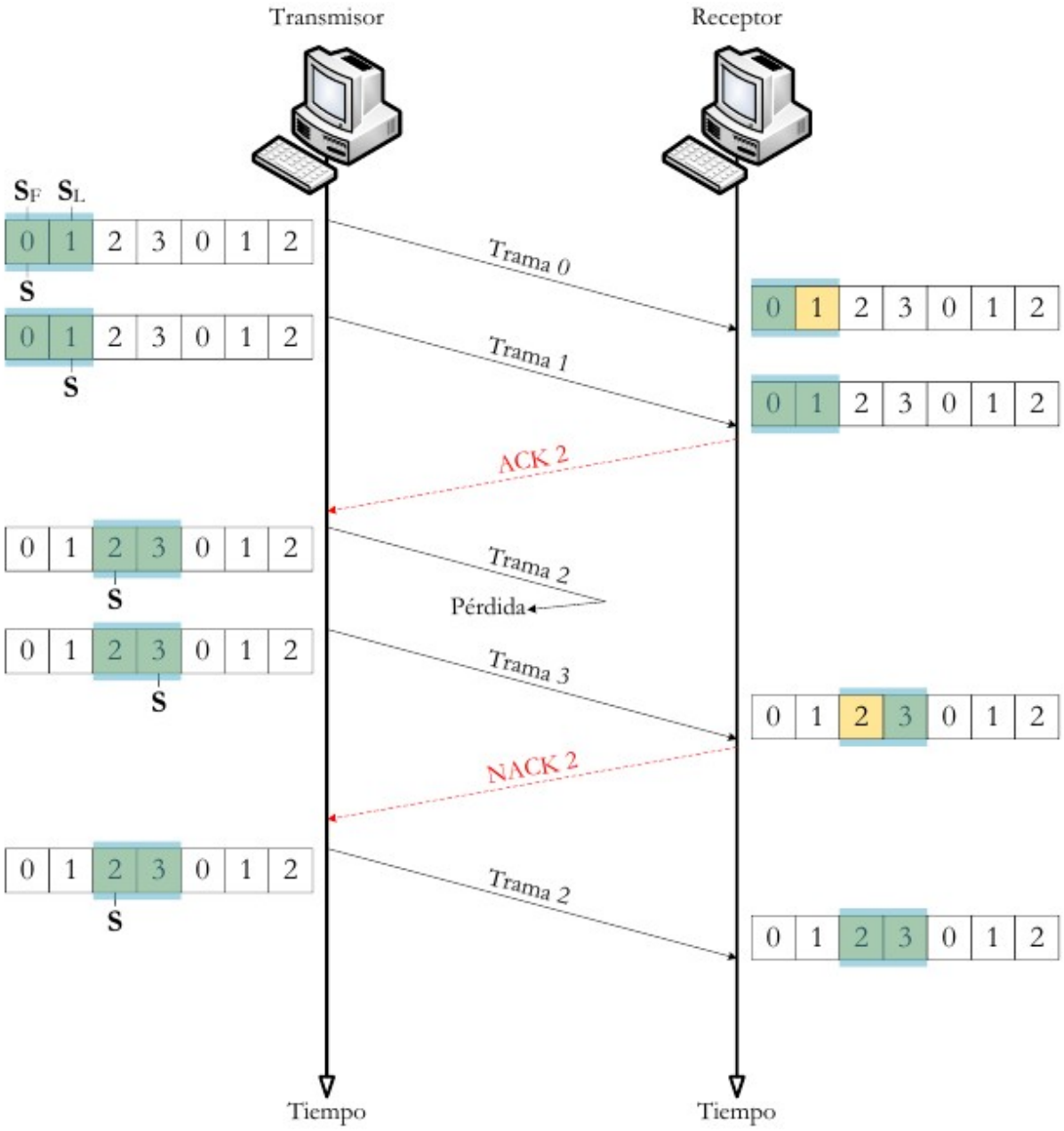
6.2.1 Ethernet (IEEE 802.3)

IEEE 802.3 fue el primer intento para estandarizar ethernet. Aunque hubo un campo de la cabecera que se definió de forma diferente, posteriormente ha habido ampliaciones sucesivas al estándar que cubrieron las ampliaciones de velocidad (Fast Ethernet, Gigabit Ethernet y los de 10, 40 y 100 Gigabits Ethernet), redes virtuales, hubs, conmutadores y distintos tipos de medios, tanto de fibra óptica como de cables de cobre (tanto par trenzado como coaxial).

Los estándares de este grupo no reflejan necesariamente lo que se usa en la práctica, aunque a diferencia de otros grupos este suele estar cerca de la realidad.


Transmisor
Receptor
Tx = 0
Trama 0
Rx = 0
Intento/s fallido/s
NACK 0
Tx = 0
Trama 0
Rx = 0
Intento exitoso
ACK 1
Tx = 1
Trama 1
Ttotal
Tiempo
Tiempo


Transmisor
Receptor
S_F
S_L
S
R
Trama 0
Trama 1
ACK 2
Trama 2
Pérdida
Time-out
Trama 3
Trama 3 descartada BIEN
Trama 2
ACK 3
Trama 3
Tiempo
Tiempo


Transmisor
Receptor
S_F S_L
0 1 2 3 0 1 2
S
Trama 0
Trama 1
ACK 2
Trama 2
Pérdida
Trama 3
NACK 2
Trama 2
Tiempo
Tiempo

Nombre	Medio	Distancia máx	Estándar
Ethernet (10 Mbps)			
10BASE5	Coaxial grueso	500 m	802.3
10BASE2	Coaxial fino	185 m	802.3a
10BASE-T	Par trenzado cat. 3 o 5	100 m	802.3i
10BASE-FL	MMF 850 nm	2 km	802.3j
FastEthernet (100 Mbps)			
100BASE-TX	Par trenzado cat. 5	100 m	802.3u
100BASE-FX	MMF 1310 nm	2 km	
GigabitEthernet (1000 Mbps)			
1000BASE-T	Par trenzado >= cat. 5	100 m	802.3ab
1000BASE-SX	MMF 850 nm	550 m	802.3z
1000BASE-LX	MMF y SMF 1310 nm	10 km	
10 GigabitEthernet (10 Gbps)			
10GBASE-T	Par trenzado >= cat 6	100 m	802.3an
10GBASE-SR	MMF 850 nm	400 m	802.3ae
10GBASE-LR	SMF	10 Km	
40 GigabitEthernet (40 Gbps)			
40GBASE-SR4	MMF	125 m	802.3ba
40GBASE-LR4	SMF	10 km	
100 GigabitEthernet (100 Gbps)			
100GBASE-SR10	MMF	125 m	802.3ba
100GBASE-LR4	SMF	10 km	

Siglas

- **MMF**: Fibra multimodo (Multi Mode Fiber)
- **SMF**: Fibra monomodo (Single Mode Fiber)
- **SR**: Corto alcance (Short Range)
- **LR**: Largo alcance (Long Range)

6.2.2 PoE (Power over Ethernet)

La **alimentación a través de Ethernet (Power over Ethernet, PoE)** es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre a un dispositivo de red (switch, punto de acceso, router, teléfono o cámara IP, etc) usando el mismo cable que se utiliza para la conexión de red. Elimina la necesidad de utilizar tomas de corriente en las ubicaciones del dispositivo alimentado y permite una aplicación más sencilla de los sistemas de alimentación ininterrumpida (SAI) para garantizar un funcionamiento las 24 horas del día, 7 días a la semana.

Power over Ethernet se regula en la norma **IEEE 802.3af**, y está diseñado de manera que no haga disminuir el rendimiento de comunicación de los datos en la red o reducir el alcance de la red. La corriente suministrada a través de la infraestructura LAN se activa de forma automática cuando se identifica un terminal compatible y se bloquea ante dispositivos preexistentes que no sean compatibles. Esta característica permite a los usuarios mezclar en la red con total libertad y seguridad dispositivos preexistentes con dispositivos compatibles con PoE.

Actualmente existen en el mercado varios dispositivos de red como switches o hubs que soportan esta tecnología. Para implementar PoE en una red que no se dispone de dispositivos que la soporten directamente se usa una unidad base (con conectores RJ45 de entrada y de salida) con un adaptador de alimentación para recoger la electricidad y una unidad terminal (también con conectores RJ45) con un cable de alimentación para que el dispositivo final obtenga la energía necesaria para su funcionamiento.

Ventajas

- PoE es una fuente de alimentación inteligente: Los dispositivos se pueden apagar o reiniciar desde un lugar remoto usando los protocolos existentes, como el Protocolo simple de administración de redes (SNMP, Simple Network Management Protocol).
- PoE simplifica y abarata la creación de un suministro eléctrico altamente robusto para los sistemas: La centralización de la alimentación a través de concentradores (hubs) PoE significa que los sistemas basados en PoE se pueden enchufar al Sistema de alimentación ininterrumpida (SAI) central, que ya se emplea en la mayor parte de las redes informáticas formadas por más de uno o dos PC, y en caso de corte de electricidad, podrá seguir funcionando sin problemas.
- Los dispositivos se instalan fácilmente allí donde pueda colocarse un cable LAN, y no existen las limitaciones debidas a la proximidad de una base de alimentación (dependiendo la longitud del cable se deberá utilizar una fuente de alimentación de mayor voltaje debido a la caída del mismo, a mayor longitud mayor perdida de voltaje, superando los 25 metros de cableado aproximadamente).
- Un único juego de cables para conectar el dispositivo Ethernet y suministrarle alimentación, lo que simplifica la instalación y ahorra espacio.
- La instalación no supone gasto de tiempo ni de dinero ya que no es necesario realizar un nuevo cableado.
- PoE dificulta enormemente cortar o destrozar el cableado: Generalmente el cableado se encuentra unido a bandejas en los huecos del techo o detrás de conductos de plástico de muy difícil acceso. Cualquier corte de estos cables resultará obvio al momento para quien pase por el lugar y, por supuesto, para los usuarios de los ordenadores que serán incapaces de proseguir con su trabajo.

Desventajas

- Ausencia de estándares tecnológicos para la interoperabilidad de equipos.
- Para poder usar **PoE**, todos los dispositivos de Red (Hub/Switch, Cámaras IP, Puntos de Acceso,...) deben ser compatibles con esta norma.

El estándar original IEEE 802.3af-2003 de PoE proporciona hasta **15,4 W** de potencia de CC (mínimo 44 V DC y 350 mA) para cada dispositivo. Sólo se aseguran 12,95 W en el dispositivo puesto que cierta energía se disipa en el cable.

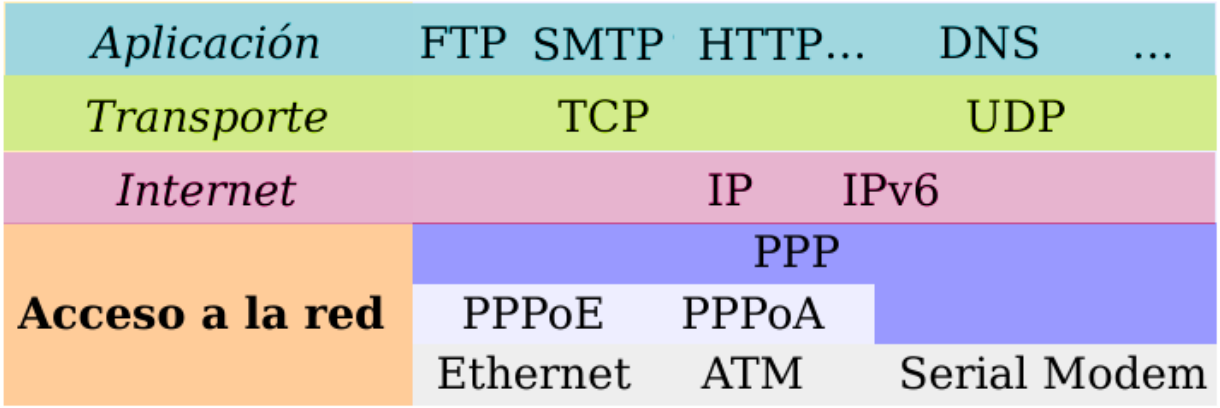
El estandar actualizado IEEE 802.3af-2009 de PoE también conocido como **PoE+** o PoE plus, proporciona hasta **25,5 W** de potencia. Algunos vendedores han anunciado productos que dicen ser compatibles con el estándar 802.3af y ofrecen hasta 51 W de potencia en un solo cable utilizando los cuatro pares del cable de categoría 5.

Comparativa PoE y PoE+

Propiedad	802.3af (802.3at Tipo1)	802.3at Tipo 2
Potencia en el origen	15.40 W	34.20 W
Potencia para dispositivo final	12.95 W	25.50 W
Voltaje en el origen	44.0–57.0 V	50.0–57.0 V
Voltaje para el dispositivo final	37.0–57.0 V	42.5–57.0 V
Intensidad máxima	350 mA	600 mA
Resistencia máxima del cable	20 Ω (Categoría 3)	12.5 Ω (Categoría 5)

6.2.3 Punto a punto

Ubicación de PPP dentro de la arquitectura TCP/IP



Point-to-point Protocol (en español Protocolo punto a punto), también conocido por su acrónimo **PPP**, es un protocolo de nivel de enlace estandarizado en el documento **RFC 1661**. Comúnmente usado para establecer una conexión directa entre dos nodos de red. Puede proveer autentificación de conexión, cifrado de transmisión (usando ECP, RFC 1968), y compresión. PPP es usado en varios tipos de redes físicas incluyendo, cable serial, línea telefónica, line troncal, telefonía celular, especializado en enlace de radio y enlace de fibra óptica como SONET. PPP también es usado en las conexiones de acceso a internet (mercadeado como "broadband"). Los Proveedores de Servicio de Internet (ISPs) han usado PPP para que accedan a internet los usuarios de dial-up, desde que los paquetes de IP no pueden ser transmitidos via modem, sin tener un protocolo de enlace de datos. Dos derivados del PPP son:

- Point to Point Protocolo over Ethernet (PPPoE)
- Point to Point Protocol over ATM (PPPoA)

Son usados comúnmente por Provedores de Servivicio de Internet (ISPs) para establecer una Linea Suscriptora Digital (DSL) de servicios de internet para clientes. Por tanto, se trata de un protocolo asociado a la pila TCP/IP de uso en Internet.

Estructura de la trama

Delimitador	Dirección	Control	Protocolo	Datos	FCS	Delimitador
1 Byte	1 Byte	1 Byte	1 o 2 Bytes	Variable	2 o 4 Bytes	1 Byte
01111110	11111111	00000011				01111110

La dirección 11111111 es la dirección de broadcast. Al tratarse de enlaces punto a punto no existe dirección concreta.

La secuencia de control 00000011 indica transmisión de datos sin secuencia. Se provee un servicio de enlace no orientado a conexión

PPPoE

PPPoE (Point-to-Point Protocol over Ethernet o Protocolo Punto a Punto sobre Ethernet) es un protocolo de red para la encapsulación PPP sobre una capa de Ethernet. Es utilizada mayoritariamente para proveer conexión de banda ancha mediante servicios de cablemódem y DSL. Este ofrece las ventajas del protocolo PPP como son la autenticación, cifrado, mantención y compresión. En esencia, es un protocolo, que permite implementar una capa IP sobre una conexión entre dos puertos Ethernet, pero con las características de software del protocolo PPP, por lo que es utilizado para virtualmente «marcar» a otra máquina dentro de la red Ethernet, logrando una conexión «serial» con ella, con la que se pueden transferir paquetes IP, basado en las características del protocolo PPP.

Esto permite utilizar software tradicional basado en PPP para manejar una conexión que no puede usarse en líneas seriales pero con paquetes orientados a redes locales como Ethernet para proveer una conexión clásica con autenticación para cuentas de acceso a Internet. Además, las direcciones IP en el otro lado de la conexión sólo se asignan cuando la conexión PPPoE es abierta, por lo que admite la reutilización de direcciones IP (direccionamiento dinámico).

El objetivo y funcionamiento de PPPoE es análogo al protocolo PPP sobre RTC con el que a finales de los 90 y bajo un stack tcp, se establecía un enlace ip punto a punto a través de la red telefonica conmutada (RTC), permitiendo utilizar por encima una serie de protocolos de nivel de aplicación tipo http, ftp, telnet, etc.

PPPoE fue desarrollado por UUNET, Redback y RouterWare. El protocolo está publicado en la RFC 2516.

PPPoA

PPPoA (Point-to-Point Protocol over ATM o Protocolo Punto a Punto sobre ATM), es un protocolo de red para la encapsulación PPP en capas ATM AAL5.

El protocolo PPPoA se utiliza principalmente en conexiones de banda ancha, como cable y DSL. Este ofrece las principales funciones PPP como autenticación, cifrado y compresión de datos. Actualmente tiene alguna ventaja sobre PPPoE debido a que reduce la pérdida de calidad en las transmisiones. Al igual que PPPoE, PPPoA puede usarse en los modos VC-MUX y LLC.

Este protocolo se define en la RFC 2364

6.3 Dispositivos

6.3.1 Dominios

Dominios de colisión

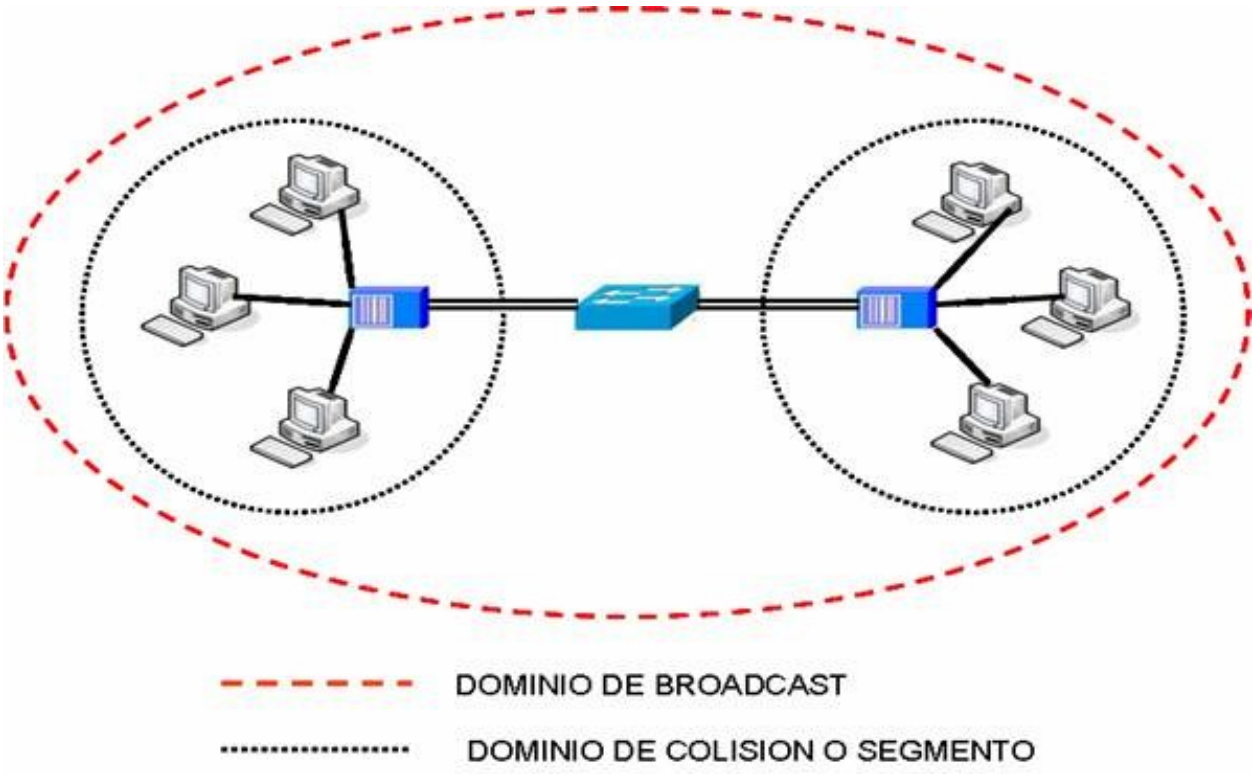
En Ethernet el medio de transmisión es compartido, entonces a medida que se aumentan nodos a un segmento será más complicado acceder al medio, dado que solo un nodo puede transmitir información a la vez. Cuando intentan acceder dos o más nodos al medio al mismo tiempo se presentan colisiones y estas a su vez generan retransmisiones.

La solución para este problema es dividir un segmento en varios dominios de colisión. Para lograr este objetivo se usan dispositivos de capa 2 como puentes y switches.

En un principio el dispositivo más popular para esta tarea era el puente. Este solo tiene dos puertos y es capaz de dividir un dominio de colisión en dos, gracias a decisiones que toma basado netamente en las direcciones MAC de los nodos de la red.

Un switch es básicamente un puente rápido multipuerto, que puede contener docenas de puertos. En vez de crear dos dominios de colisión, cada puerto crea su propio dominio de colisión. Este dispositivo crea y mantiene de forma dinámica una tabla de memoria de contenido direccionable, que contiene toda la información MAC necesaria para cada puerto.

Un dominio de colisión es una parte de la red o segmento en el cual puede haber colisiones, cada vez que ocurre una colisión todas las transmisiones en la red son detenidas por un tiempo aleatorio.



Los dispositivos que pueden segmentar la red en dominios de colisión son los de capa 2 y de capa 3, como los puentes, switches y routers.

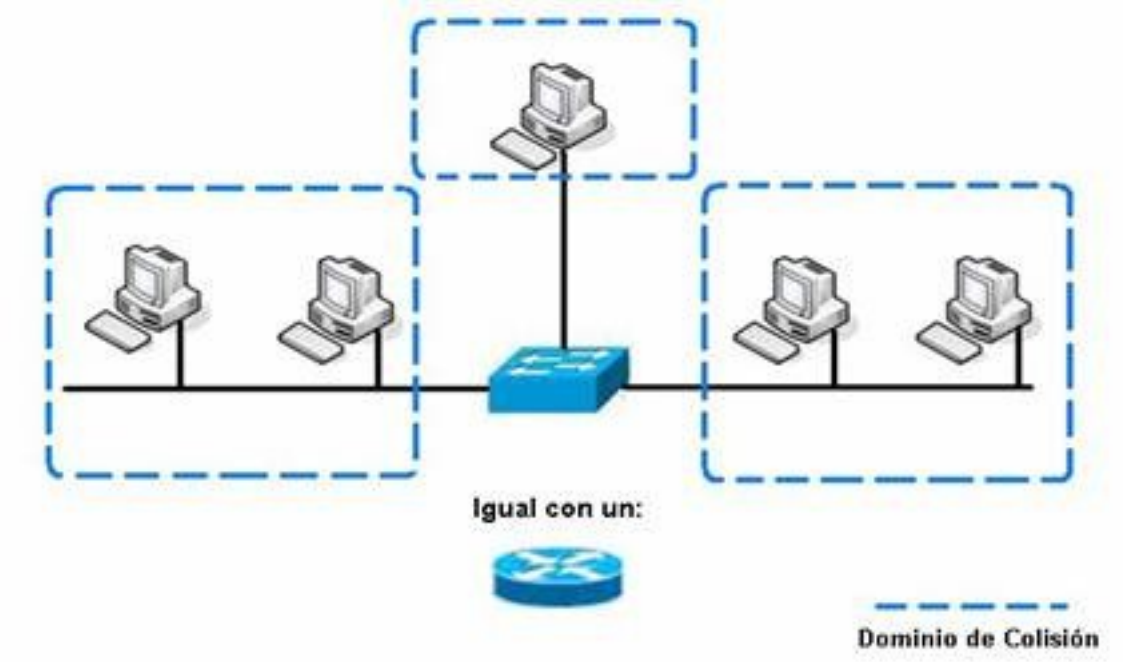
Cuando se usan dispositivos de capa 1, lo que se esta haciendo es aumentar la cobertura de la red al permitirle extenderse. El problema es que todos los dispositivos que se anexen a ese segmento compartirán el mismo dominio de colisión, se aumentara el tráfico en la red, las colisiones y el rendimiento de la red será muy deficiente.

Segmentos

La capacidad para reconocer dominios de colisión es muy importante. Los dispositivos de capa 1 usados en una red generan un solo dominio de colisión. Los dispositivos de capa 2 (puentes y switches) son capaces de hacer un seguimiento de la dirección MAC de cada nodo y reconocer en que segmento de la red se encuentra, es decir que son capaces de controlar el flujo de tráfico al nivel de capa 2.

Al usar puentes y switches el dominio de colisión se divide en partes más pequeñas y a su vez cada parte se convierte en un domino de colisión independiente. Al encontrar menos host en un dominio de colisión es más probable que el medio este disponible para poder transmitir.

En el mundo de las redes de datos el término segmento se emplea en numerosas ocasiones. En el ámbito de las topologías físicas de una red se entiende segmento como la **sección de una red limitada por puentes, routers o switches**.



Difusión (Broadcast) de capa 2

En ocasiones los hosts de la red se ven en situaciones en las cuales necesitan la dirección MAC de otro nodo para acceder a alguna información requerida, pero en la tabla ARP del host no se encuentra dicha dirección. Entonces se envía una petición ARP que es en forma de broadcast.

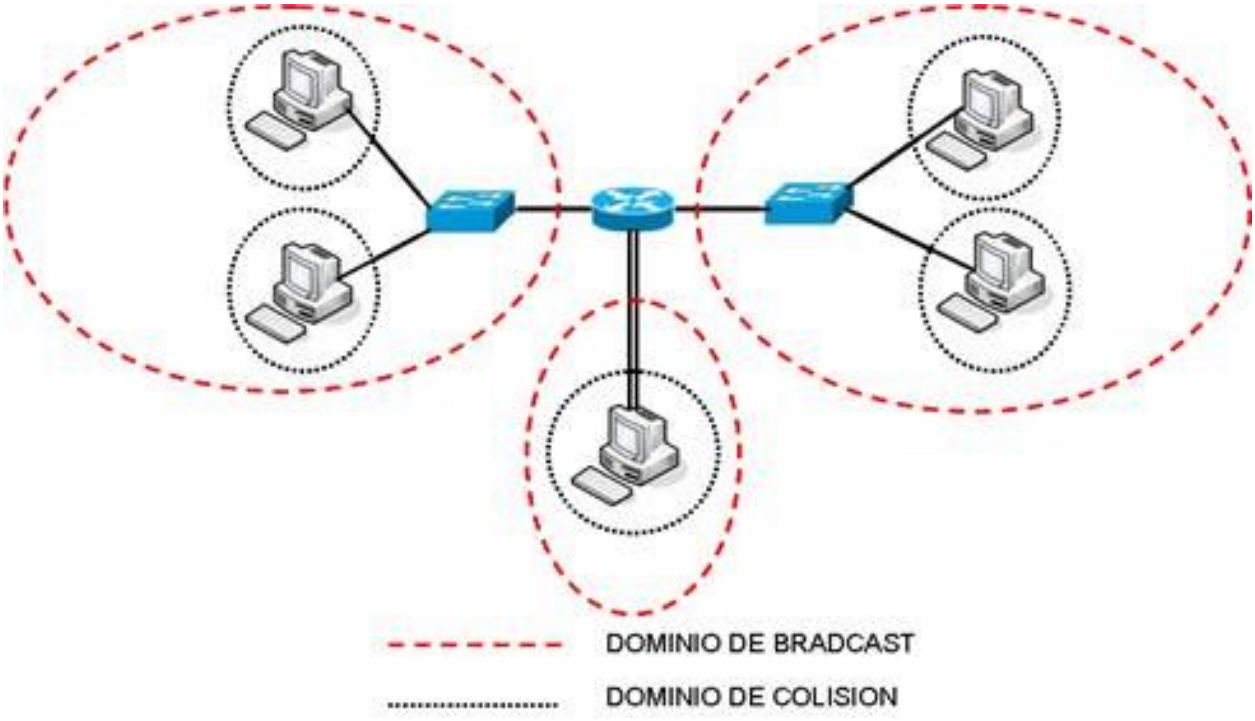
El broadcast se usa para lograr llegar a todos los dominios de colisión. El broadcast de capa 2 se envía con una dirección MAC de la siguiente forma: 0xFFFFFFFFFFFF y todas las tarjetas de red deben responder a este llamado.

Dominios de difusión (Broadcast)

Un dominio de broadcast es un conjunto de dominios de colisión que se encuentran integrados por uno o más dispositivos de capa 2.

Cuando aumentan los dominios de colisión cada host puede acceder al medio de mejor manera, pero estos se pueden ver sobrepasados por la difusión de broadcast, estos deben ser controlados mediante la adición a la red de dispositivos de capa 3, dado que no envían broadcasts.

El envío de información en la capa 3 se basa en la dirección IP destino.



6.3.2 Adaptadores de red

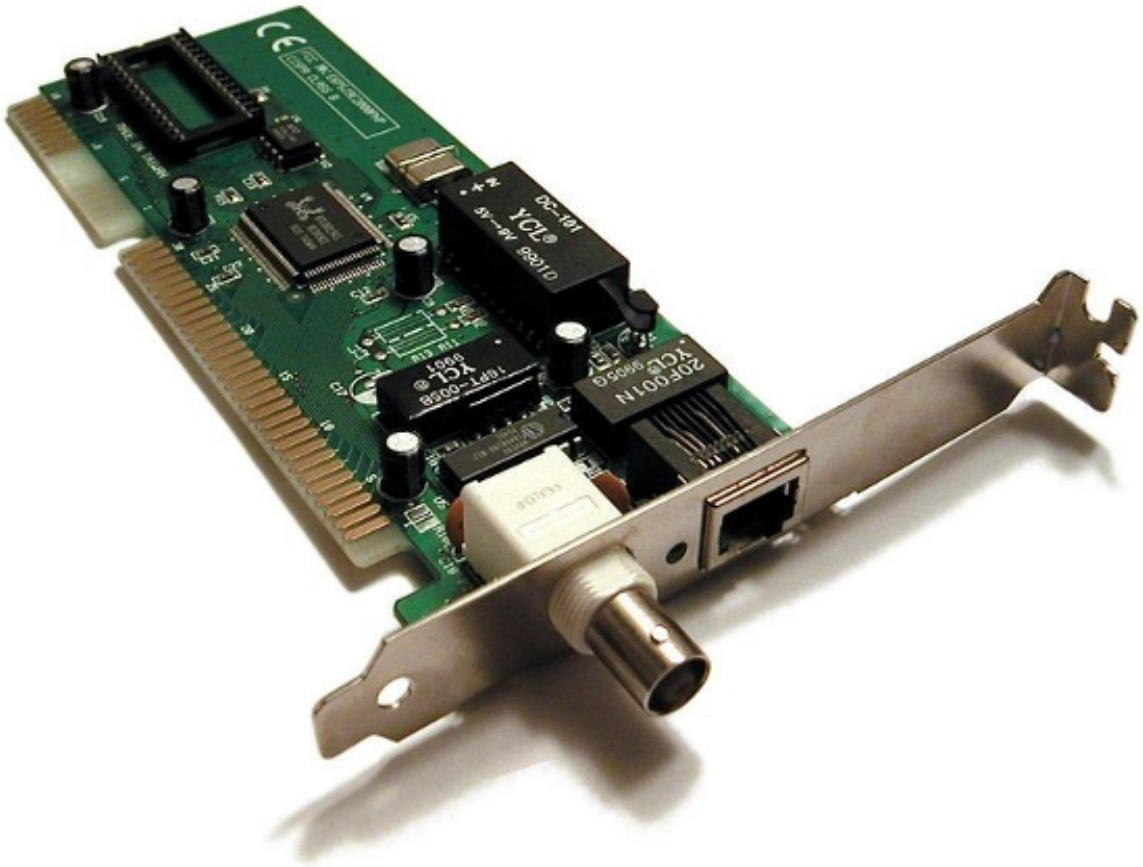
Una **tarjeta de red** o **adaptador de red** es un periférico que permite la comunicación con aparatos conectados entre sí y también permite compartir recursos entre dos o más computadoras. A las tarjetas de red también se les llama **NIC** (por network interface card; en español «tarjeta de interfaz de red»). Hay diversos tipos de adaptadores en función del tipo de cableado o arquitectura que se utilice en la red (coaxial fino, coaxial grueso, Token Ring, etc.), pero actualmente el más común es del tipo Ethernet utilizando una interfaz o conector RJ-45.

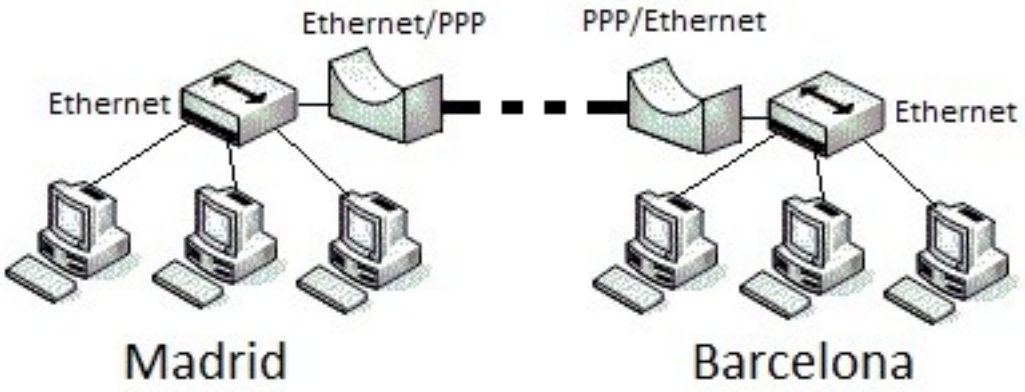
6.3.3 Puentes

Un **puente de red** o **bridge** es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Este interconecta segmentos de red (o divide una red en segmentos) haciendo la transferencia de datos de una red hacia otra con base en la dirección física de destino de cada paquete. En definitiva, un bridge conecta segmentos de red formando una sola subred (permite conexión entre equipos sin necesidad de routers). Funciona a través de una tabla de direcciones MAC detectadas en cada segmento al que está conectado. Cuando detecta que un nodo de uno de los segmentos está intentando transmitir datos a un nodo del otro, el bridge copia la trama para la otra subred, teniendo la capacidad de desechar la trama (filtrado) en caso de no tener dicha subred como destino. Para conocer por dónde enviar cada trama que le llega (encaminamiento) incluye un mecanismo de aprendizaje automático (autoaprendizaje) por lo que no necesitan configuración manual.

6.3.4 Switches

Un **conmutador** o **switch** es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.




Ethernet/PPP
PPP/Ethernet
Ethernet
Ethernet
Madrid
Barcelona

Un conmutador en el centro de una red en estrella.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las redes de área local.

Tipos:

- compacto
- de configuración modular
- apilable
- multicapa (multilayer)
- gestionable

Switch compacto

Estos switches de configuración fija son los que más comúnmente estamos acostumbrados a ver en las redes locales y cibercafés, en las cuales los switches sólo soportan una tecnología y cuyas características no podemos cambiar, es decir, si compramos un switch de 24 puertos FastEthernet no podremos agregarle mas puertos.

Para unir 2 switches en cascada existen dos posibilidades:

- **Uplink**
- MDI/**MDIX** (Auto Cross)

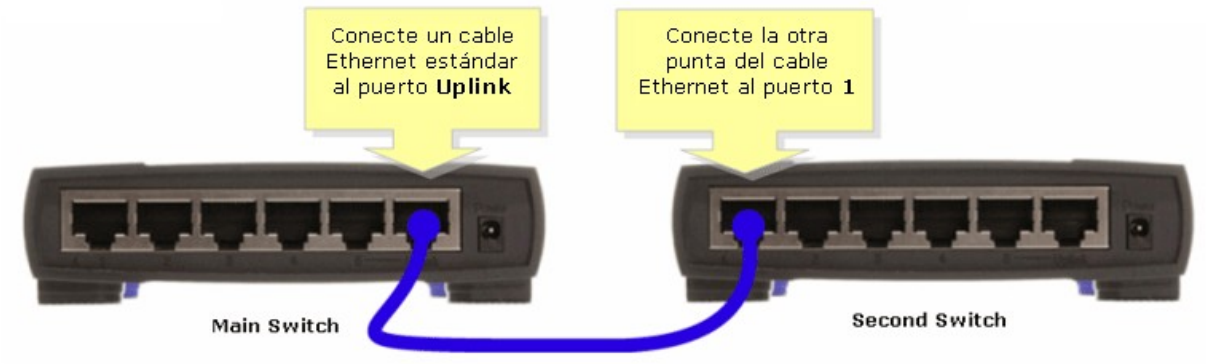
Antiguamente se usaban puertos UPLINK para unir dos hubs o dos switches, usándose cables cruzados para ello. Por ejemplo, en un switch de 6 puertos, el puerto 6 solía ser uplink.

La forma de conexión se muestra a continuación:

Los switches más avanzados soportan MDIX, lo cual permite utilizar un cable directo para conectar 2 switches entre sí utilizando cualquier puerto. El propio switch detecta el tipo de conexión (Auto Cross), que es equivalente a usar un cable crossover (568A 568B).

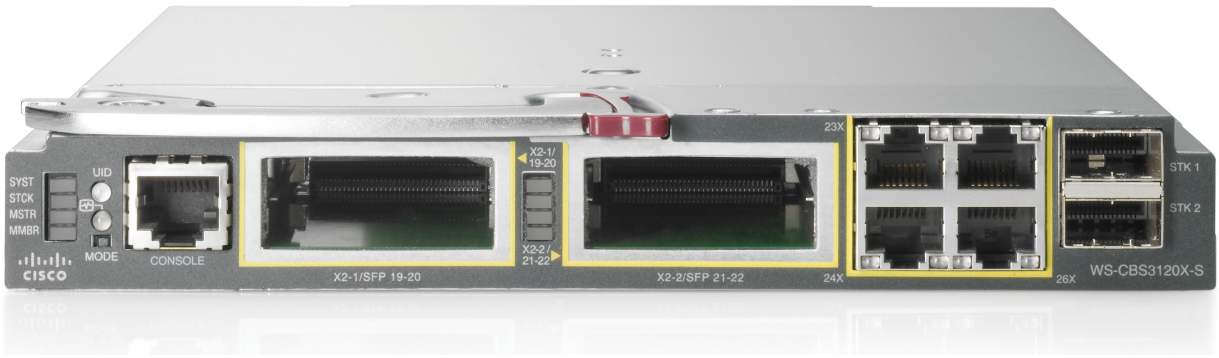
Los puertos estándar para las estaciones terminales se conocen como MDI (Media Dependent Interface), y los puertos estándar para los concentradores y conmutadores se conoce como MDIX (Media Dependent Interface Crossover) .

En los concentradores (hubs) y conmutadores (switches) las interfaces MDI se usan para conectar a otros hubs o switches sin el cable de red cruzado (que sería lo habitual) y se conocen como puertos MDI o puertos uplink. Estas interfaces son especiales y normalmente pueden ser configuradas manualmente o por software para que se comporten como MDI o MDIX. Existen interfaces que cambian su estado de MDI a MDIX automáticamente.



Switch de configuración modular

Estos switches están diseñados con ranuras que permiten insertar tarjetas en linea que le proporcionan nuevas funcionalidades, de tal forma que es posible agregar mas puertos Fast Ethernet, Modems o puertos de conexión Gigabit Ethernet, claro está que el switch en cuestión solo soporta un número y modelos determinados de tarjetas.



Transceptores SFP

Un transceptor es un dispositivo que cuenta con **un transmisor y un receptor** que comparten parte de la circuitería o se encuentran dentro de la misma caja.

El módulo de factor de forma pequeño (SFP: **Small Form-factor Pluggable**) es un transceptor (en inglés transceiver) modular óptico de intercambio dinámico para conectar dos equipos de telecomunicaciones, normalmente switches o routers. . .

Los módulos **SFP** fueron desarrollados para velocidades de **1 Gbit/s**. No todos son ópticos (los hay de cobre) y los hay de muchos más tipos que 1000BaseSX ó 1000BaseLX (como por ejemplo, hay SFP de 1000BaseT, 1000BaseZX, SONET/SDH).

El transceptor SFP no ha sido estandarizado por ningún organismo de normalización oficial, sino que se especifica mediante un acuerdo multi-fuente entre fabricantes competidores. SFP fue diseñado después de la interfaz GBIC, y permite una mayor densidad de puertos (número de transceptores por cm a lo largo del borde de una placa) que el GBIC, que es la razón por la SFP también se conoce como mini-GBIC.

La versión mejorada de Small Form Factor Pluggable (**SFP+**) admite velocidades de datos de hasta **10 Gbit/s**. La especificación SFP+ se publicó el 9 de mayo de 2006, y la versión 4.1 fue publicada el 6 de julio de 2009. SFP+ soporta 10 Gigabit Ethernet y 8 Gbit/s en redes Fibre Channel (usadas comúnmente en redes Storage Area Networks (SAN)). Es un formato popular de la industria con el apoyo de muchos fabricantes de componentes de red.

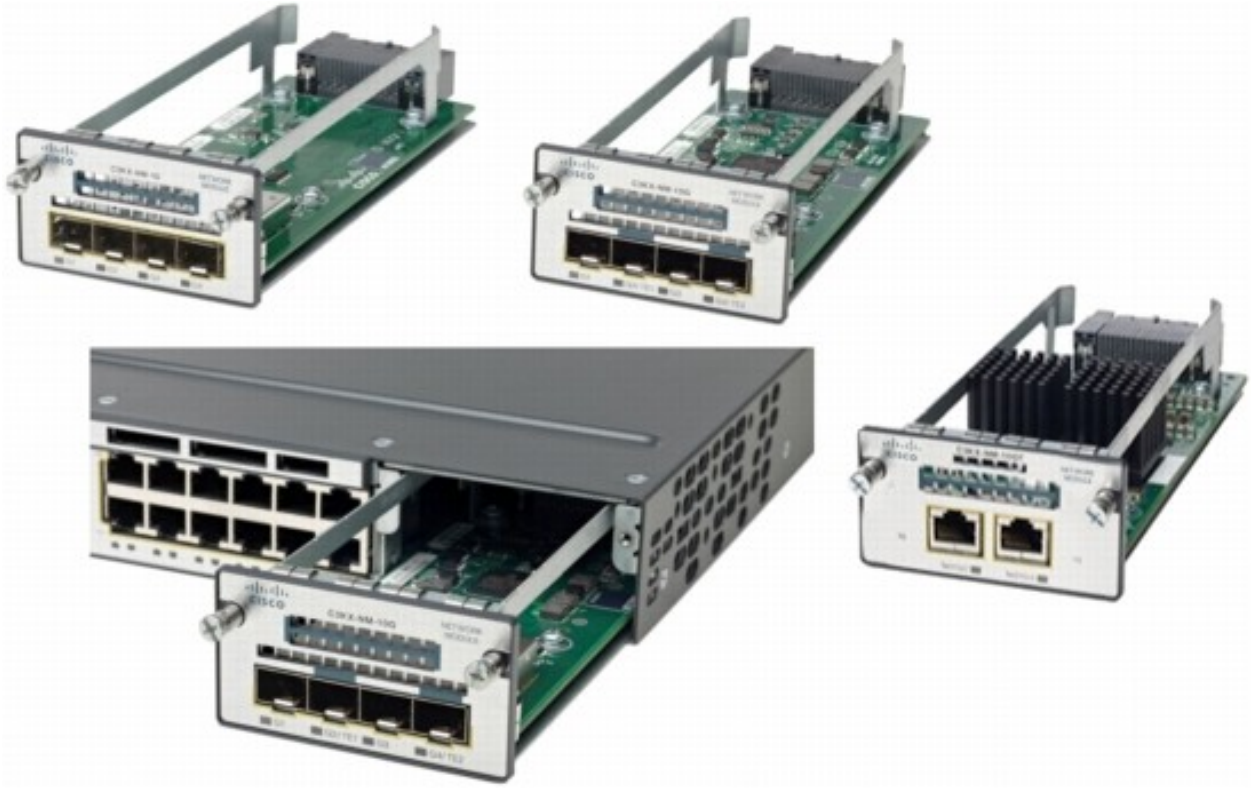


Figura 1: Módulos de switch

Figura 2: Módulos de switch más actuales

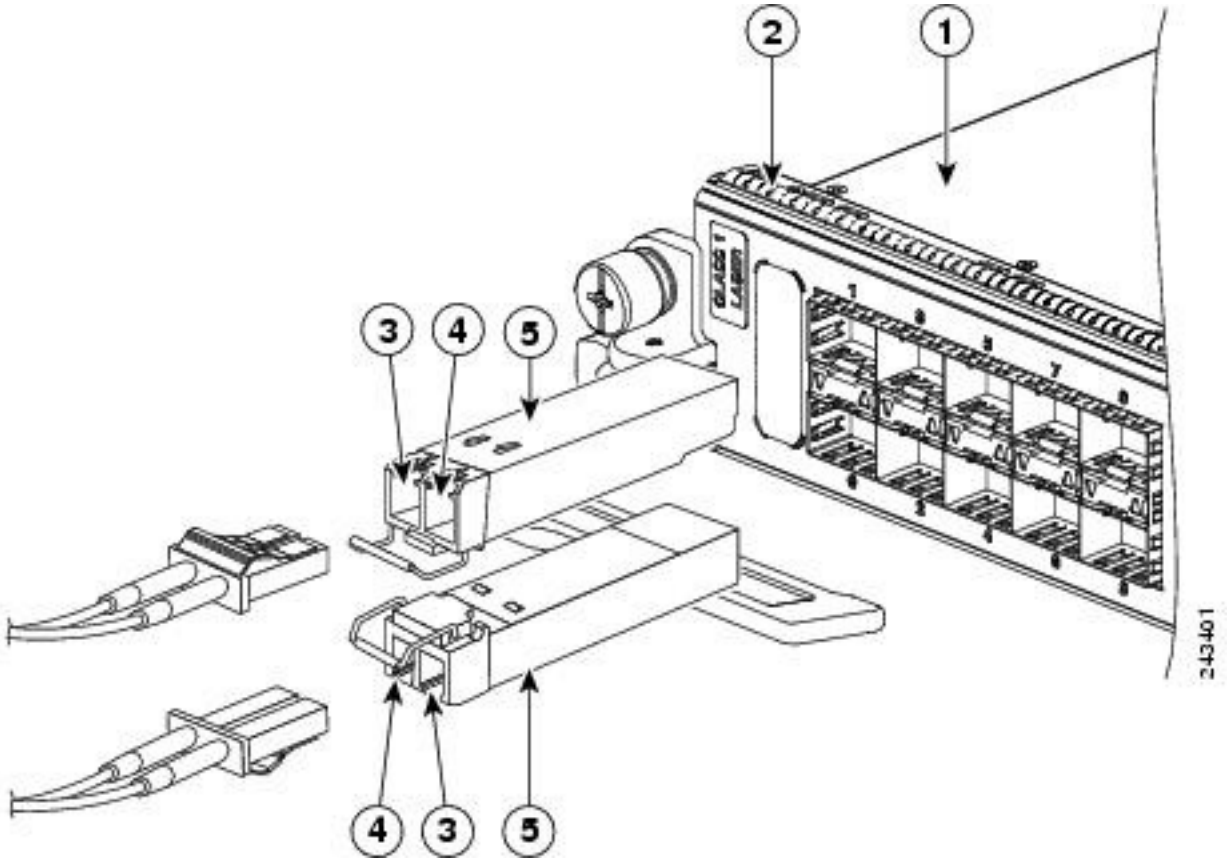


Figura 3: Transceptores SFP - Esquema

Figura 4: Transceptores SFP - Foto

Figura 5: Transceptores CFP - Foto

Transceptores CFP

El módulo de factor de forma C (**CFP: C Form-factor Pluggable**) es un transceptor para la transmisión de señales digitales de alta velocidad. La C indica la letra latina C para expresar el número 100 (centum), ya que el estándar fue desarrollado principalmente para sistemas Ethernet 100 Gigabit.

El transceptor CFP se especifica mediante un acuerdo multi-fuente entre fabricantes competidores. El CFP fue diseñado posteriormente a la interface SFP, pero es significativamente más rápido para soportar **40 y 100 Gbit/s**.

Switch apilable

A esta configuración de switch se les conoce como en stack o stackwise. Se trata de conectar con cables de alta velocidad varios switches, el objetivo es obtener tolerancia a fallos, ofreciendo una configuración redundante.

Figura 6: Cisco Catalyst 3750-X frontal y trasero

Un grupo de switches (stack) puede apilarse (uniéndolos con enlaces de alta velocidad) y comportarse como un único switch con la capacidad de puertos de la suma de todos ellos. Por ejemplo 12 swiches de 48 puertos cada uno, equivalen a un switch de 576 puertos.

Los enlaces que unen los switch del stack pueden alcanzar los 20 Gbps.

Dentro de la pila (stack) existe un switch maestro y otro de respaldo (backup). El switch Master y el Backup se sincronizan constantemente para tener la misma configuración Si el Master falla, el Backup se convierte en el nuevo Master y otro switch del stack toma el rol de Backup.

Switch multicapa (multilayer)

Son los conmutadores que, además de las funciones tradicionales de la capa 2, incorporan algunas funciones de enrutamiento o routing, como por ejemplo la determinación del camino basado en informaciones de capa de red (capa 3 del modelo OSI), validación de la integridad del cableado de la capa 3 por checksum y soporte a los protocolos de routing tradicionales (RIP, OSPF, etc)

Los conmutadores de capa 3 (Layer 3) soportan también la definición de redes virtuales (VLAN), y según modelos posibilitan la comunicación entre las diversas VLAN sin la necesidad de utilizar un router externo.

Por permitir la unión de segmentos de diferentes dominios de difusión o broadcast, los switches de capa 3 son particularmente recomendados para la segmentación de redes LAN muy grandes, donde la simple utilización de switches de capa 2 provocaría una pérdida de rendimiento y eficiencia de la LAN, debido a la cantidad excesiva de broadcasts.

Se puede afirmar que la implementación típica de un switch de capa 3 es más escalable que un enrutador, pues éste último utiliza las técnicas de enrutamiento a nivel 3 y enrutamiento a nivel 2 como complementos, mientras que los switches sobreponen la función de enrutamiento encima del encaminamiento, aplicando el primero donde sea necesario.

Asimismo existen en el mercado algunos switches denominados Layer 3+ (Layer 3 Plus). Básicamente, incorporan a las funcionalidades de un conmutador de la capa 3; la habilidad de implementar la políticas y filtros a partir de informaciones de la capa 4 o superiores, como puertos TCP/UDP, SNMP, FTP, etc.

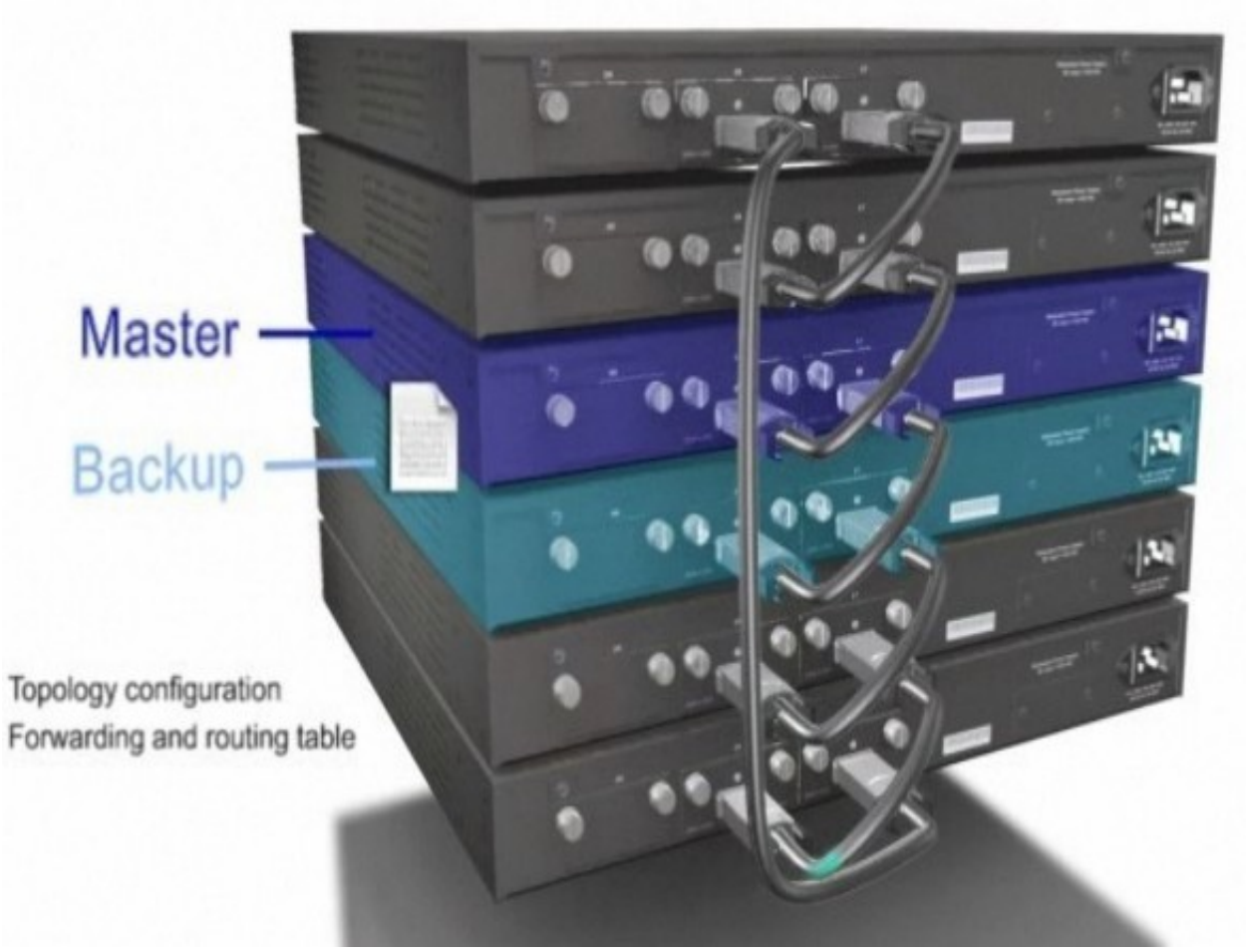


Figura 7: Switch apilable (Maestro y Backup)

El icono utilizado para un switch multicapa es el siguiente:

Switch gestionable

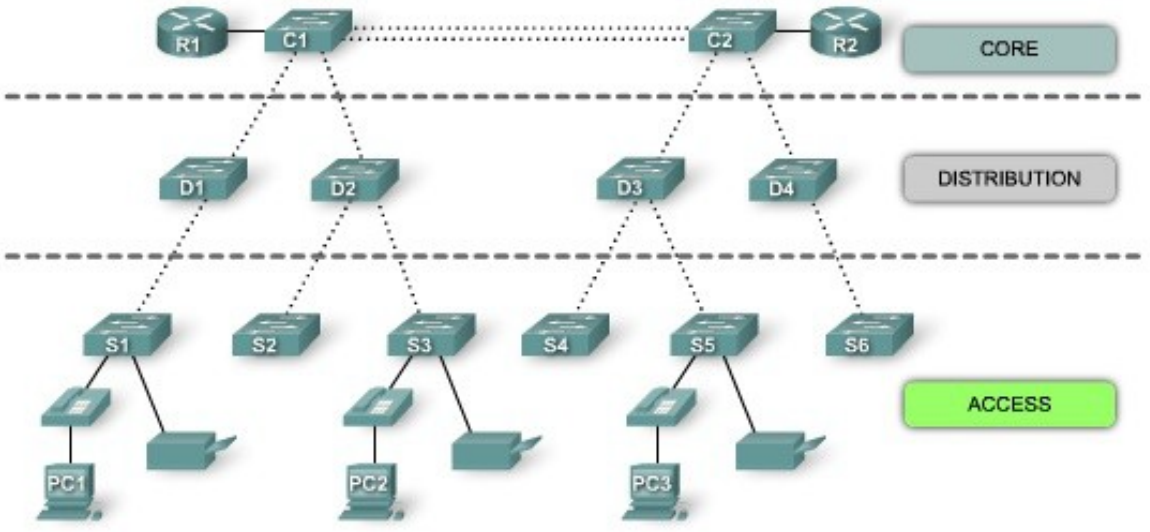
Los switches multicapa (L3 o superiores) soportan la administración a través de red. Se accede a ellos a través de una dirección IP mediante servicios telnet, ssh o incluso web. Permiten la administración de diversos parámetros como pueden ser la creación y gestión de VLANs, el soporte de STP o RSTP, agregación de puertos (trunk), etc.

6.3.5 Distribución

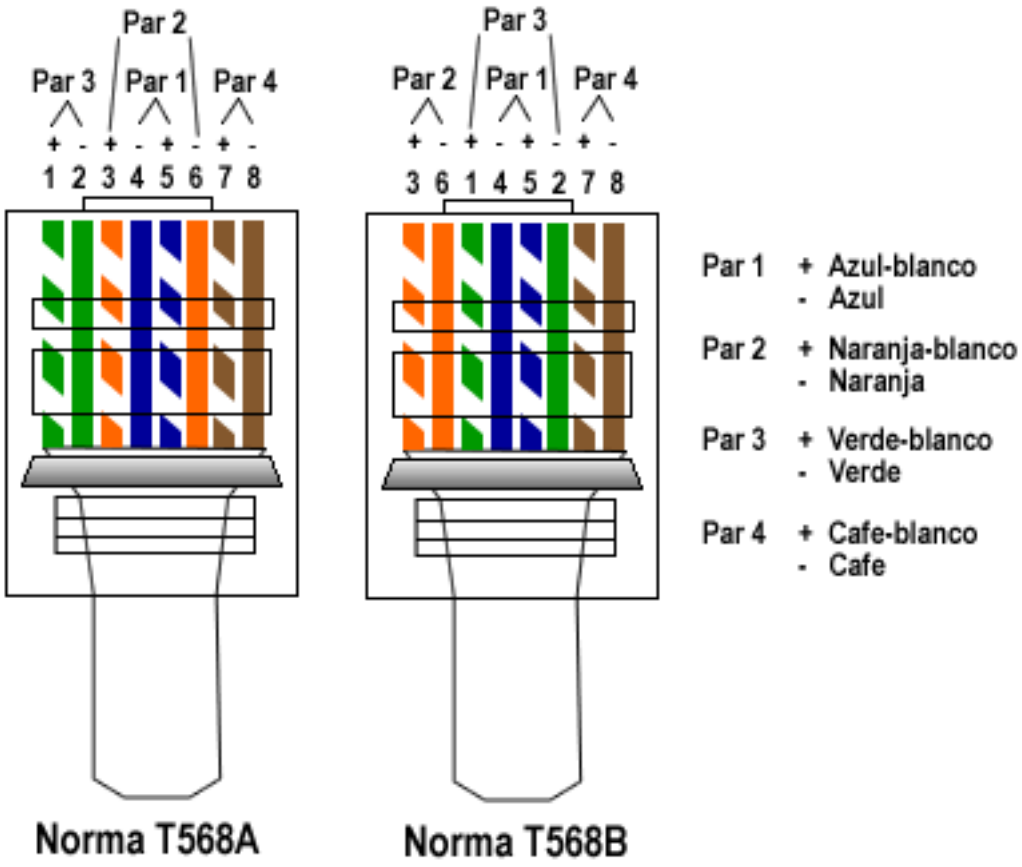
Ciertos fabricantes utilizan un diseño de red jerárquica consistente en dividir la red en capas discretas. Cada capa proporciona funciones específicas que definen su papel dentro de la red global. Mediante la separación de las diversas funciones que existen en una red, el diseño de la red se convierte en modular, lo que facilita la escalabilidad y el rendimiento.

El modelo de diseño jerárquico típico se divide en tres capas:

- núcleo (CORE)
- distribución (DISTRIBUTION)
- acceso (ACCESS)



6.3.6 Cableado entre dispositivos



Cable Recto (Straight Through):

Es el cable cuyas puntas están armadas con las misma norma (T568A T568A ó T568B T568B). Se utiliza entre dispositivos que funcionan en distintas capas del Modelo de Referencia OSI.

- De PC a Switch/Hub.
- De Switch a Router.

Cable Cruzado (Crossover):

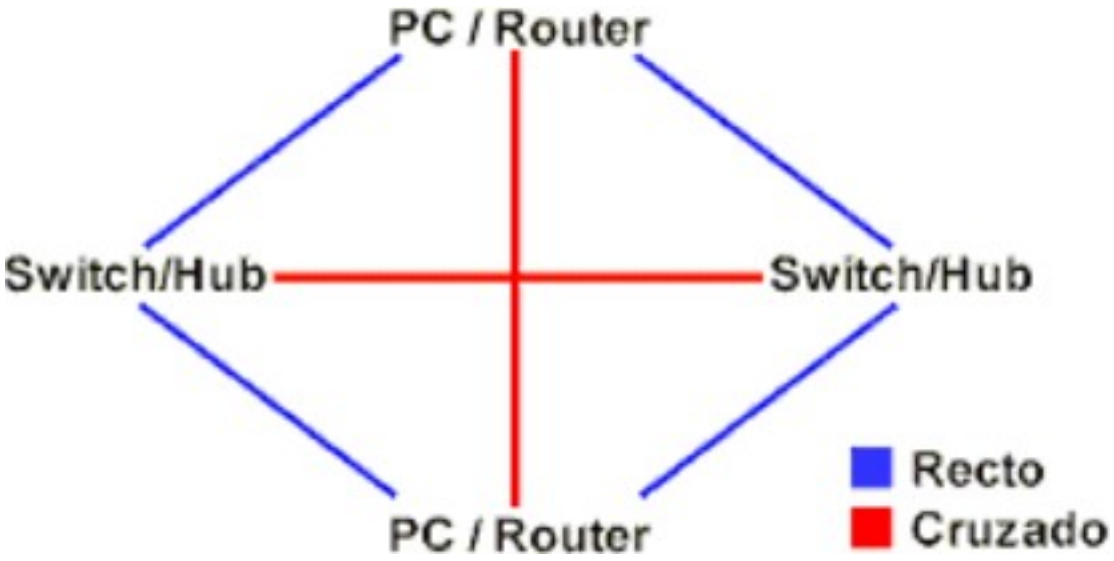
Es el cable cuyas puntas están armadas con distinta norma (T568A T568B). Se utiliza entre dispositivos que funcionan en la misma capa del Modelo de Referencia OSI.

- De PC a PC.
- De Switch/Hub a Switch/Hub.
- De Router a Router (el cable serial se considera cruzado).

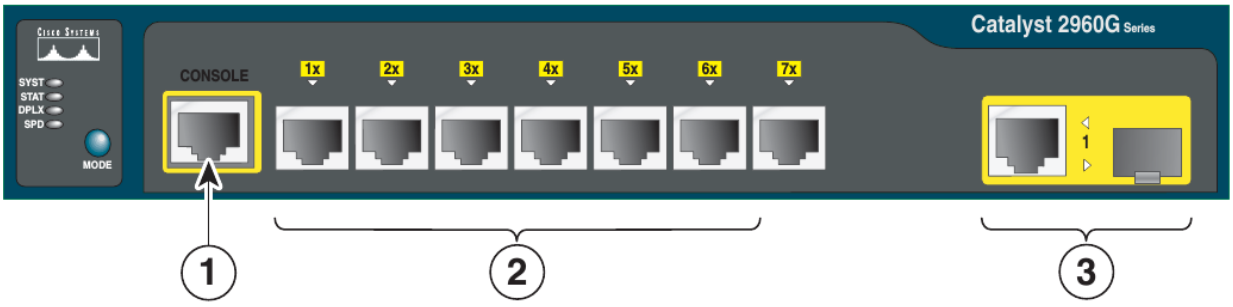
6.3.7 Otras características de los switches

Puertos

Cada una de las entradas al switch se denomina puerto. Normalmente los puertos son para conectores RJ-45, aunque algunos pueden ser para conectores SC o LC de fibra óptica.



La disposición y función de los puertos varían entre distintos modelos de switch, aunque por los general suelen tener la siguiente:



1. Console port (No siempre se encuentra disponible)
2. Puertos normales (10/100/1000 Mbps) para conexión de equipos.
3. Otros puertos (para UPLINK, TRUNK o incluso entrada de PoE)

Ejemplo

El puerto de consola (console port)

Algunos switches (además de los routers) disponen de un puerto especial, denominado **Console Port**. Este puerto es muy importante pues permite realizar la configuración del dispositivo a través de él de forma directa. **Es necesario un cable rollover**.

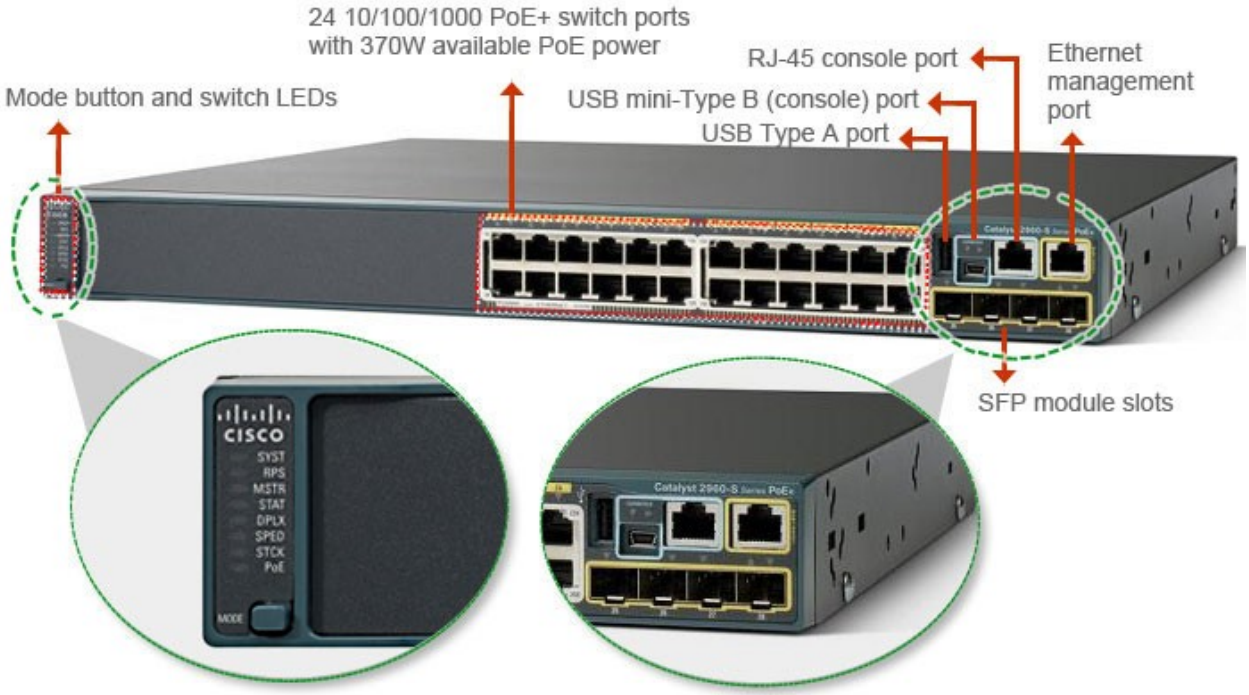
El cable Rollover (también conocido como cable de consola Cisco o cable Yost) es un tipo de cable de módem nulo que se utiliza a menudo para conectar un terminal de ordenador al puerto de consola del switch o router. Este cable es generalmente plano (y tiene un color azul claro) para ayudar a distinguirlo de otros tipos de cableado de red.

Se pone el nombre de rollover debido a las patillas en un extremo se invierten de el otro.

En el caso de que nuestro ordenador no disponga de puerto serie DB-9 y solo disponga de USB necesitaremos además un adaptador USB a DB-9.

WS-C2960S-24PS-L
Cisco Catalyst 2960-S Series Switch

- 24 Ethernet 10/100/1000 PoE+ ports
- 370W PoE capacity
- Four 1G Small Form-Factor Pluggable (SFP)
- USB interfaces for management and file transfers
- LAN Base or LAN Lite Cisco IOS Software feature set
- SmartOperations tools that simplify deployment and reduce the cost of network administration



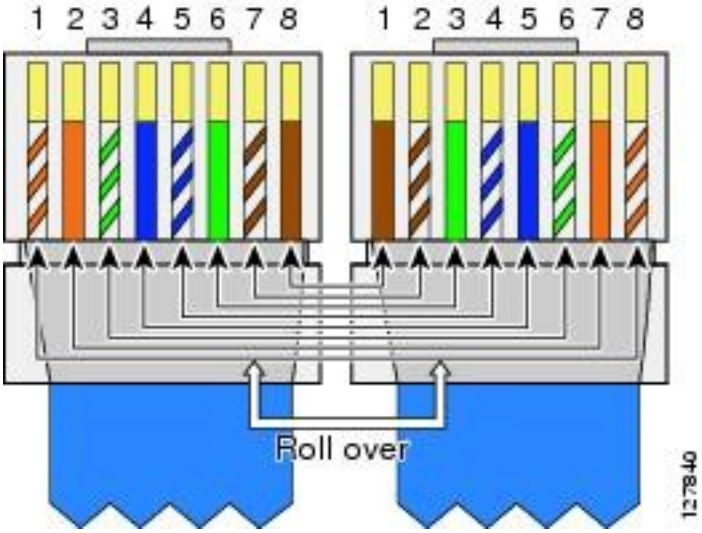


Figura 8: Cable rollover

Figura 9: Adaptador DB-9 a RJ-45
Todo en uno: conector DB-9 más cable rollover

Para acceder a la configuración del switch o router a través de un puerto de consola haremos uso de los siguientes programas:

- Hyperterminal (en Windows)
- minicom (en Linux)

Modos de conmutación.

Existen básicamente dos formas mediante las cuales es conmutada la información hasta el destino:

- método de corte (*Cut-Through*)
- almacenamiento y envío (*Store-and-Forward*)

El **método de corte** es el de menor latencia pero con mayor cantidad de errores, consiste en comenzar a transmitir la trama tan pronto como se conoce la dirección MAC de destino, para poder usar este modo, tanto el origen como el destino deben operar a la misma velocidad (de forma síncrona), para no dañar la trama. El problema de este tipo de switch es que no detecta tramas corruptas causadas por colisiones (conocidos como *runts*), ni errores de CRC. Cuanto mayor sea el número de colisiones en la red, mayor será el ancho de banda que consume al encaminar tramas corruptas.

Una mejora de este modo es el método conocido como libre de fragmentos, cuando se reciben los primeros 64 bytes que incluyen el encabezado de la trama es cuando inicia la conmutación, este modo verifica la confiabilidad de direccionamiento y la información del protocolo de control de enlace lógico (Logical Link Control, LLC) para asegurar que el destino y manejo de los datos sean correctos.

El último de los métodos es el de **almacenamiento y envío**, el switch recibe toda la trama antes de iniciar a enviarla, esto le da al switch la posibilidad de verificar la secuencia de verificación de trama (FCS), para asegurarse de que la trama ha sido recibida de forma confiable y enviarla al destino. Este método asegura operaciones sin error y aumenta la confianza de la red. Pero el tiempo utilizado para guardar y chequear cada trama añade un tiempo de demora importante al procesamiento de las mismas. La demora o delay total es proporcional al tamaño de las tramas: cuanto mayor es la trama, más tiempo toma este proceso.

Los conmutadores *cut-through* son más utilizados en pequeños grupos de trabajo y pequeños departamentos. En esas aplicaciones es necesario un buen volumen de trabajo o throughput, ya que los errores potenciales de red quedan en el nivel del segmento, sin impactar la red corporativa.

Los conmutadores *store-and-forward* son utilizados en redes corporativas, donde es necesario un control de errores.

Port security

Es una característica de los switches Cisco que nos permite retener las direcciones MAC conectadas a un puerto y permitir solamente esas direcciones MAC registradas comunicarse a través de ese puerto del switch.

Nos permite:

- Restringir el acceso a los puertos del switch según la MAC.
- Restringir el número de MACs por puerto en el switch.
- Reaccionar de diferentes maneras a violaciones de las restricciones anteriores.
- Establecer la duración de las **asociaciones MAC-Puerto**.

Si un dispositivo **con otra dirección MAC** intenta comunicarse a través de un puerto de la LAN, **port-security deshabilitará el puerto**.

Port mirroring (Puerto espejo)

Es una función que tienen los switches para copiar todo el tráfico de un puerto específico a otro puerto. Esta función generalmente se utiliza para atrapar todo el tráfico de una red y poder analizarlo (con herramientas como **wireshark** por ejemplo).

El puerto espejo en un sistema de switch **Cisco** generalmente se refiere a un Analizador de Puertos del switch (**Switched Port Analyzer: SPAN**) algunas otras marcas usan otros nombres para esto, tal como Roving Analysis Port (RAP) en los switches 3Com.

MACsec

Media Access Control de Seguridad (MACsec) es una tecnología de seguridad estándar de la industria que proporciona una comunicación segura para todo el tráfico en enlaces Ethernet. MACsec proporciona seguridad de punto a punto de enlaces Ethernet entre nodos conectados directamente-y es capaz de identificar y prevenir la mayoría de las amenazas a la seguridad, incluida la denegación de servicio, intrusión, man-in-the-middle, enmascaramiento, las escuchas telefónicas pasivo, y los ataques de reproducción. MACsec está estandarizado en IEEE 802.1AE.

Una vez que un enlace punto a punto Ethernet ha habilitado MACsec, todo el tráfico que atraviesa el enlace es asegurado mediante el uso de controles de **integridad de datos y cifrado si se desea**.

Las comprobaciones de integridad de datos verifican la integridad de los datos en ambos lados del enlace asegurado Ethernet. MACsec añade una cabecera de 8 bytes y una cola de 16 bytes a todas las tramas Ethernet que atraviesan el enlace, y la cabecera y la cola son revisados por la interfaz de recepción para asegurar que los datos no se vieron comprometidos al atravesar el enlace. Si la comprobación de integridad de datos detecta algo irregular sobre el tráfico , el tráfico se desecha.

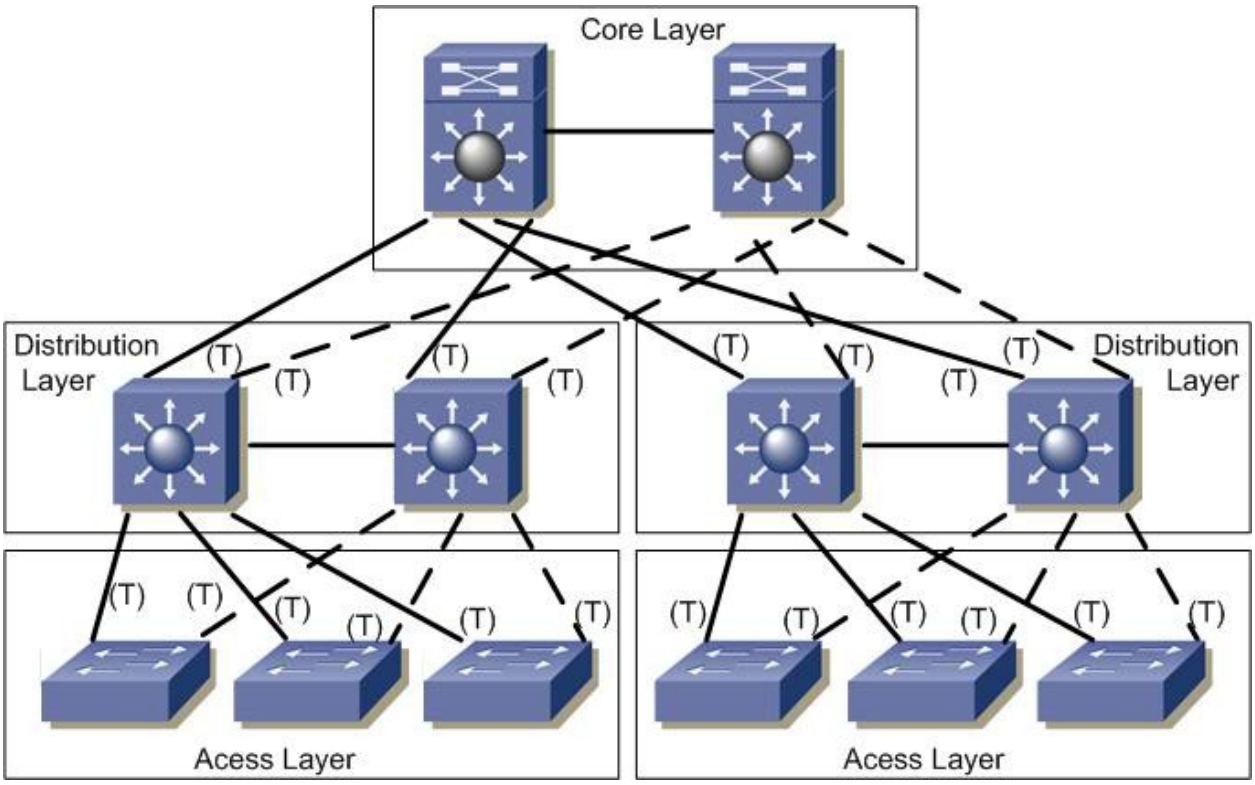
MACsec también se puede utilizar para cifrar todo el tráfico en el enlace Ethernet. El cifrado utilizado por MACsec asegura que los datos de la trama Ethernet no pueden ser vistos por cualquier persona al monitorear el tráfico en el enlace. El cifrado MACsec es opcional y configurable por el usuario.

STP

STP (Spanning Tree Protocol) o protocolo de árbol de extensión es un protocolo basado en estándares que se usa **para evitar bucles** de switcheo. Cuando se comprobó la eficiencia de los switches para realizar la conmutación en grandes redes, se inicio su incorporación de manera copiosa hasta el punto de crear redes con switches anidados, formando una estructura de árbol jerárquico plagado de rutas redundantes que son recomendadas para ofrecer más confiabilidad y tolerancia a las fallos, pero que pueden generar efectos indeseables como los bucles y pueden llegar a convertirse en tormentas de broadcast que rápidamente abrumen la red.

Los bucles ocurren cuando hay rutas alternativas hacia un mismo destino (sea una máquina o segmento de red). Estas rutas alternativas son necesarias para proporcionar redundancia y así ofrecer una mayor fiabilidad a la red, dado que en caso de que un enlace falle, los otros puede seguir soportando el tráfico de ésta. Los problemas aparecen cuando utilizamos dispositivos de interconexión de nivel de enlace, como un puente de red o un conmutador de paquetes.

Cuando existen bucles en la topología de red, los dispositivos de interconexión de nivel de enlace de datos reenvían indefinidamente las tramas broadcast y multicast, creando así un bucle infinito que consume tanto el ancho de banda de la red como CPU de los dispositivos de enrutamiento. Esto provoca que se degrade el rendimiento de la red en muy poco tiempo, pudiendo incluso llegar a quedar inutilizable. Al no existir un campo TTL (tiempo de vida) en las tramas de capa 2, éstas se quedan atrapadas indefinidamente hasta que un administrador de sistemas rompa el bucle. Un router, por el contrario, sí podría evitar este tipo de reenvíos indefinidos. La solución consiste en permitir la existencia de enlaces físicos redundantes, pero creando una topología lógica libre de bucles. STP calcula una única ruta libre de bucles entre los dispositivos de la red pero manteniendo los enlaces redundantes desactivados como reserva, con el fin de activarlos en caso de fallo.



Si la configuración de STP cambia, o si un segmento en la red redundante llega a ser inalcanzable, el algoritmo reconfigura los enlaces y restablece la conectividad, activando uno de los enlaces de reserva. Si el protocolo falla, es posible que ambas conexiones estén activas simultáneamente, lo que podrían dar lugar a un bucle de tráfico infinito en la LAN.

El árbol de expansión (Spanning tree) permanece vigente hasta que ocurre un cambio en la topología, situación que el protocolo es capaz de detectar de forma automática. El máximo tiempo de duración del árbol de expansión es de cinco minutos. Cuando ocurre uno de estos cambios, el puente raíz actual redefine la topología del árbol de expansión o se elige un nuevo puente raíz.

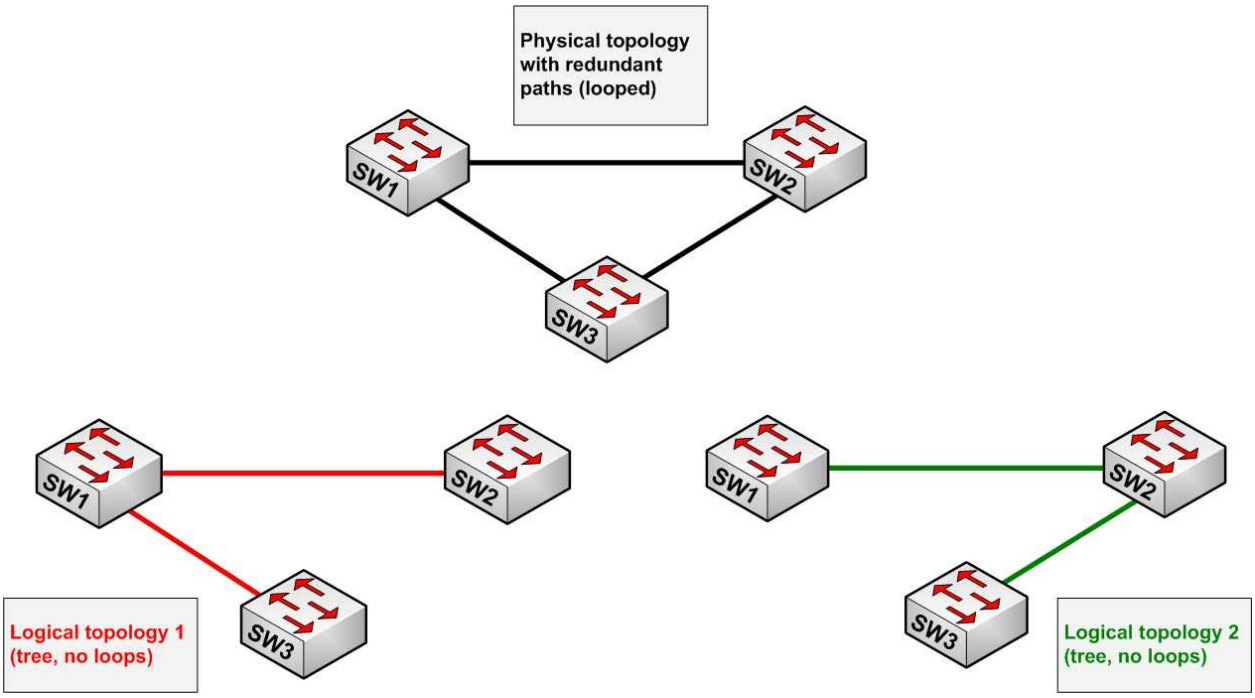
El algoritmo transforma una red física con forma de malla, en la que existen bucles, por una red lógica en forma de árbol (libre de bucles). Los puentes se comunican mediante mensajes de configuración llamados Bridge Protocol Data Units (BPDU).

STP actúa contra los bucles, haciendo que cada switch que opera con este protocolo envíe un mensaje denominado BPDU desde cada uno de sus puertos para que los demás sepan de su existencia. Luego con la ayuda del STA (Spanning Tree Algorithm), se detectan cuales son las rutas redundantes y son bloqueadas.

El resultado es la eliminación de los bucles mediante la creación de un árbol jerárquico, pero en caso de ser necesitadas la rutas alternativas pueden ser activadas.

Existen múltiples variantes del STP debido, principalmente, al tiempo que tarda en converger el algoritmo utilizado. Una de estas variantes es el **Rapid Spanning Tree Protocol (RSTP)**, que hoy en día ha reemplazado el uso del STP original.

Como extensión de RSTP, además tenemos **Multiple Spanning Tree Protocol (MSTP)**, que tiene características más novedosas.



CDP

CDP (**Cisco Discovery Protocol**, 'protocolo de descubrimiento de Cisco', es un **protocolo de red propietario** de nivel 2, desarrollado por Cisco Systems y usado en la mayoría de sus equipos. Es utilizado para compartir información sobre otros equipos Cisco directamente conectados, tal como la versión del sistema operativo y la dirección IP. CDP también puede ser usado para realizar encaminamiento bajo demanda (ODR, On-Demand Routing), que es un método para incluir información de encaminamiento en anuncios CDP, de forma que los protocolos de encaminamiento dinámico no necesiten ser usados en redes simples.

Los dispositivos Cisco envían anuncios a la dirección de destino de multidifusión. Los anuncios CDP (si está soportados y configurados en el IOS) se envían por defecto cada 60 segundos en las interfaces que soportan cabeceras SNAP, incluyendo Ethernet, Frame Relay y ATM. Cada dispositivo Cisco que soporta CDP almacena la información recibida de otros dispositivos en una tabla que puede consultarse usando el comando show cdp neighbor. La información de la tabla CDP se refresca cada vez que se recibe un anuncio y la información de un dispositivo se descarta tras tres anuncios no recibidos por su parte (tras 180 segundos usando el intervalo de anuncio por defecto).

La información contenida en los anuncios CDP varía con el tipo de dispositivo y la versión del sistema operativo que corra. Dicha información incluye la versión del sistema operativo, el nombre de equipo, todas la direcciones de todos los protocolos configurados en el puerto al que se envía la trama CDP (por ejemplo, la dirección IP), el identificador del puerto desde el que se envía el anuncio, el tipo y modelo de dispositivo, la configuración duplex/simplex, el dominio VTP, la VLAN nativa, el consumo energético (para dispositivos PoE) y demás información específica del dispositivo. El protocolo está habilitado por defecto en todos las interfaces de los equipos CISCO. Para deshabilitarlo de forma global se utiliza el comando no cdp run en modo enable y para deshabilitarlo en una interfaz concreta se utiliza el comando no cdp enable en la configuración de dicha interfaz.

Port trunking (link aggregation)

Permite combinar varios enlaces físicos en un enlace lógico (trunk), que funciona como un único puerto de mayor ancho de banda

Características:

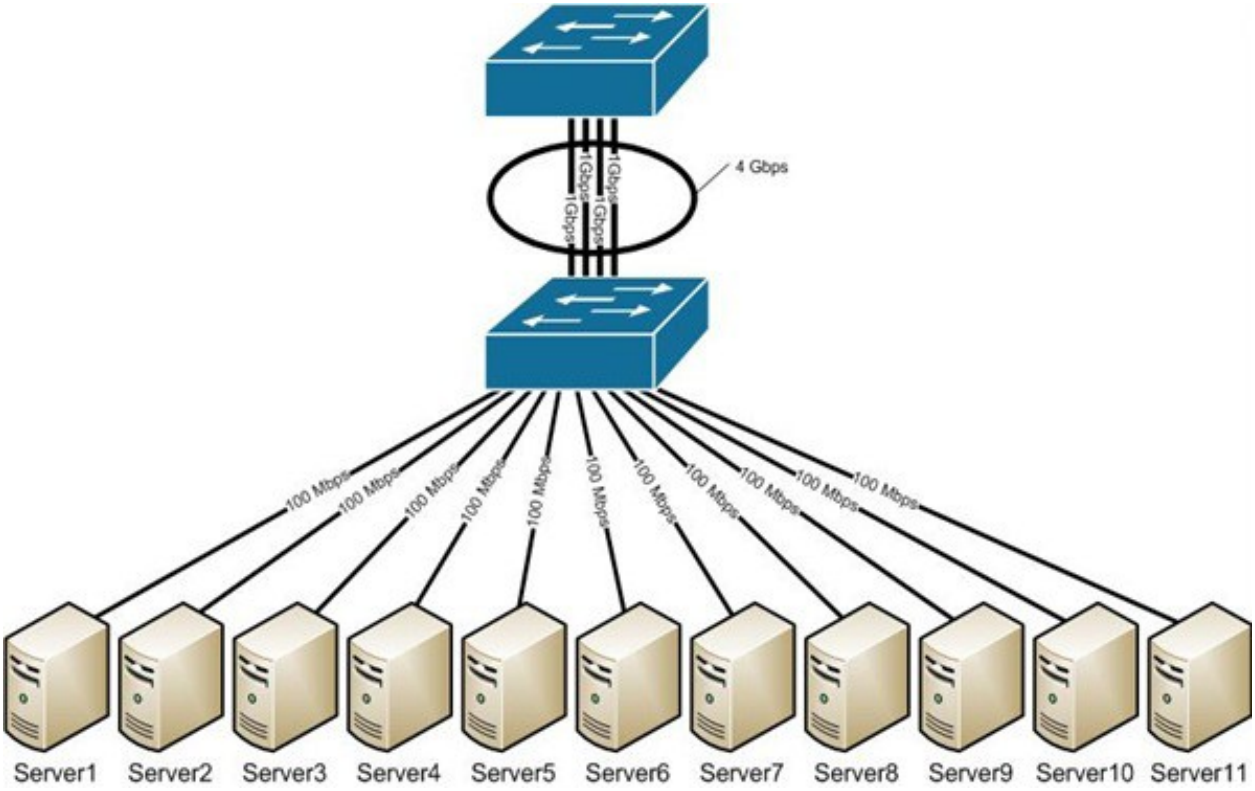
- Aumenta el ancho de banda entre 2 switches
- Implica redundancia, lo que mejora la fiabilidad
- Es una solución escalable
- Puede usarse para aumentar el ancho de banda entre un switch y un equipo de la red

Cisco denomina esta técnica como EtherChannel.

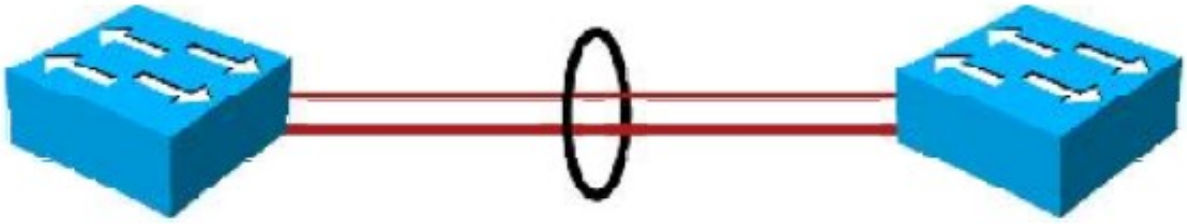
EtherChannel nos permite sumar la velocidad de cada puerto físico y así obtener un único enlace troncal de alta velocidad.

Cuando tenemos muchos servidores que salen por un único enlace troncal, puede que el tráfico colapse el enlace. Una de las soluciones más prácticas es el uso de EtherChannel.

De esta manera sumamos la velocidad de los puertos que agregamos al enlace lógico.



Modos de configuración:



Podemos configurar un **EtherChannel** de 3 formas diferentes:

- **Mode ON**: no se realiza ningún tipo de negociación, todos los puertos se ponen activos. No utiliza ningún protocolo.

- **PAgP (Port Aggregation Protocol)**: es un protocolo propietario de **Cisco**. El switch negocia con el otro extremo qué puertos deben ponerse activos.

- **LACP (Link Aggregation Control Protocol)**: protocolo abierto con estándar IEEE 802.3ad y 802.3ax.

Recomendaciones

Antes de configurar nuestro **EtherChannel** tener en cuenta las siguientes recomendaciones:

- No se debe configurar un puerto en dos grupos diferentes.
- No se debe configurar un puerto en dos modos diferentes, **LACP** y **PAgP**.
- No configurar **Switched Port Analyzer** (SPAN) como parte de un EtherChannel.
- No configurar securización de puertos.
- Asignar todos los puertos del EtherChannel a la **misma VLAN** o configurar todos como troncales.
- Verificar que todos los puertos del grupo están en un **mismo modo de encapsulación**, ISL o 802.1Q

VLAN

Algunos switches L3 (de capa 3) soportan la creación de LAN virtuales o VLAN.

Una **VLAN** (acrónimo de virtual LAN, «**red de área local virtual**») es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4).

6.4 Referencias

- Comunicaciones y Redes de Computadores – W. Stallings - 7a edición

- Redes de Computadoras - Andrew S. Tanenbaum – 4a edición.
- Implementing Cisco Switched Networks. 2009.
- Acceso al medio (PDF)
- Documentación sobre EtherChannel, Port Mirroring, Port Security y otros

6.5 Actividades

1. Explica cuáles son las principales funciones de la capa de enlace.
2. En redes Ethernet la capa de enlace se dividen en dos subcapas, ¿cuáles? Explica cada una de ellas brevemente.
3. Haz un esquema de una trama 802.3 y explica las diferencias con la trama Ethernet original.
4. Busca información acerca del protocolo HDLC. ¿Qué significan las siglas? ¿Qué protocolos se basan en él? ¿Cuál es el formato de una trama HDLC?
5. Haz una comparativa entre una trama HDLC y una trama PPP.
6. Calcula el CRC para el siguiente caso:
   - Información a transmitir: `111101001101`
   - Polinomio generador: `10101`
7. Busca información acerca del polinomio generador utilizado en Ethernet para generar el CRC-32.
8. Busca información acerca del significado de las siglas MTU. ¿Cuál es la MTU para Ethernet?
9. En medios compartidos con división estática del canal, indicar las 4 técnicas utilizadas y donde se emplea cada una de ellas.
10. En medios compartidos con división dinámica del canal, indicar las 2 técnicas estudiadas y donde se emplea cada una de ellas.
11. Explica la técnica CSMA/CD.
12. Explica la técnica Token Ring (paso de testigo)
13. Explica la técnica de control de flujo mediante ventana deslizante.
14. Explica la técnica de control de errores ARQ de vuelta atrás N.
15. Explica qué son y para qué sirven las tecnologías PoE y PoE+.
16. Para las siguientes versiones Ethernet nombra un estándar que haga uso de cable de par trenzado, indicando nombre, tipo de cable, distancia y norma.
    1. Ethernet 10 Mbps
    2. Ethernet 100 Mbps (FastEthernet)
    3. Ethernet 1000 Mbps (Gigabit Ethernet)
    4. Ethernet 10000 Mbps (10 Gigabit Ethernet)
17. Para las siguientes versiones Ethernet nombra un estándar que haga uso de cable de fibra óptica multimodo, indicando nombre, distancia y norma.
    1. Ethernet 1 Gbps (Gigabit Ethernet)
    2. Ethernet 10 Gbps (10 Gigabit Ethernet)
    3. Ethernet 40 Gbps (40 Gigabit Ethernet)

4. Ethernet 100 Gbps (100 Gigabit Ethernet)

18. ¿Qué se entiende por dominio de colisión y dominio de difusión?
19. ¿Para qué sirven los puertos UPLINK de un switch?
20. Si un switch tiene soporte MDIX en sus puertos, significa que . . .
21. Haz un esquema del cableado de par trenzado y su distribución de hilos en:

1. cable directo (straight)
2. cable cruzado (crossover)
3. cable invertido (rollover)

22. Para los siguientes tipos de switches y fabricantes busca un modelo:

▪	Cisco	3com	Linksys	D-Link
Compacto				
Modular				
Apilable				
Multicapa				

23. Para los modelos anteriores mostrar un imagen y especificaciones técnicas.
24. ¿Qué son y para qué sirven los transceptores (transceiver en inglés)?
25. ¿Qué velocidades se alcanzan con los transceptores SFP y CFP?
26. Símbolo del switch multicapa.
27. ¿Qué tipos de cables de par trenzado se utilizan para conectar los siguientes dispositivos entre si?

▪	Computador	Switch	Router
Computador			
Switch			
Router			

28. Explica qué es y para qué sirve STP y RSTP.
29. Explica qué es y para qué sirve la agregación de enlaces.
30. Para la planificación de la red local que se realizó en el Tema 4, buscar los switches adecuados suponiendo que tenemos 2 switch de distribución (en el distribuidor de cada edificio) y múltiples switch de planta. La conexión entre los switch de distribución y los de planta se realiza por fibra óptica.
31. Imagina que te dan un switch y te piden que lo configures. Indica los pasos que debes seguir para tener acceso a él.
32. Visita la página http://www.tp-link.com/en/emulators.html y elige 3 switches. Para cada uno de ellos indica qué características soporta de las vistas este tema.

CAPÍTULO 7

REDES INALÁMBRICAS

7.1 Conceptos generales

7.1.1 Tecnologías inalámbricas

Las redes inalámbricas hacen uso de un medio sin cables para la transmisión de la información mediante ondas electromagnéticas. Actualmente su uso está ampliamente extendido debido al soporte tecnológico existente y a la movilidad que proporcionan. Se emplean diversas tecnologías según el ámbito en el que operan.

- Redes Personales: **WPAN** (Wireless PAN)
- Redes Locales: **WLAN** (Wireless LAN)
- Redes Metropolitanas: **WMAN** (Wireless MAN)
- Redes Amplias: **WWAN** (Wireless WAN)

7.1.2 Topología celular o en celdas

Las redes de telefonía móvil y otras redes inalámbricas similares están constituidas por un conjunto de estaciones cada una de las cuales tiene un área de cobertura. De esta forma, el territorio se divide en **celdas**, en teoría, de forma hexagonal, controladas cada una por una estación terrestre, que soportan un número limitado de llamadas. Cuando un usuario se encuentra en determinada célula, será atendido por su estación correspondiente. Pero si al desplazarse pasa a otra célula, entonces será otra estación la que le permita seguir manteniendo la conversación.

En las zonas limítrofes, las células se solapan, de forma que el usuario no pierda la cobertura cuando pasa de una a otra. Cada estación utiliza un rango de frecuencias específico y diferente del de las células que la rodean, que son adyacentes a ella, pues en caso contrario podrían producirse interferencias entre células. Células no adyacentes si pueden usar el mismo rango de frecuencias. El conjunto de todas las celdas de una red forman la zona de **cobertura**.

Tipos de celdas según su extensión

- Pequeñas celdas

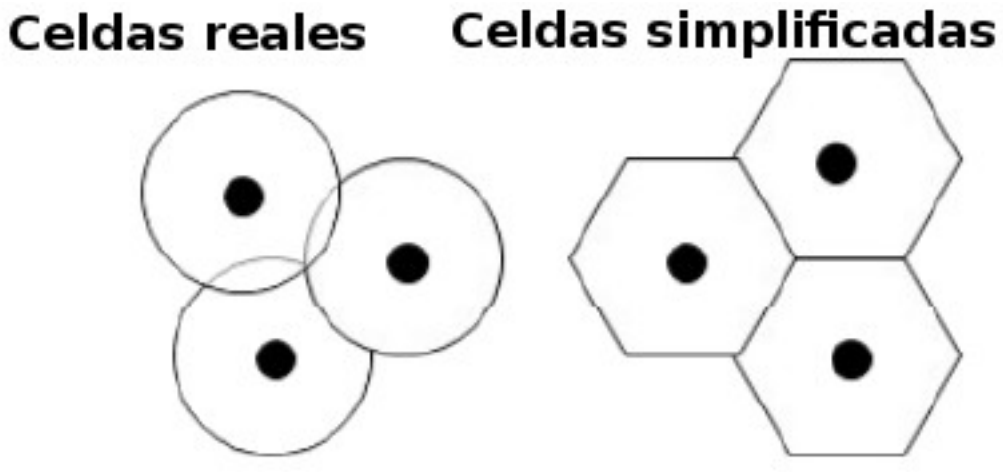


Figura 1: Celdas reales vs simplificadas

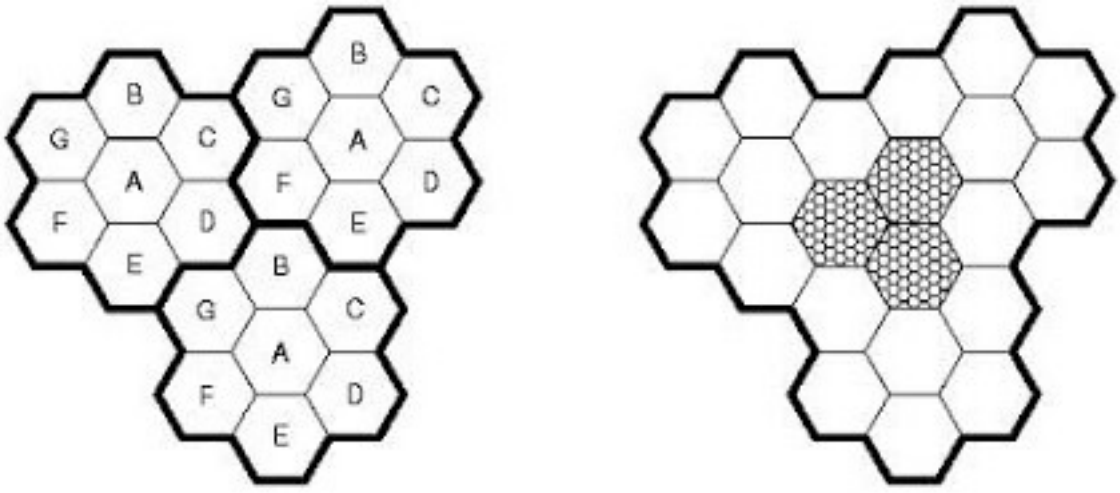
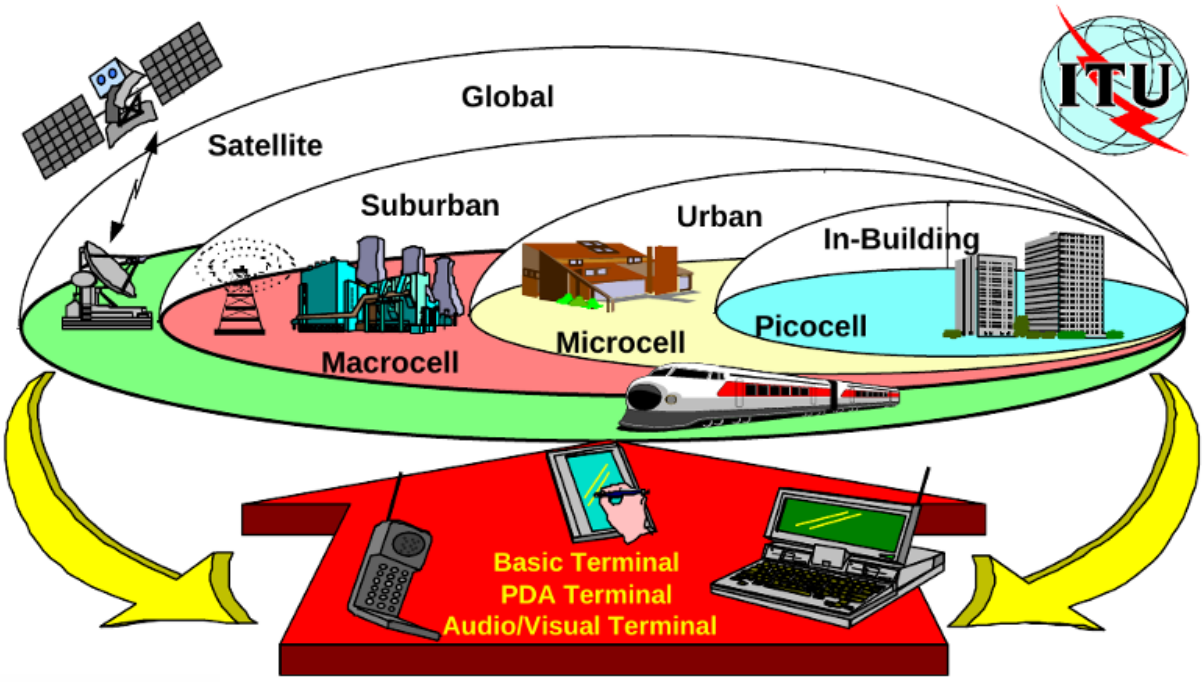


Figura 2: Celdas simplificadas

- Femtocelda (Interior - Indoor)
- Picocelda (Exterior - Outdoor)
- Microcelda (Exterior - Outdoor)

- Macroceldas



7.2 Estándares

A continuación se muestra un gráfico de tipos de redes inalámbricas atendiendo a su distancia y velocidades.

7.2.1 WPAN: Bluetooth

Bluetooth es una especificación industrial para Redes Inalámbricas de Área Personal (WPAN) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la **banda ISM de los 2,4 GHz**. Los principales objetivos que se pretenden conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles.
- Eliminar los cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales.

Los dispositivos que con mayor frecuencia utilizan esta tecnología pertenecen a sectores de las telecomunicaciones y la informática personal, como PDA, teléfonos móviles, computadoras portátiles, ordenadores personales, impresoras o cámaras digitales.

Estos dispositivos se clasifican como «Clase 1», «Clase 2» o «Clase 3» en referencia a su potencia de transmisión. A mayor potencia mayor distancia.

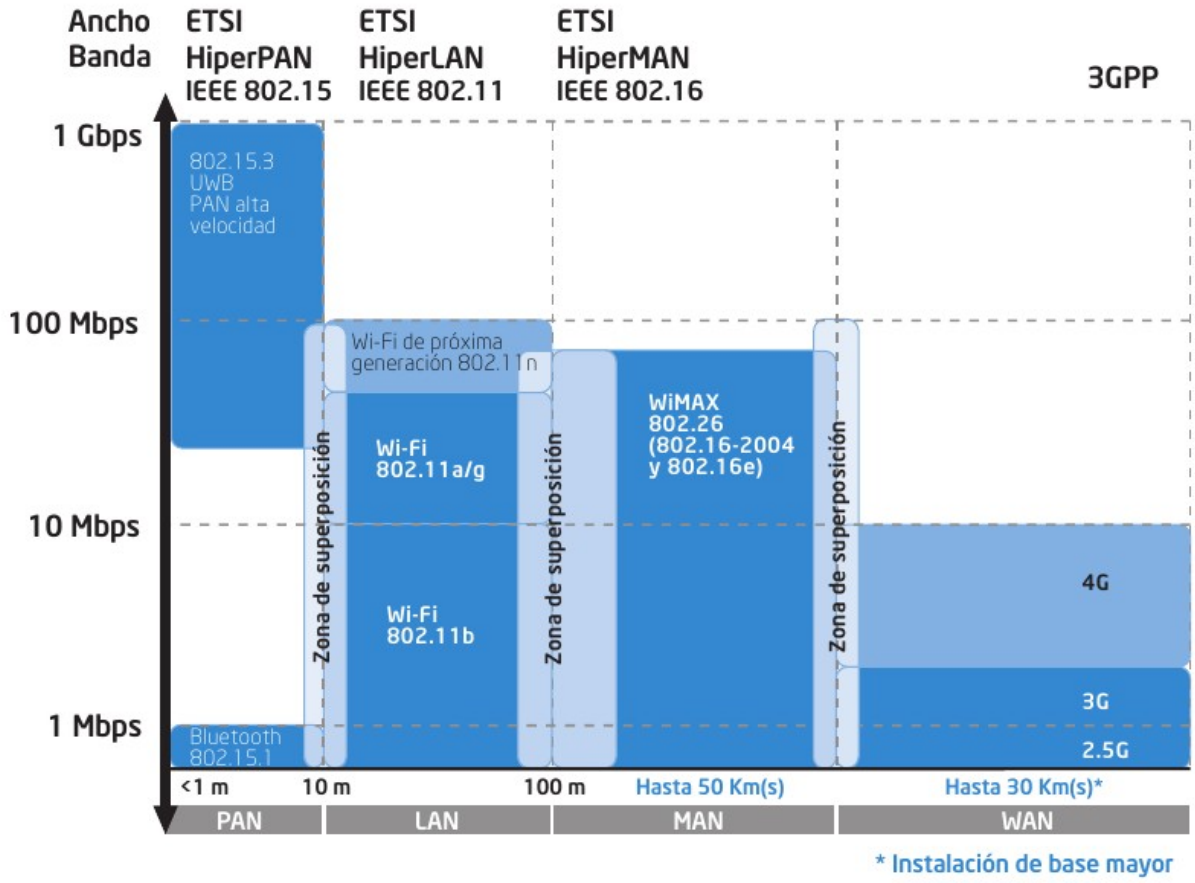


Figura 3: Tecnologías inalámbricas - Comparativa

Figura 4: Logo Bluetooth

Clase	Potencia máxima permitida (mW)	Potencia máxima permitida (dBm)	Alcance(aproximado)
Clase 1	100 mW	20 dBm	~30 metros
Clase 2	2.5 mW	4 dBm	~10-5 metros
Clase 3	1 mW	0 dBm	~1 metro

En la mayoría de los casos, la cobertura efectiva de un dispositivo de clase 2 se extiende cuando se conecta a un transceptor de clase 1. Esto es así gracias a la mayor sensibilidad y potencia de transmisión del dispositivo de clase 1, es decir, la mayor potencia de transmisión del dispositivo de clase 1 permite que la señal llegue con energía suficiente hasta el de clase 2. Por otra parte la mayor sensibilidad del dispositivo de clase 1 permite recibir la señal del otro pese a ser más débil.

Los dispositivos con Bluetooth también pueden clasificarse según su ancho de banda:

Versión	Ancho de banda
Versión 1.2	1 Mbit/s
Versión 2.0 + EDR	3 Mbit/s
Versión 3.0 + HS	24 Mbit/s
Versión 4.0	24 Mbit/s

Las prestaciones fueron publicadas por el **Bluetooth Special Interest Group (SIG)**. El SIG las anunció formalmente el 20 de mayo de 1998. Hoy cuenta con una membresía de más de 14.000 empresas en todo el mundo. Fue creado por Ericsson, IBM, Intel, Toshiba y Nokia, y posteriormente se sumaron muchas otras compañías. Todas las versiones de los estándares de Bluetooth están diseñadas para la compatibilidad hacia abajo, que permite que el último estándar cubra todas las versiones anteriores.

Versiones

Bluetooth v1.0 y v1.0b

Las versiones 1.0 y 1.0b han tenido muchos problemas, y los fabricantes tenían dificultades para hacer sus productos interoperables. Las versiones 1.0 y 1.0b incluyen en hardware de forma obligatoria la dirección del dispositivo Bluetooth (BD_ADDR) en la transmisión (el anonimato se hace imposible a nivel de protocolo), lo que fue un gran revés para algunos servicios previstos para su uso en entornos Bluetooth.

Bluetooth v1.1 (2002)

- Ratificado como estándar IEEE 802.15.1-2002
- Se corrigieron muchos errores en las especificaciones 1.0b.
- Añadido soporte para canales no cifrados.
- Indicador de señal recibida (RSSI).

Bluetooth v1.2 (2003)

Las principales mejoras son las siguientes:

- Una conexión más rápida y Discovery (detección de otros dispositivos bluetooth).
- Salto de frecuencia adaptable de espectro ampliado (AFH), que mejora la resistencia a las interferencias de radio frecuencia, evitando el uso de las frecuencias de lleno en la secuencia de saltos.
- Mayor velocidad de transmisión en la práctica, de hasta 721 kbit/s, que en v1.1.
- Introdujo el control de flujo y los modos de retransmisión de L2CAP.

Bluetooth v2.0 + EDR (2004)

Fue lanzado en 2004 y es compatible con la versión anterior 1.2. La principal diferencia es la introducción de una velocidad de datos mejorada (EDR «Enhanced Data Rate» «mayor velocidad de transmisión de datos») para acelerar la transferencia de datos. La tasa nominal de EDR es de 3 Mbit / s, aunque la tasa de transferencia de datos práctica es de 2,1 Mbit / s.

Bluetooth v2.1 + EDR (2007)

Bluetooth Core Version especificación 2.1 + EDR es totalmente compatible con 1.2, y fue adoptada el 26 de julio de 2007.

Bluetooth v3.0 + HS (2009)

Aprobado por el Bluetooth SIG el 21 de abril de 2009. Bluetooth 3.0 + HS soporta velocidades de transferencia de datos teórica de hasta 24 Mbits entre sí, aunque no a través del enlace Bluetooth propiamente dicho. La conexión Bluetooth nativa se utiliza para la negociación y el establecimiento mientras que el tráfico de datos de alta velocidad se realiza mediante un enlace 802.11. Su principal novedad es AMP (Alternate MAC / PHY), la adición de 802.11 como transporte de alta velocidad. Estaban inicialmente previstas dos tecnologías para incorporar en AMP: 802.11 y UWB, pero finalmente UWB no se encuentra en la especificación.

La incorporación de la transmisión a alta velocidad no es obligatoria en la especificación y por lo tanto, los dispositivos marcados con «+ HS» incorporan el enlace 802.11 de alta velocidad de transferencia de datos. Un dispositivo Bluetooth 3.0, sin el sufijo «+ HS» no apoyará la alta velocidad.

Bluetooth v4.0 (2010)

El SIG de Bluetooth ha completado la especificación del Núcleo de Bluetooth en su versión 4.0, que incluye **Bluetooth clásico**, **Bluetooth de alta la velocidad** y protocolos **Bluetooth de bajo consumo**. Bluetooth de alta velocidad se basa en Wi-Fi, y Bluetooth clásico consta de protocolos Bluetooth heredados. Esta versión ha sido adoptada el 30 de junio de 2010. Bluetooth de baja energía (BLE) es un subconjunto de Bluetooth v4.0 con una pila de protocolo completamente nuevo.

7.2.2 WLAN: Wi-Fi

Figura 5: Logo Wi-Fi

Wi-Fi (/wafa/; en algunos países hispanoparlantes /wifi/) es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wi-Fi, tales como: un ordenador personal, una consola de videojuegos, un smartphone o un reproductor de audio digital, pueden conectarse a Internet a través de un punto de

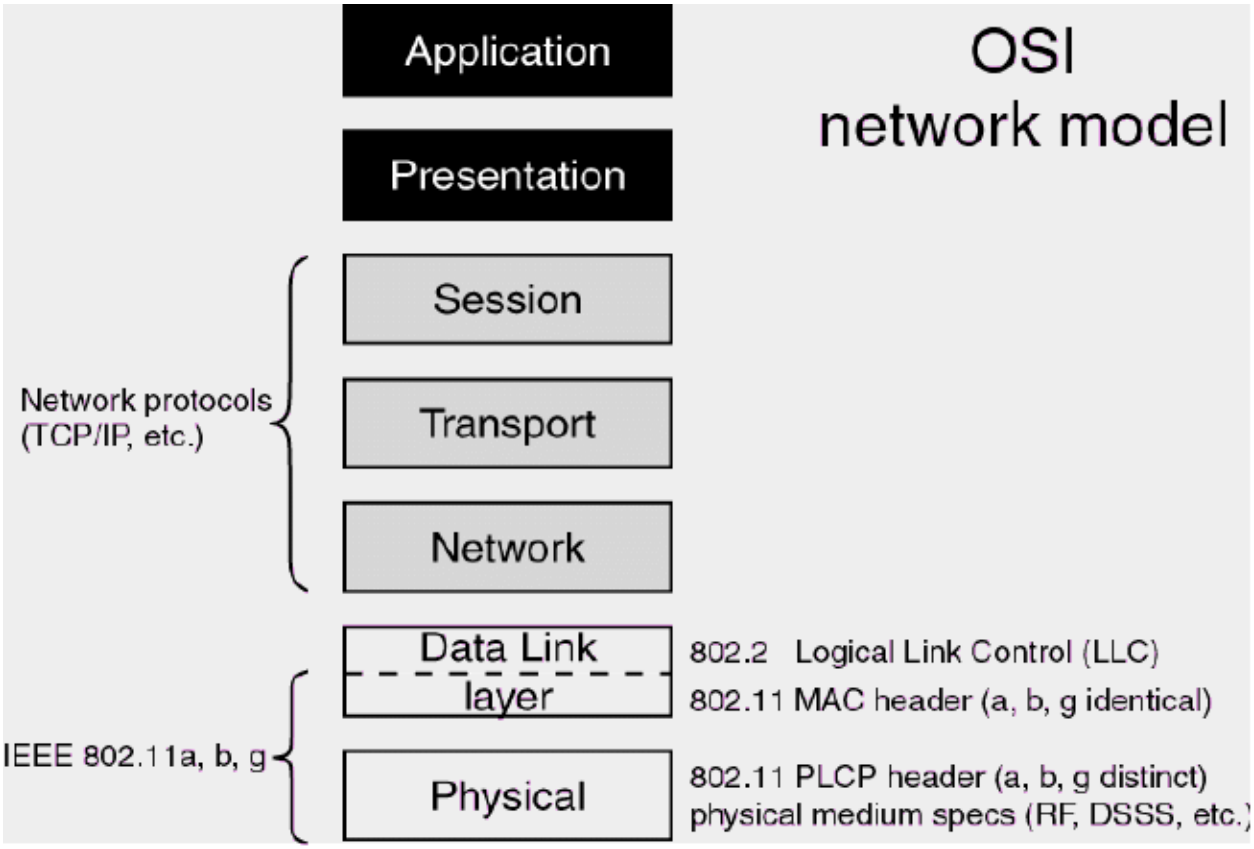
acceso de red inalámbrica. Dicho **punto de acceso** (o **hotspot**) tiene un alcance de unos 20 metros en interiores y al aire libre una distancia mayor. Pueden cubrir grandes áreas la superposición de múltiples puntos de acceso.

Esta nueva tecnología surgió por la necesidad de establecer un mecanismo de conexión inalámbrica que fuese compatible entre los distintos dispositivos. Buscando esa compatibilidad fue que en 1999 las empresas 3com, Airones, Intersil, Lucent Technologies, Nokia y Symbol Technologies se reunieron para crear la Wireless Ethernet Compatibility Alliance, o WECA, actualmente llamada **Wi-Fi Alliance**. El objetivo de la misma fue designar una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad de equipos.

De esta forma, en abril de 2000 WECA certifica la interoperabilidad de equipos según la norma IEEE 802.11b, bajo la marca Wi-Fi. Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tengan el sello Wi-Fi pueden trabajar juntos sin problemas, independientemente del fabricante de cada uno de ellos. Se puede obtener un listado completo de equipos que tienen la certificación Wi-Fi en Alliance - Certified Products.

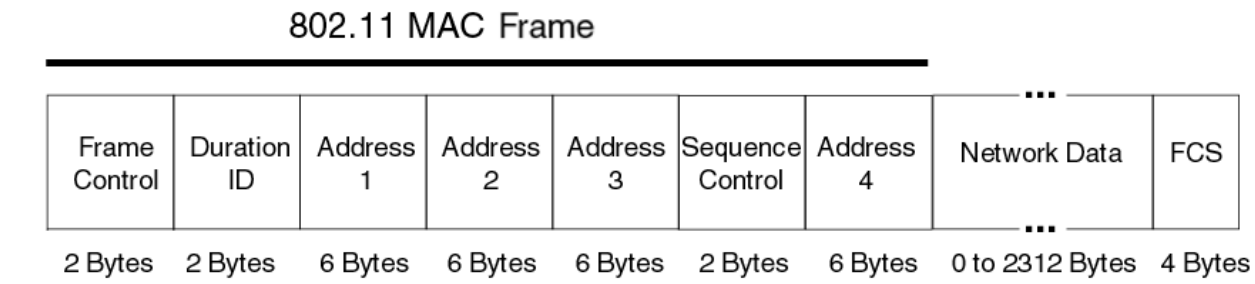
En el año 2002 la asociación WECA estaba formada ya por casi 150 miembros en su totalidad. La familia de **estándares 802.11** ha ido naturalmente evolucionando desde su creación, mejorando el rango y velocidad de la transferencia de información, entre otras cosas.

La norma IEEE 802.11 fue diseñada para sustituir el equivalente a las capas físicas y MAC de la norma 802.3 (Ethernet). Esto quiere decir que en lo único que se diferencia una red Wi-Fi de una red Ethernet es en cómo se transmiten las tramas o paquetes de datos; el resto es idéntico. Por tanto, una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales (LAN) de cable 802.3 (Ethernet).



Trama 802.11 (Wi-Fi)

Comparativa cabecera de trama wifi vs ethernet



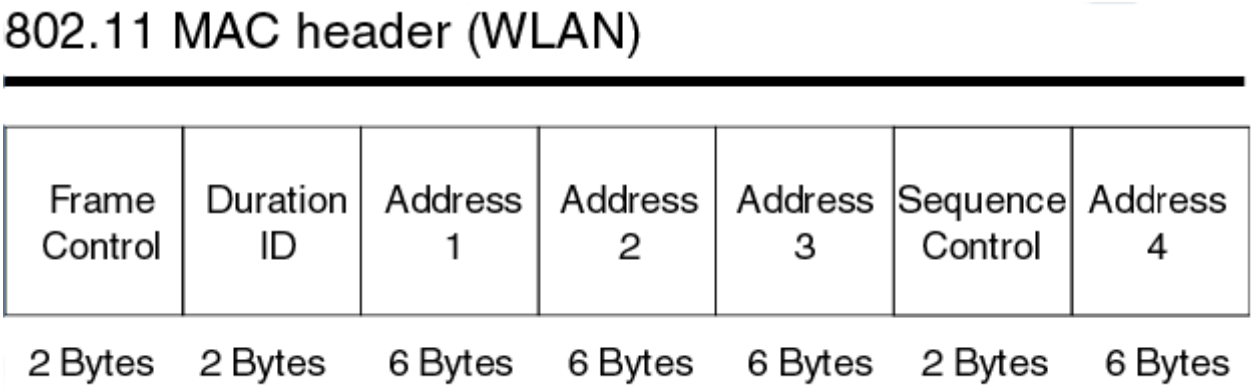


Figura 6: **Cabecera 802.11**

- **Dirección 1** (Destination Address (**DA**)): dirección MAC del nodo final.
- **Dirección 2** (Source Address (**SA**)): dirección MAC del nodo inicial.
- **Dirección 3** (Receiver Address (**RA**)): dirección MAC que identifica el dispositivo wireless que es el receptor inmediato de la trama.
- **Dirección 4** (Transmitter Address (**TA**)): dirección MAC que identifica el dispositivo wireless que transmite la trama.

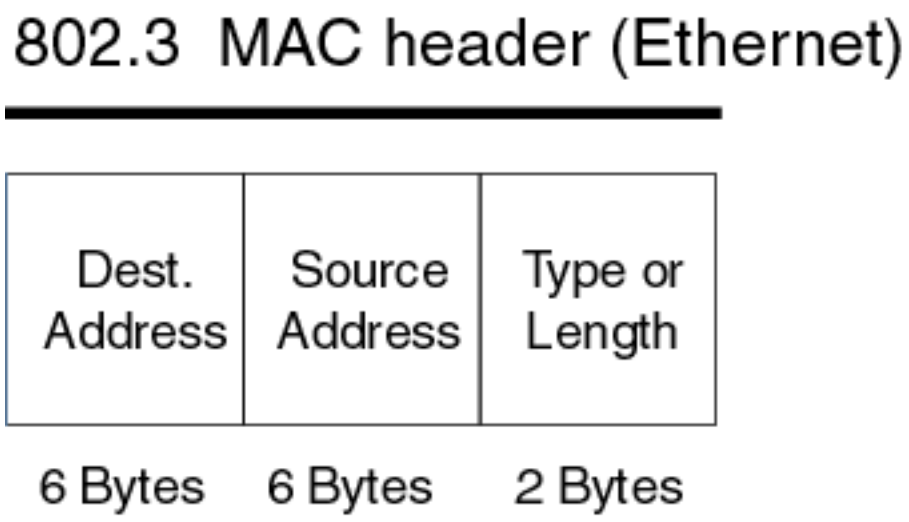


Figura 7: **Cabecera 802.3**

- **Dirección 1** (Destination Address (**DA**)): dirección MAC del nodo final.
- **Dirección 2** (Source Address (**SA**)): dirección MAC del nodo inicial.

CSMA/CA

Para el control de la transmisión se utilizan dos protocolos complementarios: **CSMA/CA** y **RTS/CTS**.

El mecanismo definido en el CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance, **acceso múltiple con escucha de portadora y evasión de colisiones**) es una adaptación del CSMA/CD utilizado en las redes Ethernet, pero modificado para tener en cuenta la limitación de las comunicaciones por radiofrecuencia según la cual una estación transmitiendo no puede detectar una colisión con otra transmisión simultánea. El algoritmo dicta que un equipo que desea transmitir, antes de hacerlo ha de escuchar para comprobar si ya existe otra estación enviando datos. En caso de no ser así podrá transmitir, pero si ya hubiera algún equipo transmitiendo deberá esperar un tiempo aleatorio y transcurrido este, volver a comprobar si el medio esta ocupado por otra transmisión. Este algoritmo presenta varios problemas. Uno es que existe la posibilidad de que dos o mas equipos comprueben a la vez si se esta transmitiendo y al detectar que el canal esta libre, empiecen a emitir de forma simultanea. Este problema deberá ser solucionado por protocolos superiores como TCP que se encargarán de detectar pérdidas de información y pedir la retransmisión de esta. Así mismo, al ser el tiempo de espera, cuando se detecta el canal ocupado, tomado de forma aleatoria se consigue paliar en parte el problema de la concurrencia de equipos al comprobar el uso del canal. Otro es el problema conocido como "**terminal oculto**", que se muestra en la siguiente ilustración.

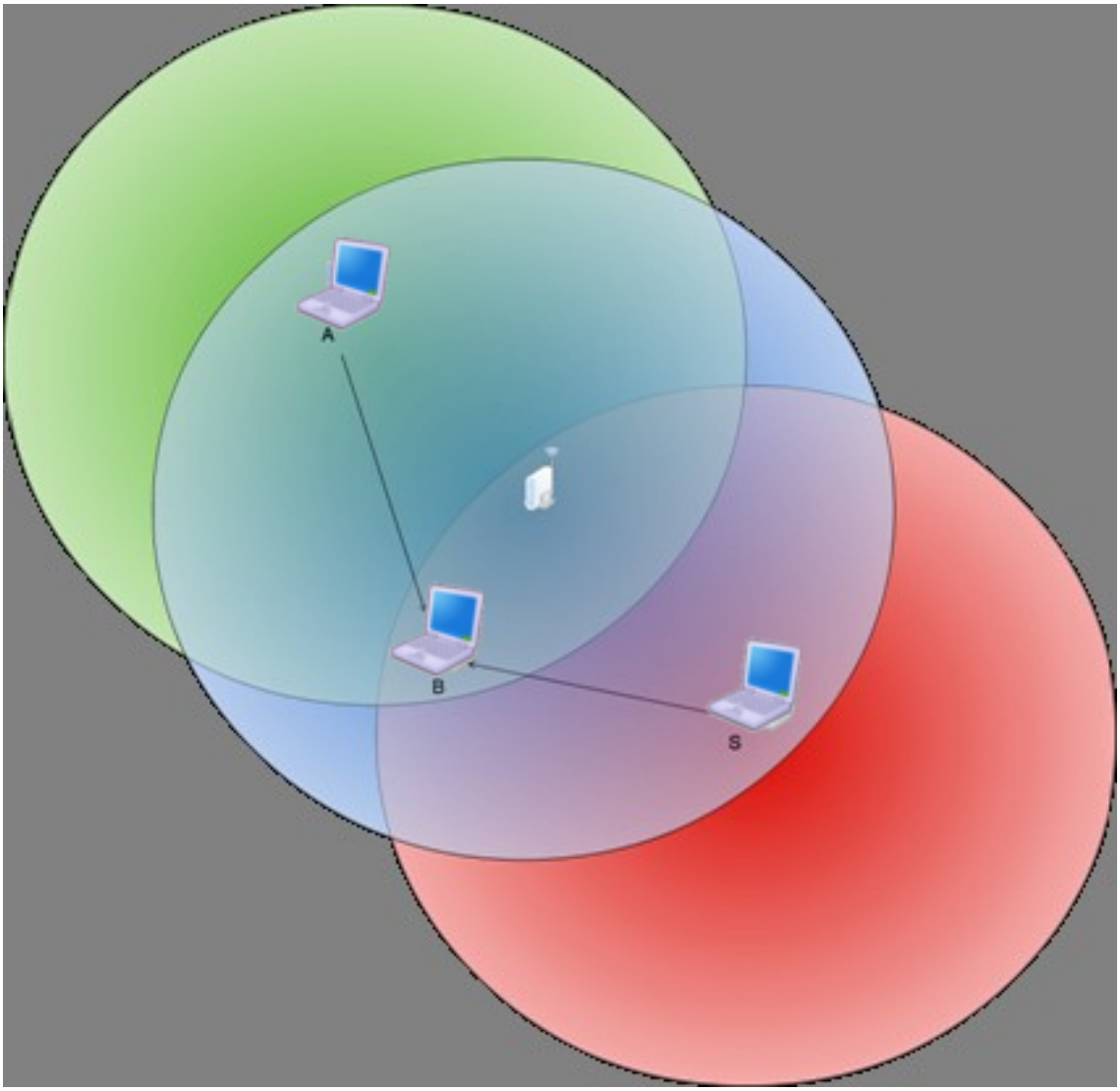


Figura 8: Estaciones inalàmbriques A, B y S

Este problema se produce cuando, estando los terminales "A", "B" y "S" en la misma celda, cuya cobertura esta mostrada en azul, un terminal "A" tiene visibilidad de otro terminal "B" pero no de un terminal "S", como se ve por su área de cobertura mostrada en verde. Un caso típico en el que puede pasar esto es que se encuentren en fila por lo que la distancia de "A" a "B" sea relativamente corta, pero la de "A" a "S" suficientemente larga como para que no se detecten, pero sin embargo "B" al estar a mitad de camino si tenga recepción de "S", cuya área de cobertura se muestra en rojo. Esta situación también puede suceder por elementos arquitectónicos que impidan la visibilidad entre "A" y "S", pero si permitan la comunicación entre "S" y "B" y entre "A" y "B".

En esta situación el terminal "S" puede emitir para enviar información a "B". Si el terminal "A" así mismo quisiera transmitir, escucharía el canal, y al no tener visibilidad de "S" encontrará el canal vacío y transmitirá. El problema surge del hecho de que "B" sí tiene visibilidad de ambos terminales, así que detectará ambas señales de forma simultánea, que interferirán y harán la comunicación inválida, y lo peor es que ni "A" ni "S" tendrán constancia del problema, así que la situación puede dilatarse en el tiempo indefinidamente.

Para solventar este problema, así como alguno más (por ejemplo la iteración entre clientes 802.11b y 802.11g) se implementó en estas redes Wi-Fi el protocolo RTS/CTS. Es obligatorio para los equipos tener implementado este protocolo, pero no lo es tenerlo activado, aunque por defecto suele estar activo para evitar problemas como el del terminal oculto.

Cuando el protocolo RTS/CTS esta activado, se añade al CSMA/CA, de manera que una vez que el terminal que ha detectado que nadie está transmitiendo, **enviará una trama RTS (Request To Send) al terminal destino**, indicándole que desea transmitir y, entre otros datos, cuanto tiempo (en bytes) durará esa transmisión. Si en terminal destino está en condiciones de recibir la información, **responderá con una trama CTS (Clear To Send)** repitiendo así mismo la información que indica cuanto tiempo durará la transmisión. Con este intercambio, se consigue que **el canal quede reservado** y los demás equipos sepan que han de esperar al menos el tiempo que se indica en las tramas RTS y CTS para poder transmitir ellos, y puesto que tanto emisor como receptor transmiten la información, todos aquellos sistemas que pudieran interferir con esa transmisión recibirán la trama RTS, la CTS o ambas.

Normas 802.11 más importantes

La familia de estándares desarrollados por la IEEE para tecnologías de **red inalámbricas (redes wifi)**. Originalmente ofrecía una velocidad de transmisión de 1 o 2 Mbps en la banda de frecuencia wifi de **2.4 GHz**. Se le conoce popularmente como **WIFI (WIreless-FIdelity)**. Tiene un área de cobertura aproximada de 100 metros.

Norma	Velocidad	Frecuencia	Año
802.11a	54 Mbps	5 Ghz (OFDM)	1999
802.11b	11 Mbps	2,4 Ghz (DSSS)	1999
802.11g	54 Mbps	2,4 Ghz (OFDM)	2003
802.11G +	108 Mbps	2,4 Ghz	
802.11n	300 Mbps	2,4 / 5 Ghz	2009
802.11ac	1 Gbps	5 Ghz	2014
802.11ad	7 Gbps	2,4 / 5 / 60 Ghz	2015?

Otras normas

- **802.11h**: regula la potencia de emisión de las redes Wifi, el objetivo es cumplir los **reglamentos europeos para redes inalámbricas a 5 GHz**.
- **802.11i**: Estándar de seguridad para redes wifi aprobado a mediados de 2004. En él se define al protocolo de **encriptación WPA2** basado en el algoritmo AES. Pretende mejorar la seguridad del cifrado wifi y añadir autenticación.
- **802.11j**: Estándar wifi **equivalente al 802.11h, en la regulación japonesa**.
- **802.11ac**: Estándar de conexión WiFi en desarrollo, con notables mejorías respecto a 802.11n, para que sea de uso común se calcula que será en 2014. Se utiliza parte de los estándares 802.11a y n. **Puede suministrar una velocidad de transmisión de más de 1 Gbps en la banda de 5 GHz**.
- **802.11ad**: Una propuesta de un estándar de conexión WiFi diseñado con WiGig, la evolución del 802.11ac. Para que sea de uso popular se calcula que será en 2015. Se utiliza parte de los estándares 802.11n y ac. Puede suministrar una velocidad de transmisión de **hasta 7 Gbps teóricos** en la banda de 60 GHz sin licencia, aunque también funciona en la de 2,4 y 5GHz, serán **routers tri-banda**. La banda de 60 GHz será usada en enlaces de corta distancia, y su señal es muy direccional. Otra ventaja es que el consumo de energía disminuirá con una misma tasa de datos de 802.11n o ac, siendo más eficiente para móviles y portátiles.

Seguridad y fiabilidad

Uno de los problemas a los cuales se enfrenta actualmente la tecnología Wi-Fi es la progresiva saturación del espectro radioeléctrico, debido a la masificación de usuarios, esto afecta especialmente en las conexiones de larga distancia (mayor de 100 metros). En realidad Wi-Fi está diseñado para conectar ordenadores a la red a distancias reducidas, cualquier uso de mayor alcance está expuesto a un excesivo riesgo de interferencias.

Un muy elevado porcentaje de redes son instalados sin tener en consideración la seguridad convirtiendo así sus redes en redes abiertas (o completamente vulnerables ante el intento de acceder a ellas por terceras personas), sin proteger la información que por ellas circulan. De hecho, la configuración por defecto de muchos dispositivos Wi-Fi es muy insegura (routers, por ejemplo) dado que a partir del identificador del dispositivo se puede conocer la clave de éste; y por tanto acceder y controlar el dispositivo se puede conseguir en sólo unos segundos.

El acceso no autorizado a un dispositivo Wi-Fi es muy peligroso para el propietario por varios motivos. El más obvio es que pueden utilizar la conexión. Pero además, accediendo al Wi-Fi se puede monitorizar y registrar toda la información que se transmite a través de él (incluyendo información personal, contraseñas. . . .).

Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el WEP, el WPA, o el WPA2 que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos. La mayoría de las formas son las siguientes:

- WEP, cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una "clave" de cifrado antes de enviarlo al aire. Este tipo de cifrado no está muy recomendado debido a las grandes vulnerabilidades que presenta ya que cualquier cracker puede conseguir sacar la clave, incluso aunque esté bien configurado y la clave utilizada sea compleja.
- WPA: presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como dígitos alfanuméricos.
- Filtrado de MAC, de manera que sólo se permite acceso a la red a aquellos dispositivos autorizados. Es lo más recomendable si solo se va a usar con los mismos equipos, y si son pocos.
- Ocultación del punto de acceso: se puede ocultar el punto de acceso (Router) de manera que sea invisible a otros usuarios.

- El protocolo de seguridad llamado WPA2 (estándar 802.11i), que es una mejora relativa a WPA. En principio es el protocolo de seguridad más seguro para Wi-Fi en este momento. Sin embargo requieren hardware y software compatibles, ya que los antiguos no lo son.

Sin embargo, no existe ninguna alternativa totalmente fiable, ya que todas ellas son susceptibles de ser vulneradas.

La **Wi-Fi Alliance** distingue:

- **WPA-Personal y WPA2-Personal** (con PSK, clave pre-compartida)
- **WPA-Enterprise y WPA2-Enterprise** (autenticación 802.1x/EAP)

Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de **cifrado AES (Advanced Encryption Standard)** superior al TKIP utilizado en WPA.

El WPA-Enterprise requiere de una infraestructura de autenticación 802.1x con un **servidor de autenticación**, generalmente un **servidor RADIUS**. Este presta un servicio AAA (*Authentication, Authorization and Accounting*, 'autenticación, autorización y contabilización')

El problema de las claves compartidas está en que todo usuario con acceso a la red conoce la clave, por lo que, si se quiere retirar el acceso a un usuario o grupo de usuarios o si la clave es descubierta por personas no autorizadas, se debe cambiar la clave y comunicarla a todos los usuarios de la red para que la cambien en sus dispositivos, procedimiento que suele ser lento e inseguro. Este problema es especialmente preocupante en entornos empresariales o con muchos usuarios, como en los centros docentes y universitarios.

El **estándar IEEE 802.1x** ofrece una solución a este problema, tanto a redes 802.3 como a 802.11. Consiste en que **cada usuario tiene sus propias credenciales de acceso a la red y se autentica con ellas**, independientemente de que ademas se utilice o no una clave compartida para acceder a la red.

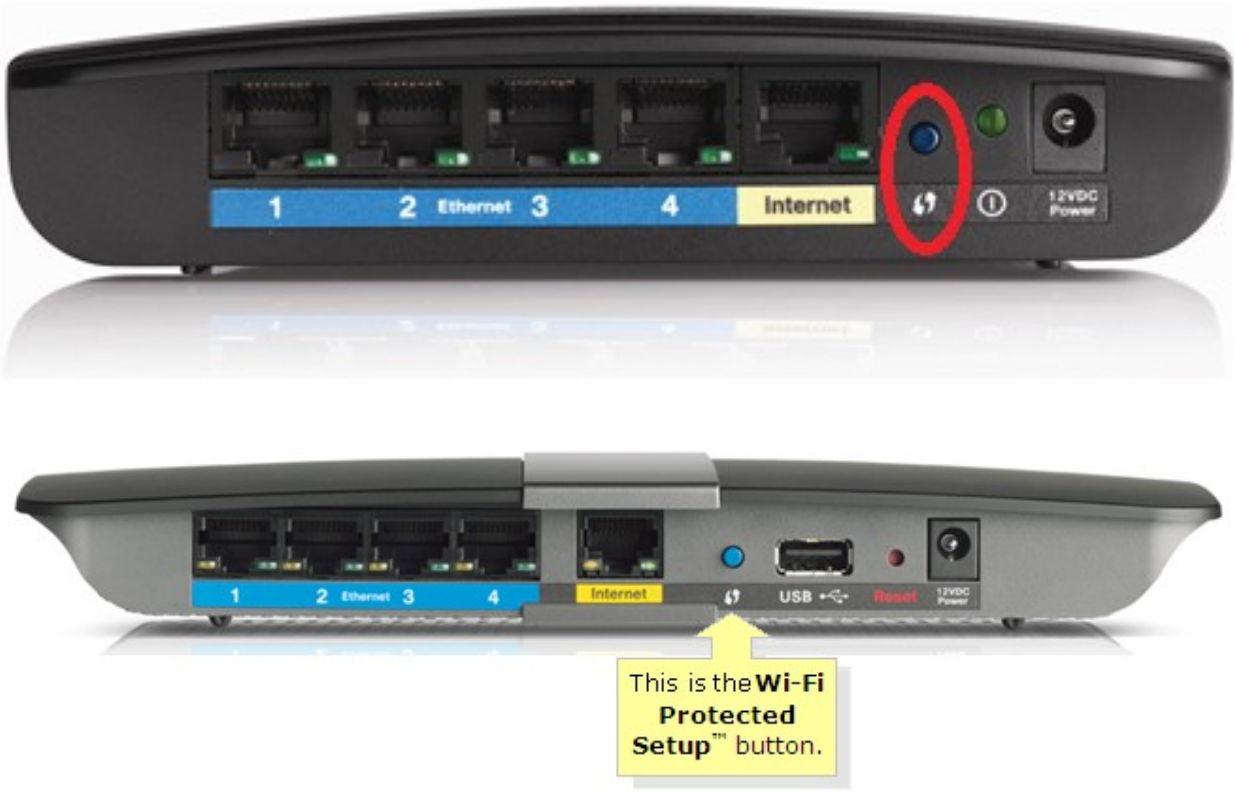
Siglas:

- PSK: PreShared Key
- EAP: Extensible Authentication Protocol

WPS (Wi-Fi Protected Setup)

WPS (Wi-Fi Protected Setup) es un estándar de 2007, promovido por la Wi-Fi Alliance para facilitar la creación de redes WLAN. En otras palabras, WPS no es un mecanismo de seguridad por sí, se trata de la definición de diversos

mecanismos para facilitar la configuración de una red WLAN segura con WPA2, pensados para minimizar la intervención del usuario en entornos domésticos o pequeñas oficinas (**SOHO: Small Office Home Office**). Concretamente, WPS define los mecanismos a través de los cuales los diferentes dispositivos de la red obtienen las credenciales (SSID y PSK) necesarias para iniciar el proceso de autenticación.



Arquitectura técnica

WPS define una arquitectura con tres elementos con roles diferentes:

- **Registrar (matriculador)**: dispositivo con la autoridad de generar o revocar las credenciales en la red. Tanto un AP como cualquier otra estación o PC de la red pueden tener este rol. Puede haber más de un Registrar en una red.
- **Enrollee (matriculado)**: dispositivo que solicita el acceso a la red WLAN.
- **Authenticator (autenticador)**: AP funcionando de proxy entre el Registrar y el Enrollee.

Métodos

WPS contempla cuatro tipos de configuraciones diferentes para el intercambio de credenciales, PIN (Personal Identification Number), PBC (Push Button Configuration), NFC (Near Field Communications) y USB (Universal Serial Bus):

- **PIN**: tiene que existir un PIN asignado a cada elemento que vaya a asociarse a la red. Este PIN tiene que ser conocido tanto por el Registrar, como por el usuario (Enrollee). Es necesaria la existencia de una interfaz (e.g. pantalla y teclado) para que el usuario pueda introducir el mencionado PIN.
- **PBC**: la generación y el intercambio de credenciales son desencadenados a partir que el usuario presiona un botón (físico o virtual) en el AP (o en otro elemento Registrar) y otro en el dispositivo. Notar que en el corto lapso de tiempo entre que se presiona el botón en el AP y se presiona en el dispositivo, cualquier otra estación próxima puede ganar acceso a la red.

- **NFC**: intercambio de credenciales a través de comunicación NFC. La tecnología NFC (Near Field Communication), basada en RFID (Radio Frequency IDentification) permite la comunicación sin hilos entre dispositivos próximos (0 - 20 cm). Entonces, el dispositivo Enrollee se tiene que situar al lado del Registrar para desencadenar la autenticación. De esta manera, cualquier usuario que tenga acceso físico al Registrar, puede obtener credenciales válidas.
- **USB**: con este método, las credenciales se transfieren mediante un dispositivo de memoria flash (e.g. pendrive) desde el Registrar al Enrollee.

Los métodos PBC, NFC y USB pueden usarse para configurar dispositivos sin pantalla ni teclado (e.g. impresoras, webcams, etc.), pero aunque el estándar contempla NFC y USB, todavía no se certifican estos mecanismos. Actualmente sólo el método PIN es obligatorio en todas las estaciones para obtener la certificación WPS; PBC es obligatorio sólo en APs.

Vulnerabilidades

Existe una falla de seguridad descubierta en diciembre del 2011 por Stefan Viehböck, la cual afecta a routers inalámbricos que tienen la función WPS (también llamada **QSS: Quick Security Setup**), la misma que en dispositivos actuales se encuentra habilitada por defecto. La falla **permite a un atacante recuperar el PIN WPS y con la misma la clave pre-compartida de la red WPA/WPA2** usando ataques de fuerza bruta en pocas horas. Los usuarios deben deshabilitar la función WPS como solución temporal. En ciertos dispositivos, es posible que no se pueda realizar dicho procedimiento.

7.2.3 WMAN: WiMAX

WiMAX, siglas de Worldwide Interoperability for Microwave Access (interoperabilidad mundial para acceso por microondas), es una norma de transmisión de datos que utiliza las ondas de radio en las **frecuencias de 2,3 a 3,5 GHz** y puede tener una cobertura de **hasta 50 km y 70 Mbps**. En el estandar WiMAX2 (IEEE 802.16m) teóricamente sería posible alcanzar hasta 1 Gbps en reposo y 100 Mbps en movimiento en la descarga mediante la agrupación de canales.

Es una tecnología dentro de las conocidas como tecnologías de última milla, también conocidas como bucle local que permite la recepción de datos por microondas y retransmisión por ondas de radio. El estándar que define esta tecnología es el **IEEE 802.16**. Una de sus ventajas es dar servicios de banda ancha en zonas donde el despliegue de cable o fibra por la baja densidad de población presenta unos costos por usuario muy elevados (zonas rurales).

El único organismo habilitado para certificar el cumplimiento del estándar y la interoperabilidad entre equipamiento de distintos fabricantes es el **Wimax Forum**: todo equipamiento que no cuente con esta certificación, no puede garantizar su interoperabilidad con otros productos.

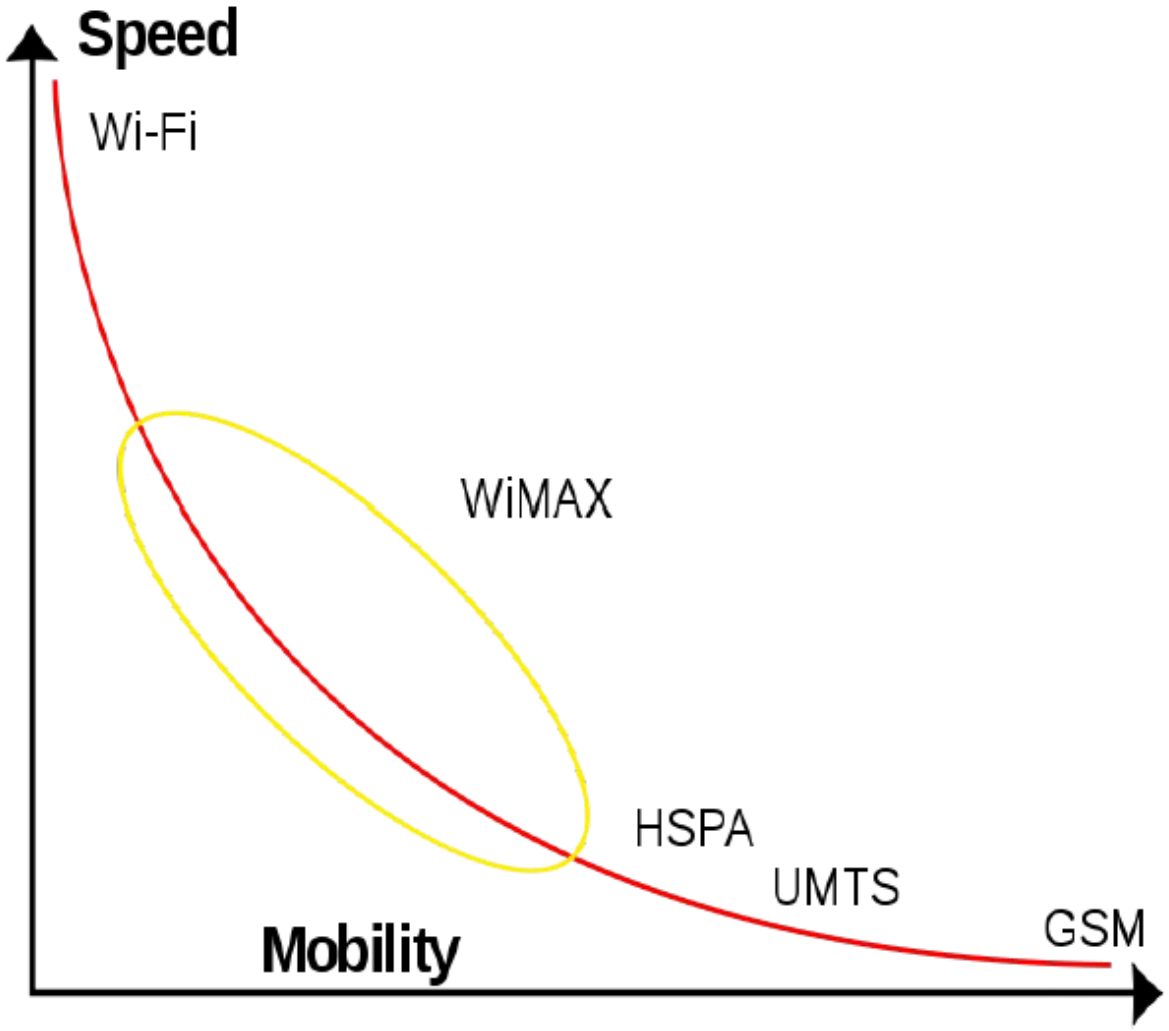
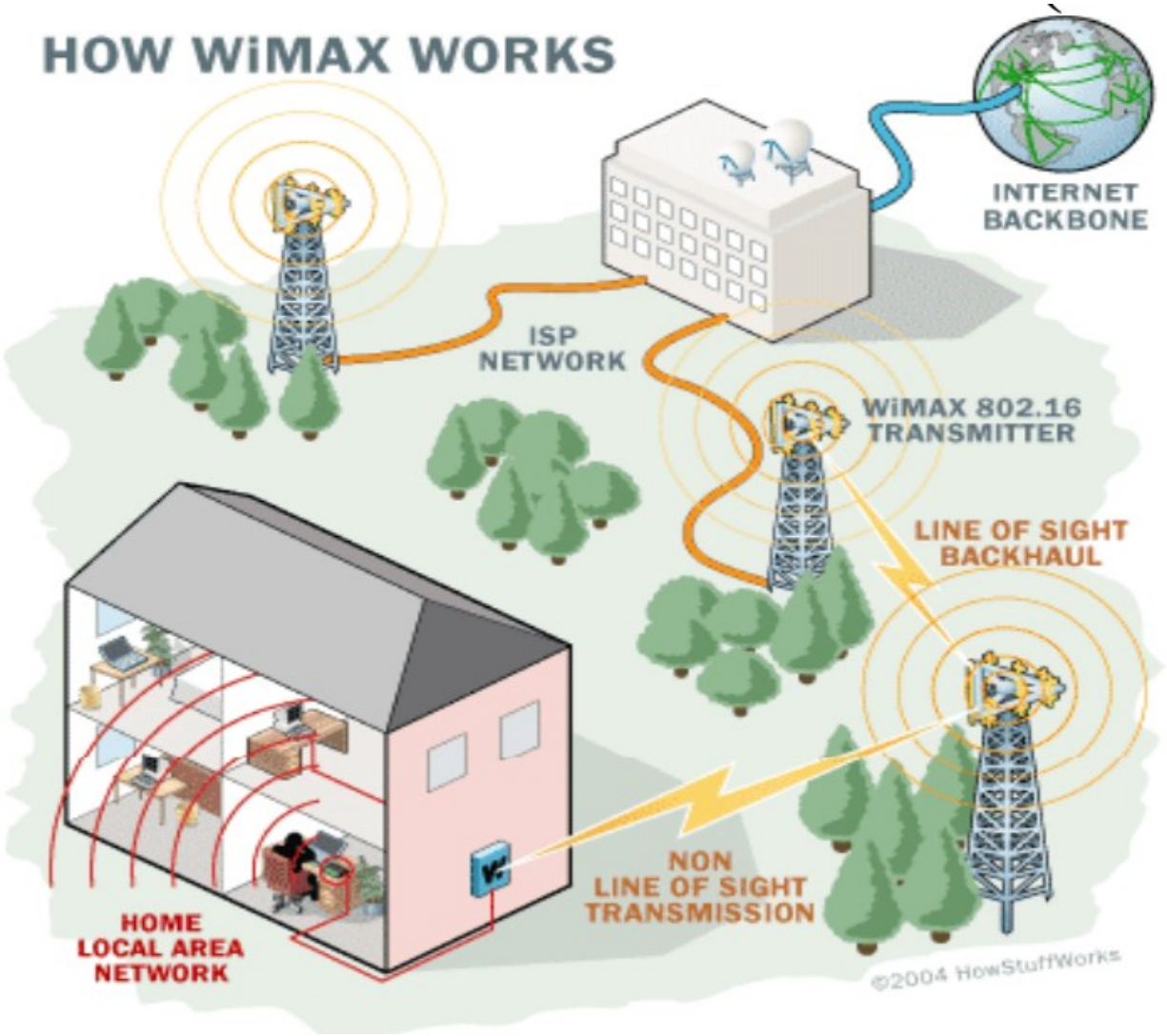


Figura 9: Wireless Speed vs Mobility.png

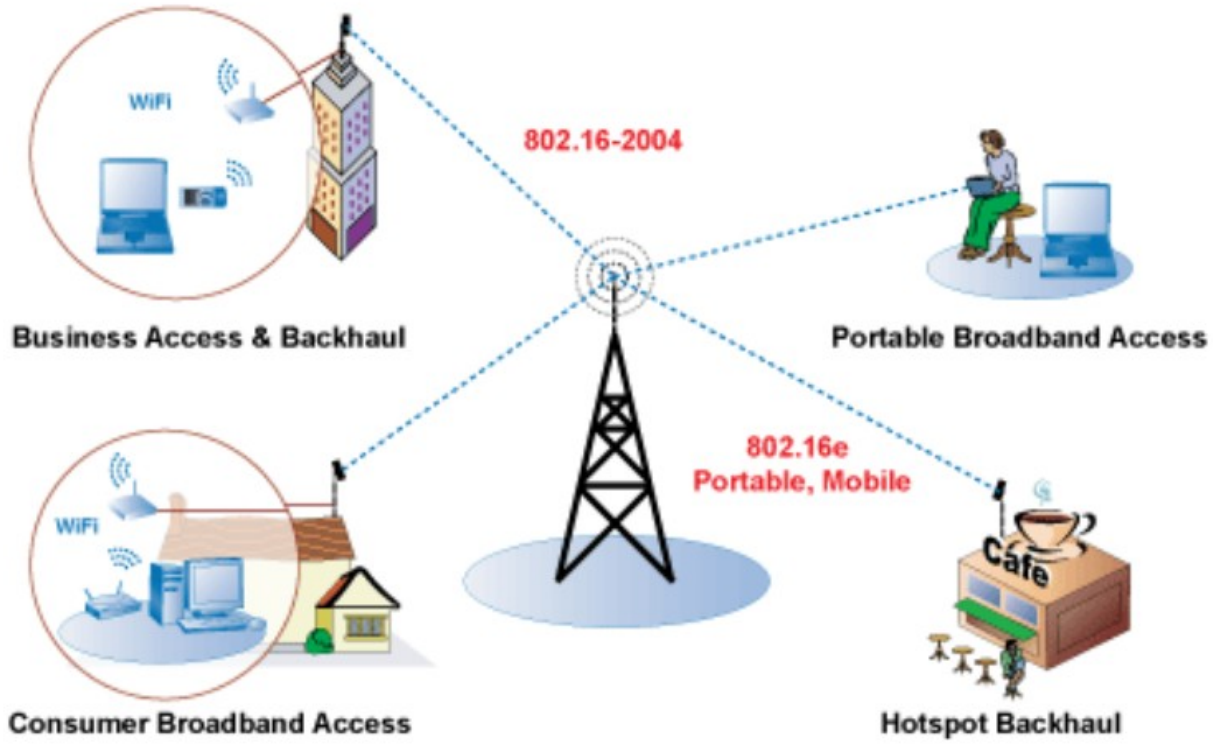
El WiMAX se puede utilizar para una serie de aplicaciones, incluyendo conexiones de banda ancha para Internet, puntos de acceso, etc. Es similar a Wi-Fi, pero puede funcionar para distancias mucho mayores.

El ancho de banda y rango del WiMAX lo hacen adecuado para las siguientes aplicaciones potenciales:

- Proporcionar conectividad portátil de banda ancha móvil a través de ciudades y países por medio de una variedad de dispositivos.
- Proporcionar una alternativa inalámbrica al cable y línea de abonado digital (DSL) de «última milla» de acceso de banda ancha.
- Proporcionar datos, telecomunicaciones (VoIP) y servicios de IPTV (triple play).


HOW WiMAX WORKS
INTERNET BACKBONE
ISP NETWORK
WiMAX 802.16 TRANSMITTER
LINE OF SIGHT BACKHAUL
NON LINE OF SIGHT TRANSMISSION
HOME LOCAL AREA NETWORK
©2004 HowStuffWorks

- Proporcionar una fuente de conexión a Internet como parte de un plan de continuidad del negocio.
- Para redes inteligentes y medición.



WiMAX vs LMDS

LMDS (Local Multipont Delivery Service): es una tecnología inalámbrica de acceso a la banda ancha, es también denominada como **WiBAS (Wireless Broadband Access System)**.

- Es un servicio de acceso inalámbrico de banda ancha regulado por el IEEE y se describe el 802 por LAN/MAN Standards Committee a través de los esfuerzos del Grupo de Trabajo **IEEE 802.16.1**.
- Trabaja fundamentalmente en la banda de los **26 GHz** y los 29 GHz, según las regulaciones locales aplicables. En los Estados Unidos, las frecuencias de 31,0 a 31,3 GHz se consideran también las frecuencias de LMDS.
- Está pensada para trabajar en modo punto a punto o punto-multipunto.
- Las radiocomunicaciones en la banda de 26 GHz **necesitan visibilidad directa entre antenas**.
- El abastecimiento del servicio LMDS, viene **limitado por las características del medio** y las exigencias de disponibilidad contratadas, entre otros factores técnicos.
- Se puede hablar de **distancias máximas entre 2,5 Km y 14 Km**, aunque las utilizaciones típicas de LMDS acostumbran a cubrir distancias de entre 3 y 5 Km., con un grado de disponibilidad muy alto.

WiMAX es una tecnología basada en estándares que permite la entrega de última milla de acceso inalámbrico de banda ancha como una alternativa al cable y DSL».

- La tecnología se basa en el estándar IEEE 802.16 (también denominado Broadband Wireless Access).

- Trabaja en la banda de **2 a 11 GHz**, por tanto, no le afectan las limitaciones de propagación de la banda de 26 GHz.
- Proporciona transmisión inalámbrica de datos usando varios de modos de transmisión, de punto a multipunto para portátiles y acceso a Internet completamente móvil.
- Una diferencia principal es que WiMAX puede trabajar **tanto sin visibilidad directa, como con visibilidad directa**.
- Otra diferencia fundamental es la capacidad de WiMAX de **adaptarse a las condiciones variables del medio**, mediante mecanismos de control de potencia emitida, modulación adaptativa y selección automática de frecuencia que permiten una combinación de abastecimiento y de velocidad de transmisión de datos superior.

7.2.4 WWAN: 4G

Evolución de la tecnología móvil

Generación	Tecnología
0G	▪ Radio analógica AM/FM (años 40)
1G	▪ Primeros teléfonos móviles: FM (años 80) ▪ **TACS** [Total Access Communication System]
2G	▪ Transmisión digital de voz (años 90) ▪ **GSM** [Global System for Mobile Communications]
2G transitional (2.5G, 2.75G)	▪ Nuevos servicios, p.j. MMS ▪ **GPRS** [General Packet Radio Service] ▪ EDGE [Enhaced Data rates for GSM Evolution]
3G	▪ Transmisión digital de voz y datos ▪ **UMTS** [Universal Mobile Telecommunications System]
3G transitional (3.5G, 3.75G, 3.9G)	▪ **HSPA** [High Speed Packet Access] / **LTE** [Long Term Evolution]
4G LTE Advanced (E-UTRA)	▪ **E-UTRA (LTE Advanced)**

3GPP

El **Proyecto Asociación de Tercera Generación** o más conocido por el acrónimo inglés **3GPP 3rd Generation Partnership Project** es una colaboración de grupos de asociaciones de telecomunicaciones, conocidos como Miembros Organizativos.

Miembros organizativos

Organización	Procedencia	Web
The Association of Radio Industries and Businesses (**ARIB**)	Japón	www.arib.or.jp
The Alliance for Telecommunications Industry Solutions (**ATIS**)	Estados Unidos	www.atis.org
China Communications Standards Association (**CCSA**)	China	www.ccsa.org.cn
The European Telecommunications Standards Institute (**ETSI**)	Europa	www.etsi.org
Telecommunications Technology Association (**TTA**)	Corea del Sur	www.tta.or.kr
Telecommunication Technology Committee (**TTC**)	Japón	www.ttc.or.jp

El objetivo inicial del 3GPP era asentar las especificaciones de un sistema global de comunicaciones de tercera generación 3G para móviles basándose en las especificaciones del sistema evolucionado «Global System for Mobile Communications» GSM dentro del marco del proyecto internacional de telecomunicaciones móviles 2000 de la Unión Internacional de Telecomunicaciones ITU. Más tarde el objetivo se amplió incluyendo el desarrollo y mantenimiento de:

- El Sistema Global de telecomunicaciones móviles GSM incluyendo las tecnologías de radio-acceso evolucionadas del GSM (cómo por ejemplo GPRS o el EDGE).
- Un sistema de tercera generación evolucionado y más allá del sistema móvil basado en las redes de núcleo evolucionadas del 3GPP y las tecnologías de radio-acceso apoyadas por los miembros del proyecto (cómo por ejemplo la tecnología UTRAN y sus modos FDD y TDD).
- Un Subsistema Multimedia IP (IMS) desarrollado en un acceso de forma independiente.

La estandarización 3GPP abarca radio, redes de núcleo y arquitectura de servicio. El proyecto 3GPP se estableció en Diciembre del año 1988 y no se tiene que confundir con el Proyecto Asociación de Tercera Generación 2 (3GPP2), que tiene por objetivo la especificación de los estándares por otra tecnología 3G basada en el sistema IS95 (CDMA), y que es más conocido por el acrónimo CDMA2000. El equipo de apoyo 3GPP, también conocido como el Centro de Competencias Móviles se encuentra situado en las oficinas de la ETSI en Sophia Antípolis (Francia).

Los sistemas 3GPP se encuentran desplegados por la mayoría del territorio donde el mercado GSM está establecido. Mayormente encontramos sistemas de Versión 6, pero desde 2010, con el mercado de teléfonos inteligentes creciendo de forma exponencial, el interés por los sistemas HSPA+ y LTE está impulsando a las compañías a adoptar sistemas Versión 7 y de más avanzados.

Desde 2005, los sistemas 3GPP están siendo desarrollados en los mismos mercados que los sistemas 3GPP2 de tecnología CDMA. Eventualmente los estándares 3GPP2 desaparecerán dejando a los 3GPP como únicos estándares de tecnología móvil.

LTE

3GPP Long Term Evolution Country Map.svg

Comparativa LTE frente a LTE Advanced

▪	LTE versión 8	LTE Advanced
Pico de velocidad en bajada	300 Mbit/s	1 Gbit/s
Pico de velocidad en subida	75 Mbit/s	500 Mbit/s

Especificaciones de la ITU

El UIT-R (sector de las Radiocomunicaciones de la Unión Internacional de Telecomunicaciones) emitió en 2008 los requisitos que deberían cumplir la telefonía móvil y el servicio de acceso a Internet para ser considerados como 4G. Estas especificaciones se conocen como IMT-Advanced (International Mobile Telecommunications-Advanced)

Entre las especificaciones están:

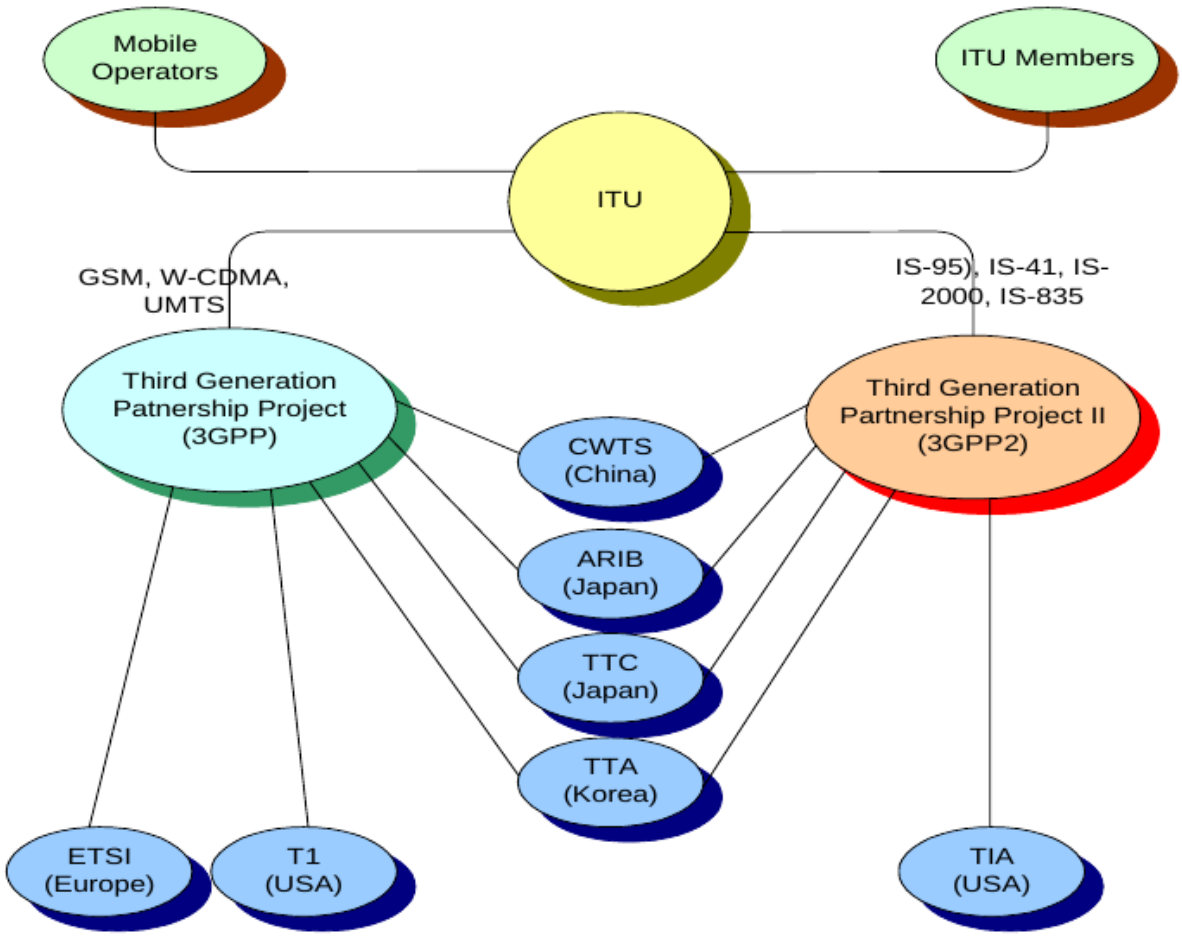


Figura 10: 3GPP vs 3GPP2

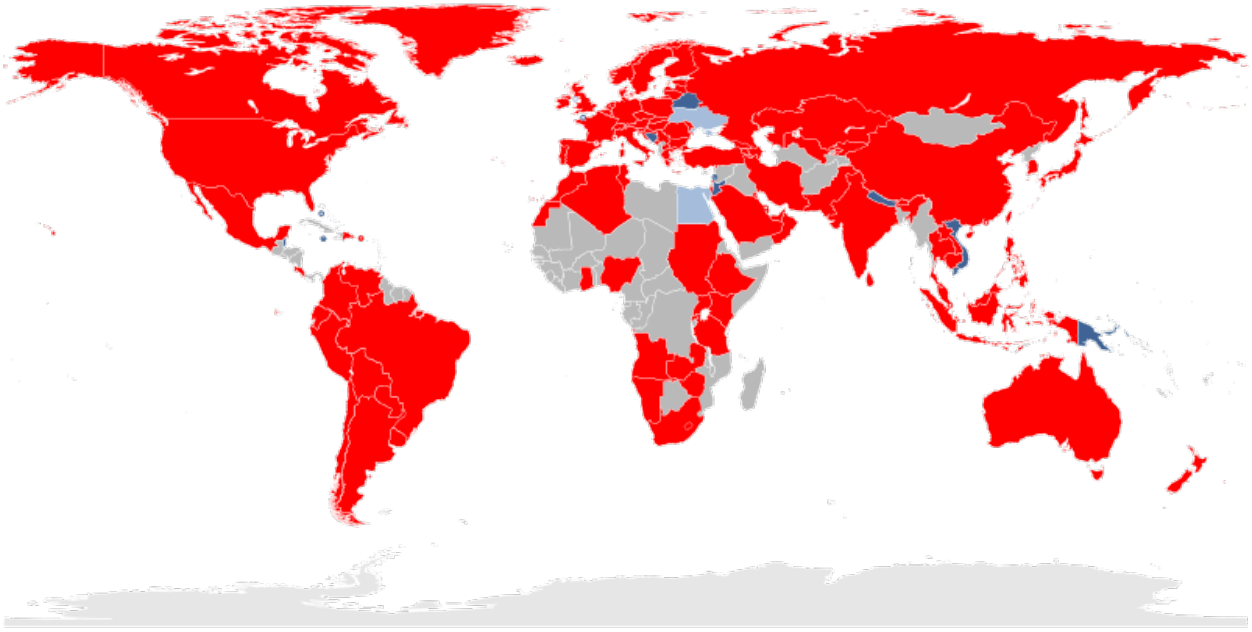


Figura 11: Lugares donde se ha adoptado la tecnología LTE (Julio 2017)

- En ROJO: Lugares con servicios de LTE comercial
- En AZUL: Lugares con despliegue de red LTE comercial en marcha o en proyecto
- En GRIS: Lugares donde se están ejecutando pruebas en sistemas LTE (pre-acuerdo inicial)

- Servicio basado en protocolos de Internet (IP)
- Interoperatividad con estándares inalámbricos existentes.
- Una velocidad de datos nominal de 100 Mbit/s, mientras que el usuario se mueve físicamente a altas velocidades relativas a la estación, y 1 Gbit/s, mientras que el usuario y la estación se encuentran en posiciones relativamente fijas. Simplificando, 100 Mb/s en movimiento y 1Gb/s en reposo.
- Uso y compartición dinámica de los recursos de la red para soportar más usuarios simultáneos por celda.
- Ancho de banda del canal escalable de 5–20 MHz, opcionalmente hasta 40 MHz.
- Diversas mejoras en el uso del espectro.

Nota: Para las comunicaciones inalámbricas 3G, la ITU ya había emitido unas especificaciones conocidas como IMT-2000.

7.3 Dispositivos

7.3.1 Antenas

Una antena es un dispositivo (**conductor metálico**) diseñado con el objetivo de **emitir o recibir ondas electromagnéticas** hacia el espacio libre. Una antena transmisora transforma voltajes en ondas electromagnéticas, y una receptora realiza la función inversa.

Existe una gran diversidad de tipos de antenas. En unos casos deben expandir en lo posible la potencia radiada, es decir, no deben ser directivas o direccionales (ejemplo: una emisora de radio comercial o una estación base de teléfonos móviles), otras veces deben serlo para canalizar la potencia en una dirección y no interferir a otros servicios (antenas entre estaciones de radioenlaces). También es una antena la que está integrada en la computadora portátil para conectarse a las redes Wi-Fi.

Diagramas de radiación

Es la representación gráfica de las características de radiación de una antena, en función de la dirección (coordenadas en azimut y elevación). Lo más habitual es **representar la densidad de potencia radiada**, aunque también se pueden encontrar diagramas de polarización o de fase. Atendiendo al diagrama de radiación, podemos hacer una clasificación general de los tipos de antena y podemos definir la **directividad de la antena (antena isotrópica, antena directiva, antena bidireccional, antena omnidireccional, . . .)**

Figura 12: Diagrama de radiación

Clases de antenas según su forma

Existen 4 tipos básicos de antenas:

- antenas de hilo,
- antenas de apertura (parabólica)
- antenas planas

Asimismo, las agrupaciones de estas antenas (arrays) se suelen considerar en la literatura como otro tipo básico de antena.

Antenas de hilo

Las antenas de hilo son antenas cuyos elementos radiantes son conductores de hilo que tienen una sección despreciable respecto a la longitud de onda de trabajo. Se utilizan extensamente en las bandas de MF, HF, VHF y UHF. Se pueden encontrar agrupaciones de antenas de hilo. Ejemplos de antenas de hilo son:

- El **monopolo** vertical
- El **dipolo** y su evolución, la antena Yagi
- La antena logarítmica, usada para televisión analógica

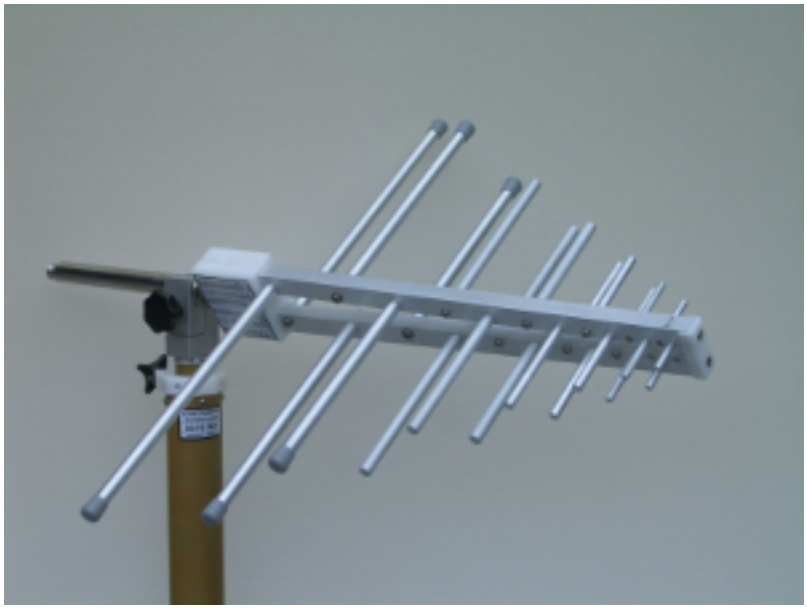


Figura 13: Antena logarítmica

- La antena espira
- La antena helicoidal es un tipo especial de antena que se usa principalmente en VHF y UHF. Un conductor describe una hélice, consiguiendo así una polarización circular.

Antenas de apertura

Las antenas de apertura son aquellas que utilizan superficies o aperturas para direccionar el haz electromagnético de forma que concentran la emisión y recepción de su sistema radiante en una dirección. **La más conocida y utilizada es la antena parabólica**, tanto en enlaces de radio terrestres como de satélite.

Hay varios tipos de antenas de apertura, como la antena de bocina, la antena parabólica, la antena parabólica del Radar Doppler y superficies reflectoras en general.

Antenas planas

Un tipo particular de antena plana son las antenas de apertura sintética, típicas de los radares de apertura sintética (SAR).

Antenas de Array

Las antenas de array están formadas por un conjunto de dos o más antenas idénticas distribuidas y ordenadas de tal forma que en su conjunto se comportan como una única antena con un diagrama de radiación propio.

La característica principal de los arrays de antenas es que su diagrama de radiación es modificable, pudiendo adaptarlo a diferentes aplicaciones/necesidades. Esto se consigue controlando de manera individual la amplitud y fase de la señal que alimenta a cada uno de los elementos del array.

Atendiendo a la distribución de las antenas que componen un array podemos hacer la siguiente clasificación:

- **Arrays lineales**: Los elementos están dispuestos sobre una línea.

- **Arrays planos**: Los elementos están dispuestos bidimensionalmente sobre un plano.
- **Arrays conformados**: Los elementos están dispuestos sobre una superficie curva.

7.3.2 Puntos de acceso (AP: Access Point)

Uso de canales

Existen 14 canales, aunque en Europa solo se utilizan 13.

Si deseamos crear una red Wi-Fi cuya cobertura esté soportada por varios puntos de acceso, deberemos de establecer los canales de los distintos puntos de acceso de forma que no se solapen. Canales Wi-Fi en 2,4 GHz

Por ello se recomienda utilizar los canales 1, 6 y 11. También pueden usarse 2, 7 y 12. Otra posibilidad son 3, 8 y 13.

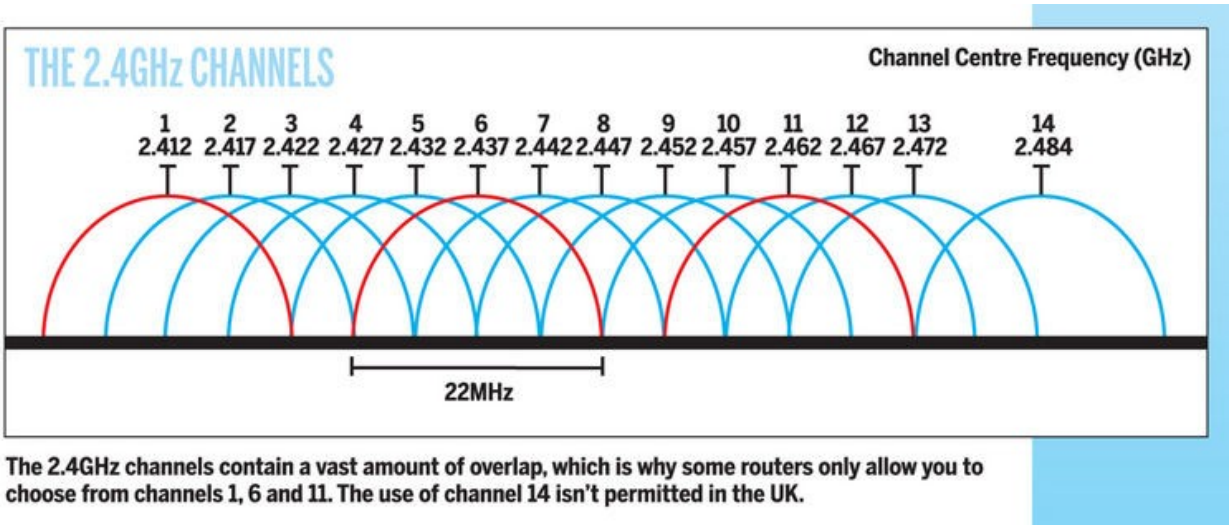
Modos básicos de funcionamiento

Un punto de acceso (AP) puede configurar de muchas maneras, según la funcionalidad que queramos proporcionarle. Los modos básicos son:

- Modo punto de acceso
- Modo repetidor
- Modo puente (bridge)

Modo Punto de Acceso

Canal	Frecuecia (MHz)	Norte America	Japón	Mayor parte del mundo
1	2412	Yes	Yes	Yes
2	2417	Yes	Yes	Yes
3	2422	Yes	Yes	Yes
4	2427	Yes	Yes	Yes
5	2432	Yes	Yes	Yes
6	2437	Yes	Yes	Yes
7	2442	Yes	Yes	Yes
8	2447	Yes	Yes	Yes
9	2452	Yes	Yes	Yes
10	2457	Yes	Yes	Yes
11	2462	Yes	Yes	Yes
12	2467	No	Yes	Yes
13	2472	No	Yes	Yes
14	2484	No	11b only	No



The 2.4GHz channels contain a vast amount of overlap, which is why some routers only allow you to choose from channels 1, 6 and 11. The use of channel 14 isn't permitted in the UK.

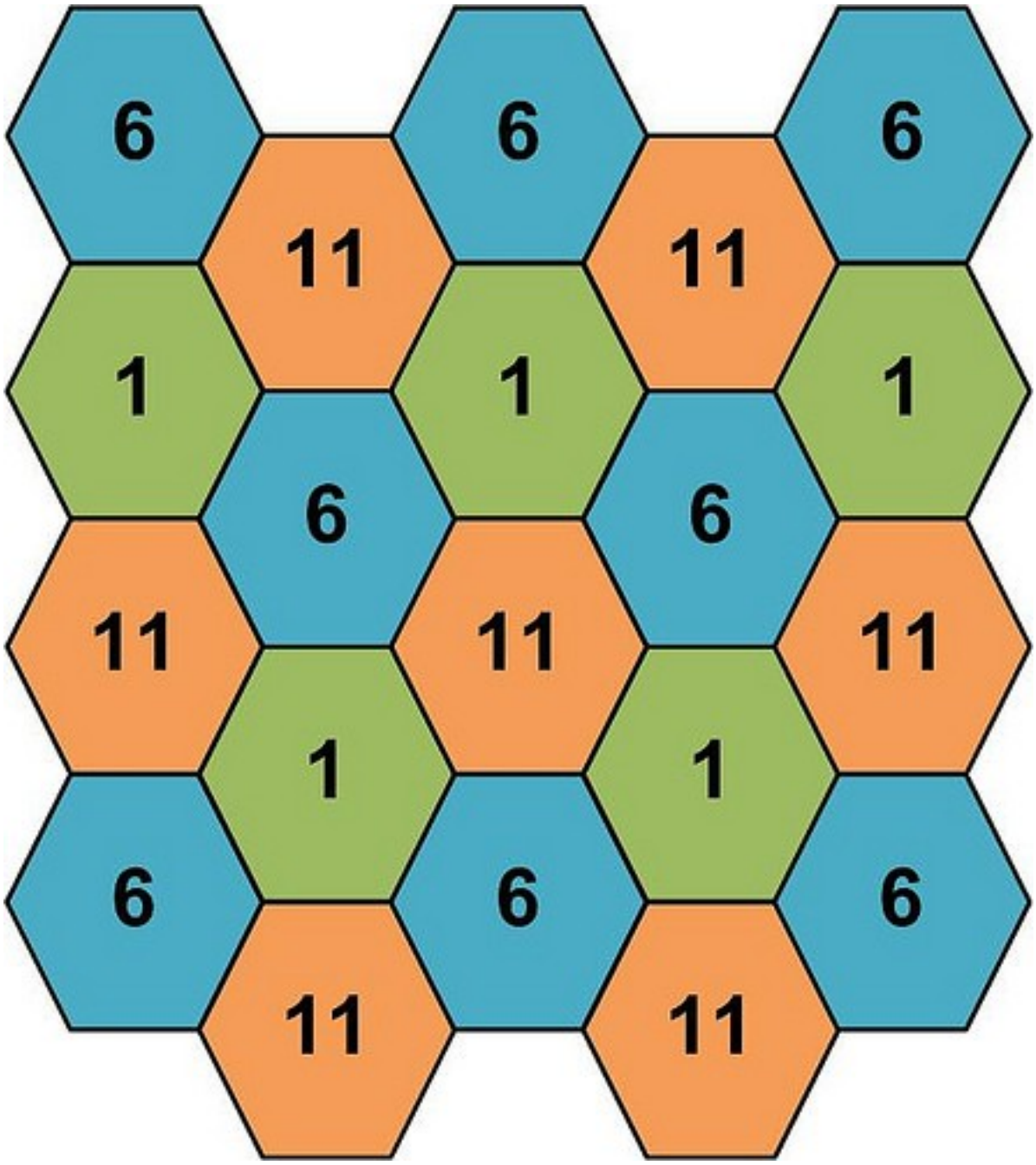


Figura 14: Topología celular con canales 1, 6 y 11

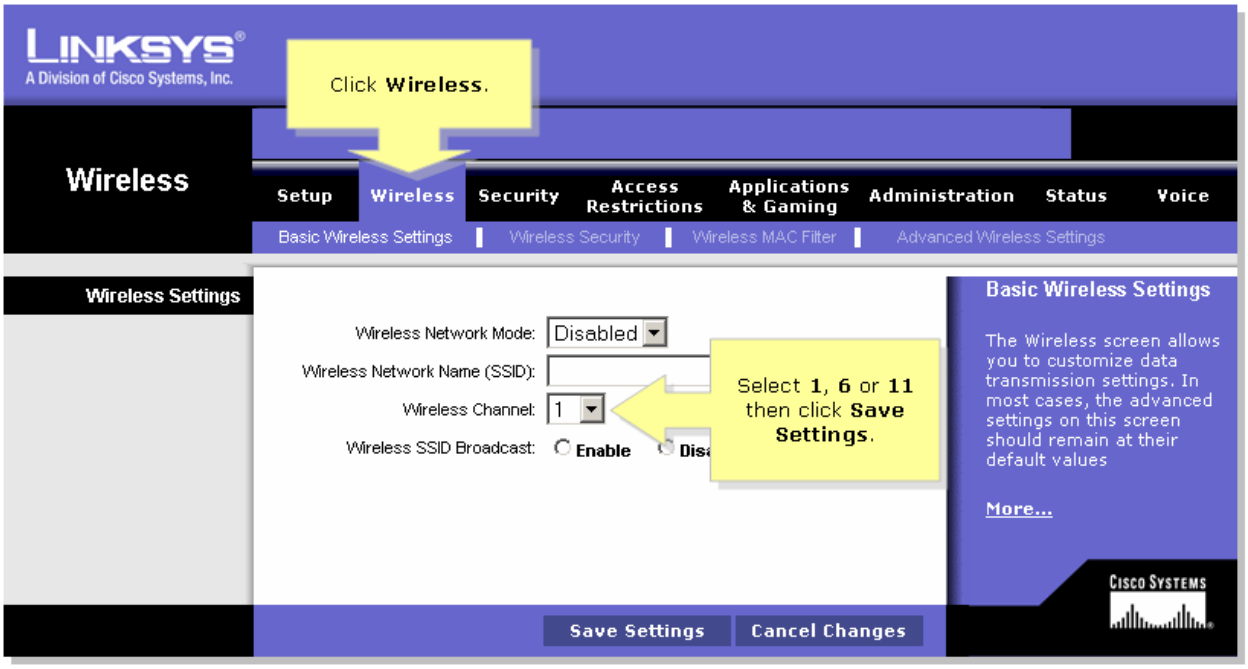


Figura 15: Selección de canal en un punto de acceso

En el modo de punto de acceso, los clientes deben utilizar el mismo SSID (nombre de red inalámbrica) y canal que el AP con el fin de conectarse. Si la seguridad inalámbrica está activada en el AP, será necesario que el cliente introduzca una contraseña para conectarse a la AP. En el modo de punto de acceso, múltiples clientes pueden conectarse al punto de acceso al mismo tiempo.

Modo Repetidor

En el modo de repetidor, el AP aumenta el alcance de la red inalámbrica mediante la ampliación de la cobertura inalámbrica de otro punto de acceso o router inalámbrico. Los puntos de acceso y router inalámbrico (si existiese) debe estar dentro del alcance del otro. Asegúrese de que todos los clientes, puntos de acceso y el router inalámbrico utilizan el mismo SSID (nombre de red inalámbrica) y el mismo canal.

Modo Puente (Bridge)

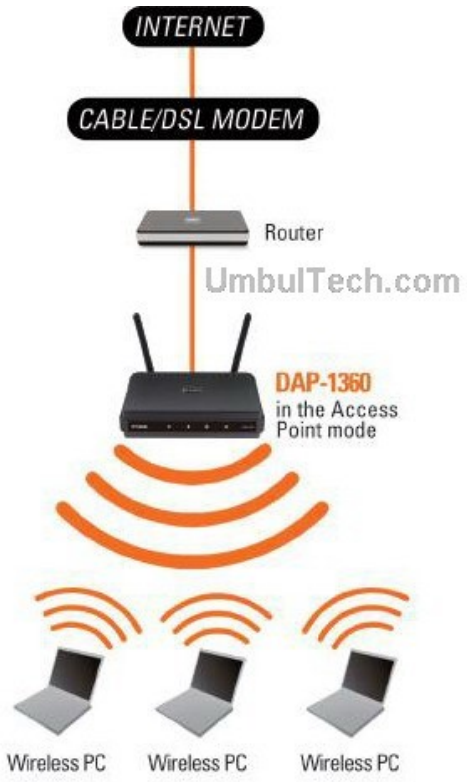
En el modo de puente, el AP se conectan dos LAN separadas que no pueden ser fácilmente conectadas entre sí mediante un cable. Por ejemplo, si hay dos LANs cableadas separadas por un pequeño patio, sería costoso enterrar los cables para la conexión entre las dos partes. Una mejor solución es utilizar dos AP para conectar de forma inalámbrica las dos LAN. En el modo de puente, ambas unidades AP no actuan como puntos de acceso.

Nota: El modo de puente no se especifica en los estándares Wi-Fi o IEEE. Este modo sólo funciona con dos unidades idénticas que soporten este modo. La comunicación con otros puntos de acceso (incluso de la misma marca) no está garantizada.

Interconexión de dispositivos inalámbricos

Existen dos modos:

- **Modo ad hoc (no se utiliza AP)**
- **Modo infraestructura**



Wireless PCs Using the DAP-1360 as a Central Connection Point

7.3.3 Routers inalámbricos

Actualmente en hogares y pequeñas oficinas se utiliza frecuentemente unos dispositivos de enrutamiento básico entre la red local e Internet. Son **routers** que disponen de varios puertos RJ45 dispuestos a modo de **switch** y una antena que hace la función de **punto de acceso**.

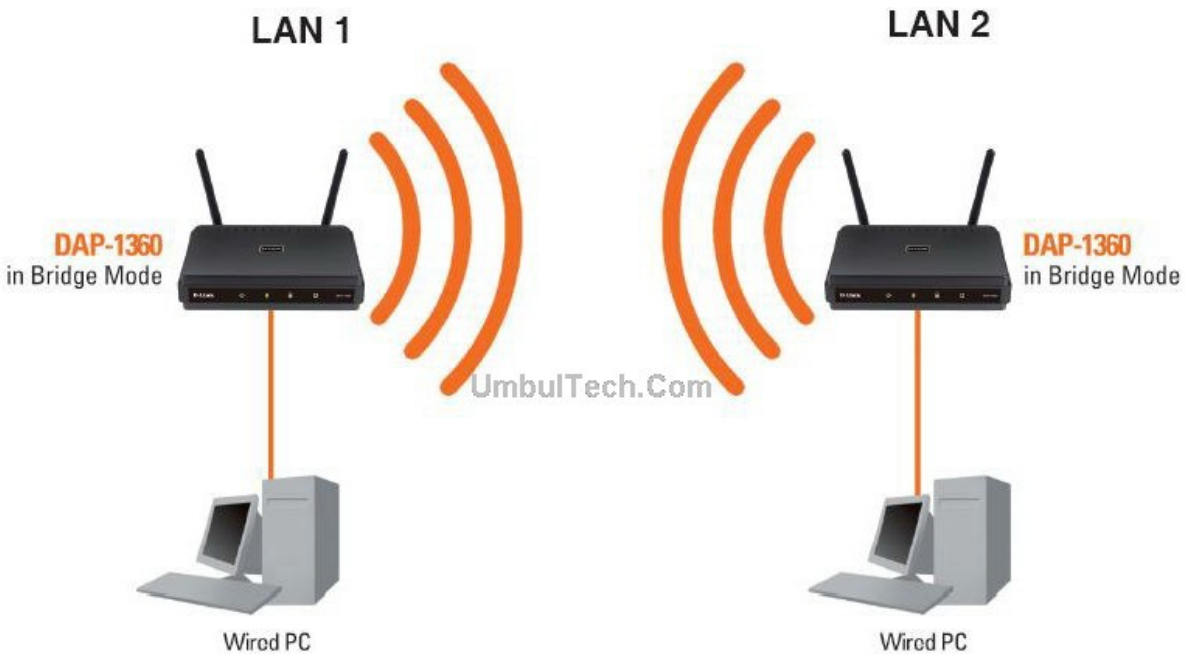
7.4 Referencias

- http://www.blogadder.info/2010/11/basic-guidelines-wireless-n-access.html
- http://recursostic.educacion.es/observatorio/web/es/cajon-de-sastre/38-cajon-de-sastre/961-monografico-redes-wifi
- http://www.xataka.com/moviles/que-es-lte

7.5 Actividades

1. Busca en Internet las siglas ISP e WISP. ¿Qué significan?
2. ¿Qué significan las siglas WPAN, WLAN, WMAN y WWAN? Pon un ejemplo de tecnología empleada en cada una de ellas.
3. Busca 3 dispositivos que tengan soporte para Bluetooth 4 de baja energía. Escribir sus características, foto y sito web de venta.


INTERNET
Wireless Router
DAP-1360
in Repeater Mode
UmbulTech.Com
Wireless PC
Wireless PC
Wireless PC



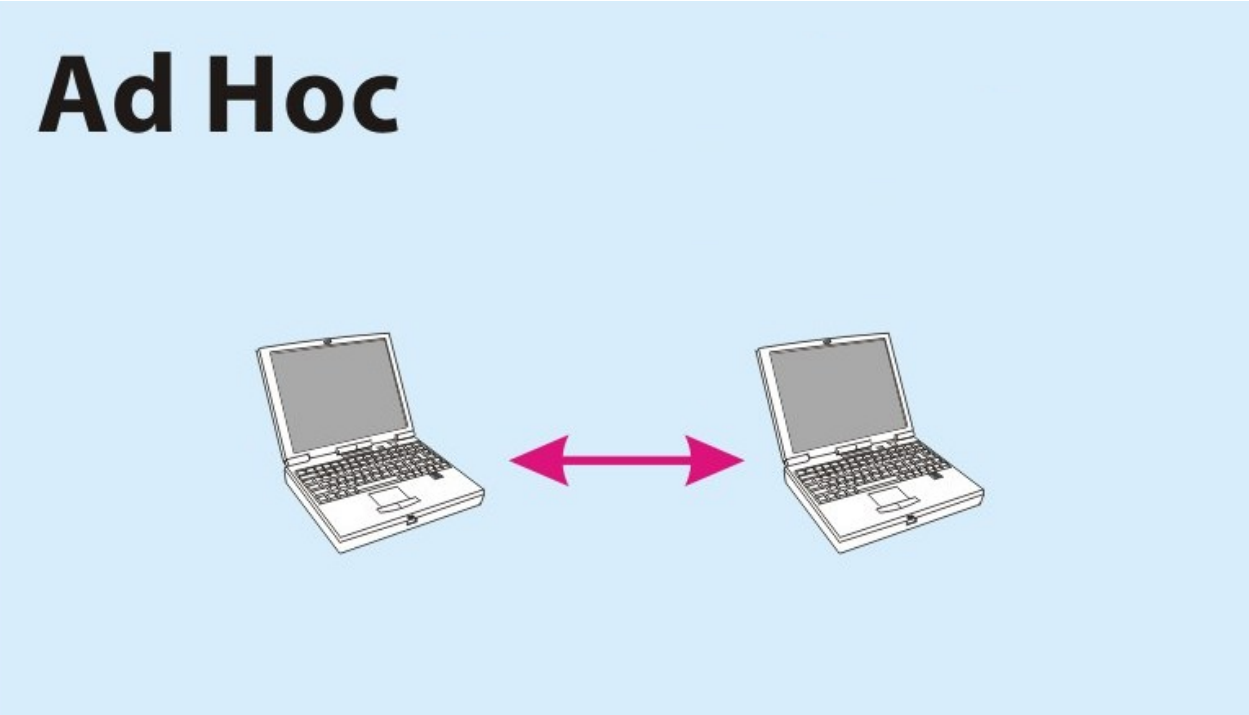


Figura 16: Modo ad hoc (no se utiliza AP)

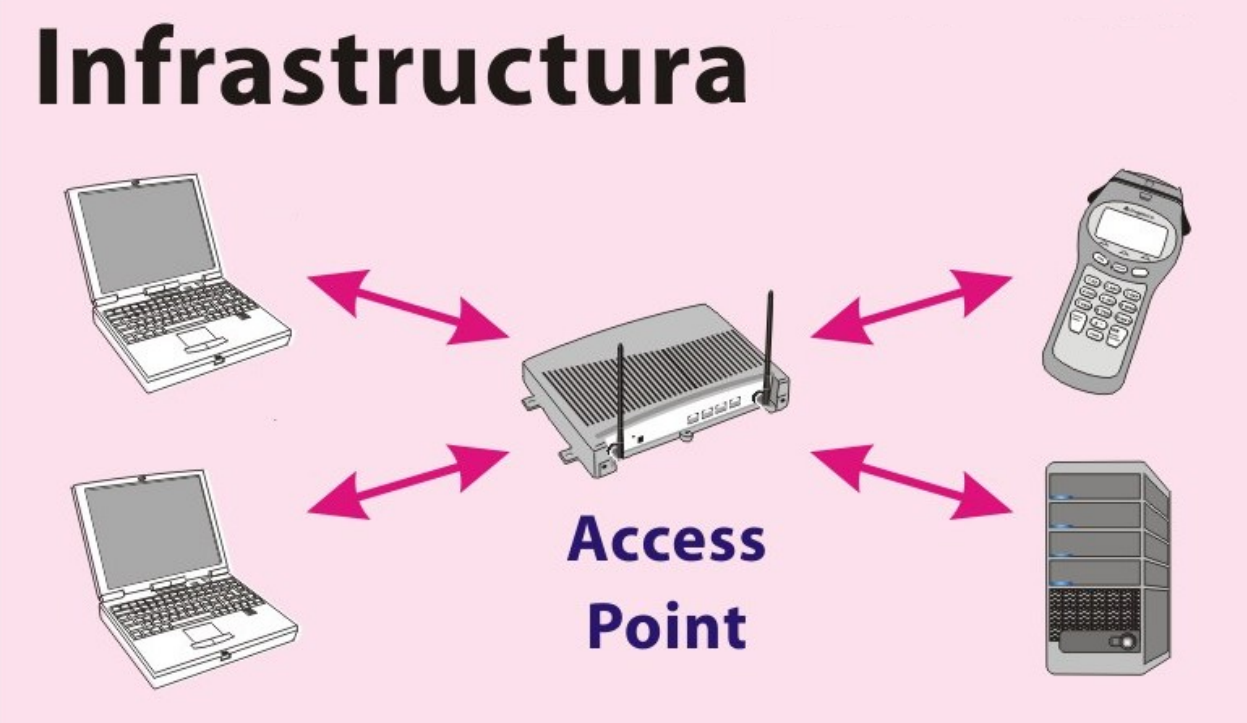


Figura 17: Modo infraestructura

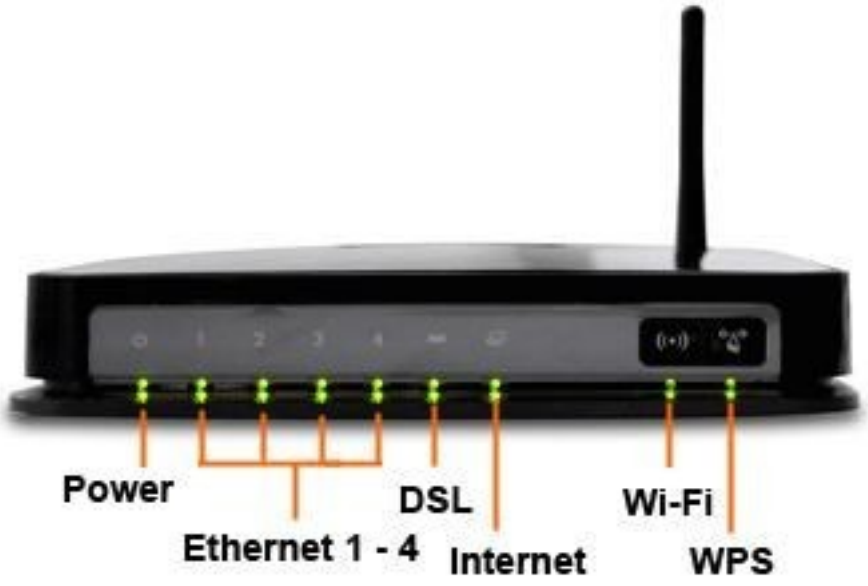


Figura 18: Router inalámbrico

4. Busca 3 teléfonos móviles con soporte 4G (LTE Advanced).
5. ¿Por qué al estándar IEEE 802.15.1 se le conoce también como Bluetooth? ¿Quién le puso dicho nombre?
6. ¿Por qué al estándar IEEE 802.11 se le conoce también como Wi-Fi? ¿Quién le puso dicho nombre?
7. Para redes WPAN, existe una tecnología conocida como UWB (UltraWideBand). Indica en que se diferencia de Bluetooth y qué aplicaciones tiene.
8. Explica cuáles son las ventajas e inconvenientes del uso de Wi-Fi frente a Ethernet.
9. Haz un esquema de una trama 802.11 y compárala con una trama 802.3.
10. Explica la técnica CSMA/CA y RTS/CTS.
11. Explica los distintos métodos de seguridad que implementan los puntos de acceso: cifrado, filtros, ...
12. Indica qué tipo y características de producto ofrecido en http://www.edimax.es/es/produce_detail.php?pd_id=348&pl1_id=3&pl2_id=73.
13. ¿Qué es WPS referido a Wi-Fi?
14. Es posible configurar un punto de acceso como puente y punto de acceso simultáneamente. Explica la respuesta.
15. Realiza una configuración Ad-hoc entre dos equipos inalámbricos. Indicar los pasos seguidos y realizar algunas capturas de pantalla.
16. Imagina que te dan un punto de acceso y te piden que lo configures. Indica los pasos que debes seguir para tener acceso a él.
17. Visita la página http://www.tp-link.com/en/support/emulators/ y elige 3 puntos de acceso. Para cada uno de ellos indica qué características soporta de las vistas este tema.

CAPÍTULO 8

LA CAPA DE RED

8.1 Conceptos generales

Internet no es un nuevo tipo de red física, sino un conjunto de tecnologías que permiten interconectar redes muy distintas entre sí. Internet no es dependiente de la máquina ni del sistema operativo utilizado. De esta manera, podemos transmitir información entre un servidor Unix y un ordenador que utilice Windows. O entre plataformas completamente distintas como Macintosh, Alpha o Intel. Es más: entre una máquina y otra generalmente existirán redes distintas: redes Ethernet, redes Token Ring e incluso enlaces vía satélite. Como vemos, está claro que no podemos utilizar ningún protocolo que dependa de una arquitectura en particular. Lo que estamos buscando es un método de interconexión general que sea válido para cualquier plataforma, sistema operativo y tipo de red. La familia de protocolos que se eligieron para permitir que **Internet** sea una **Red de redes** es TCP/IP. Nótese aquí que hablamos de familia de protocolos ya que son muchos los protocolos que la integran, aunque en ocasiones para simplificar hablemos sencillamente del protocolo TCP/IP.

El protocolo TCP/IP tiene que estar a un nivel superior del tipo de red empleado y funcionar de forma transparente en cualquier tipo de red. Y a un nivel inferior de los programas de aplicación (páginas WEB, correo electrónico...) particulares de cada sistema operativo. Todo esto nos sugiere el siguiente modelo de referencia:

- Capa de aplicación (HTTP, SMTP, FTP, TELNET...)
- Capa de transporte (UDP, TCP)
- Capa de red (IP)
- Capa de acceso a la red (Ethernet, Token Ring...)
- Capa física (cable coaxial, par trenzado...)

El nivel más bajo es la **capa física**. Aquí nos referimos al medio físico por el cual se transmite la información. Generalmente será un cable aunque no se descarta cualquier otro medio de transmisión como ondas o enlaces vía satélite.

La **capa de acceso a la red** determina la manera en que las estaciones (ordenadores) envían y reciben la información a través del soporte físico proporcionado por la capa anterior. Es decir, una vez que tenemos un cable, ¿cómo se transmite la información por ese cable? ¿Cuándo puede una estación transmitir? ¿Tiene que esperar algún turno o transmite sin

más? ¿Cómo sabe una estación que un mensaje es para ella? Pues bien, son todas estas cuestiones las que resuelve esta capa.

Las dos capas anteriores quedan a un nivel inferior del protocolo TCP/IP, es decir, no forman parte de este protocolo.

La **capa de red** define la forma en que un mensaje se transmite a través de distintos tipos de redes hasta llegar a su destino. El principal protocolo de esta capa es el IP aunque también se encuentran a este nivel los protocolos ARP, ICMP e IGMP. Esta capa proporciona el direccionamiento IP y determina la ruta óptima a través de los encaminadores (routers) que debe seguir un paquete desde el origen al destino.

La **capa de transporte** (protocolos TCP y UDP) ya no se preocupa de la ruta que siguen los mensajes hasta llegar a su destino. Sencillamente, considera que la comunicación extremo a extremo está establecida y la utiliza. Además añade la noción de puertos, como veremos más adelante.

Una vez que tenemos establecida la comunicación desde el origen al destino nos queda lo más importante, ¿qué podemos transmitir? La **capa de aplicación** nos proporciona los distintos servicios de Internet: correo electrónico, páginas Web, FTP, TELNET, ...

La familia de protocolos TCP/IP fue diseñada para permitir la interconexión entre distintas redes. El mejor ejemplo de interconexión de redes es Internet: se trata de un conjunto de redes unidas mediante **encaminadores o routers**. Un router es un dispositivo que separa 2 o más redes.

8.1.1 Concepto de capa de red

La capa de red se ocupa del control de la subred. La principal función de este nivel es la del **encaminamiento**, es decir, el tratamiento de cómo elegir la ruta más adecuada para que el bloque de datos del nivel de red (paquete) llegue a su destino. Cada destino está identificado univocamente en la subred por una dirección.

Otra función importante de esta capa es el **tratamiento de la congestión**. Cuando hay muchos paquetes en la red, unos obstruyen a los otros generando cuellos de botella en los puntos más sensibles. Un sistema de gestión de red avanzado evitará o paliará estos problemas de congestión.

Entre el emisor y el receptor se establecen comunicaciones utilizando protocolos determinados. El mismo protocolo debe estar representado tanto en el emisor como en el receptor.

El concepto de red está relacionado con las **direcciones IP** que se configuren en cada ordenador, no con el cableado. Es decir, si tenemos varias redes dentro del mismo cableado solamente los ordenadores que permanezcan a una misma red podrán comunicarse entre sí. Para que los ordenadores de una red puedan comunicarse con los de otra red es necesario que existan routers que interconecten las redes. Un **router** o encaminador no es más que **un ordenador con varias direcciones IP, una para cada red**, que permita el tráfico de paquetes entre sus redes.

La capa de red se encarga de fragmentar cada mensaje en paquetes de datos llamados **datagramas IP** y de enviarlos de forma independiente a través de la red de redes. Cada datagrama IP incluye un campo con la dirección IP de destino. Esta información se utiliza para enrutar los datagramas a través de las redes necesarias que los hagan llegar hasta su destino.

Nota: Cada vez que visitamos una página web o recibimos un correo electrónico es habitual atravesar un número de redes comprendido entre 10 y 20, dependiendo de la distancia de los hosts. El tiempo que tarda un datagrama en atravesar 20 redes (20 routers) suele ser inferior a 600 milisegundos.

La dirección IP es el identificador de cada host dentro de su red de redes. Cada host conectado a una red tiene una dirección IP asignada, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host. En el caso de Internet, no puede haber dos ordenadores con 2 direcciones IP (públicas) iguales. Pero sí podríamos tener dos ordenadores con la misma dirección IP siempre y cuando pertenezcan a redes independientes entre sí (sin ningún camino posible que las comunique).

Las direcciones IP se clasifican en:

- **Direcciones IP públicas**. Son visibles en todo Internet. Un ordenador con una IP pública es accesible (visible) desde cualquier otro ordenador conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.
- **Direcciones IP privadas (reservadas)**. Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por routers. Se utilizan en las empresas para los puestos de trabajo. Los ordenadores con direcciones IP privadas pueden salir a Internet por medio de un router (o proxy) que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a ordenadores con direcciones IP privadas.

A su vez, las direcciones IP pueden ser:

- **Direcciones IP estáticas (fijas)**. Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas.
- **Direcciones IP dinámicas**. Un host que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un módem. Los proveedores de Internet utilizan direcciones IP dinámicas debido a que tienen más clientes que direcciones IP (es muy improbable que todos se conecten a la vez).

Las direcciones IP están formadas por 4 bytes (32 bits). Se suelen representar de la forma a.b.c.d donde cada una de estas letras es un número comprendido **entre el 0 y el 255**. Por ejemplo la dirección IP del servidor de IBM (www.ibm.com) es 129.42.18.99.

Las direcciones IP se pueden representar

- en **decimal** (lo habitual), desde **0.0.0.0** hasta **255.255.255.255**
- en **hexadecimal**, desde **00.00.00.00** hasta **FF.FF.FF.FF**
- en **binario**, desde **00000000.00000000.00000000.00000000** hasta **11111111.11111111.11111111.11111111**

Las tres direcciones siguientes representan a la misma máquina (podemos utilizar una calculadora científica para realizar las conversiones).

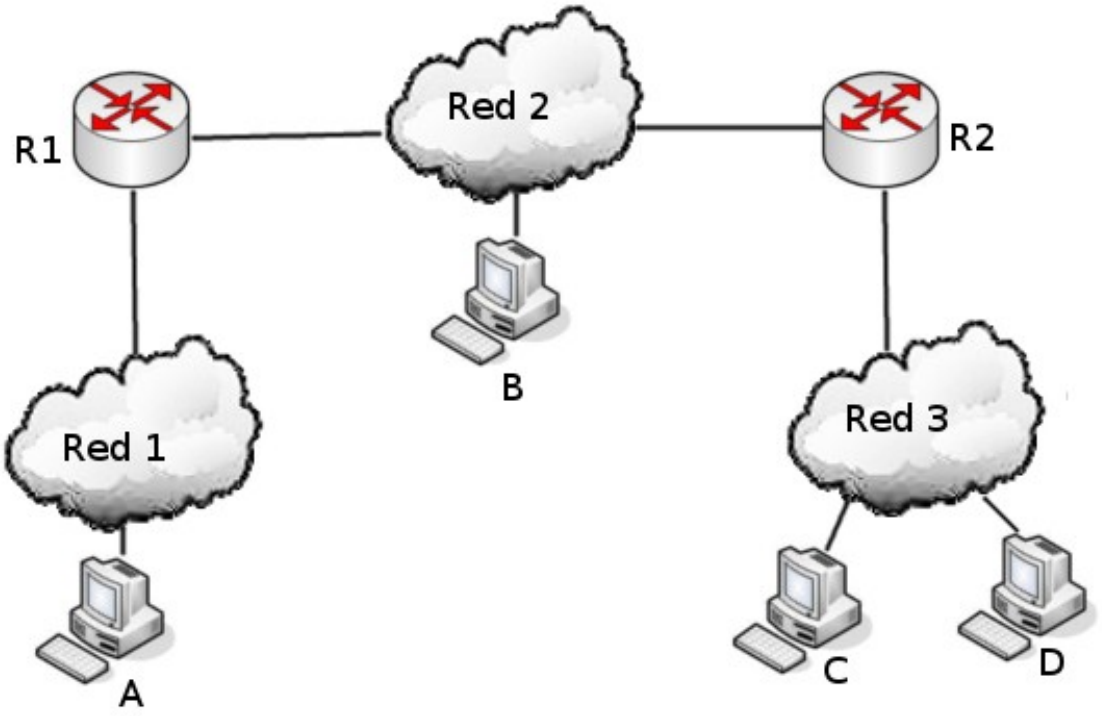
- decimal: 128.10.2.30
- hexadecimal: 80.0A.02.1E
- binario: 10000000.00001010.00000010.00011110

Ejemplo

En una red TCP/IP es posible tener, por ejemplo, servidores web y servidores de correo para uso interno. Obsérvese que todos los servicios de Internet se pueden configurar en pequeñas redes internas TCP/IP.

A continuación veremos un ejemplo de interconexión de 3 redes. Cada host (ordenador) tiene una dirección física que viene determinada por su adaptador de red. Estas direcciones se corresponden con la capa de acceso al medio y se utilizan para comunicar dos ordenadores que pertenecen a la misma red. Para identificar globalmente un ordenador dentro de un conjunto de redes TCP/IP se utilizan las direcciones IP (capa de red). Observando una dirección IP sabremos si pertenece a nuestra propia red o a una distinta (todas las direcciones IP de la misma red comienzan con los mismos números, según veremos más adelante).

Host	Red	Dirección IP	Dirección física
A	Red 1	192.168.0.10	00-60-52-0B-B7-7D
R1		192.168.0.1	00-E0-4C-AB-9A-FF
	Red 2	10.10.0.1	A3-BB-05-17-29-D0
B		10.10.0.7	00-E0-4C-33-79-AF
R2		10.10.0.2	B2-42-52-12-37-BE
	Red 3	200.3.107.1	00-E0-89-AB-12-92
C		200.3.107.73	A3-BB-08-10-DA-DB
D		200.3.107.200	B2-AB-31-07-12-93



En el ejemplo anterior, supongamos que el ordenador 200.3.107.200 (D) envía un mensaje al ordenador con 200.3.107.73 (C). Como ambas direcciones comienzan con los mismos números, D sabrá que ese ordenador se encuentra dentro de su propia red y el mensaje se entregará de forma directa. Sin embargo, si el ordenador 200.3.107.200 (D) tuviese que comunicarse con 10.10.0.7 (B), D advertiría que el ordenador destino no pertenece a su propia red y enviaría el mensaje al router R2 (es el ordenador que le da salida a otras redes). El router entregaría el mensaje de forma directa porque B se encuentra dentro de una de sus redes (la Red 2).

8.1.2 Direcciones IP

¿Quién reparte las direcciones IP?

En un principio se encargó de ello el IANA (Internet Assigned Numbers Authority). Actualmente tanto las direcciones como los nombres son administrados por la **ICANN**.

La **Corporación de Internet para la Asignación de Nombres y Números** (en inglés: Internet Corporation for Assigned Names and Numbers; ICANN) es una organización sin fines de lucro creada el 18 de septiembre de 1998 con objeto de encargarse de cierto número de tareas realizadas con anterioridad a esa fecha por otra organización, la IANA. Su sede radica en California y está sujeta a las leyes de dicho Estado.

ICANN es una organización que opera a nivel multinacional/internacional) y es la responsable de asignar las direcciones del protocolo IP, de los identificadores de protocolo, de las funciones de gestión del sistema de dominio y de la administración del sistema de servidores raíz.

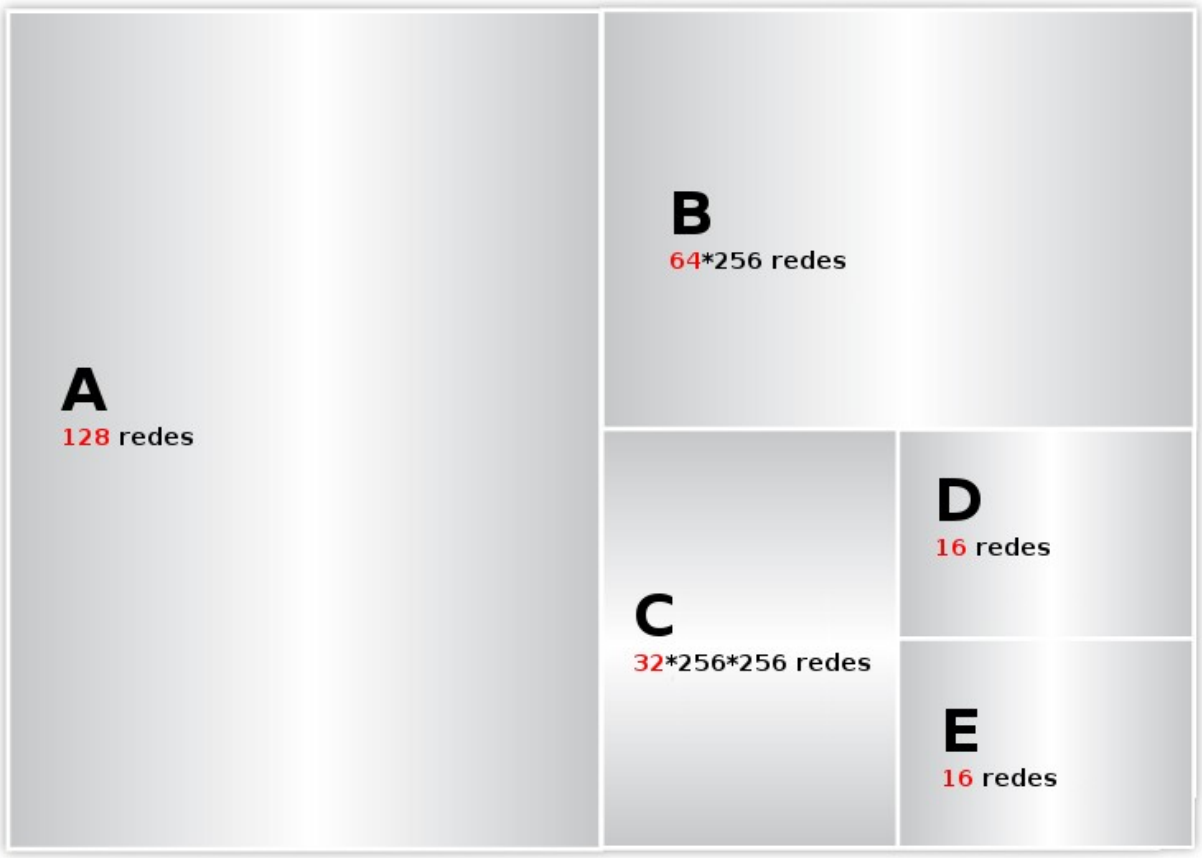
La ICANN (Corporación de Internet para la Asignación de Nombres y Números) delega los recursos de Internet a los **RIRs**, y a su vez los RIRs siguen sus políticas regionales para una posterior subdelegación de recursos a sus clientes, que incluyen Proveedores de servicios y organizaciones para uso propio.

Un **Registro Regional de Internet o Regional Internet Registry (RIR)** es una organización que supervisa la asignación y el registro de recursos de números de Internet dentro de una región particular del mundo. Los recursos incluyen direcciones IP (tanto IPv4 como IPv6) y números de sistemas autónomos (para su uso en encaminamiento BGP).

Hay actualmente 5 RIRs en funcionamiento:

- American Registry for Internet Numbers (**ARIN**) para América Anglosajona.
- RIPE Network Coordination Centre (**RIPE NCC**) para Europa, el Oriente Medio y Asia Central.
- Asia-Pacific Network Information Centre (**APNIC**) para Asia y la Región Pacífica.
- Latin American and Caribbean Internet Address Registry (**LACNIC**) para América Latina y el Caribe.
- African Network Information Centre (**AfriNIC**) para África

¿Cómo se reparten las direcciones IPv4?



Existen un total de 3^{32} direcciones IP (4.294.967.296).

- La mitad (2.147.483.648) están destinadas a redes de clase A: (16.777.216 IPs por cada una de las 128 redes de clase A).
- Un cuarto (1.073.741.824) están destinadas a redes de clase B: (65.536 IPs por cada una de las 16.384 redes de clase B).
- Un octavo (536.870.912) están destinadas a redes de clase C: (256 IPs por cada una de las 2.097.152 redes de clase C)
- Un dieciseisavo (268.435.456) están destinadas la clase D (Multicast).
- Otro dieciseisavo (268.435.456) están destinadas a la clase E (Experimental).

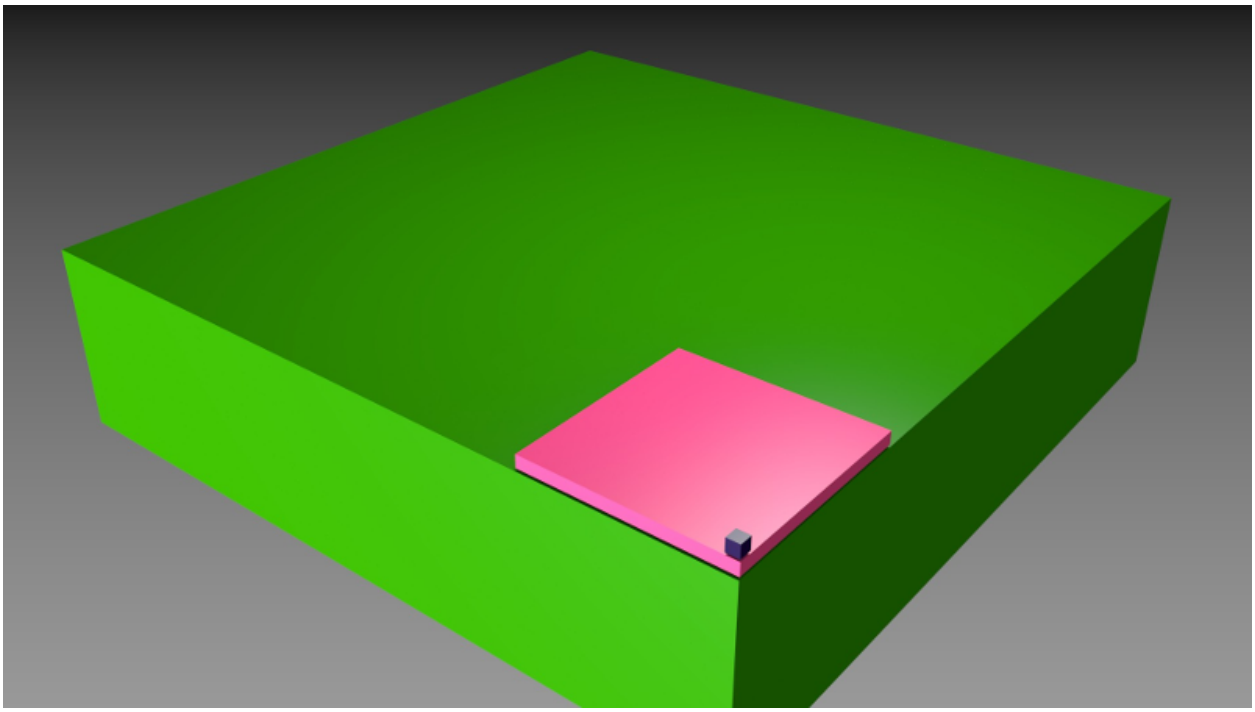


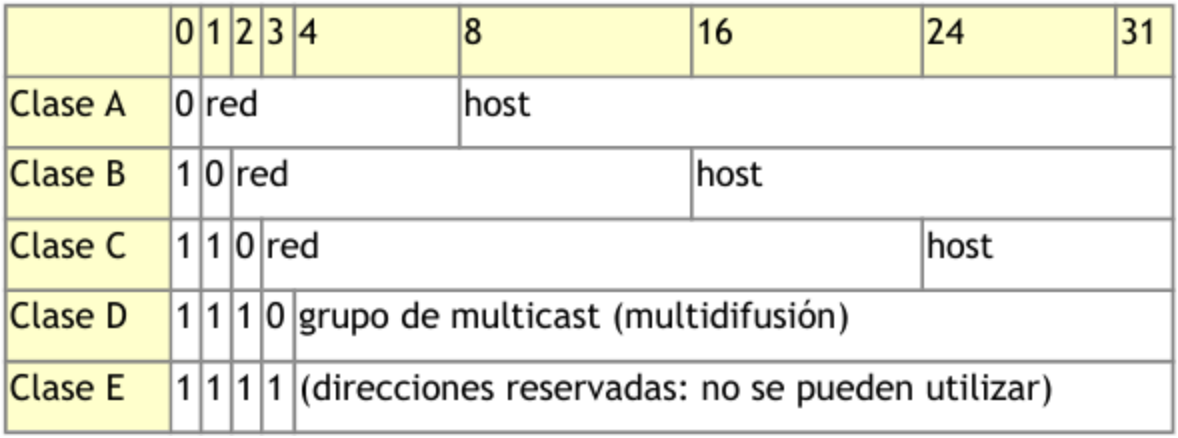
Figura 1: Tamaño relativo de cada clase.
Clase C: (**256 IPs**).Arriba Clase B: (**65.536 IPs**). En medio Clase A: (**16.777.216 IPs**). Abajo

Clases

¿Cuántas direcciones IP existen? Si calculamos 2 elevado a 32 obtenemos más de 4000 millones de direcciones distintas. Sin embargo, no todas las direcciones son válidas para asignarlas a hosts. Las direcciones IP no se encuentran aisladas en Internet, sino que pertenecen siempre a alguna red. Todas las máquinas conectadas a una misma red se caracterizan en que los primeros bits de sus direcciones son iguales. De esta forma, las direcciones se dividen conceptualmente en dos partes:

- el identificador de red
- el identificador de host.

Dependiendo del número de hosts que se necesiten para cada red, las direcciones de Internet se han dividido en las **clases primarias A, B y C**. La **clase D** está formada por direcciones que identifican no a un host, sino a un grupo de ellos. Las direcciones de **clase E** no se pueden utilizar (están reservadas).



	0	1	2	3	4	8	16	24	31
Clase A	0	red				host			
Clase B	1	0	red				host		
Clase C	1	1	0	red				host	
Clase D	1	1	1	0	grupo de multicast (multidifusión)				
Clase E	1	1	1	1	(direcciones reservadas: no se pueden utilizar)				

–

Clase	Formato(r=red, h=host)	Nº de redes	Nº de hosts por red	Rango de direcciones de redes	Máscara de subred
A	r.h.h.h	128	16.777.214	0.0.0.0 - 127.0.0.0	255.0.0.0
B	r.r.h.h	16.384	65.534	128.0.0.0 - 191.255.0.0	255.255.0.0
C	r.r.r.h	2.097.152	254	192.0.0.0 - 223.255.255.0	255.255.255.0
D	grupo	▪	▪	224.0.0.0 - 239.255.255.255	▪
E	no válidas	▪	▪	240.0.0.0 - 255.255.255.255	▪

Nota: Las direcciones usadas en Internet están definidas en la RFC 1166

Nota:

Difusión (broadcast) y multidifusión (multicast) El término difusión (broadcast) se refiere a todos los hosts de una red; multidifusión (multicast) se refiere a varios hosts (aquellos que se hayan suscrito dentro de un mismo grupo). Siguiendo esta misma terminología, en ocasiones se utiliza el término unidifusión para referirse a un único host.

Direcciones IP especiales y reservadas

No todas las direcciones comprendidas entre la 0.0.0.0 y la 223.255.255.255 son válidas para un host: algunas de ellas tienen significados especiales. Las **principales direcciones especiales** se resumen en la siguiente tabla. Su interpretación depende del host desde el que se utilicen.

Bits de red	Bits de host	Significado	Ejemplo
todos 0		Mi propio host	0.0.0.0
todos 0	host	Host indicado dentro de mi red	0.0.0.10
red	todos 0	Red indicada	192.168.1.0
todos 1		Difusión a internet. Se acota a mi red.	255.255.255.255
red	todos 1	Difusión a la red indicada	192.168.1.255
127	cualquier valor válido	Loopback (mi propio host)	127.0.0.1

OBSERVACIONES:

- La red 0 y la red 127 (ambas de clase A) son especiales. Perdemos nada menos que 2*16.777.216 IPs que no pueden asignarse a ningún host concreto.
- En cada red existen 2 direcciones especiales: la primera del rango (dirección de red) y la última del rango (dirección de broadcast). Por tanto si tenemos la red 192.168.0.x con 256 IPs, sólo pueden destinarse a hosts 254 direcciones (192.168.0.0 es la dirección de red y 192.168.0.255 es la dirección de broadcast)

Difusión o broadcasting es el envío de un mensaje a todos los ordenadores que se encuentran en una red. La dirección de loopback (normalmente 127.0.0.1) se utiliza para comprobar que los protocolos TCP/IP están correctamente instalados en nuestro propio ordenador. Lo veremos más adelante, al estudiar el comando PING.

Las direcciones de redes siguientes se encuentran **reservadas para su uso en redes privadas (intranets)**. Una dirección IP que pertenezca a una de estas redes se dice que es una dirección IP privada.

Clase	Rango de direcciones privadas de redes
A	**10**.0.0.0
B	**172.16**.0.0 - **172.31**.0.0
C	**192.168.0**.0 - **192.168.255**.0

Los anteriores rangos vienen especificados en el RFC 1918.

Ademas según el RFC 3330, se reserva la red **169.254**.0.0 para el uso de link-local, más conocido como **APIPA** (Automatic Private Internet Protocol Addressing - Direccionamiento Privado Automático del Protocolo de Internet). Este sistema es usado por sistemas Windows cuando no detectan la presencia de ningún servidor DHCP.

Por ejemplo, si estamos construyendo una red privada con un número de ordenadores no superior a 254 podemos utilizar una red reservada de clase C. Al primer ordenador le podemos asignar la dirección 192.168.23.1, al segundo 192.168.23.2 y así sucesivamente hasta la 192.168.23.254. Como estamos utilizando direcciones reservadas, tenemos la garantía de que no habrá ninguna máquina conectada directamente a Internet con alguna de nuestras direcciones. De esta manera, no se producirán conflictos y desde cualquiera de nuestros ordenadores podremos acceder a la totalidad de los servidores de Internet (si utilizásemos en un ordenador de nuestra red una dirección de un servidor de Internet, nunca podríamos acceder a ese servidor).

Definiciones

Intranet Red privada que utiliza los protocolos TCP/IP. Puede tener salida a Internet o no. En el caso de tener salida a Internet, el direccionamiento IP permite que los hosts con direcciones IP privadas puedan salir a Internet pero impide el acceso a los hosts internos desde Internet. Dentro de una intranet se pueden configurar todos los servicios típicos de Internet (web, correo, mensajería instantánea, etc.) mediante la instalación de los correspondientes servidores. La idea es que las intranets son como «internets» en miniatura o lo que es lo mismo, Internet es una intranet pública gigantesca.

Extranet Unión de dos o más intranets. Esta unión puede realizarse mediante líneas dedicadas (RDSI, X.25, frame relay, punto a punto, etc.) o a través de Internet.

Internet La mayor red pública de redes TCP/IP.

CASO PRÁCTICO

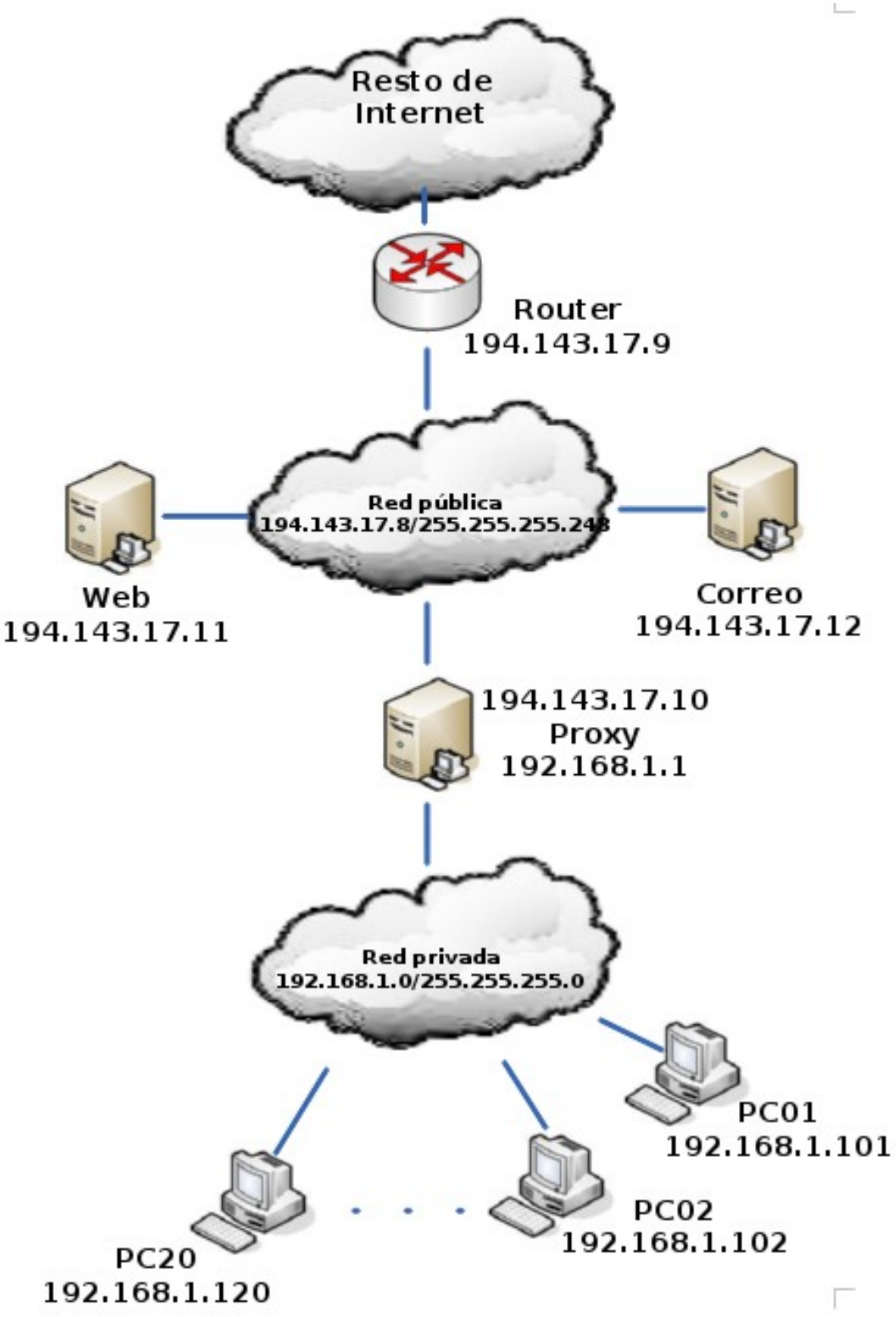
Una empresa dispone de una línea frame relay con direcciones públicas contratadas desde la 194.143.17.8 hasta la 194.143.17.15 (la dirección de la red es 194.143.17.8, su dirección de broadcasting 194.143.17.15 y su máscara de red 255.255.255.248). La línea frame relay está conectada a un router. Diseñar la red para:

- 3 servidores (de correo, web y proxy)
- 20 puestos de trabajo

Los 20 puestos de trabajo utilizan direcciones IP privadas y salen a Internet a través del Proxy. En la configuración de red de cada uno de estos 20 ordenadores se indicará la dirección «192.168.1.1» en el cuadro «Puerta de enlace». La puerta de enlace (puerta de salida o gateway) es el ordenador de nuestra red que nos permite salir a otras redes. El Proxy tiene dos direcciones IP, una de la red privada y otra de la red pública. Su misión es dar salida a Internet a la red privada, pero no permitir los accesos desde el exterior a la zona privada de la empresa.

Los 3 servidores y el router utilizan direcciones IP públicas, para que sean accesibles desde cualquier host de Internet. La puerta de enlace de Proxy, Correo y Web es 194.143.17.9 (Router).

Obsérvese que **la primera y última dirección de todas las redes son direcciones IP especiales que no se pueden utilizar para asignarlas a hosts. La primera es la dirección de la red y la última, la dirección de difusión o broadcasting**. La máscara de subred de cada ordenador se ha indicado dentro de su red después de una barra: PC1, PC2, ... , PC20 y Proxy (para su IP 192.168.1.1) tienen la máscara 255.255.255.0 y Router, Web, Correo y Proxy (para su IP 194.143.17.10), la máscara 255.255.255.248. El concepto de máscara de subred se estudia a continuación.


Resto de Internet
Router
194.143.17.9
Red pública
194.143.17.8/255.255.255.248
Web
194.143.17.11
Correo
194.143.17.12
194.143.17.10
Proxy
192.168.1.1
Red privada
192.168.1.0/255.255.255.0
PC01
192.168.1.101
PC02
192.168.1.102
PC20
192.168.1.120

8.1.3 Máscara de red y subred

Una máscara de subred es aquella dirección que enmascarando nuestra dirección IP, nos indica si otra dirección IP pertenece a nuestra subred o no.

La siguiente tabla muestra las máscaras de subred correspondientes a cada clase:

Clase	Máscara de subred
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Si expresamos la máscara de subred de clase A en notación binaria, tenemos:

11111111.00000000.00000000.00000000

Los unos indican los bits de la dirección correspondientes a la red y los ceros, los correspondientes al host. Según la máscara anterior, el primer byte (8 bits) es la red y los tres siguientes (24 bits), el host. Por ejemplo, la dirección de clase A 35.120.73.5 pertenece a la red 35.0.0.0.

Supongamos una subred con máscara 255.255.0.0, en la que tenemos un ordenador con dirección 148.120.33.110. Si expresamos esta dirección y la de la máscara de subred en binario, tenemos:

```
148.120.33.110      10010100.01111000.00100001.01101110 (dirección de una máquina)
255.255.0.0         11111111.11111111.00000000.00000000 (dirección de su máscara de␣
↪red)
148.120.0.0         10010100.01111000.00000000.00000000 (dirección de su subred)
                    <-------RED------> <------HOST------>
```

Al hacer el producto binario de las dos primeras direcciones (donde hay dos 1 en las mismas posiciones ponemos un 1 y en caso contrario, un 0) obtenemos la tercera.

Si hacemos lo mismo con otro ordenador, por ejemplo el 148.120.33.89, obtenemos la misma dirección de subred. Esto significa que ambas máquinas se encuentran en la misma subred (la subred 148.120.0.0).

```
148.120.33.89     10010100.01111000.00100001.01011001 (dirección de una máquina)
255.255.0.0       11111111.11111111.00000000.00000000 (dirección de su máscara de red)
148.120.0.0       10010100.01111000.00000000.00000000 (dirección de su subred)
```

En cambio, si tomamos la 148.115.89.3, observamos que no pertenece a la misma subred que las anteriores.

```
148.115.89.3     10010100.01110011.01011001.00000011 (dirección de una máquina)
255.255.0.0      11111111.11111111.00000000.00000000 (dirección de su máscara de red)
148.115.0.0      10010100.01110011.00000000.00000000 (dirección de su subred)
```

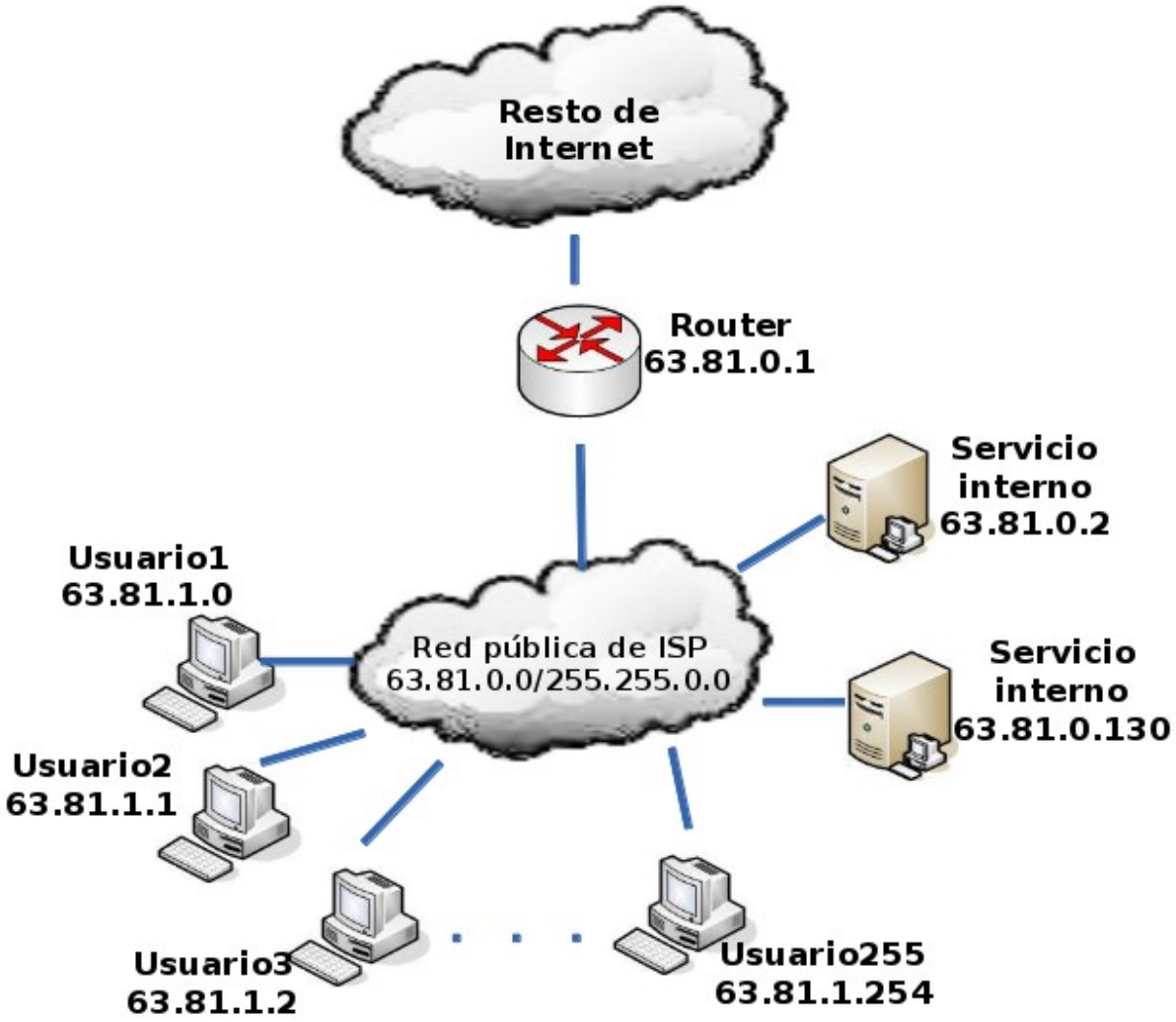
Cálculo de la dirección de difusión.– Ya hemos visto que el producto lógico binario (AND) de una IP y su máscara devuelve su dirección de red. Para calcular su dirección de difusión, hay que hacer la suma lógica en binario (OR) de la IP con el inverso (NOT) de su máscara.

En una red de redes TCP/IP no puede haber hosts aislados: todos pertenecen a alguna red y todos tienen una dirección IP y una máscara de subred (si no se especifica se toma la máscara que corresponda a su clase). Mediante esta máscara un ordenador sabe si otro ordenador se encuentra en su misma subred o en otra distinta. Si pertenece a su misma subred, el mensaje se entregará directamente. En cambio, si los hosts están configurados en redes distintas, el mensaje se enviará a la puerta de salida o router de la red del host origen. Este router pasará el mensaje al siguiente de la cadena y así sucesivamente hasta que se alcance la red del host destino y se complete la entrega del mensaje.

EJEMPLO

Los proveedores de Internet habitualmente disponen de una o más redes públicas para dar acceso a los usuarios que se conectan por módem. El proveedor va cediendo estas direcciones públicas a sus clientes a medida que se conectan y liberándolas según se van desconectando (direcciones dinámicas). Supongamos que cierto **ISP (proveedor de servicios de Internet)** dispone de la red 63.81.0.0 con máscara 255.255.0.0. Para uso interno utiliza las direcciones que comienzan por 63.81.0 y para ofrecer acceso a Internet a sus usuarios, las direcciones comprendidas entre la 63.81.1.0 hasta la 63.81.1.254 (las direcciones 63.81.0.0 y 63.81.255.255 están reservadas).

Si un usuario conectado a la red de este ISP tiene la dirección 63.81.1.1 y quiere transferir un archivo al usuario con IP 63.81.1.2, el primero advertirá que el destinatario se encuentra en su misma subred y el mensaje no saldrá de la red del proveedor (no atravesará el router).



Las máscaras 255.0.0.0 (clase A), 255.255.0.0 (clase B) y 255.255.255.0 (clase C) suelen ser suficientes para la mayoría de las redes privadas. Sin embargo, las redes más pequeñas que podemos formar con estas máscaras son de 254 hosts y para el caso de direcciones públicas, su contratación tiene un coste muy alto. Por esta razón suele ser habitual dividir las redes públicas de clase C en subredes más pequeñas. A continuación se muestran las posibles divisiones de una red de clase C. **La división de una red en subredes se conoce como subnetting**.

Máscara de subred	Bina-rio	Nº de su-bredes	Nº de hosts por subred	Ejemplos de subredes (x=a.b.c por ejem-plo, 192.168.1)
255.255.255.**0**	00000000	**1**	254	x.0
255.255.255.**128**	10000000	**2**	126	x.0, x.128
255.255.255.**192**	11000000	**4**	62	x.0, x.64, x.128, x.192
255.255.255.**223**	11100000	**8**	30	x.0, x.32, x.64, x.96, x.128, ...
255.255.255.**240**	11110000	**16**	14	x.0, x.16, x.32, x.48, x.64, ...
255.255.255.**248**	11111000	**32**	6	x.0, x.8, x.16, x.24, x.32, x.40, ...
255.255.255.**252**	11111100	**64**	2	x.0, x.4, x.8, x.12, x.16, x.20, ...
255.255.255.**254**	11111110	128	0	ninguna posible
255.255.255.**255**	11111111	256	0	ninguna posible

Obsérvese que en el caso práctico que explicamos un poco más arriba se utilizó la máscara 255.255.255.248 para crear una red pública con 6 direcciones de hosts válidas (la primera y última dirección de todas las redes se excluyen). Las máscaras con bytes distintos a 0 o 255 también se pueden utilizar para particionar redes de clase A o de clase B. Por ejemplo, la máscara 255.255.192.0 dividiría una red de clase B en 4 subredes de 16382 hosts (2 elevado a 14, menos 2) cada una.

8.1.4 Configuración de clientes

Supongamos que deseamos configurar el soporte de red para el equipo que viene en el siguiente esquema. Para ello debemos de establecer los siguientes parámetros:

- Dirección IP
- Máscara de red
- **Puerta de enlace**
- Servidores de resolución de nombres (DNS)

Normalmente estos parámetros son configurados dinámicamente mediante DHCP por el Router de salida.

No obstante también es posible su configuración de forma manual.

Enrutamiento en el cliente

Un parámetro de importancia capital en una intranet es la configuración de la ruta por defecto en los clientes, que les permitirá salir a Internet. Para cada cliente deberemos establecer una **puerta de enlace o gateway** que es la dirección IP por la que el tráfico de red puede acceder a Internet. En el ejemplo anterior esta IP es **192.168.1.1**.

Dicha IP suele ser la IP interna (a menudo privada) del router. Dicha dirección y la dirección de todos los equipos clientes deben hallarse dentro de la misma red (en este caso 192.168.1.0)

Si la puerta de enlace no se halla configurada o está incorrectamente configurada en los clientes, es imposible que los equipos puedan comunicarse con Internet.

A continuación mostramos como configurar, en el cliente, la puerta de enlace haciendo uso del terminal de texto. Tanto en Windows como en Linux se hace uso del comando **route** (aunque su sintaxis es ligeramente diferente en cada caso).

Ver puerta de enlace configurada

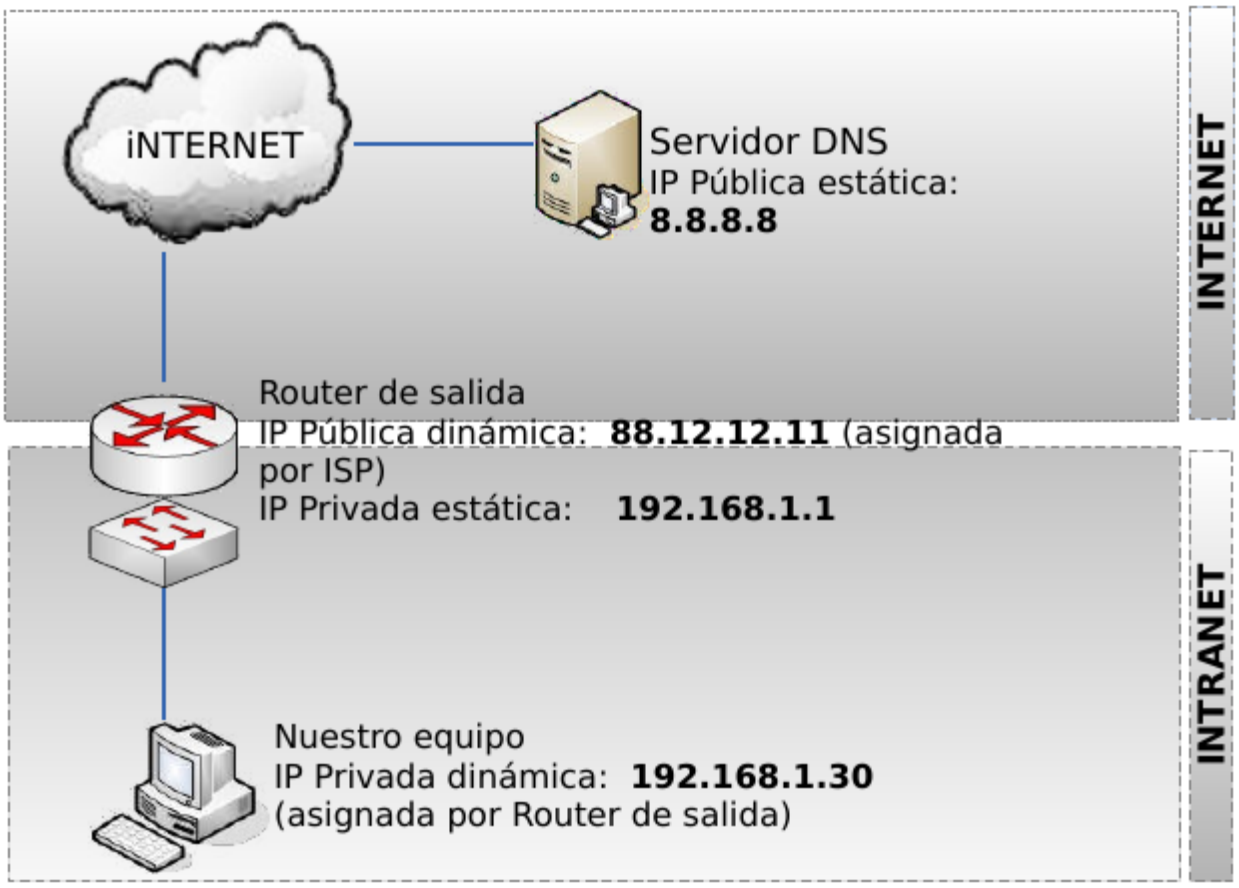


Figura 2: Esquema de referencia

```
route print
```

```
route
```

Borrar o añadir puerta de enlace

```
route delete 0.0.0.0 mask 0.0.0.0 192.168.1.1
route add    0.0.0.0 mask 0.0.0.0 192.168.1.1
```

```
route del default gw 192.168.1.1
route add default gw 192.168.1.1
```

Configuración del soporte básico de red

Visualización de configuración actual

Podemos ver los parámetros de la red con los siguientes comandos:

```
ipconfig /all            # (IP/Máscara, Puerta de enlace, DNS)
```

```
ifconfig                 # (IP/Máscara)
route                    # (Puerta de enlace)
cat /etc/resolv.conf     # (DNS)
```

Configuración dinámica de IP/Máscara, Puerta de Enlace y servidores DNS

```
ipconfig /release        # (Liberamos)
ipconfig /renew          # (Renovamos)
```

```
dhclient -r eth0          # (Liberamos)
dhclient eth0             # (Renovamos)
```

Configuración estática de IP/Máscara, Puerta de Enlace y servidores DNS

```
netsh
interface
ip

set address "Conexión de área local" static   \
        192.168.1.30                          \
        255.255.255.0                         \
        192.168.1.1                           \
        1

set dns "Conexión de área local" static       \
        8.8.8.8

commit
exit
```

```
ifconfig eth0 192.168.1.30 netmask 255.255.255.0
route add default gw 192.168.1.1
echo "nameserver 8.8.8.8" >> /etc/resolv.conf
```

Comprobación básica (Windows y Linux)

Una vez configurado el soporte de red procederemos a comprobar su correcto funcionamiento. Para ello deben seguirse los siguientes pasos en el orden indicado. Si alguno de los pasos falla, deberemos de corregir el error antes de proseguir.

1. Comprobamos la pila TCP/IP del Sistema Operativo

   `ping 127.0.0.1`

2. Comprobamos la tarjeta de red

   `ping 192.168.1.30`

3. Comprobamos las tablas de rutas

   `route print` (Windows) `route` (Linux)

4. Comprobamos el cable

   `ping 192.168.1.1`

5. Comprobamos la salida a Internet

   `ping 8.8.8.8`

6. Comprobamos la resolución de nombres

   `ping www.google.es`

Utilidades de red (Windows y Linux)

Para examinar equipos de la red

- ettercap

Para examinar puertos abiertos de nuestro equipo

- netstat

Para examinar puertos abiertos de otros equipos

- nmap

Para examinar tráfico en una red de difusión

- wireshark

8.2 Estándares

8.2.1 Protocolo IP

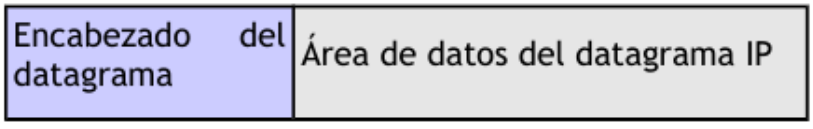
IP es el principal protocolo de la capa de red. Este protocolo define la unidad básica de transferencia de datos entre el origen y el destino, atravesando toda la red de redes. Además, el software IP es el encargado de elegir la ruta más adecuada por la que los datos serán enviados. Se trata de un sistema de entrega de paquetes (llamados **datagramas IP**) que tiene las siguientes características:

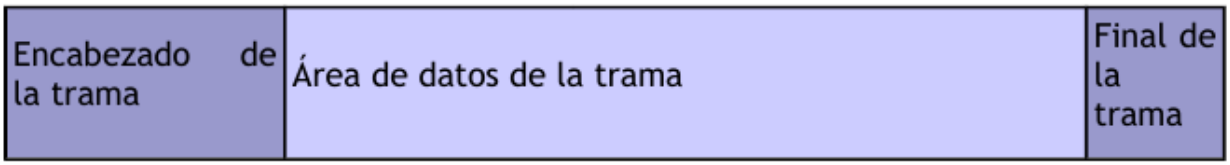
- Es **no orientado a conexión** debido a que cada uno de los paquetes puede seguir rutas distintas entre el origen y el destino. Entonces pueden llegar duplicados o desordenados.
- Es **no fiable** porque los paquetes pueden perderse, dañarse o llegar retrasados.

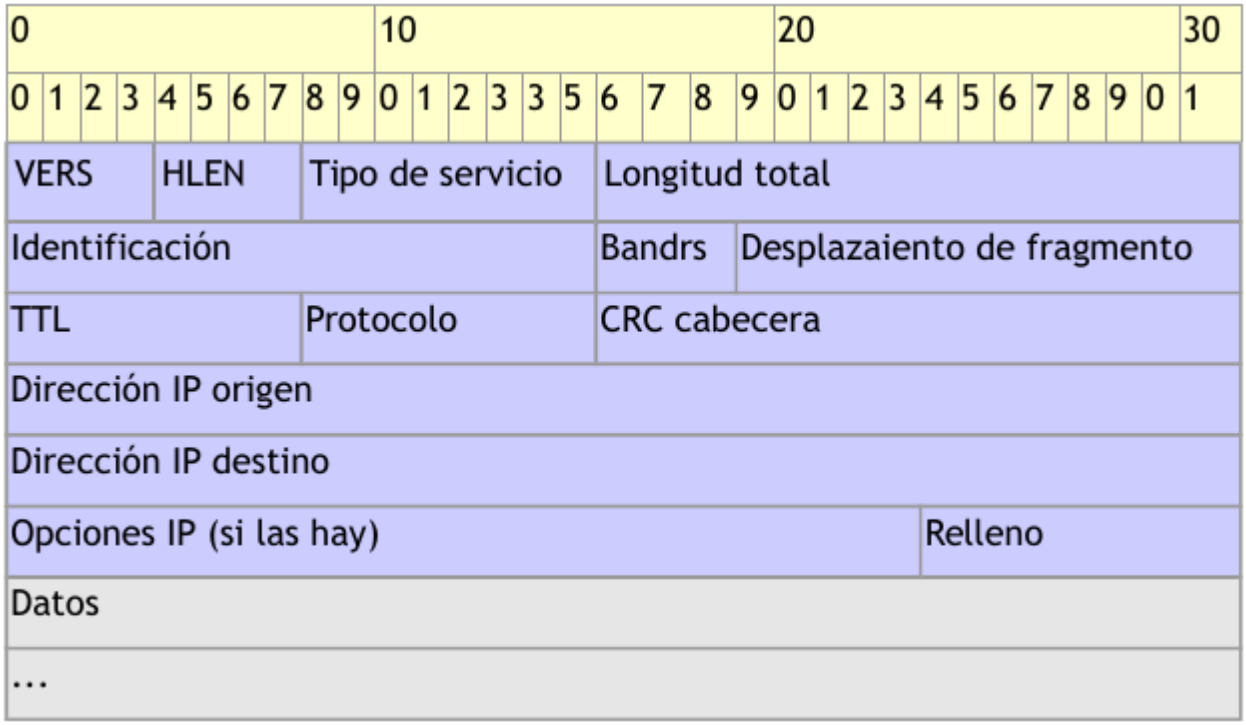
Nota: El protocolo IP está definido en la RFC 791

Formato del datagrama IP

El datagrama IP es la unidad básica de transferencia de datos entre el origen y el destino. Viaja en el campo de datos de las tramas físicas (recuérdese la trama Ethernet) de las distintas redes que va atravesando. Cada vez que un datagrama tiene que atravesar un router, el datagrama saldrá de la trama física de la red que abandona y se acomodará en el campo de datos de una trama física de la siguiente red. Este mecanismo permite que un mismo datagrama IP pueda atravesar redes distintas: enlaces punto a punto, redes ATM, redes Ethernet, redes Token Ring, etc. El propio datagrama IP tiene también un campo de datos: será aquí donde viajen los paquetes de las capas superiores.







Campos del datagrama IP

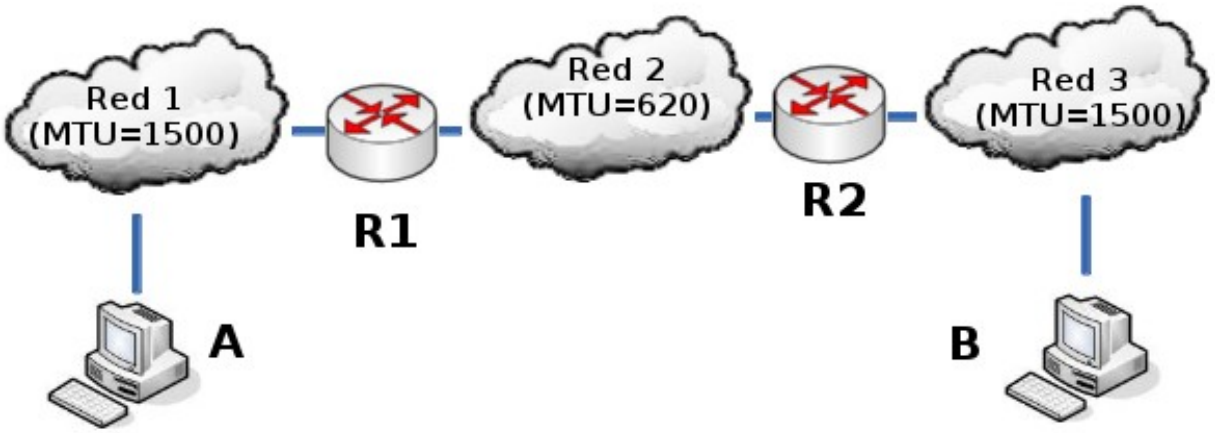
- **VERS (4 bits)**. Indica la versión del protocolo IP que se utilizó para crear el datagrama. Actualmente se utiliza la versión 4 (IPv4) aunque ya se están preparando las especificaciones de la siguiente versión, la 6 (IPv6).
- **HLEN (4 bits)**. Longitud de la cabecera expresada en múltiplos de 32 bits. El valor mínimo es 5, correspondiente a 160 bits = 20 bytes.
- **Tipo de servicio (Type Of Service)**. Los 8 bits de este campo se dividen a su vez en:
  - **Prioridad (3 bits)**. Un valor de 0 indica baja prioridad y un valor de 7, prioridad máxima.
  - Los siguientes tres bits indican cómo se prefiere que se transmita el mensaje, es decir, son sugerencias a los encaminadores que se encuentren a su paso los cuales pueden tenerlas en cuenta o no.
    - **Bit D** (Delay). Solicita retardos cortos (enviar rápido).
    - **Bit T** (Throughput). Solicita un alto rendimiento (enviar mucho en el menor tiempo posible).
    - **Bit R** (Reliability). Solicita que se minimice la probabilidad de que el datagrama se pierda o resulte dañado (enviar bien).
  - Los siguiente dos bits no tienen uso.
- **Longitud total (16 bits)**. Indica la longitud total del datagrama expresada en bytes. Como el campo tiene 16 bits, la máxima longitud posible de un datagrama será de 65535 bytes.
- ** Identificación (16 bits)**. Número de secuencia que junto a la dirección origen, dirección destino y el protocolo utilizado identifica de manera única un datagrama en toda la red. Si se trata de un datagrama fragmentado, llevará la misma identificación que el resto de fragmentos.
- **Banderas o indicadores (3 bits)**. Sólo 2 bits de los 3 bits disponibles están actualmente utilizados. El bit de Más fragmentos (MF) indica que no es el último datagrama. Y el bit de No fragmentar (NF) prohíbe la fragmentación del datagrama. Si este bit está activado y en una determinada red se requiere fragmentar el datagrama, éste no se podrá transmitir y se descartará.

- **Desplazamiento de fragmentación (13 bits)**. Indica el lugar en el cual se insertará el fragmento actual dentro del datagrama completo, medido en unidades de 64 bits. Por esta razón los campos de datos de todos los fragmentos menos el último tienen una longitud múltiplo de 64 bits. Si el paquete no está fragmentado, este campo tiene el valor de cero.
- **Tiempo de vida o TTL (8 bits)**. Número máximo de segundos que puede estar un datagrama en la red de redes. Cada vez que el datagrama atraviesa un router se resta 1 a este número. Cuando llegue a cero, el datagrama se descarta y se devuelve un mensaje ICMP de tipo «tiempo excedido» para informar al origen de la incidencia.
- **Protocolo (8 bits)**. Indica el protocolo utilizado en el campo de datos: 1 para ICMP, 2 para IGMP, 6 para TCP y 17 para UDP.
- **CRC cabecera (16 bits)**. Contiene la suma de comprobación de errores sólo para la cabecera del datagrama. La verificación de errores de los datos corresponde a las capas superiores.
- **Dirección origen (32 bits)**. Contiene la dirección IP del origen.
- **Dirección destino (32 bits)**. Contiene la dirección IP del destino.
- **Opciones IP**. Este campo no es obligatorio y especifica las distintas opciones solicitadas por el usuario que envía los datos (generalmente para pruebas de red y depuración).
- **Relleno**. Si las opciones IP (en caso de existir) no ocupan un múltiplo de 32 bits, se completa con bits adicionales hasta alcanzar el siguiente múltiplo de 32 bits (recuérdese que la longitud de la cabecera tiene que ser múltiplo de 32 bits).

Fragmentación

Ya hemos visto que las tramas físicas tienen un campo de datos y que es aquí donde se transportan los datagramas IP. Sin embargo, este campo de datos no puede tener una longitud indefinida debido a que está limitado por el diseño de la red. **El MTU de una red es la mayor cantidad de datos que puede transportar su trama física**. El MTU de las redes Ethernet es 1500 bytes y el de las redes Token-Ring, 8192 bytes. Esto significa que una red Ethernet nunca podrá transportar un datagrama de más de 1500 bytes sin fragmentarlo.

Un encaminador (router) fragmenta un datagrama en varios si el siguiente tramo de la red por el que tiene que viajar el datagrama tiene un MTU inferior a la longitud del datagrama. Veamos con el siguiente ejemplo cómo se produce la fragmentación de un datagrama.



Supongamos que el host A envía un datagrama de 1400 bytes de datos (1420 bytes en total) al host B. El datagrama no tiene ningún problema en atravesar la red 1 ya que 1420 < 1500. Sin embargo, no es capaz de atravesar la red 2 (1420 >= 620). El router R1 fragmenta el datagrama en el menor número de fragmentos posibles que sean capaces

de atravesar la red 2. Cada uno de estos fragmentos es un nuevo datagrama con la misma Identificación pero distinta información en el campo de Desplazamiento de fragmentación y el bit de Más fragmentos (MF). Veamos el resultado de la fragmentación:

Fragmento 1: Long. total = 620 bytes; Desp = 0; MF=1 (contiene los primeros 600 bytes de los datos del datagrama original)

Fragmento 2: Long. total = 620 bytes; Desp = 600; MF=1 (contiene los siguientes 600 bytes de los datos del datagrama original)

Fragmento 3: Long. total = 220 bytes; Desp = 1200; MF=0 (contiene los últimos 200 bytes de los datos del datagrama original)

El router R2 recibirá los 3 datagramas IP (fragmentos) y los enviará a la red 3 sin reensamblarlos. Cuando el host B reciba los fragmentos, recompondrá el datagrama original. Los encaminadores intermedios no reensamblan los fragmentos debido a que esto supondría una carga de trabajo adicional, a parte de memorias temporales. Nótese que el ordenador destino puede recibir los fragmentos cambiados de orden pero esto no supondrá ningún problema para el reensamblado del datagrama original puesto que cada fragmento guarda suficiente información.

Si el datagrama del ejemplo hubiera tenido su bit No fragmentar (NF) a 1, no hubiera conseguido atravesar el router R1 y, por tanto, no tendría forma de llegar hasta el host B. El encaminador R1 descartaría el datagrama.

CIDR (Classless Inter-Domain Routing)

Encaminamiento Inter-Dominios sin Clases

Pronunciado como «cider» or «cedar», se introdujo en 1993 y representa la última mejora en el modo como se interpretan las direcciones IP. Su introducción permitió una mayor flexibilidad al dividir rangos de direcciones IP en redes separadas. De esta manera permitió:

Un uso más eficiente de las cada vez más escasas direcciones IPv4. Un mayor uso de la jerarquía de direcciones ("agregación de prefijos de red"), disminuyendo la sobrecarga de los enrutadores principales de Internet para realizar el encaminamiento. Los bloques CIDR IPv4 se identifican usando una sintaxis similar a la de las direcciones IPv4: cuatro números decimales separados por puntos, seguidos de una barra de división y un número de 0 a 32; **A.B.C.D/N**. El número tras la barra es la **longitud de prefijo**, contando desde la izquierda, y representa el número de bits comunes a todas las direcciones incluidas en el bloque CIDR.

Decimos que una dirección IP está incluida en un bloque CIDR, y que encaja con el prefijo CIDR, si los N bits iniciales de la dirección y el prefijo son iguales. Por tanto, para entender CIDR es necesario visualizar la dirección IP en binario. Dado que la longitud de una dirección IPv4 es fija, de 32 bits, un prefijo CIDR de N-bits deja 32 N bits sin encajar, y hay $2^{(32\ N)}$ combinaciones posibles con los bits restantes. Esto quiere decir que $2^{(32\ N)}$ direcciones IPv4 encajan en un prefijo CIDR de N-bits.

Nótese que los prefijos **CIDR cortos** (números cercanos a 0) permiten encajar un mayor número de direcciones IP, mientras que prefijos **CIDR largos** (números cercanos a 32) permiten encajar menos direcciones IP. CIDR también se usa con direcciones IPv6, en las que la longitud del prefijo varia desde 0 a 128, debido a la mayor longitud de bit en las direcciones, con respecto a IPv4. En el caso de IPv6 se usa una sintaxis similar a la comentada: el prefijo se escribe como una dirección IPv6, seguida de una barra y el número de bits significativos.

CIDR usa máscaras de subred de longitud variable (VLSM) para asignar direcciones IP a subredes de acuerdo a las necesidades de cada subred. De esta forma, la división red/host puede ocurrir en cualquier bit de los 32 que componen la dirección IP. Este proceso puede ser recursivo, dividiendo una parte del espacio de direcciones en porciones cada vez menores, usando máscaras que cubren un mayor número de bits.

Las direcciones de red CIDR/VLSM se usan a lo largo y ancho de la Internet pública, y en muchas grandes redes privadas. El usuario normal no ve este uso puesto en práctica, al estar en una red en la que se usarán, por lo general, direcciones de red privadas recogidas en el RFC 1918. El término VLSM (**Variable Lenght Subnet Mask - Máscara de Subred de Longitud Variable**) se usa generalmente cuando se habla de redes privadas, mientras que CIDR se usa cuando se habla de Internet (red pública).

Tabla de conversión de prefijos CIDR

CIDR	Clase	Hosts[1]	Máscara
/32	1/256 C	1	255.255.255.255
/31	1/128 C	2	255.255.255.254
/30	1/64 C	4	255.255.255.252
/29	1/32 C	8	255.255.255.248
/28	1/16 C	16	255.255.255.240
/27	1/8 C	32	255.255.255.224
/26	1/4 C	64	255.255.255.192
/25	1/2 C	128	255.255.255.128
/24	1 C	256	255.255.255.000
/23	2 C	512	255.255.254.000
/22	4 C	1024	255.255.252.000
/21	8 C	2048	255.255.248.000
/20	16 C	4096	255.255.240.000
/19	32 C	8192	255.255.224.000
/18	64 C	16384	255.255.192.000
/17	128 C	32768	255.255.128.000
/16	256 C, 1 B	65536	255.255.000.000
/15	512 C, 2 B	131072	255.254.000.000
/14	1024 C, 4 B	262144	255.252.000.000
/13	2048 C, 8 B	524288	255.248.000.000
/12	4096 C, 16 B	1048576	255.240.000.000
/11	8192 C, 32 B	2097152	255.224.000.000
/10	16384 C, 64 B	4194304	255.192.000.000
/9	32768 C, 128B	8388608	255.128.000.000
/8	65536 C, 256B, 1 A	16777216	255.000.000.000
/7	131072 C, 512B, 2 A	33554432	254.000.000.000
/6	262144 C, 1024 B, 4 A	67108864	252.000.000.000
/5	524288 C, 2048 B, 8 A	134217728	248.000.000.000
/4	1048576 C, 4096 B, 16 A	268435456	240.000.000.000
/3	2097152 C, 8192 B, 32 A	536870912	224.000.000.000
/2	4194304 C, 16384 B, 64 A	1073741824	192.000.000.000
/1	8388608 C, 32768 B, 128 A	2147483648	128.000.000.000

Otro beneficio de CIDR es la posibilidad de **agregar prefijos de encaminamiento**, un proceso conocido como «**supernetting**». Una dirección IP puede encajar en varios prefijos CIDR de longitudes diferentes. Por ejemplo, dieciséis redes /24 contíguas pueden ser agregadas y publicadas en los enrutadores de Internet como una sola ruta /20 (si los primeros 20 bits de sus respectivas redes coinciden). Dos redes /20 contiguas pueden ser agregadas en una /19, etc…

Esto permite una reducción significativa en el número de rutas que los enrutadores en Internet tienen que conocer (y una reducción de memoria, recursos, etc…) y previene una explosión de tablas de encaminamiento, que podría sobrecargar a los routers e impedir la expansión de Internet en el futuro.

Superredes

Para muchas organizaciones una dirección de red de clase C es poco.

[1] En la práctica hay que restar 2 a este número. La dirección menor (más baja - todos los bits de host a 0) del bloque se usa para identificar a la propia red (toda la red), y la dirección mayor (la más alta - todos los bits de host a 1) se usa como dirección de broadcast. Por tanto, en un bloque CIDR /24 podríamos disponer de 2^8 2 = 254 direcciones IP para asignar a dispositivos.

Solución: Agrupar direcciones consecutivas (tienen un prefijo común) de redes de clase C para asignarlas a una organización.

Esto permite asignar espacio de direcciones a organizaciones con redes de tamaño medio, evitando utilizar direcciones de clase B.

Ejemplo de agrupamiento:

```
193.40.128.0 = 11000001 00101000 1000 0000 00000000
193.40.129.0 = 11000001 00101000 1000 0001 00000000
.
.
.
193.40.142.0 = 11000001 00101000 1000 1110 00000000
193.40.143.0 = 11000001 00101000 1000 1111 00000000
```

La dirección de red/máscara sería 193.40.128.0/20 (255.255.240.0)

```
Máscara en binario: 11111111  11111111  11110000  00000000.
```

Existen 2^{12}-2 (4096-2) direcciones IP para hosts

8.2.2 Protocolo ARP

Dentro de una misma red, las máquinas se comunican enviándose tramas físicas. Las tramas Ethernet contienen campos para las direcciones físicas de origen y destino (6 bytes cada una):

8 bytes	6 bytes	6 bytes	2 bytes	64-1500 bytes	4 bytes
Preámbulo	Dirección física destino	Dirección física origen	Tipo de trama	Datos de la trama	CRC

8 bytes 6 bytes 6 bytes 2 bytes 64-1500 bytes 4 bytes Preámbulo Dirección físicadestino Dirección físicaorigen Tipo de trama Datos de la trama CRC El problema que se nos plantea es cómo podemos conocer la dirección física de la máquina destino. El único dato que se indica en los datagramas es la dirección IP de destino. ¿Cómo se pueden entregar entonces estos datagramas? Necesitamos obtener la dirección física de un ordenador a partir de su dirección IP. Esta es justamente la misión del protocolo ARP (Address Resolution Protocol, protocolo de resolución de direcciones).

Nota: ARP se utiliza en **redes con mecanismos de difusión** (Ethernet, FDDI, Token-Ring, etc.) El protocolo ARP está definido en RFC 826, RFC 1042 y RFC 1390

Vamos a retomar el ejemplo introductorio de este Capítulo. El host A envía un datagrama con origen 192.168.0.10 y destino 10.10.0.7 (B). Como el host B se encuentra en una red distinta al host A, el datagrama tiene que atravesar el router 192.168.0.1 (R1). Se necesita conocer la dirección física de R1.

Es entonces cuando entra en funcionamiento el protocolo ARP: A envía un mensaje ARP a todas las máquinas de su red preguntando «¿Cuál es la dirección física de la máquina con dirección IP 192.168.0.1?». La máquina con dirección 192.168.0.1 (R1) advierte que la pregunta está dirigida a ella y responde a A con su dirección física (00-E0-4C-AB-9A-FF). Entonces A envía una trama física con origen 00-60-52-0B-B7-7D y destino 00-E0-4C-AB-9A-FF conteniendo el datagrama (origen 192.168.0.10 y destino 10.10.0.7). Al otro lado del router R2 se repite de nuevo el proceso para conocer la dirección física de B y entregar finalmente el datagrama a B. El mismo datagrama ha viajado en dos tramas físicas distintas, una para la red 1 y otra para la red 2.

Host	Red	Dirección IP	Dirección física
A	Red 1	192.168.0.10	00-60-52-0B-B7-7D
R1		192.168.0.1	00-E0-4C-AB-9A-FF
	Red 2	10.10.0.1	A3-BB-05-17-29-D0
B		10.10.0.7	00-E0-4C-33-79-AF
R2		10.10.0.2	B2-42-52-12-37-BE
	Red 3	200.3.107.1	00-E0-89-AB-12-92
C		200.3.107.73	A3-BB-08-10-DA-DB
D		200.3.107.200	B2-AB-31-07-12-93

Observemos que las preguntas ARP son de difusión (se envían a todas las máquinas). Estas preguntas llevan además la dirección IP y dirección física de la máquina que pregunta. La respuesta se envía directamente a la máquina que formuló la pregunta.

Tabla ARP (caché ARP)

Cada ordenador almacena una tabla de direcciones IP y direcciones físicas. Cada vez que formula una pregunta ARP y le responden, inserta una nueva entrada en su tabla. La primera vez que C envíe un mensaje a D tendrá que difundir previamente una pregunta ARP, tal como hemos visto. Sin embargo, las siguientes veces que C envíe mensajes a D ya no será necesario realizar nuevas preguntas puesto que C habrá almacenado en su tabla la dirección física de D. Sin embargo, para evitar incongruencias en la red debido a posibles cambios de direcciones IP o adaptadores de red, se asigna un tiempo de vida de cierto número de segundos a cada entrada de la tabla. Cuando se agote el tiempo de vida de una entrada, ésta será eliminada de la tabla.

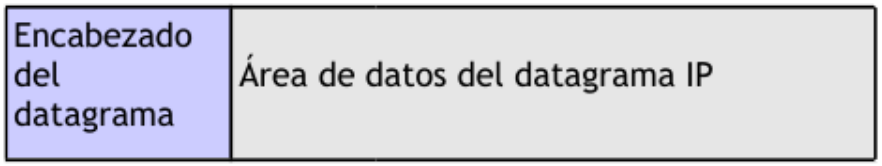
Las tablas ARP reducen el tráfico de la red al evitar preguntas ARP innecesarias. Pensemos ahora en distintas maneras para mejorar el rendimiento de la red. Después de una pregunta ARP, el destino conoce las direcciones IP y física del origen. Por lo tanto, podría insertar la correspondiente entrada en su tabla. Pero no sólo eso, sino que todas las estaciones de la red escuchan la pregunta ARP: podrían insertar también las correspondientes entradas en sus tablas. Como es muy probable que otras máquinas se comuniquen en un futuro con la primera, habremos reducido así el tráfico de la red aumentando su rendimiento.

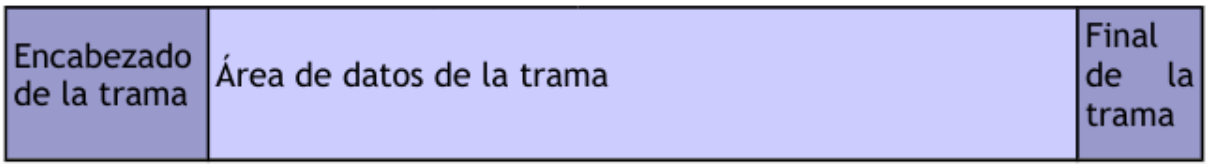
Esto que hemos explicado es para comunicar dos máquinas conectadas a la misma red. Si la otra máquina no estuviese conectada a la misma red, sería necesario atravesar uno o más routers hasta llegar al host destino. La máquina origen, si no la tiene en su tabla, formularía una pregunta ARP solicitando la dirección física del router y le transferiría a éste el mensaje. Estos pasos se van repitiendo para cada red hasta llegar a la máquina destino.

8.2.3 Protocolo ICMP

Debido a que el protocolo IP no es fiable, los datagramas pueden perderse o llegar defectuosos a su destino. El protocolo ICMP (Internet Control Message Protocol, protocolo de mensajes de control y error) se encarga de informar al origen si se ha producido algún error durante la entrega de su mensaje. Pero no sólo se encarga de notificar los errores, sino que también transporta distintos mensajes de control.

El protocolo ICMP únicamente informa de incidencias en la red pero no toma ninguna decisión. Esto será responsabilidad de las capas superiores. Los mensajes ICMP viajan en el campo de datos de un datagrama IP, como se puede apreciar en el siguiente esquema:





Debido a que el protocolo IP no es fiable puede darse el caso de que un mensaje ICMP se pierda o se dañe. Si esto llega a ocurrir no se creará un nuevo mensaje ICMP sino que el primero se descartará sin más.

Los mensajes ICMP comienzan con un campo de 8 bits que contiene el tipo de mensaje, según se muestra en la tabla siguiente. El resto de campos son distintos para cada tipo de mensaje ICMP.

Nota: El formato y significado de cada mensaje ICMP está documentado en la RFC 792

Campo de tipo	Tipo de mensaje ICMP
0	Respuesta de eco (Echo Reply)
3	Destino inaccesible (Destination Unreachable)
4	Disminución del tráfico desde el origen (Source Quench)
5	Redireccionar (cambio de ruta) (Redirect)
8	Solicitud de eco (Echo)
11	Tiempo excedido para un datagrama (Time Exceeded)
12	Problema de Parámetros (Parameter Problem)
13	Solicitud de marca de tiempo (Timestamp)
14	Respuesta de marca de tiempo (Timestamp Reply)
15	Solicitud de información (obsoleto) (Information Request)
16	Respuesta de información (obsoleto) (Information Reply)
17	Solicitud de máscara (Addressmask)
18	Respuesta de máscara (Addressmask Reply)

Solicitud y respuesta de eco

Los mensajes de solicitud y respuesta de eco, tipos 8 y 0 respectivamente, se utilizan para comprobar si existe comunicación entre 2 hosts a nivel de la capa de red. Estos mensajes comprueban que las capas física (cableado), acceso al medio (tarjetas de red) y red (configuración IP) están correctas. Sin embargo, no dicen nada de las capas de transporte

y de aplicación las cuales podrían estar mal configuradas; por ejemplo, la recepción de mensajes de correo electrónico puede fallar aunque exista comunicación IP con el servidor de correo.

La orden **PING** envía mensajes de solicitud de eco a un host remoto e informa de las respuestas. Veamos su funcionamiento, en caso de no producirse incidencias en el camino.

1. A envía un mensaje ICMP de tipo 8 (Echo) a B
2. B recibe el mensaje y devuelve un mensaje ICMP de tipo 0 (Echo Reply) a A
3. A recibe el mensaje ICMP de B y muestra el resultado en pantalla


```
C:\>ping 172.20.9.7 -n 1
Haciendo ping a 172.20.9.7 con 32 bytes de datos:
Respuesta desde 172.20.9.7: bytes=32 tiempo<10ms TDV=128
```

En la orden anterior hemos utilizado el parámetro «-n 1» para que el host A únicamente envíe 1 mensaje de solicitud de eco. Si no se especifica este parámetro se enviarían 4 mensajes (y se recibirían 4 respuestas).

Si el host de destino no existiese o no estuviera correctamente configurado recibiríamos un mensaje ICMP de tipo 11 (Time Exceeded).

```
C:\>ping 192.168.0.6 -n 1
Haciendo ping a 192.168.0.6 con 32 bytes de datos:
Tiempo de espera agotado.
```

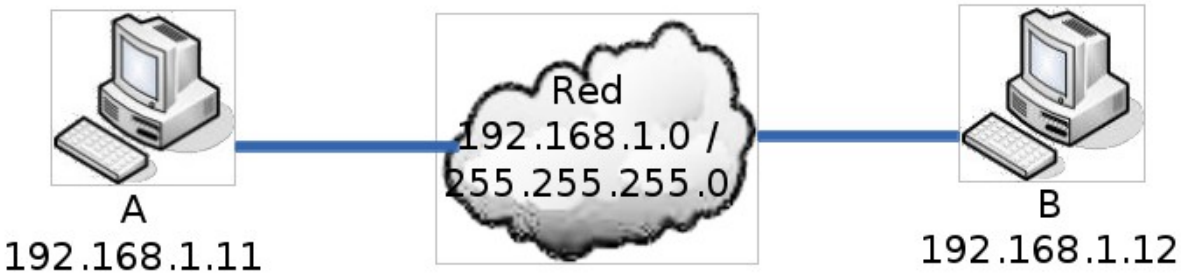
Si tratamos de acceder a un host de una red distinta a la nuestra y no existe un camino para llegar hasta él, es decir, los routers no están correctamente configurados o estamos intentando acceder a una red aislada o inexistente, recibiríamos un mensaje ICMP de tipo 3 (Destination Unreachable).

```
C:\>ping 1.1.1.1 -n 1
Haciendo ping a 1.1.1.1 con 32 bytes de datos:
Respuesta desde 192.168.0.1: Host de destino inaccesible.
```

Utilización de PING para diagnosticar errores en una red aislada

```
C:\>ping 192.168.1.12
```

- Respuesta. El cableado entre A y B, las tarjetas de red de A y B, y la configuración IP de A y B están correctos.
- Tiempo de espera agotado. Comprobar el host B y el cableado entre A y B.
- Host de destino inaccesible. Comprobar las direcciones IP y máscaras de subred de A y B porque no pertenecen a la misma red.

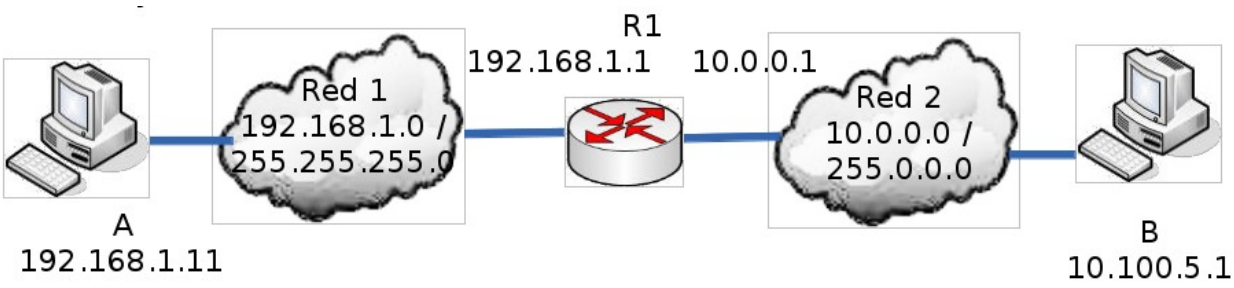


- Error. Probablemente estén mal instalados los protocolos TCP/IP del host A. Probar C:>ping 127.0.0.1 para asegurarse.

Nota: El comando ping 127.0.0.1 informa de si están correctamente instalados los protocolos TCP/IP en nuestro host. No informa de si la tarjeta de red de nuestro host está correcta.

Utilización de PING para diagnosticar errores en una red de redes

A continuación veremos un ejemplo para una red de redes formada por dos redes (1 solo router). La idea es la misma para un mayor número de redes y routers.




```
C:\>ping 10.100.5.1
```

- Respuesta. El cableado entre A y B, las tarjetas de red de A, R1 y B, y la configuración IP de A, R1 y B están correctos. El router R1 permite el tráfico de datagramas IP en los dos sentidos.
- Tiempo de espera agotado. Comprobar el host B y el cableado entre R1 y B. Para asegurarnos que el router R1 está funcionando correctamente haremos C:>ping 192.168.1.1
- Host de destino inaccesible. Comprobar el router R1 y la configuración IP de A (probablemente la puerta de salida no sea 192.168.1.1). Recordemos que la puerta de salida (gateway) de una red es un host de su propia red que se utiliza para salir a otras redes.
- Error. Probablemente estén mal instalados los protocolos TCP/IP del host A. Probar C:>ping 127.0.0.1 para asegurarse.

En el caso producirse errores de comunicación en una red de redes con más de un router (Internet es el mejor ejemplo), se suele utilizar el comando PING para ir diagnosticando los distintos routers desde el destino hasta el origen y descubrir así si el fallo es responsabilidad de la red de destino, de una red intermedia o de nuestra red.

Nota: Algunos hosts en Internet tienen deshabilitadas las respuestas de eco (mensajes ICMP tipo 0) como medida de seguridad. En estos casos hay que utilizar otros mecanismos para detectar si responde (por ejemplo, la apertura de

conexión a un puerto)

Mensajes ICMP de tiempo excedido

Los datagramas IP tienen un campo TTL (tiempo de vida) que impide que un mensaje esté dando vueltas indefinidamente por la red de redes. El número contenido en este campo disminuye en una unidad cada vez que el datagrama atraviesa un router. Cuando el TTL de un datagrama llega a 0, éste se descarta y se envía un mensaje ICMP de tipo 11 (Time Exceeded) para informar al origen.

Los mensajes ICMP de tipo 11 se pueden utilizar para hacer una traza del camino que siguen los datagramas hasta llegar a su destino. ¿Cómo? Enviando una secuencia de datagramas con TTL=1, TTL=2, TTL=3, TTL=4, etc... hasta alcanzar el host o superar el límite de saltos (30 si no se indica lo contrario). El primer datagrama caducará al atravesar el primer router y se devolverá un mensaje ICMP de tipo 11 informando al origen del router que descartó el datagrama. El segundo datagrama hará lo propio con el segundo router y así sucesivamente. Los mensajes ICMP recibidos permiten definir la traza.

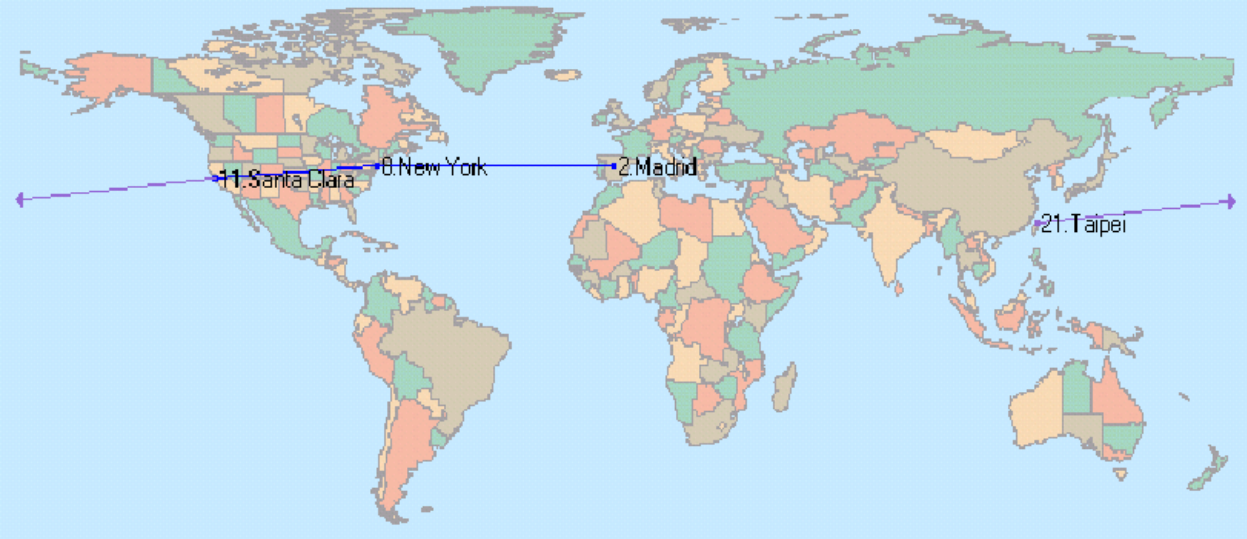
La orden **TRACERT** (**traceroute** en entornos Unix) hace una traza a un determinado host. TRACERT funciona enviando mensajes ICMP de solicitud de eco con distintos TTL; traceroute, en cambio, envía mensajes UDP. Si la comunicación extremo a extremo no es posible, la traza nos indicará en qué punto se ha producido la incidencia. Existen algunas utilidades en Internet, como Visual Route, que conocen la localización geográfica de los principales routers de Internet. Esto permite dibujar en un mapamundi el recorrido que siguen los datagramas hasta llegar a un host.

```
C:\>tracert 130.206.1.2

Traza a la dirección sun.rediris.es [130.206.1.2]
sobre un máximo de 30 saltos:

 1   1 ms   1 ms   1 ms PROXY [192.168.0.1]
 2 122 ms 118 ms 128 ms MADR-X27.red.retevision.es [62.81.1.102]
 3 143 ms 232 ms 147 ms MADR-R2.red.retevision.es [62.81.1.92]
 4 130 ms 124 ms 246 ms MADR-R16.red.retevision.es [62.81.3.8]
 5 590 ms 589 ms 431 ms MADR-R12.red.retevision.es [62.81.4.101]
 6 612 ms 640 ms 124 ms MADR-R10.red.retevision.es [62.81.8.130]
 7 259 ms 242 ms 309 ms 193.149.1.28
 8 627 ms 752 ms 643 ms 213.0.251.42
 9 137 ms 117 ms 118 ms 213.0.251.142
10 109 ms 105 ms 110 ms A1-2-1.EB-Madrid00.red.rediris.es [130.206.224.81]
11 137 ms 119 ms 122 ms A0-0-0-1.EB-Madrid3.red.rediris.es [130.206.224.86]
12 109 ms 135 ms 115 ms sun.rediris.es [130.206.1.2]

Traza completa.
```

Ejemplo de Visual Route a una dirección IP de Taiwan (203.69.112.12):

8.2.4 IPv6

Diseñado por Steve Deering de Xerox PARC y Craig Mudge, IPv6 está destinado a sustituir al estándar IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados. Pero el nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionando a futuras celdas telefónicas y dispositivos móviles con sus direcciones propias y permanentes. Al día de hoy se calcula que las dos terceras partes de las direcciones que ofrece IPv4 ya están asignadas.


11.Santa Clara
8.New York
2.Madrid
21.Taipei


IPv6

IPv4 soporta 4.294.967.296 (2^{32}) direcciones de red diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos para cada coche, teléfono, PDA o tostadora; mientras que **IPv6** soporta 340.282.366.920.938.463.463.374.607.431.768.211.456 (2^{128} ó 340 sextillones) direcciones —cerca de $4{,}3 \times 10^{20}$ (430 trillones) direcciones por cada pulgada cuadrada ($6{,}7 \times 10^{17}$ ó 670 mil billones direcciones/mm^2) de la superficie de La Tierra.

Adoptado por el **Internet Engineering Task Force (IETF)** en 1994 (cuando era llamado «IP Next Generation» o IPng), IPv6 cuenta con un pequeño porcentaje de las direcciones públicas de Internet, que todavía están dominadas por IPv4. La adopción de IPv6 ha sido frenada por la traducción de direcciones de red (NAT), que alivia parcialmente el problema de la falta de direcciones IP. Pero NAT hace difícil o imposible el uso de algunas aplicaciones P2P, como son la voz sobre IP (VoIP) y juegos multiusuario. Además, NAT rompe con la idea originaria de Internet donde todos pueden conectarse con todos. Actualmente, el gran catalizador de IPv6 es la capacidad de ofrecer nuevos servicios, como la movilidad, Calidad de Servicio (QoS), privacidad, etc. El gobierno de los Estados Unidos ha ordenado el despliegue de IPv6 por todas sus agencias federales para el año 2008.

Se espera que IPv4 se siga soportando hasta por lo menos el 2025, dado que hay muchos dispositivos heredados que no se migrarán a IPv6 nunca y que seguirán siendo utilizados por mucho tiempo.

IPv6 es la segunda versión del Protocolo de Internet que se ha adoptado para uso general. También hubo un IPv5, pero no fue un sucesor de IPv4; mejor dicho, fue un protocolo experimental orientado al flujo de streaming que intentaba soportar voz, video y audio.

Direccionamiento IPv6

El cambio más drástico de IPv4 a IPv6 es la longitud de las direcciones de red. Las direcciones IPv6, definidas en el RFC 2373 y RFC 2374, son de **128 bits**; esto corresponde a 32 dígitos hexadecimales, que se utilizan normalmente para escribir las direcciones IPv6, como se describe en la siguiente sección.

El número de direcciones IPv6 posibles es de 2^{128} 3.4 x 10^{38}. Este número puede también representarse como 1632, con 32 dígitos hexadecimales, cada uno de los cuales puede tomar 16 valores (véase combinatoria).

En muchas ocasiones las direcciones IPv6 están compuestas por dos partes lógicas: un prefijo de 64 bits y otra parte de 64 bits que corresponde al identificador de interfaz, que casi siempre se genera automáticamente a partir de la dirección MAC de la interfaz a la que está asignada la dirección.

Notación para las direcciones IPv6

Las direcciones IPv6, de 128 bits de longitud, se escriben como ocho grupos de cuatro dígitos hexadecimales.

Por ejemplo,

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

es una dirección IPv6 válida.

Si un grupo de cuatro dígitos es nulo (es decir, toma el valor «0000»), puede ser comprimido. Por ejemplo,

```
2001:0db8:85a3:0000:1319:8a2e:0370:7344
```

es la misma dirección que

```
2001:0db8:85a3::1319:8a2e:0370:7344
```

Siguiendo esta regla, si más de dos grupos consecutivos son nulos, pueden comprimirse como `::`. Si la dirección tiene más de una serie de grupos nulos consecutivos la compresión solo en uno de ellos. Así,

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

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

son todas válidas y significan lo mismo, pero

`2001::25de::cade`

es inválido porque no queda claro cuantos grupos nulos hay en cada lado.

Los ceros iniciales en un grupo pueden ser omitidos. Así,

`2001:0DB8:02de::0e13`

es lo mismo que

`2001:DB8:2de::e13`

Si la dirección es una dirección IPv4 camuflada, los últimos 32 bits pueden escribirse en base decimal; así,

`::ffff:192.168.89.9`

es lo mismo que

`::ffff:c0a8:5909`

pero no lo mismo que

- `::192.168.89.9`
- `::c0a8:5909`

El formato `::ffff:1.2.3.4` se denomina dirección **IPv4 mapeada**, y el formato `::1.2.3.4` dirección **IPv4 compatible**.

Las direcciones IPv4 pueden ser transformadas fácilmente al formato IPv6. Por ejemplo, si la dirección decimal IPv4 es `135.75.43.52` (en hexadecimal, `0x874B2B34`), puede ser convertida a `0000:0000:0000:0000:0000:0000:874B:2B34` o `::874B:2B34`. Entonces, uno puede usar la notación mixta dirección IPv4 compatible, en cuyo caso la dirección debería ser `::135.75.43.52`. Este tipo de dirección IPv4 compatible casi no está siendo utilizada en la práctica, aunque los estándares no la han declarado obsoleta.

Tipos de direcciones

IPv6 tiene tres tipos de direcciones, que se pueden clasificar según el tipo y alcance:

- Las direcciones **UNICAST**. Se envía un paquete a una interfaz.
- Las direcciones **MULTICAST** (multidifusión). Se envía un paquete de múltiples interfaces.
- Las direcciones **ANYCAST**. Se envía un paquete a la más cercana de múltiples interfaces (en términos de distancia de enrutamiento).

No hay direcciones de broadcast en IPv6. Las direcciones de multidifusión han reemplazado esta función.

Las direcciones Unicast y Anycast en IPv6 tienen los siguientes ámbitos (para las direcciones multicast, el ámbito está integrado en la estructura de dirección):

- De enlace local. El ámbito es el enlace local (nodos de la misma subred).
- Global. El alcance es global (direcciones de Internet IPv6).

Además, IPv6 tiene direcciones especiales como la dirección de bucle invertido. El ámbito de una dirección especial depende del tipo de dirección especial.

Gran parte del espacio de direcciones IPv6 está sin asignar.

Tabla muy resumida de la asignación por tipo de dirección.

Tipo de dirección	Prefijo binario	Notación IPv6
Sin especificar	00 . . . 0 (128 bits)	::/128
Loopback	00 . . . 1 (128 bits)	::1/128
Multicast	11111111 . . .	FF00::/8
Link-local unicast	1111111010 . . .	FE80::/10
Site-local unicast (obsoleto)	1111111011 . . .	FEC0::/10
Local unicast	1111110 . . .	FC00::/7
Global unicast	001 . . .	2000::/3

Paquetes IPv6

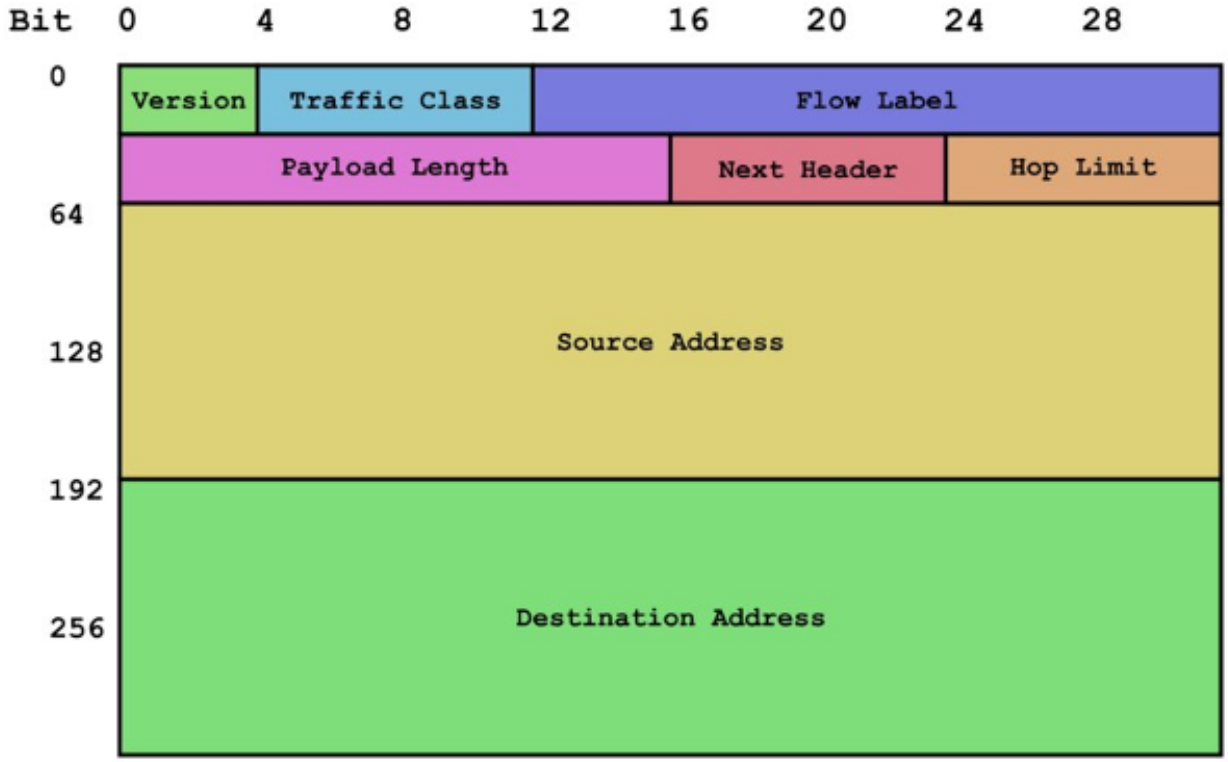


Figura 3: Estructura de la cabecera de un paquete IPv6.

Un paquete en IPv6 está compuesto principalmente de dos partes: la cabecera y los datos.

La cabecera está en los primeros 40 bytes del paquete y contiene las direcciones de origen y destino (128 bits cada una), la versión de IP (4 bits), la clase de tráfico (8 bits, Prioridad del Paquete), etiqueta de flujo (20 bits, manejo de la Calidad de Servicio), longitud del campo de datos (16 bits), cabecera siguiente (8 bits), y límite de saltos (8 bits, Tiempo de Vida). Después viene el campo de datos, con los datos que transporta el paquete, que puede llegar a 64k de tamaño en el modo normal, o más con la opción «jumbo payload».

Despliegue de IPv6

Mecanismos de transición a IPv6

El cambio de IPv4 a IPv6 ya ha comenzado. Durante 20 años se espera que convivan ambos protocolos y que la implantación de IPv6 sea paulatina. Existe una serie de mecanismos que permitirán la convivencia y la migración progresiva

tanto de las redes como de los equipos de usuario. En general, los mecanismos de transición pueden clasificarse en tres grupos:

- **Pila dual**
- **Túneles**
- **Traducción**

Pila dual

La pila dual hace referencia a una solución de nivel IP con pila dual (RFC 2893), que implementa las pilas de ambos protocolos, IPv4 e IPv6, en cada nodo de la red. Cada nodo de pila dual en la red tendrá dos direcciones de red, una IPv4 y otra IPv6.

- Pros: Fácil de desplegar y extensamente soportado.
- Contras: La topología de red requiere dos tablas de encaminamiento y dos procesos de encaminamiento. Cada nodo en la red necesita tener actualizadas las dos pilas.

Túneles

Los túneles permiten conectarse a redes IPv6 «saltando» sobre redes IPv4. Estos túneles trabajan **encapsulando los paquetes IPv6 en paquetes IPv4** teniendo como siguiente capa IP el protocolo número 41, y de ahí el nombre proto-41. De esta manera, los paquetes IPv6 pueden ser enviados sobre una infraestructura IPv4. Hay muchas tecnologías de túneles disponibles. La principal diferencia está en el método que usan los nodos encapsuladores para determinar la dirección a la salida del túnel.

Estas tecnologías incluyen túneles **6to4, ISATAP, y Teredo** que proporcionan la asignación de direcciones y túnel automático para el tráfico IPv6 Unicast host-to-host cuando los hosts de IPv6 deben atravesar redes IP4 para llegar a otras redes IPv6.

Teredo es una tecnología de transición que proporciona conectividad IPv6 a hosts que soportan IPv6 pero que se encuentran conectados a Internet mediante una red IPv4. Comparado con otros protocolos similares, la característica que lo distingue es que es capaz de realizar su función **incluso detrás de dispositivos NAT, como los routers domésticos**.

Teredo opera usando un protocolo de túneles independiente de la plataforma diseñado para proporcionar conectividad IPv6 **encapsulando los datagramas IPv6 dentro de datagramas UDP IPv4**. Estos datagramas pueden ser encaminados en Internet IPv4 y a través de dispositivos NAT. Otros nodos Teredo, también llamados Teredo relays, que tienen acceso a la red IPv6, reciben los paquetes, los desencapsulan y los encaminan.

Teredo está diseñado como una tecnología de transición con el objetivo de ser una medida temporal. En el largo plazo, todos los hosts IPv6 deberían usar la conectividad IPv6 nativa y desactivar Teredo cuando la conectividad IPv6 esté disponible.

Teredo fue desarrollado por Christian Huitema en Microsoft y fue estandarizado por la IETF como RFC 4380. El servidor teredo escucha en el **puerto UDP 3544**.

El protocolo de túneles IPv6 sobre IPv4 más común, 6to4, requiere que el final del túnel tenga una dirección IPv4 pública. Sin embargo, actualmente muchos hosts se conectan a Internet IPv4 a través de uno o varios dispositivos NAT, por lo general por el agotamiento de las direcciones IPv4. En esta situación, la única dirección IPv4 pública se asigna al dispositivo NAT y es necesario que el protocolo 6to4 esté implementado en este dispositivo. Muchos de los dispositivos NAT usados actualmente no pueden ser actualizados para implementar 6to4 por razones técnicas o económicas.

Teredo soluciona este problema encapsulando paquetes IPv6 dentro de datagramas UDP IPv4, los cuales pueden ser reenviados correctamente por NATs. Por lo tanto los hosts IPv6 que se encuentran detrás de dispositivos NAT pueden usar los túneles Teredo incluso si no disponen de una dirección IPv4 pública. Un host que implemente Teredo puede tener conectividad IPv6 sin cooperación por parte de la red local o del dispositivo NAT.

Teredo pretende ser una medida temporal. En el largo plazo todos los hosts deberían usar la conectividad nativa IPv6. El protocolo Teredo incluye una disposición para el proceso de extinción del protocolo: «Una implementación

Teredo debería proporcionar una forma para dejar de usar la conectividad Teredo cuando IPv6 haya madurado y la conectividad esté disponible usando un mecanismo menos frágil».

Miredo es un cliente libre de túneles Teredo diseñado para permitir conectividad IPv6 a ordenadores que se encuentran en redes IPv4 y que no tienen acceso directo a una red IPv6.

Miredo está incluido en muchas distribuciones Linux y BSD y también está disponible para las versiones recientes de Mac OS X.

Incluye implementaciones de los tres componentes de especificación Teredo: cliente, relay y servidor.

Está liberado bajo los términos de la licencia GNU General Public License, Miredo es software libre.

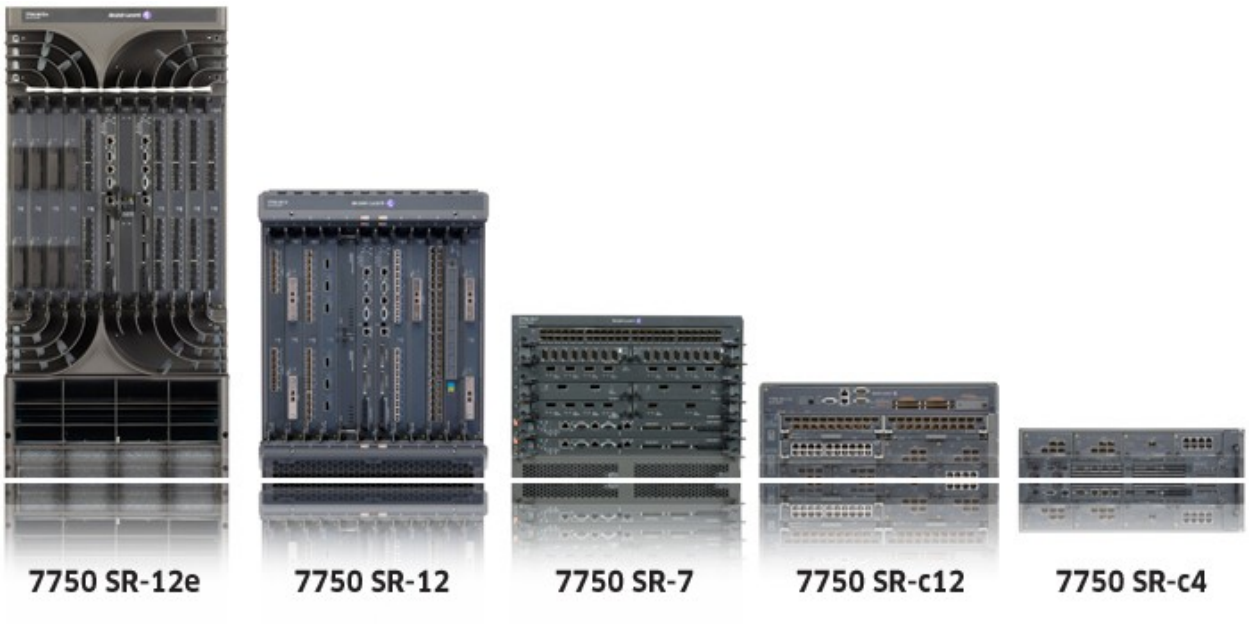
Traducción

La traducción es necesaria cuando un nodo solo IPv4 intenta comunicar con un nodo solo IPv6.

Actualmente el protocolo IPv6 está soportado en la mayoría de los sistemas operativos modernos, en algunos casos como una opción de instalación. Linux, Solaris, Mac OS, OpenBSD, FreeBSD, Windows (2k, CE) y Symbian (dispositivos móviles) son sólo algunos de los sistemas operativos que pueden funcionar con IPv6.

8.3 Dispositivos

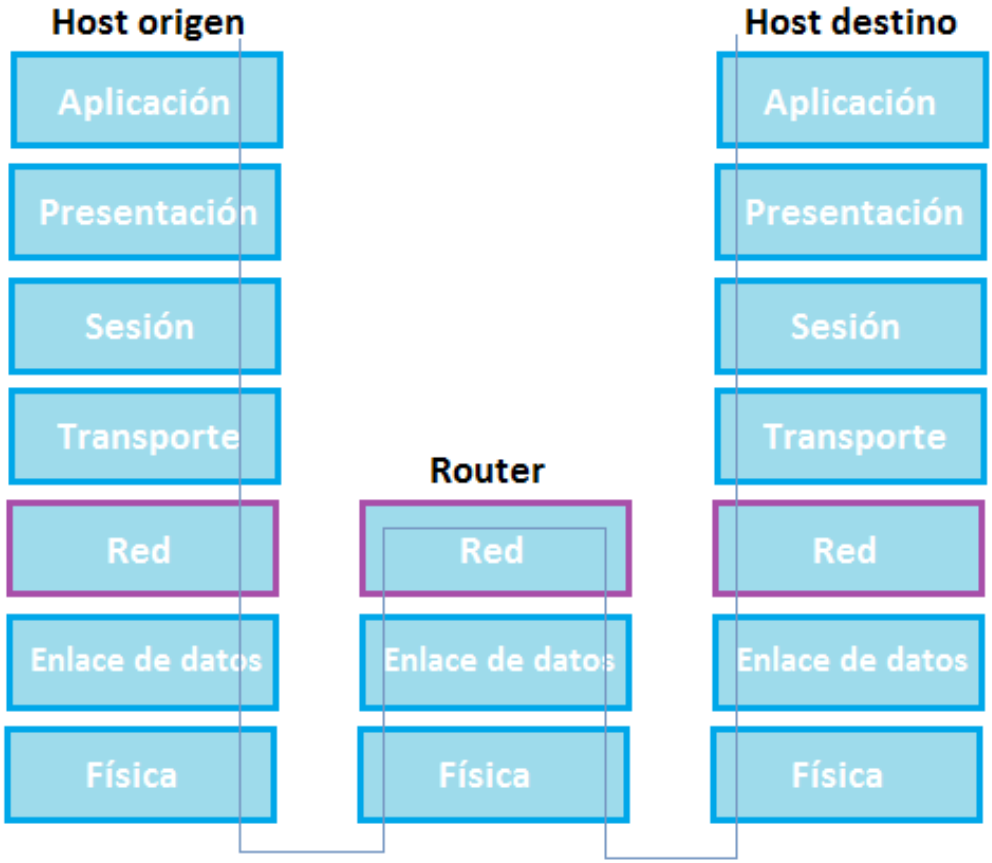
8.3.1 Routers

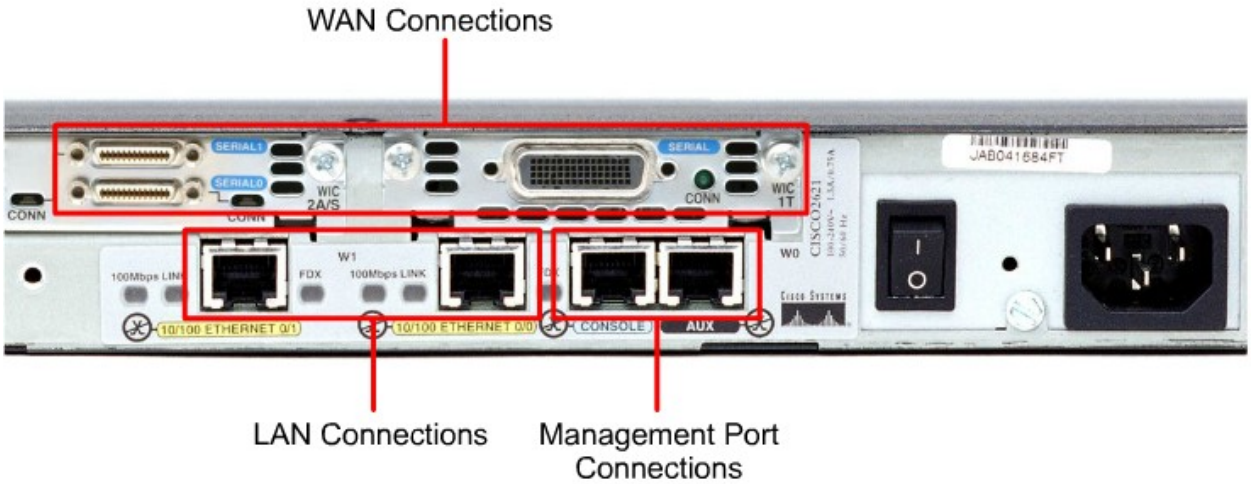


Un router —también conocido **enrutador o encaminador** de paquetes— es un dispositivo que proporciona conectividad a **nivel de red** o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador.

Conexiones

Los tres tipos básicos de conexiones de un router son:


Host origen
Aplicación
Presentación
Sesión
Transporte
Red
Enlace de datos
Física
Router
Red
Enlace de datos
Física
Host destino
Aplicación
Presentación
Sesión
Transporte
Red
Enlace de datos
Física


WAN Connections
LAN Connections
Management Port Connections
CONSOLE
AUX

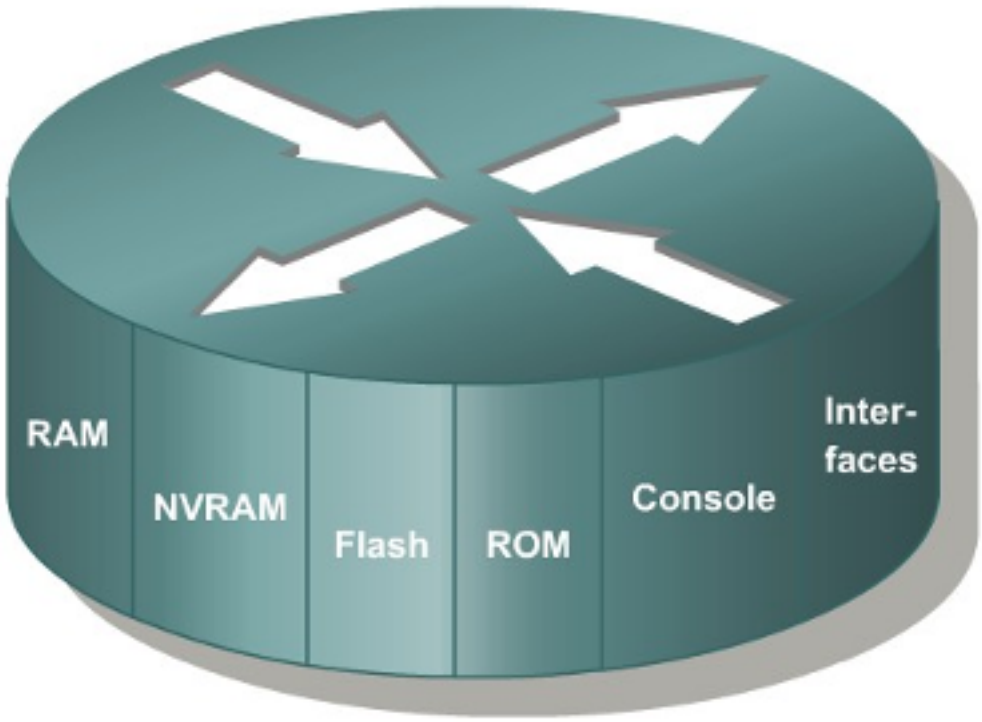
- **interfaces LAN**
- **interfaces WAN**
- **puertos de gestión**

Las interfaces LAN permiten que el router pueda conectarse a la red de área local. Esto es por lo general algún tipo de Ethernet. Sin embargo, podría haber alguna otra tecnología LAN tales como Token Ring o modo de transferencia asíncrono (ATM).

Las conexiones de red de área amplia proporcionan conexiones a través de un proveedor de servicio a un sitio lejano o con Internet. Estos pueden ser conexiones en serie o cualquier número de otras interfaces WAN. Con algunos tipos de interfaces WAN, se requiere un dispositivo externo, para conectar el router a la conexión local del proveedor de servicios. Con otros tipos de conexiones WAN, el router puede estar conectado directamente al proveedor de servicios.

La función de los puertos de gestión es diferente de las demás conexiones. Las conexiones LAN y WAN proporcionan conexiones de red a través del cual se transmiten los paquetes. El puerto de gestión proporciona una conexión basada en texto para la configuración y solución de problemas del enrutador. Las interfaces de administración comunes son la consola y el puerto auxiliar. Estos son puertos serie asíncronos EIA- 232. Se conectan a un puerto de comunicaciones en un ordenador. El equipo debe ejecutar un programa de emulación de terminal para proporcionar una sesión basada en texto con el router. A través de esta sesión el administrador de red puede administrar el dispositivo.

Almacenamiento



ROM

La memoria de solo lectura (ROM) se utiliza para almacenar de forma permanente el código de diagnóstico de inicio (Monitor de ROM). Las tareas principales de la ROM son el diagnóstico del hardware durante el arranque del router y la carga del software IOS de Cisco desde la memoria flash a la RAM. Algunos routers también tienen una versión más básica del IOS que puede usarse como fuente alternativa

de arranque. Las memorias ROM no se pueden borrar. Sólo pueden actualizarse reemplazando los chips de ROM.

RAM

La memoria de acceso aleatorio (RAM) se usa para la información de las tablas de enrutamiento, el caché de conmutación rápida, la configuración actual y las colas de paquetes. En la mayoría de los routers, la RAM proporciona espacio de tiempo de ejecución para el software IOS de Cisco y sus subsistemas. Por lo general, la RAM se divide de forma lógica en memoria del procesador principal y memoria compartida de entrada / salida (I/O). Las interfaces de almacenamiento temporal de los paquetes comparten la memoria de I/O compartida. El contenido de la RAM se pierde cuando se apaga la unidad. En general, la RAM es una memoria de acceso aleatorio dinámica (DRAM) y puede actualizarse agregando más módulos de memoria en línea doble (DIMM).

Memoria flash

La memoria flash se utiliza para almacenar una imagen completa del software IOS de Cisco. Normalmente el router adquiere el IOS por defecto de la memoria flash. Estas imágenes pueden actualizarse cargando una nueva imagen en la memoria flash. El IOS puede estar comprimido o no. En la mayoría de los routers, una copia ejecutable del IOS se transfiere a la RAM durante el proceso de arranque*. En otros routers, el IOS puede ejecutarse directamente desde la memoria flash. Agregando o reemplazando los módulos de memoria en línea simples flash (SIMMs) o las tarjetas PCMCIA se puede actualizar la cantidad de memoria flash.

NVRAM

La memoria de acceso aleatorio no volátil (NVRAM) se utiliza para guardar la configuración de inicio. En algunos dispositivos, la NVRAM se implementa utilizando distintas memorias de solo lectura programables, que se pueden borrar electrónicamente (EEPROM).En otros dispositivos, se implementa en el mismo dispositivo de memoria flash desde donde se argó el código de arranque. En cualquiera de los casos, estos dispositivos retienen sus contenidos cuando se apaga la unidad.

Proceso de arranque de un router

El proceso de arranque está conformado por cuatro etapas principales:

1. **Ejecución de la POST**

   La prueba de autocomprobación de encendido (POST) es un proceso común que ocurre en casi todas las computadoras durante el arranque. El proceso de POST se utiliza para probar el hardware del router. Cuando se enciende el router, el software en el chip de la ROM ejecuta el POST. Durante esta autocomprobación, el router ejecuta diagnósticos desde la ROM a varios componentes de hardware, entre ellos la CPU, la RAM y la NVRAM. Después de completarse la POST, el router ejecuta el programa bootstrap.

2. **Carga del programa bootstrap**

   Después de la POST, el programa bootstrap se copia de la ROM a la RAM. Una vez en la RAM, la CPU ejecuta las instrucciones del programa bootstrap. La tarea principal del programa bootstrap es ubicar al IOS y cargarlo en la RAM.

3. **Ubicación y carga del IOS**

   El IOS normalmente se almacena en la memoria flash, pero también puede almacenarse en otros lugares como un servidor TFTP (Trivial File Transfer Protocol).

   Si no se puede encontrar una imagen IOS completa, se copia una versión más básica del IOS de la ROM a la RAM. Esta versión del IOS se usa para ayudar a diagnosticar cualquier problema y puede usarse para cargar una versión completa del IOS en la RAM.

Algunos de los routers más antiguos ejecutan el IOS directamente desde la memoria flash, pero los modelos actuales copian el IOS en la RAM para que la CPU lo ejecute.

4. **Ubicación y carga del archivo de configuración**

   Ubicación del archivo de configuración de inicio. Después de cargar el IOS, el programa bootstrap busca en la NVRAM el archivo de configuración de inicio, conocido como startup-config. El archivo contiene los parámetros y comandos de configuración previamente guardados, entre ellos:

   - direcciones de interfaz
   - información de enrutamiento
   - contraseñas
   - cualquier otra configuración guardada por el administrador de red

   Si el archivo de configuración de inicio, **startup-config**, se encuentra en la **NVRAM**, se copia en la RAM como el archivo de configuración en ejecución, **running-config**.

   A partir de aquí podemos conectar al router y según la plataforma y el IOS, el router podrá realizar diferentes tareas.

8.4 Referencias

- http://www.cisco.com/web/learning/netacad/demos/CCNA2v3Demo/ch1/1_1_2/index.html
- http://www.suarezdefigueroa.es/manuel/PAR
- https://www.youtube.com/watch?v=IvVv-BaIiLk
- Tipos de direcciones IPv6

8.5 Actividades

8.5.1 Actividades de conceptos básicos

An example of using interpreted text

1. Imagina que te dan un router y te piden que lo configures. Indica los pasos que debes seguir para tener acceso a él.
2. Visita la página http://www.tp-link.com/en/support/emulators/ y elige 1 router. Haz un pequeño manual donde se explique las distintas opciones de estado y configuración de las que dispone.
3. Hemos contratado un ADSL con PepePhone. Nos sale más barato que la competencia, además si disponemos de router podemos utilizarlo. Realiza la configuración del router tal como nos indica la empresa:

```
Parámetros obligatorios (en la sección WAN)

ATM PVC VPI: 0
ATM PVC VCI: 33
PROTOCOLO DE RED: PPPoE
MODO DE ENCAPSULACIÓN: LLC
USER NAME (PPP): pepephone@pepephone
Password NAME (PPP): < pepephone > o puedes dejarlo vacio.
```

4. Direcciones IPv4. Tacha las direcciones IP inválidas.

a) 1.1.1.1

b) 2.2.2.200

c) 200.260.0.3

d) 4.4.4.4.4

e) 5.0.0.300

f) 256.244.244.4

g) 700.1000.100

h) 0.0.0.0

i) 255.255.255.255

5. Direcciones IPv4 especiales. ¿Qué significado tienen las siguientes direcciones?

   a) 127.0.0.1

   b) 127.1.1.0

   c) 127.127.127.127

   d) 127.3.3.4

   e) 0.0.0.0

   f) 255.255.255.255

   g) 10.255.255.255

   h) 192.168.1.255

   i) 172.16.255.255

   j) 10.0.0.0

   k) 172.16.0.0

   l) 192.168.0.0

6. Direcciones IP reservadas. Máscaras. Para las siguientes direcciones indicar máscara y si son o no reservadas para redes privadas.

   a) 127.0.0.1

   b) 8.8.8.8

   c) 10.2.2.2

   d) 169.254.254.254

   e) 169.254.3.2

   f) 192.168.1.254

   g) 172.16.55.55

   h) 10.0.0.1

   i) 2.2.3.0

   j) 2.1.0.0

   k) 172.16.1.0

   l) 192.168.0.1

m) 198.164.2.3

n) 1.0.0.1

7. ¿Cuántas redes privadas de clase A tenemos? ¿Cuántos equipos tiene cada una?
8. ¿Cuántas redes privadas de clase B tenemos? ¿Cuántos equipos tiene cada una?
9. ¿Cuántas redes privadas de clase C tenemos? ¿Cuántos equipos tiene cada una?
10. Direcciones IPv6. Tacha las direcciones IP inválidas para Unicast global.

    a) 2001:0db8:85a3:0000:0000:8a2e:0370:7334

    b) 2001:db8:85a3:8d3:1319:8a2e:370:7348

    c) 2001::1

    d) 2001:af:3::1

    e) 2001:0:0:0:0:0:0:1

    f) 2001::12a6::1

    g) 2002::3:abcd:2

    h) 3333:ffff::1

    i) 3777:ada:fea::34

11. Busca información acerca de qué es el EUI-64 y el EUI-64 modificado. Para la siguiente MAC (00:11:22:33:44:55) ¿cómo quedaría su EUI-64 y su EUI-64 modificado?
12. EUI-64 modificado. ¿Cuál es la MAC de tu tarjeta de red? Basándote en la dirección MAC de tu tarjeta calcula la dirección IPv6 automática de enlace local (fe80:1111:2222:3333::/10).
13. EUI-64 modificado. ¿Cuál es la MAC de tu tarjeta de red? Basándote en la dirección MAC de tu tarjeta calcula la dirección IPv6 automática global unicast (2001::/32).
14. En un instituto tenemos 2 líneas ADSL de distintos proveedores cada una con su router. Si realizamos balanceo de carga, ¿cuáles serán los beneficios obtenidos?

8.5.2 Actividades de Packet Tracer

1. Elabora un esquema donde aparezcan 2 PC conectados entre sí con IP estática privada en la red 10.0.0.0.
2. Elabora un esquema donde aparezcan 4 PC conectados a un switch con IP estática privada en la red 172.16.0.0.
3. Elabora un esquema donde aparezcan 4 PC conectados a un switch con IP dinámica privada en la red 192.168.30.0. Debes poner en la red un servidor DHCP que asigne direcciones en dicho rango.
4. Añade al ejercicio anterior un servidor web y comprueba que los clientes pueden acceder a él.
5. Añade al ejercicio anterior un servidor DNS y configura en él el nombre www.mired.es para el servidor web. Comprueba que los PC pueden acceder al servidor web mediante su nombre.
6. Elabora un esquema donde existan 3 redes de 4 equipos cada una conectadas a un router. Cada red debe tener direcciones privadas dinámicas (una red de clase A, otra de clase B y la otra de clase C). Comprueba que hay comunicación entre ellas.
7. Añade al ejercicio anterior un servidor DNS y un servidor web en la red de clase A. Configura todos los PCs para que puedan acceder al servidor web mediante el nombre dado de alta en el servidor DNS.

8.5.3 Actividades resueltas de subnetting

1. Calcular la dirección de red y dirección de broadcasting (difusión) de las máquinas con las siguientes direcciones IP y máscaras de subred (si no se especifica, se utiliza la máscara por defecto):

1. **18.120.16.250**:

```
máscara 255.0.0.0
red 18.0.0.0
broadcasting 18.255.255.255
```

2. **18.120.16.255 / 255.255.0.0**:

```
red 18.120.0.0
broadcasting 18.120.255.255
```

3. **155.4.220.39**:

```
máscara 255.255.0.0
red 155.4.0.0
broadcasting 155.24.255.255
```

4. **194.209.14.33**:

```
máscara 255.255.255.0
red 194.209.14.0
broadcasting 194.209.14.255
```

5. **190.33.109.133 / 255.255.255.0**:

```
red 190.33.109.0
broadcasting 190.33.109.255
```

2. Suponiendo que nuestro ordenador tiene la dirección IP 192.168.5.65 con máscara 255.255.255.0, indicar qué significan las siguientes direcciones especiales:

1. **0.0.0.0**: nuestro ordenador
2. **0.0.0.29**: 192.168.5.29
3. **192.168.67.0**: la red 192.168.67.0
4. **255.255.255.255**: broadcasting a la red 192.168.5.0 (la nuestra)
5. **192.130.10.255**: broadcasting a la red 192.130.10.0
6. **127.0.0.1**: 192.168.5.65 (loopback)

3. Calcular la dirección de red y dirección de broadcasting (difusión) de las máquinas con las siguientes direcciones IP y máscaras de subred:

1. **190.33.109.133 / 255.255.255.128**:

```
red 190.33.109.128
broadcasting 190.33.109.255
(133=10000101, 128=10000000, 127=01111111)
```

2. **192.168.20.25 / 255.255.255.240**:

```
red 192.168.20.16
broadcasting 192.168.20.31
(25=00011001, 240=11110000, 16=00010000, 31=00011111)
```

3. **192.168.20.25 / 255.255.255.224**:

```
red 192.168.20.0
broadcasting 192.168.20.31
(25=00011001, 224=11100000, 31=00011111)
```

4. **192.168.20.25 / 255.255.255.192**:

```
red 192.168.20.0
broadcasting 192.168.20.63
(25=00011001, 192=11000000, 63=00111111)
```

5. **140.190.20.10 / 255.255.192.0**:

```
red 140.190.0.0
broadcasting 140.190.63.255
(020=00010100, 192=11000000, 063=00111111)
```

6. **40.190.130.10 / 255.255.192.0**:

```
red 140.190.128.0
broadcasting 140.190.191.255
(130=10000010, 192=11000000, 128=10000000, 063=00111111, 191=10111111)
```

7. **140.190.220.10 / 255.255.192.0**:

```
red 140.190.192.0
broadcasting 140.190.255.255
(220=11011100, 192=11000000, 063=00111111, 255=11111111)
```

4. Viendo las direcciones IP de los hosts públicos de una empresa observamos que todas están comprendidas entre 194.143.17.145 y 194.143.17.158, ¿Cuál es (probablemente) su dirección de red, broadcasting y máscara?

   Pasamos a binario las dos direcciones. La primera tiene que estar próxima a la dirección de red y la última, a la dirección de broadcasting:

```
194.143.017.145   11000010.10001111.00010001.10010001
194.143.017.158   11000010.10001111.00010001.10011110
```

   Podemos suponer que la dirección de red es 194.143.17.144 y la de broadcasting, 194.143.17.159:

```
194.143.017.144     11000010.10001111.00010001.10010000
194.143.017.159     11000010.10001111.00010001.10011111
                    <------------------------------><-->
                                  RED                HOST
```

   Entonces la máscara será:

```
255.255.255.240     11111111.11111111.11111111.11110000
                    <------------------------------><-->
                                  RED                HOST
```

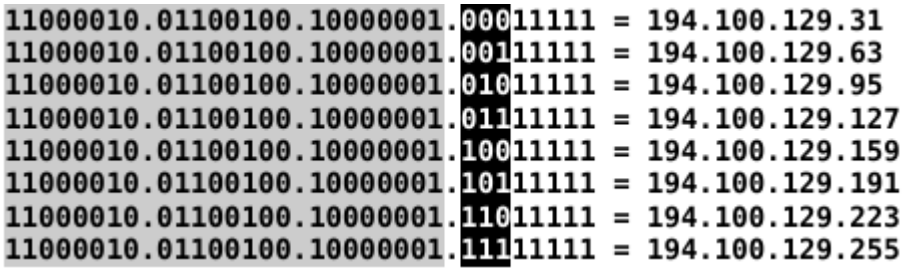
5. Un equipo tiene la IP 194.100.129.120. Si existen 8 subredes, indicar:
    1. clase y máscara por defecto
    2. máscara cuando dividimos la red en 8 subredes
    3. dirección de inicio (dirección de subred) y fin (dirección de difusión) de cada subred
    4. subred a la que pertenece la dirección IP
    5. número de IPs destinadas a equipos en cada subred

    IP 194.100.129.120. Existen 8 subredes
    1. IP de clase C. Máscara por defecto: 255.255.255.0.
    2. Subred

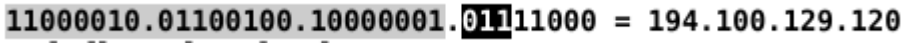
        Para obtener 8 subredes debemos ampliar la máscara anterior en 3 bits (23=8)

    3. Las direcciones de subred son:

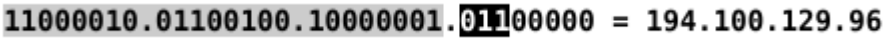
        Las direcciones de broadcast son:



    4. Nuestra IP



        se halla en la subred



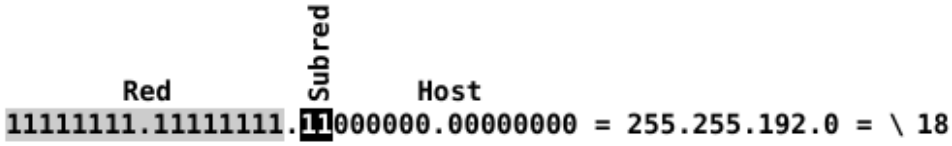
    5. Como existen 5 bits de hosts, el número total de IPs para hosts es 2^5-2
6. Un equipo tiene la IP 172.10.130.4. Si existen 4 subredes, indicar:
    1. clase y máscara por defecto

2. máscara cuando dividimos la red en 4 subredes
3. dirección de inicio (dirección de subred) y fin (dirección de difusión) de cada subred
4. subred a la que pertenece la dirección IP
5. número de IPs destinadas a equipos en cada subred

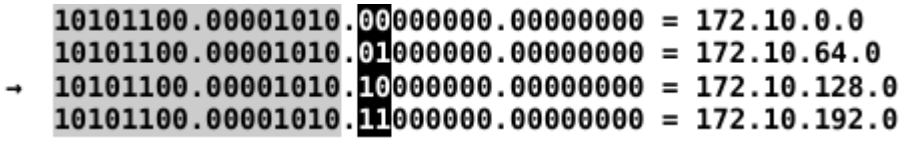
IP 172.10.130.4. Existen 4 subredes

1. IP de clase B. Máscara por defecto: 255.255.0.0.
2. Subred

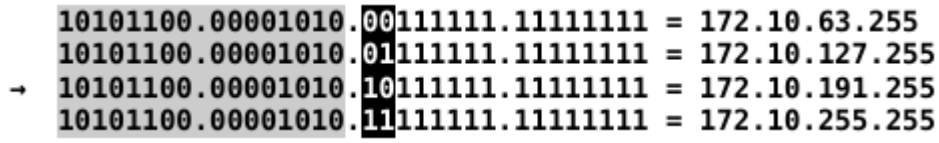
   Para obtener 4 subredes debemos ampliar la máscara anterior en 2 bits (22=4)



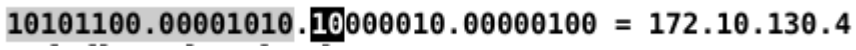
3. Las direcciones de subred son:



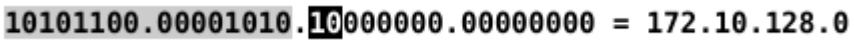
   Las direcciones de broadcast son:



4. Nuestra IP



   se halla en la subred



5. Como existen 14 bits de hosts, el número total de IPs para hosts es 214-2

8.5.4 Actividades a resolver de subnetting

1. ¿Cuál de las siguientes opciones representa la máscara 255.255.240.0?

1. /26
2. /18
3. /192
4. /20
5. /224
6. /22
7. /240

8. /16
9. /24
10. /27

2. ¿Qué máscaras de las siguientes son inválidas?

1. 255.128.255.0
2. 128.255.0.0
3. 255.0.0.255
4. 255.255.0.0
5. 255.254.0.0
6. 255.252.0.0
7. 255.248.0.0
8. 255.240.0.0
9. 255.224.0.0
10. 255.192.0.0
11. 255.128.0.0

3. Para las siguientes máscaras, indicar su formato corto en forma de longitud de prefijo.

1. 255.255.0.0
2. 255.0.0.0
3. 255.255.255.0
4. 255.128.0.0
5. 255.255.0.0
6. 255.254.0.0
7. 255.252.0.0
8. 255.248.0.0
9. 255.240.0.0
10. 255.224.0.0
11. 255.192.0.0
12. 255.128.0.0

4. ¿A qué subredes pertenecen estos hosts?

1. 192.168.10.104/27
2. 192.168.10.144/28
3. 192.176.12.242/26
4. 122.122.239.12/19

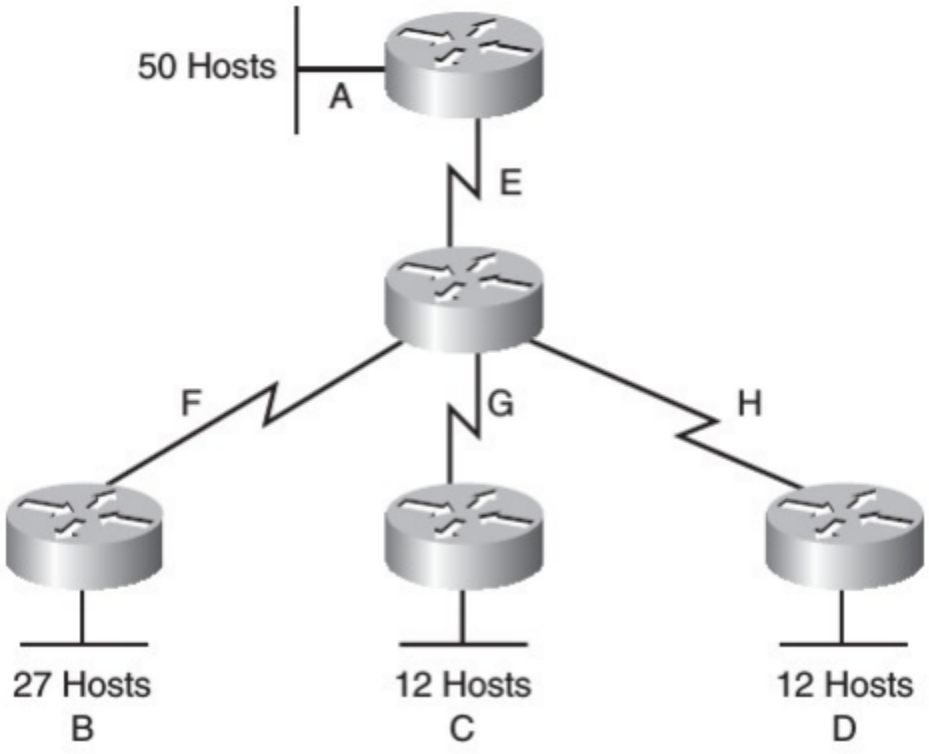
5. Dada la dirección 134.141.7.11 y la máscara 255.255.255.0, ¿Cuál es el número de subred?
6. Dada la dirección 193.193.7.7 y la máscara 255.255.255.0 ¿cuál es el número de subred y cuál es la dirección de broadcast?

7. Dada la dirección 200.1.1.130 y la máscara 255.255.255.224 ¿cuál es el número de subred y cuál es la dirección de broadcast?
8. Dada la IP 220.8.7.100/28, ¿Cuál es la dirección de subred y cuál es la dirección de broadcast?
9. Dada la dirección IP 10.141.7.11/24 ¿Cuál es la dirección de subred y cuál es la dirección de broadcast?
10. Dada la dirección 134.141.7.11/24 ¿Cuáles son las direcciones IP válidas?
11. Dada la dirección 200.2.1.130/27 ¿Cuáles son las direcciones IP válidas?
12. Dada la IP 134.141.7.7/24, ¿cuáles son las números de subred válidos?
13. Dada la IP 220.8.7.100 y la máscara 255.255.255.240, ¿cuáles son las subredes válidas?
14. ¿Cuántas direcciones IP serán asignadas en cada subred de 134.141.0.0/24?
15. ¿Cuántas direcciones IP serán asignadas en cada subred de 220.8.7.0/28?
16. ¿Cuántas direcciones IP serán asignadas en cada subred de 10.0.0.0/14?
17. ¿Cuántas direcciones IP serán asignadas en cada subred de 11.0.0.0 255.192.0.0?
18. Un equipo tiene la IP 10.10.4.4. Si existen 256 subredes, indicar:
    - clase y máscara por defecto
    - máscara cuando dividimos la red en 256 subredes
    - dirección de inicio (dirección de subred) y fin (dirección de difusión) de cada subred (sólo las tres primeras)
    - subred a la que pertenece la dirección IP
    - número de IPs destinadas a equipos en cada subred
19. Diseñas una red para un cliente, y el cliente te pide que utilices la misma máscara de subred para todas las subredes. El cliente utiliza la red 10.0.0.0 y necesita 200 subredes, con 200 hosts como máximo en cada subred. ¿Qué máscara trabajará mejor y permitirá mayor crecimiento en el número de host por subred a futuro?

8.5.5 Actividades resueltas de VLSM

Subnetting

A partir de la red **192.168.100.0/24** hacer la subredes necesarias para obtener las mostradas en la siguiente figura.



Paso 0: ¿Cuantas IPs necesitamos?

```
Red A: 52. (50 + 2 -de red y broadcast-)
Red B: 29. (27 + 2 -de red y broadcast-)
Red C: 14. (12 + 2 -de red y broadcast-)
Red D: 14. (12 + 2 -de red y broadcast-)
Red E:  4. ( 2 + 2 -de red y broadcast-)
Red F:  4. ( 2 + 2 -de red y broadcast-)
Red G:  4. ( 2 + 2 -de red y broadcast-)
Red H:  4. ( 2 + 2 -de red y broadcast-)
```

Total: 52+29+14+14+4+4+4+4

Paso 1: ¿Tenemos espacio suficiente?

Comprobamos que disponemos de suficiente espacio de direcciones. Como una la red 192.168.100.0/24 dispone de 8 bits para hosts, tenemos 2^8 = 256 IPs (muchas más de las que necesitamos).

Paso 2: ¿Como las distribuimos?

```
Para la red A: Necesitamos un bloque de 64 IPs (2^6) >= 52
Para la red B: Necesitamos un bloque de 32 IPs (2^5) >= 29
Para la red C: Necesitamos un bloque de 16 IPs (2^4) >= 14
Para la red D: Necesitamos un bloque de 16 IPs (2^4) >= 14
Para la red E: Necesitamos un bloque de  4 IPs (2^2) >=  4
Para la red F: Necesitamos un bloque de  4 IPs (2^2) >=  4
Para la red G: Necesitamos un bloque de  4 IPs (2^2) >=  4
Para la red H: Necesitamos un bloque de  4 IPs (2^2) >=  4
```

Nota: En el párrafo anterior la notación 2^6 es equivalente a 2^6. Así con el resto de potencias.

```
Red A: 6 bits para hosts. Por tanto 2 bits para subred. Máscara: /26.
Red B: 5 bits para hosts. Por tanto 3 bits para subred. Máscara: /27.
Red C: 4 bits para hosts. Por tanto 4 bits para subred. Máscara: /28.
Red D: 4 bits para hosts. Por tanto 4 bits para subred. Máscara: /28.
Red E: 2 bits para hosts. Por tanto 6 bits para subred. Máscara: /30.
Red F: 2 bits para hosts. Por tanto 6 bits para subred. Máscara: /30.
Red G: 2 bits para hosts. Por tanto 6 bits para subred. Máscara: /30.
Red H: 2 bits para hosts. Por tanto 6 bits para subred. Máscara: /30.
```

Paso 3: Realizamos distribución

A continuación se muestra un cuadro de cómo hemos distribuido las subredes. No es la única solución. Podríamos haber escogido otra forma de distribuirlas, siempre que respetemos la máscara que debemos asignar a cada una y el número de IPs por subred.

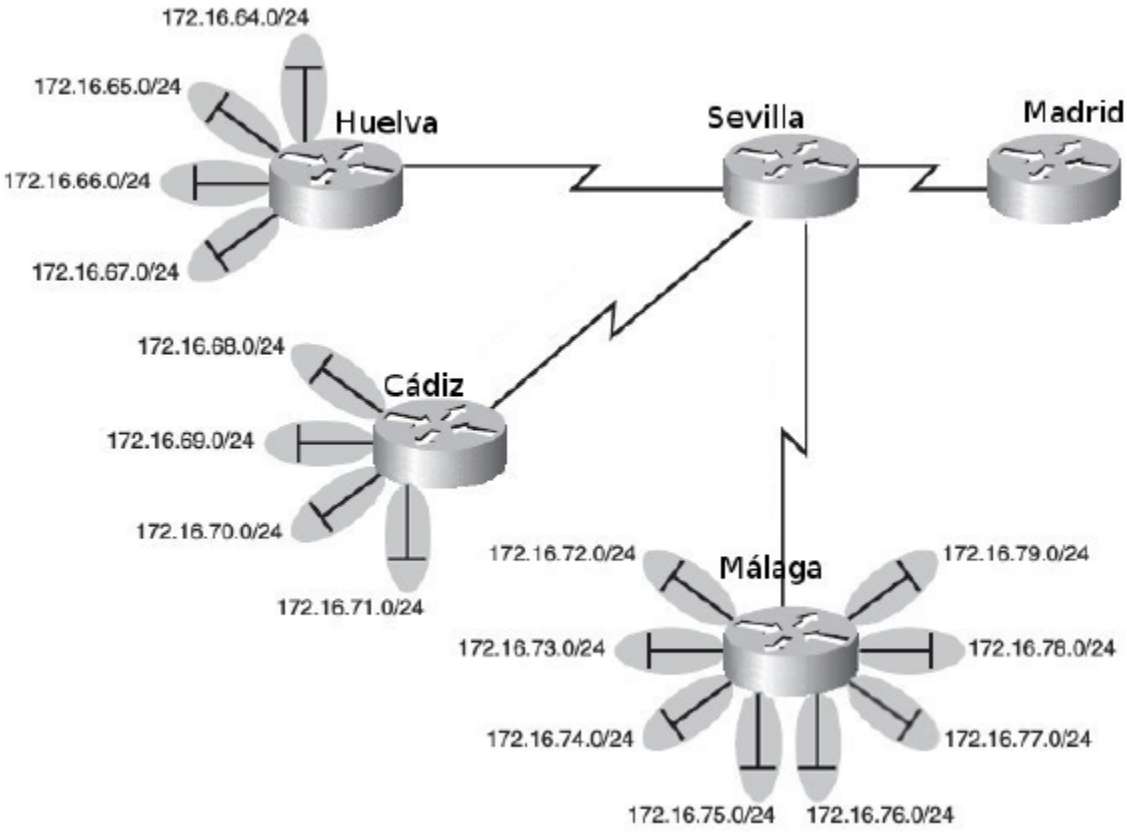
x=192.168.100

/24	/25	/26	/27	/28	/29	/30	Red	IPs	Hosts
x.0	x.0	x.0	x.0	x.0	x.0	x.0	E	4	2
						x.4	F	4	2
					x.8	x.8	G	4	2
						x.12	H	4	2
				x.16	Uso futuro			16	14
			x.32	Uso futuro				32	30
		x.64	A					64	62
	x.128	x.128	x.128	B				32	30
			x.160	x.160	C			16	14
				x.176	D			16	14
		x.192	Uso futuro					64	62
TOTAL								256	234

Las redes quedan de la siguiente forma:

```
Red A: 192.168.100.64/26
Red B: 192.168.100.128/27
Red C: 192.168.100.160/28
Red D: 192.168.100.176/28
Red E: 192.168.100.0/30
Red F: 192.168.100.4/30
Red G: 192.168.100.8/30
Red H: 192.168.100.12/30
```

Supernetting. Resumen de rutas



Resumen de Huelva

172.16.64.0 = 10101100.00010000.010000**00**.00000000

172.16.65.0 = 10101100.00010000.010000**01**.00000000

172.16.66.0 = 10101100.00010000.010000**10**.00000000

172.16.67.0 = 10101100.00010000.010000**11**.00000000

22 bits son comunes.

Por tanto la ruta resumida es 172.16.64.0/22

Resumen de Cádiz

172.16.68.0 = 10101100.00010000.01000100.00000000
172.16.69.0 = 10101100.00010000.01000101.00000000
172.16.70.0 = 10101100.00010000.01000110.00000000
172.16.71.0 = 10101100.00010000.01000111.00000000

22 bits son comunes.

Por tanto la ruta resumida es 172.16.68.0/22

Resumen de Málaga

172.16.72.0 = 10101100.00010000.01001000.00000000
172.16.73.0 = 10101100.00010000.01001001.00000000
172.16.74.0 = 10101100.00010000 01001010.00000000
172.16.75.0 = 10101100.00010000 01001011.00000000
172.16.76.0 = 10101100.00010000.01001100.00000000
172.16.77.0 = 10101100.00010000.01001101.00000000
172.16.78.0 = 10101100.00010000.01001110.00000000
172.16.79.0 = 10101100.00010000.01001111.00000000

21 bits son comunes.

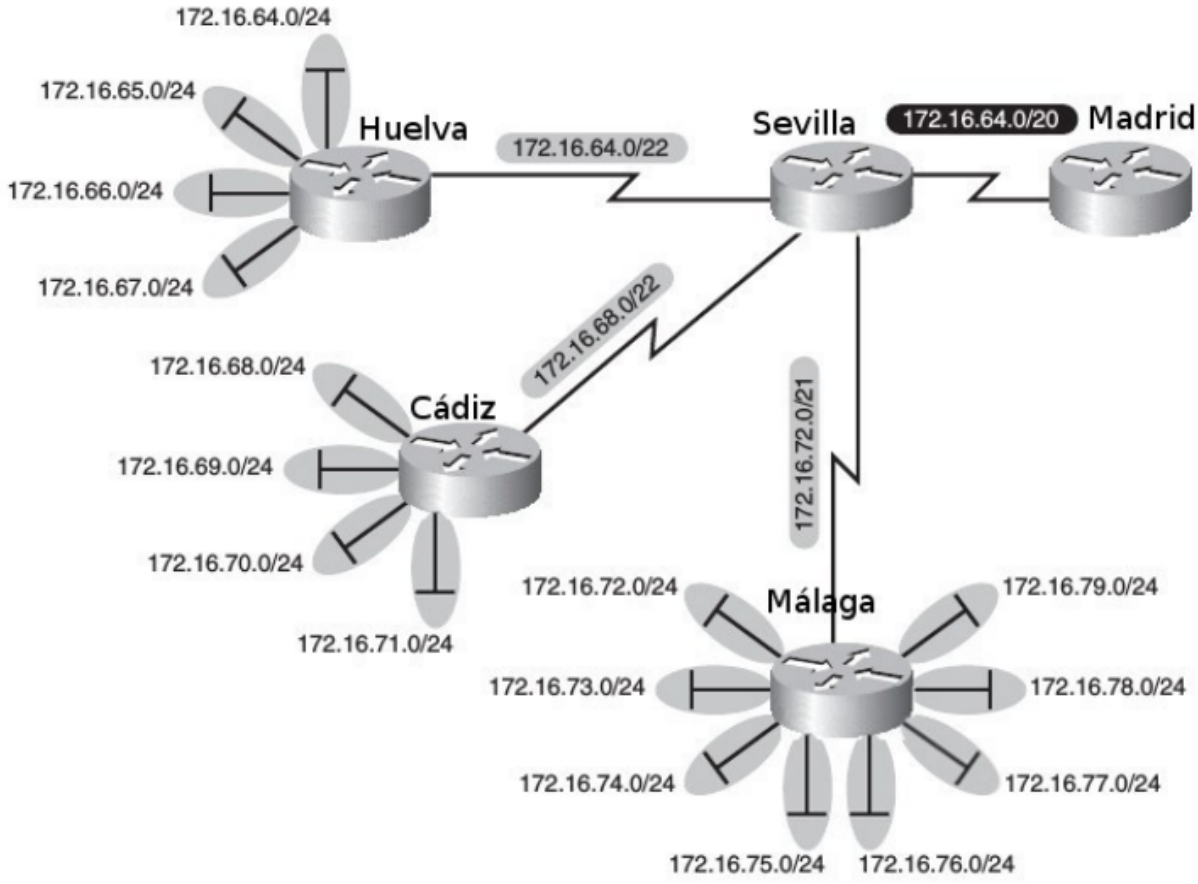
Por tanto la ruta resumida es 172.16.72.0/21

Resumen de Sevilla

172.16.64.0 = 10101100.00010000.01000000.00000000
172.16.68.0 = 10101100.00010000.01000100.00000000
172.16.72.0 = 10101100.00010000.01001000.00000000

20 bits son comunes.

Por tanto la ruta resumida es 172.16.64.0/20



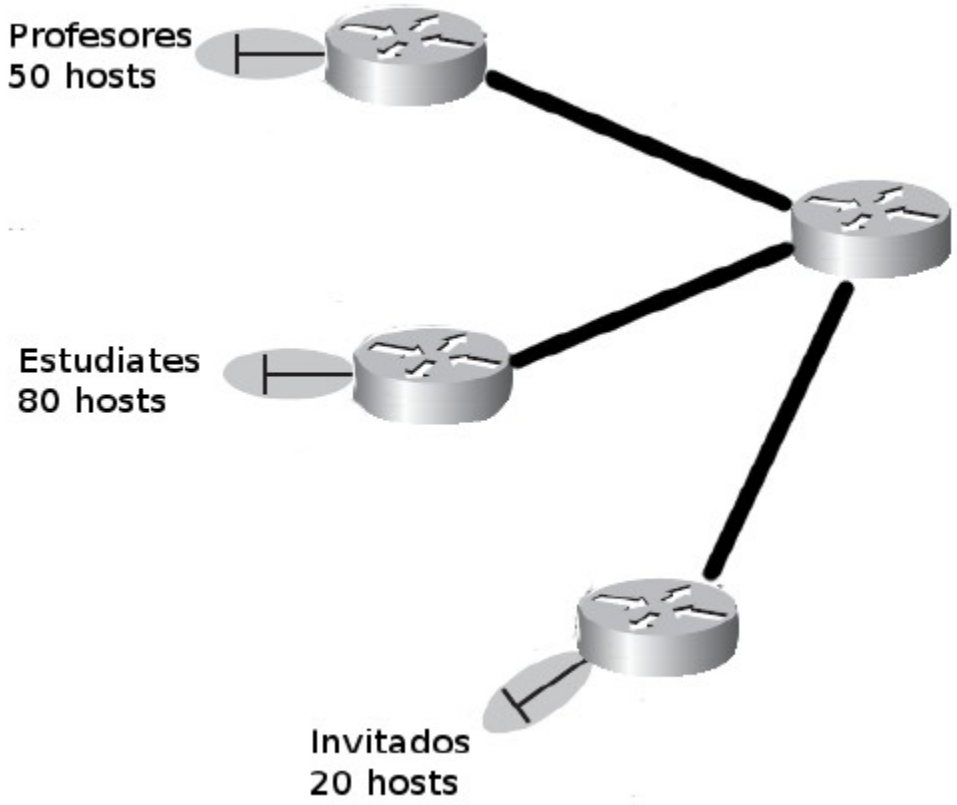
Resultado final

/20	/21	/22	/23	/24
172.16.64.0 Sevilla	172.16.64.0	172.16.64.0 Huelva	172.16.64.0	172.16.64.0
				172.16.65.0
			172.16.66.0	172.16.66.0
				172.16.67.0
		172.16.68.0 Cádiz	172.16.68.0	172.16.68.0
				172.16.69.0
			172.16.68.0	172.16.68.0
				172.16.71.0
	172.16.72.0 Málaga	172.16.72.0	172.16.72.0	172.16.72.0
				172.16.73.0
			172.16.74.0	172.16.74.0
				172.16.75.0
		172.16.76.0	172.16.76.0	172.16.76.0
				172.16.77.0
			172.16.78.0	172.16.78.0
				172.16.79.0

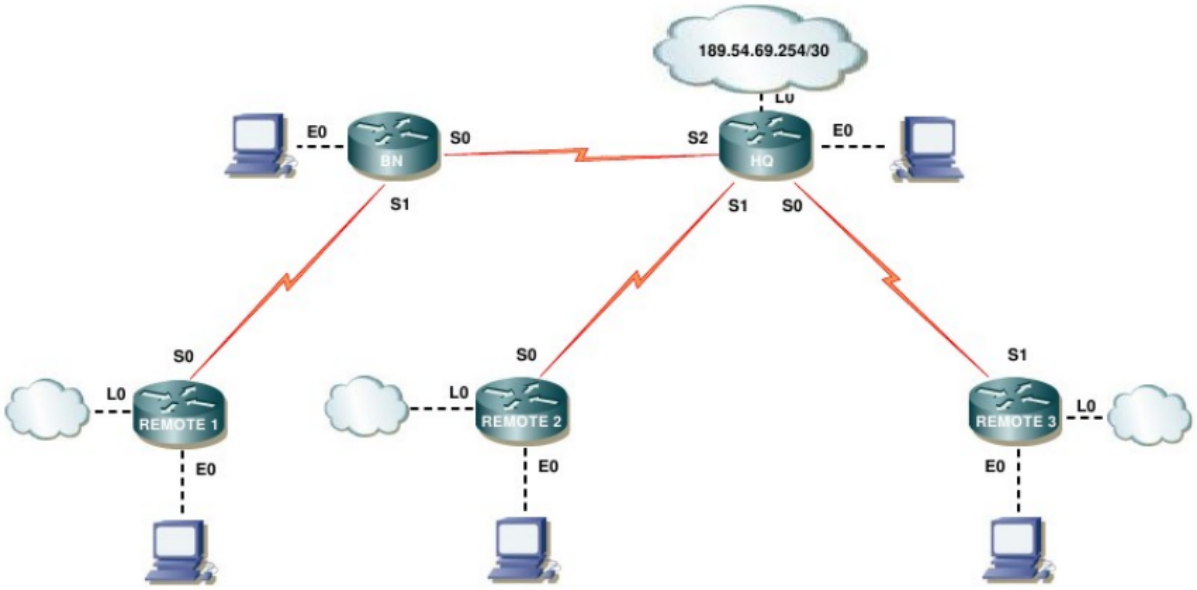
8.5.6 Actividades a resolver de VLSM

1. Dada la red 192.168.0.0/24, desarrolle un esquema de direccionamiento que cumpla con los siguientes requerimientos. Use VLSM, es decir, optimice el espacio de direccionamiento tanto como sea posible.

- Una subred de 50 hosts para ser asignada a los Profesores
- Una subred de 80 hosts para ser asignada a los Estudiantes
- Una subred de 20 hosts para ser asignada a los Invitados
- Tres subredes de 2 hosts para ser asignada a los enlaces entre routers.

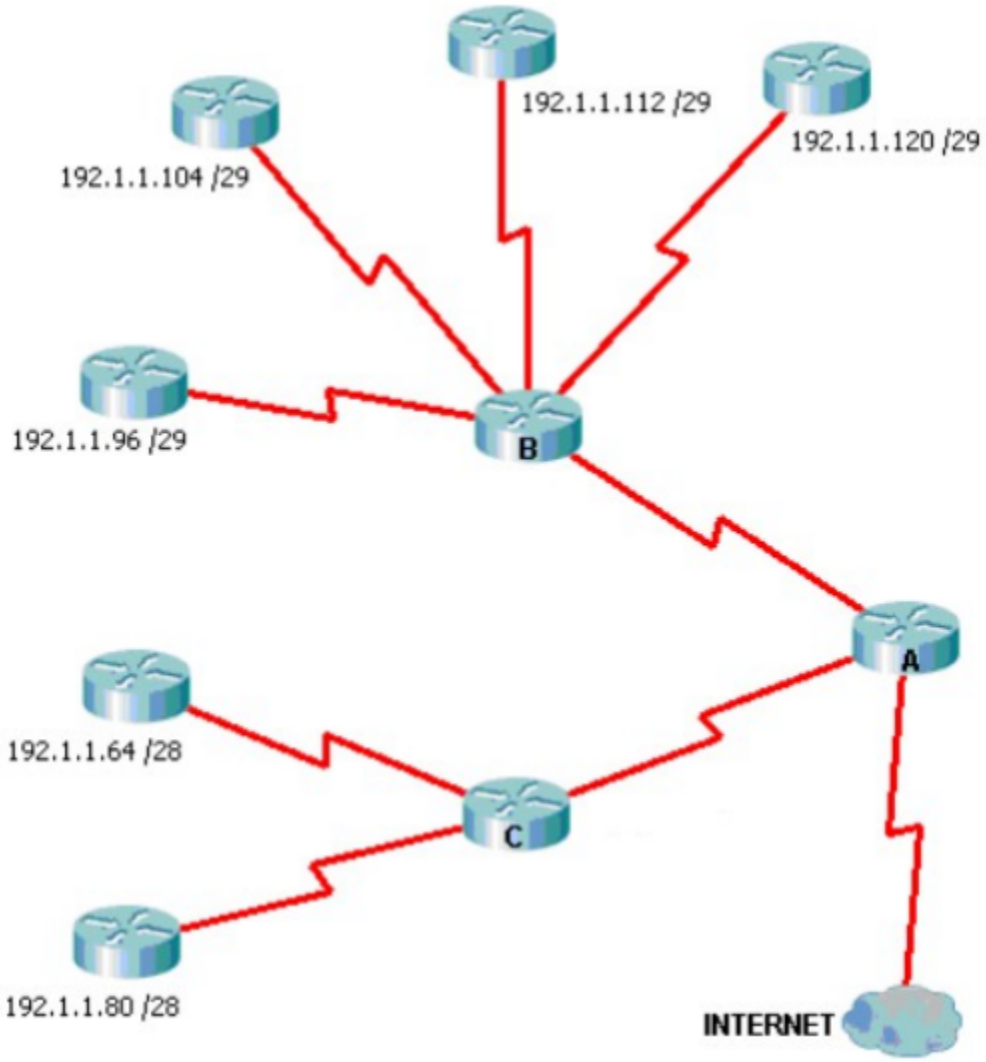


2. Usted es el administrador de la red para una escuela primaria local. Su primera tarea es hacer que la correcta distribución de IPs en la red. El ISP le ha dado a usted la dirección de red 177.19.156.0 y máscara 255.255.252.0. Realice el subnetting necesario según el esquema que se muestra más abajo. Comience las asignaciones de direcciones con el 177.19.157.0.



Subred	Interface	Num. de hosts	Dirección de red	Máscara de red
HQ	E0	90		
	L0	2		
Remote 1	E0	60		
	L0	30		
	S0	2		
Remote 2	E0	128		
	L0	60		
	S0	2		
BN	E0	60		
	S0	2		
Remote 3	E0	30		
	L0	30		
	S1	2		

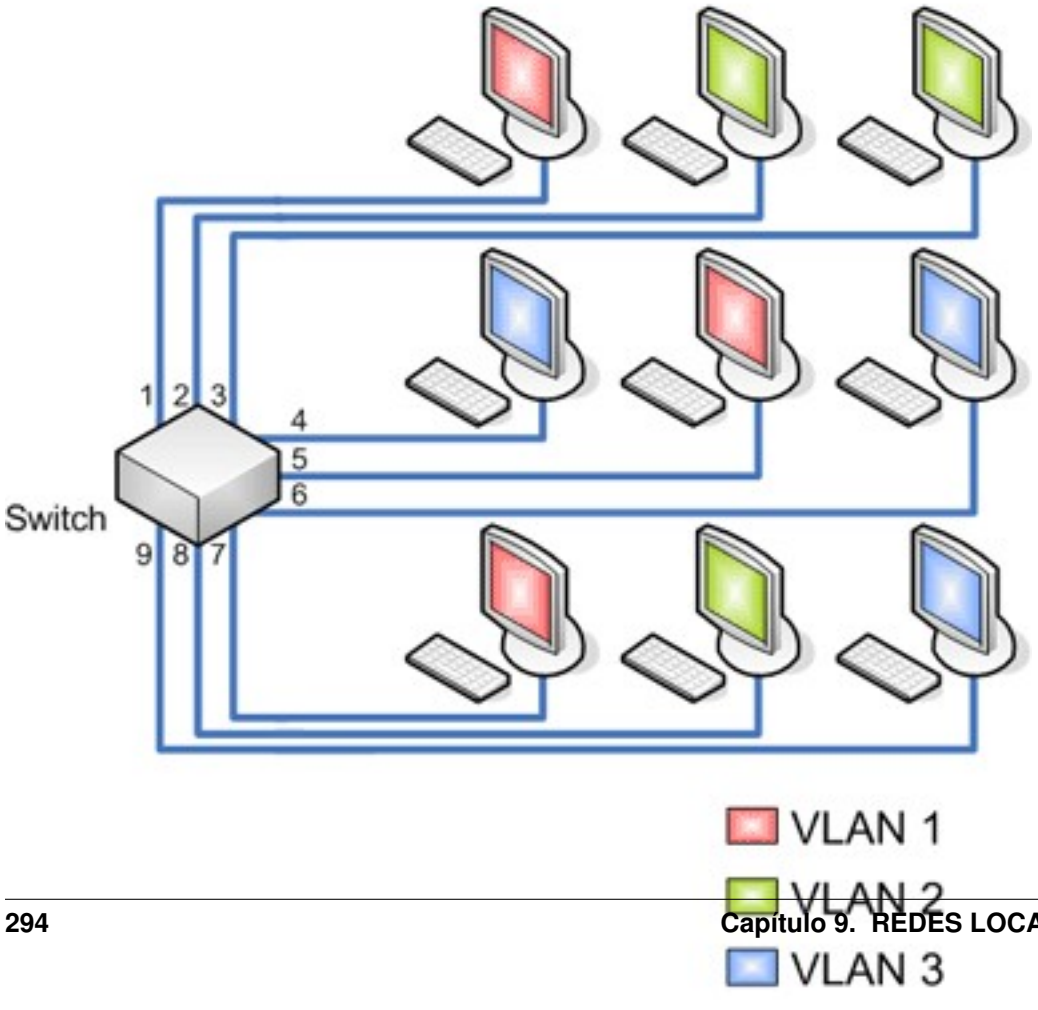
3. Sumarización de rutas. Tenemos esta red VLSM con subnetting y debemos averiguar cuál va a ser la dirección que va a publicar en Internet el router A.


192.1.1.112 /29
192.1.1.104 /29
192.1.1.120 /29
192.1.1.96 /29
B
A
192.1.1.64 /28
C
192.1.1.80 /28
INTERNET

CAPÍTULO 9

REDES LOCALES VIRTUALES

9.1 Introducción



Una **VLAN** (acrónimo de virtual LAN, «**red de área local virtual**») es un método para crear **redes lógicas independientes** dentro de una misma red física. Varias VLAN **pueden coexistir en un único conmutador físico** o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3).

9.1.1 Tipos de VLAN

Las dos aproximaciones más habituales para la asignación de miembros de una VLAN son las siguientes:

- VLAN estáticas
- VLAN dinámicas

Las **VLAN estáticas** también se denominan VLAN basadas en el **puerto**. Las asignaciones en una VLAN estática se crean mediante la asignación de los puertos de un switch o conmutador a dicha VLAN. Cuando un dispositivo entra en la red, automáticamente asume su pertenencia a la VLAN a la que ha sido asignado el puerto. Si el usuario cambia de puerto de entrada y necesita acceder a la misma VLAN, el administrador de la red debe cambiar manualmente la asignación a la VLAN del nuevo puerto de conexión en el switch.

En las **VLAN dinámicas**, el administrador de la red puede asignar los puertos que pertenecen a una VLAN de manera automática basándose en información tal como la **dirección MAC** del dispositivo que se conecta al puerto o el nombre de usuario utilizado para acceder al dispositivo. En este procedimiento, el dispositivo que accede a la red, hace una consulta a la base de datos de miembros de la VLAN.

9.1.2 Características

- Las VLANs permiten dividir la red local en redes virtuales
- Los equipos de la red que pertenecen a la misma VLAN pueden comunicarse entre ellos como si estuvieran conectados al mismo switch
- La comunicación entre estaciones de diferentes VLANs requiere un dispositivo de nivel 3
- A cada VLAN se le asigna un identificador de distinto color:
  - Los puertos de los switches quedan coloreados
  - Los puertos que unen switches se considera que pertenecen a la unión de los colores de los dos switches
- Sólo se envía una trama por un puerto cuando la LAN origen y destino tienen el mismo color (es decir, ambos puertos pertenecen a la misma VLAN)

9.1.3 Ventajas

- Permiten reconfigurar si hay un cambio sin tocar cables ni switches
- Aumenta la seguridad
- Aumenta el rendimiento de la red al separar dominios de difusión
- La organización de la red se basa en las tareas de los usuarios y no en su localización física.

9.2 Conceptos generales

9.2.1 Tipos de puertos

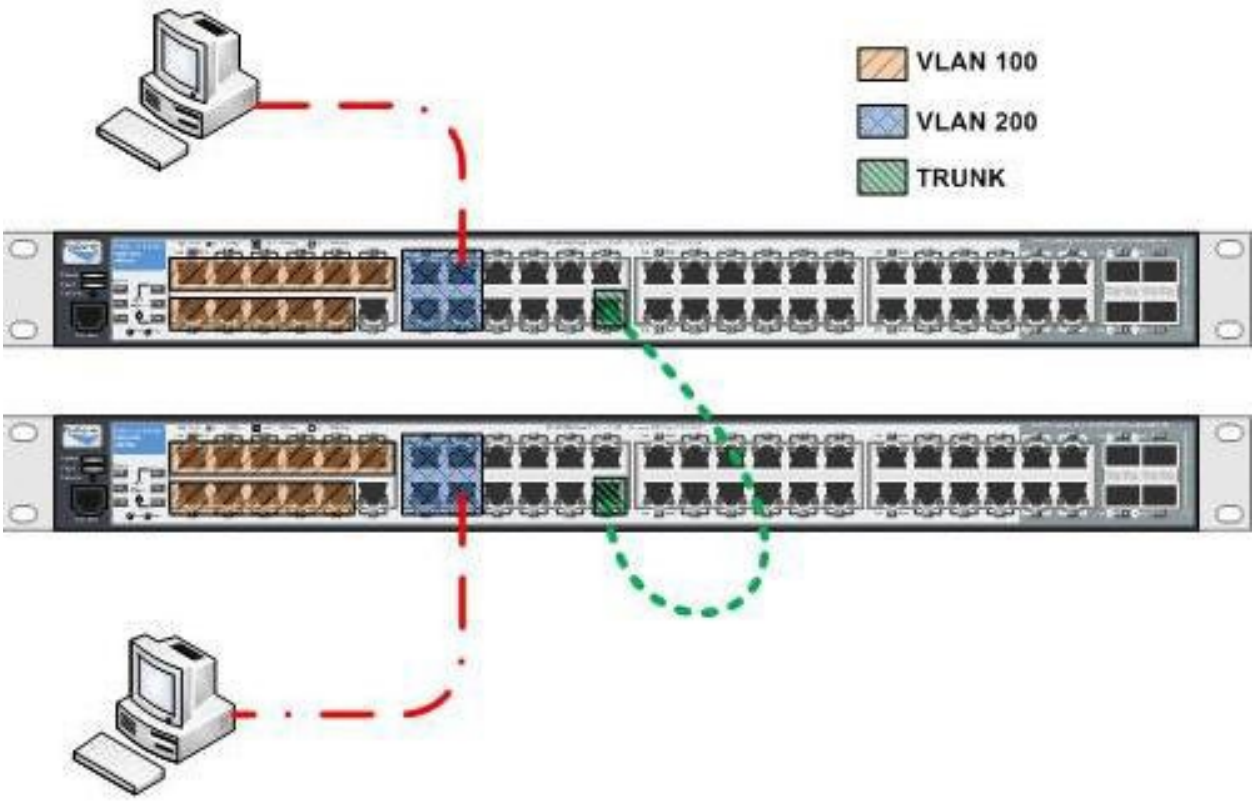
En un switch, atendiendo a su función dentro de la VLAN, existirán dos tipos de puertos:

- Puertos de **acceso (access)**
- Puertos **troncales (trunk)**

Los **puertos de acceso** son aquellos a los que se conectan directamente los equipos terminales (ordenadores o periféricos). Por ellos **solo viajan tramas pertenecientes a una única VLAN**.

Los **puertos troncales** son aquellos por los que **circulan tramas de una o más VLANs**. Para distinguir el tráfico de las distinta VLANs **es necesario etiquetar las tramas** indicando que VLAN pertenecen.

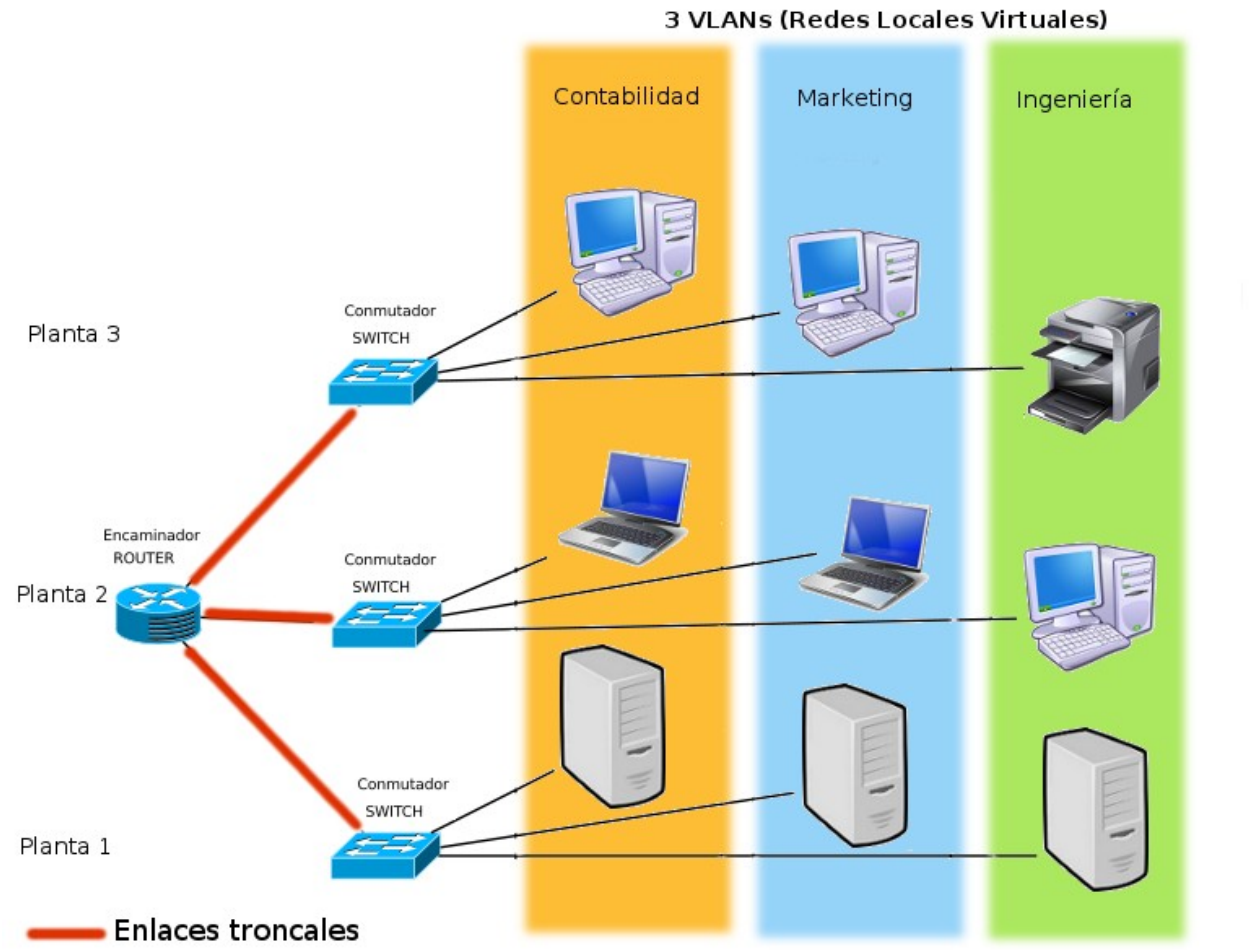
9.2.2 Enlaces troncales (trunk)



Los enlaces troncales o trunks, son enlaces capaces de transportar el tráfico de más de una VLAN y se suele utilizar para **interconectar dos switches, un switch y un router**, incluso interconectar un switch y un servidor al cual se le ha instalado una NIC especial capaz de soportar trunking. Los enlaces troncales nos permiten transportar de forma lógica las VLANs utilizando un enlace físico.

Un enlace troncal (trunk) puede ser un único enlace físico o estar conformado por varios de ellos usando la técnica de agregación (link agregation) que permite combinar varios enlaces físicos en un enlace lógico que funciona como un único puerto de mayor ancho de banda.

Otras denominaciones para la agregación de enlaces son Trunking o Bonding. Cisco lo denomina EtherChannel (Modos: ON, PAgP o LACP).



9.2.3 Etiquetado

Los puertos de un switch pueden estar etiquetados (**tagged**) o no etiquetados (**untagged**).

En un enlace troncal es necesario diferenciar el tráfico de cada una de las VLANs, de tal forma que se le asigna a cada trama entrante un identificador llamado VLAN-ID. Para poder identificar el tráfico en un enlace troncal existen dos

tipos de etiquetado:

- **ISL** (Inter-Switch Link Protocol)
- **IEEE 802.1Q**

ISL (Inter-Switch Link Protocol)

ISL es un protocolo propietario de Cisco que está en desuso. Este protocolo no altera la trama original, porque éste encapsula la trama Ethernet con una nueva cabecera de 26 bytes, que contiene al identificador VLAN (VLAN ID), y además añade un campo de secuencia de chequeo de trama (FCS ó CRC) de 4 bytes al final de la trama, como se muestra en la figura. Por lo tanto, como la trama ha sido encapsulada por ISL con nueva información, solamente los dispositivos que conozcan ISL podrán leer estas nuevas tramas.

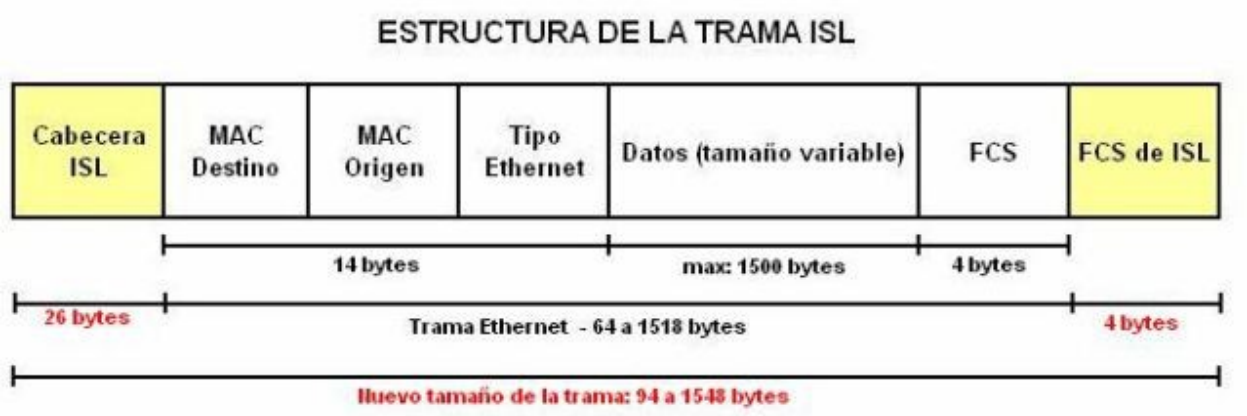


Figura 1: VLAN - Trama ISL

IEEE 802.1Q

El estándar IEEE 802.1Q (también llamado dot1q) especifica el etiquetado de tramas como un método para implementar VLANs. Insertando un campo de 4 bytes dentro de la trama Ethernet para identificar a que VLAN pertenece la información que se está transportando entre dispositivos de capa 2.

El proceso de insertar el campo IEEE 802.1Q dentro de la trama Ethernet provoca que el campo FCS sea inválido, debido a que se ha alterado la trama, por lo tanto es esencial que un nuevo FCS sea recalculado, basado en la nueva trama que contiene al campo IEEE 802.1Q. Este proceso es automáticamente desarrollado por el switch antes de que la trama sea enviada por el enlace troncal.

Este método es el más popular por ser empleado por switches de diferentes fabricantes, ofreciendo compatibilidad entre equipos. Incluso los switches Cisco pueden manejar este estándar.

9.2.4 VLAN nativa

Normalmente un puerto de switch configurado como un puerto troncal envía y recibe tramas Ethernet etiquetadas con IEEE 802.1q. Si un switch recibe **tramas Ethernet sin etiquetar** en su puerto troncal, se remiten a la VLAN que se configura en el switch como VLAN nativa. Ambos lados del enlace troncal deben configurarse para estar en la misma VLAN nativa.

La VLAN nativa **es la vlan a la que pertenecía un puerto en un switch antes de ser configurado como trunk**. Sólo se puede tener una VLAN nativa por puerto. En los equipos de Cisco Systems la VLAN nativa por defecto es la **VLAN 1**. Por la VLAN 1 además de datos, se manda información sobre PAgP, CDP, VTP.

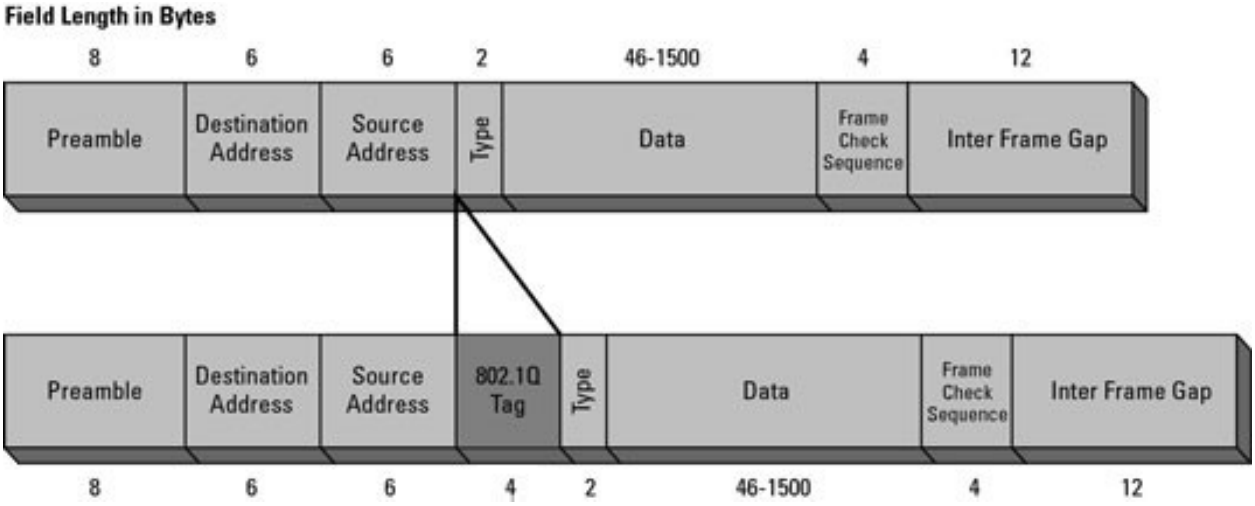


Figura 2: VLAN - Trama 802.1Q

Para establecer un trunking 802.1Q a ambos lados debemos tener la misma VLAN nativa porque la encapsulación todavía no se ha establecido y los dos switches deben hablar sobre un link sin encapsulación (usan la native VLAN) para ponerse de acuerdo en estos parámetros.

9.3 Protocolos

9.3.1 DTP

DTP (**Dynamic Trunking Protocol**) es un protocolo propietario creado por Cisco Systems que opera entre switches Cisco, el cual **automatiza la configuración de trunking** (etiquetado de tramas de diferentes VLAN's con ISL o 802.1Q) en enlaces Ethernet.

DTP se habilita automáticamente en un puerto del switch cuando se configura un modo de trunking adecuado en dicho puerto. Para ello el administrador debe ejecutar el comando *switchport mode* adecuado al configurar el puerto: **switchport mode {access | trunk | dynamic auto | dynamic desirable}**. Con el comando **switchport nonegotiate** se desactiva DTP.

En switches Catalyst 2960 de Cisco el **modo dynamic auto es el modo por defecto**. El puerto aguardará pasivamente la indicación del otro extremo del enlace para pasar a modo troncal. Para ello envía periódicamente tramas DTP al puerto en el otro lado del enlace indicando que es capaz de establecer un enlace troncal. Esto no quiere decir que lo solicita, sino que sólo lo informa. Si el puerto remoto está configurado en modo on o dynamic desirable se establece el enlace troncal correctamente. Sin embargo, si los dos extremos están en modo dynamic auto no se establecerá el enlace como troncal, sino como acceso.

9.3.2 VTP

VTP son las siglas de **VLAN Trunking Protocol**, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite **centralizar y simplificar la administración en un domino de VLANs**, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos. El protocolo VTP nace como una herramienta de administración para redes de cierto tamaño, donde la gestión manual se vuelve inabordable.

VTP opera en 3 modos distintos:

- Servidor
- Cliente
- Transparente

Servidor

Es el modo por defecto. Desde él se pueden crear, eliminar o modificar VLANs. **Su cometido es anunciar su configuración al resto de switches del mismo dominio VTP** y sincronizar dicha configuración con la de otros servidores, basándose en los mensajes VTP recibidos a través de sus enlaces **trunk**. Debe haber al menos un servidor. Se recomienda autenticación MD5.

Cliente

En este modo no se pueden crear, eliminar o modificar VLANs, tan sólo sincronizar esta información basándose en los mensajes VTP recibidos de servidores en el propio dominio. Un cliente VTP sólo guarda la información de la VLAN para el dominio completo mientras el switch está activado. Un reinicio del switch borra la información de la VLAN.

Transparente

Desde este modo tampoco se pueden crear, eliminar o modificar VLANs que afecten a los demás switches. La información VLAN en los switches que trabajen en este modo sólo se puede modificar localmente. Su nombre se debe a que no procesa las actualizaciones VTP recibidas, tan sólo las reenvía a los switches del mismo dominio.

Los administradores cambian la configuración de las VLANs en el switch en modo servidor. Después de realizar cambios, estos son distribuidos a todos los demás dispositivos en el dominio VTP a través de los enlaces permitidos en el trunk (VLAN 1, por defecto), lo que minimiza los problemas causados por las configuraciones incorrectas y las inconsistencias. Los dispositivos que operen en modo cliente, automáticamente aplicarán la configuración que reciban del dominio VTP. En este modo no se podrán crear VLANs, sino que sólo se podrá aplicar la información que reciba de las publicaciones VTP.

El modo por defecto de los swicthes es el de servidor VTP. Se recomienda el uso de este modo para redes de pequeña escala en las que la información de las VLANs es pequeña y por tanto de fácil almacenamiento en las NVRAMs de los switches.

En redes de mayor tamaño, el administrador debe elegir qué switches actúan como servidores, basándose en las capacidades de éstos (los mejor equipados serán servidores y los demás, clientes).

El VTP sólo aprende sobre las VLAN de rango normal (ID de VLAN 1 a 1005). Las VLAN de rango extendido (ID mayor a 1005) no son admitidas por el VTP.

9.4 Caso práctico

9.4.1 Uso del módulo HWIC-4ESW (4 puertos de switch)

El HWIC-4ESW es el equivalente de un conmutador de capa 2 por lo que no se le puede asignar direcciones IP a los puertos físicos. Lo que se puede hacer es crear un SVI L3 (SVI: Interfaz Virtual del Switch) y asignar el puerto dentro de la VLAN.

Comandos IOS básicos

```
Router> ?
Router> enable
```

Crear una VLAN

```
Router# vlan database
Router(vlan)# vlan 10
Router(vlan)# exit
```

Asignar una IP a la VLAN

```
Router# configure terminal
Router(config)# interface vlan 10
Router(config-if)# ip address 192.168.5.1 255.255.255.0
Router(config-if)# exit
```

Y asignar las interfaces dentro de esa VLAN

```
Router(config)# interface FastEthernet0/1/x
Router(config-if)# switchport access vlan 10
Router(config-if)# exit
```

9.5 Referencias

- VLAN Trunks

9.6 Actividades

9.6.1 Actividades de teoría

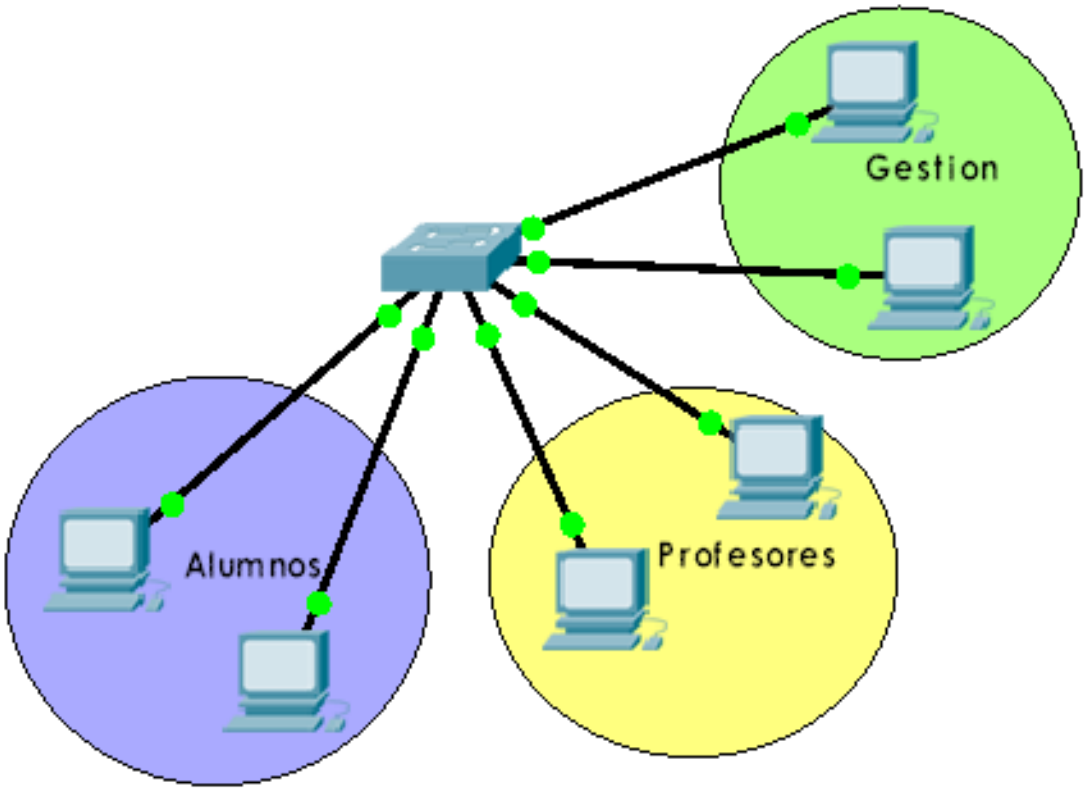
1. ¿Qué tipos de VLAN existen más frecuentemente? Explicar.
2. En referencia a las VLAN, ¿qué tipos de puertos existen?. Explicar.
3. En los enlaces troncales, ¿es aconsejable utilizar agregación de enlaces? ¿Por qué?
4. ¿Qué tipos de etiquetado se utilizan en las tramas para distinguirlas unas de otras como pertenecientes a alguna VLAN? Explicar.
5. Rellena la siguiente tabla.

Protocolo	Propietario de CISCO	Nivel OSI	Función
CDP			
STP			
DTP			
VTP			

¿Qué significan las siglas de cada protocolo?

9.6.2 Actividades de Packet Tracer

1. Configura un switch con 3 VLANs (Alumnos, Profesores, Gestión), según el esquema que se muestra a continuación. Todos los ordenadores deben estar en la misma red IP privada, pero sólo deberán verse entre sí los que se hallen en la misma VLAN.



Habilitando módulo HWIC-4ESW (4 port switch)

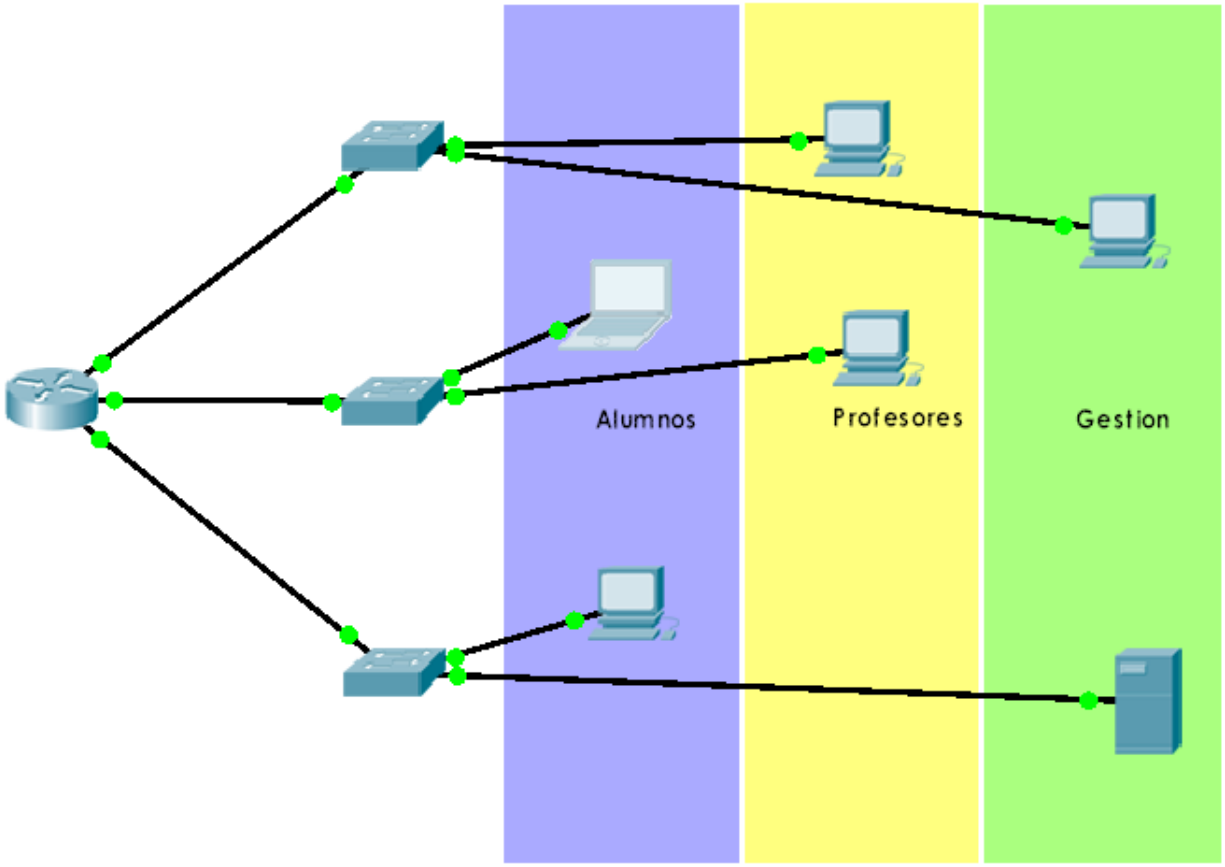
Asignar una IP a la VLAN

```
Router# configure terminal
Router(config)# interface vlan 10
Router(config-if)# ip address 192.168.5.1 255.255.255.0
Router(config-if)# exit
```

Asignar interfaces dentro de esa VLAN

```
Router(config)# interface range FastEthernet0/1/x-y
Router(config-if-range)# switchport access vlan 10
Router(config-if-range)# exit
```

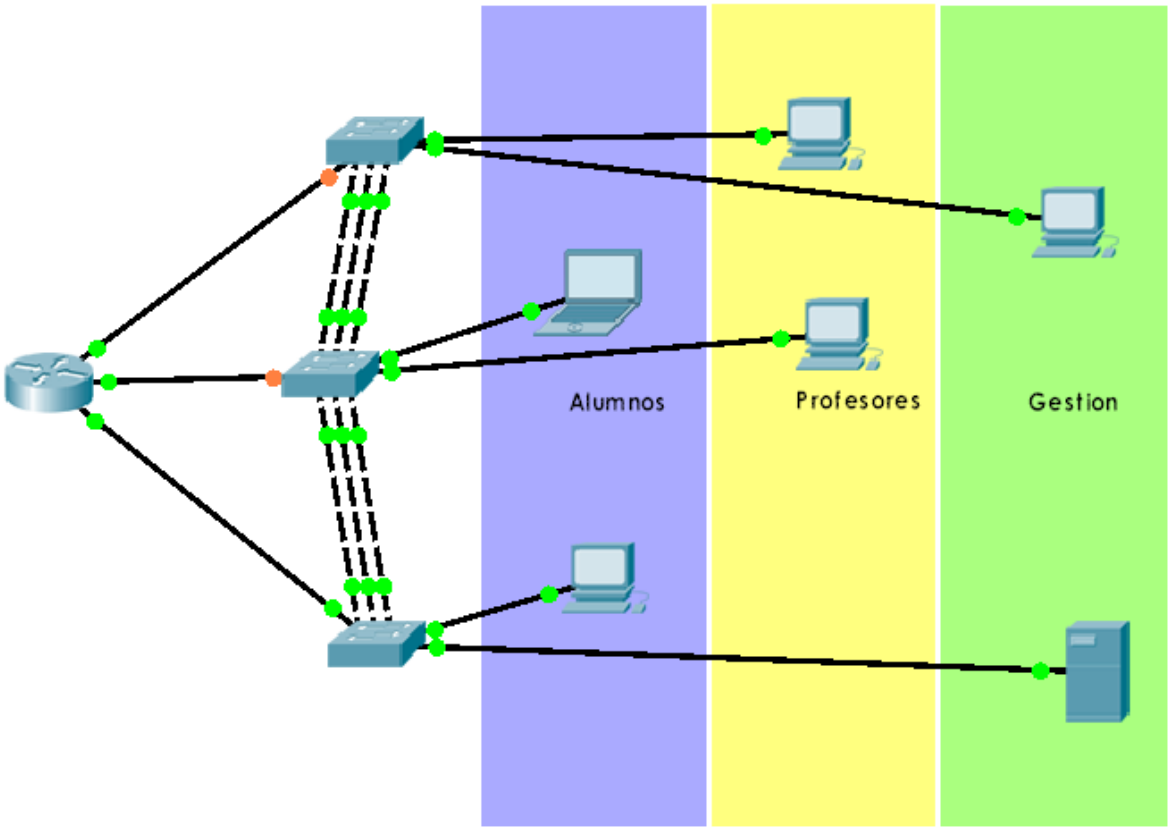
2. Utilizando la misma red IP privada anterior, con las mismas VLANs, realizar el siguiente esquema. Las conexiones de los switches al router son enlaces troncales. Comprobar que existe comunicación entre los equipos de la misma VLAN.



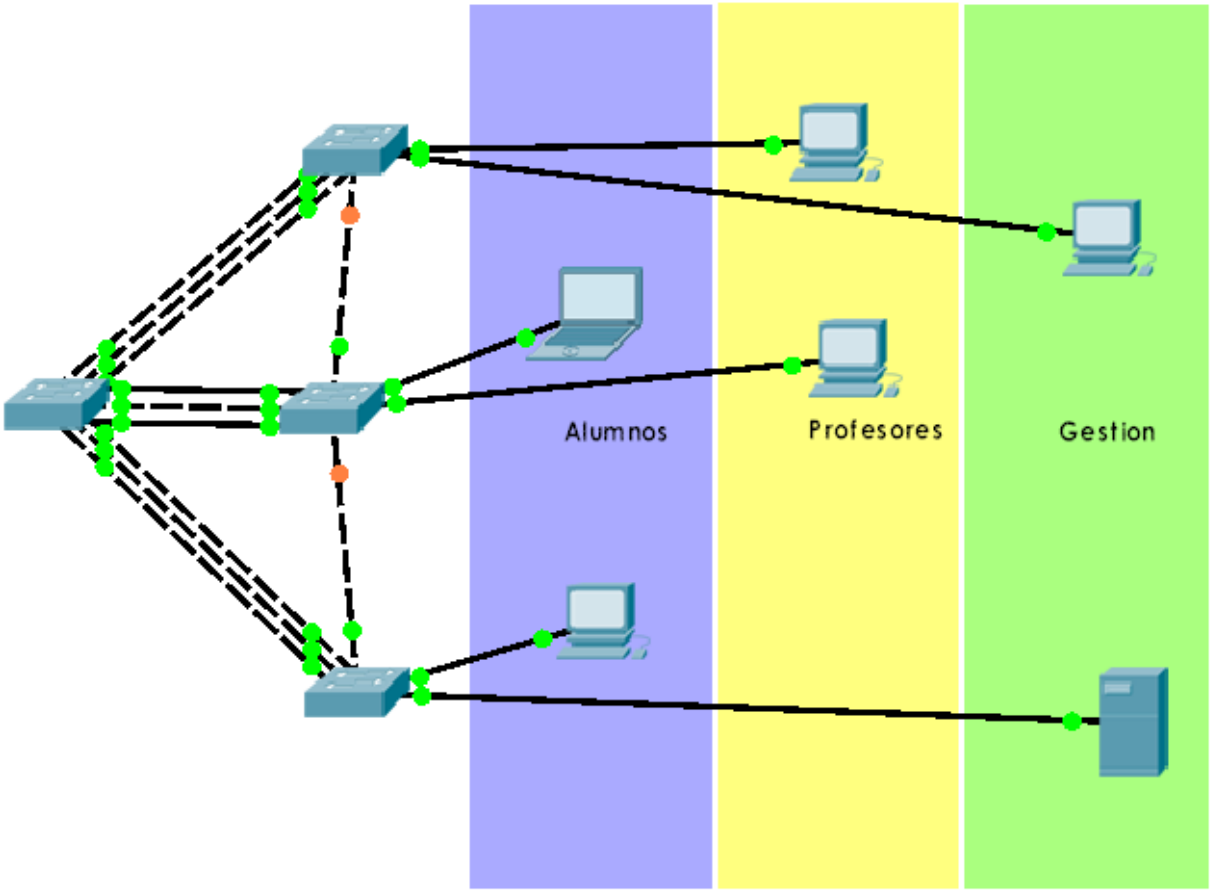
Comandos para agregación de enlaces

```
Switch(config)# interface range FastEthernet0/x-y
Switch(config-if-range)# switchport mode trunk
Switch(config-if-range)# channel-group z mode on
Switch(config-if-range)# exit
```

3. Modifica el esquema anterior para añadir agregación de enlaces de la siguiente forma. Comprueba el correcto funcionamiento. ¿Por qué se han desactivado dos enlaces? ¿Qué protocolo es responsable de ello? ¿Por qué crees que se han desactivado esos y no otros enlaces?



4. Modifica el esquema anterior para que la agregación de enlaces sea como la que se muestra a continuación. Sustituye el router por un switch. Comprueba el correcto funcionamiento. ¿Por qué crees que se han desactivado esos y no otros enlaces?



Comandos para uso de VTP

En el switch principal

```
Switch(config)# vtp mode server
Switch(config)# vtp domain prueba
Switch(config)# vlan 10
Switch(config-vlan)# name alumnos
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name profesores
Switch(config-vlan)# exit
```

En los switches secundarios

```
Switch(config)# vtp mode client
```

5. Elimina todas las VLANs que has creado en el esquema anterior y vuelve a crearlas haciendo uso de VTP. Para ello configura el switch principal como VTP mode server y los switches secundarios como VTP mode client. Comprueba el correcto funcionamiento.

CAPÍTULO 10

ENCAMINAMIENTO

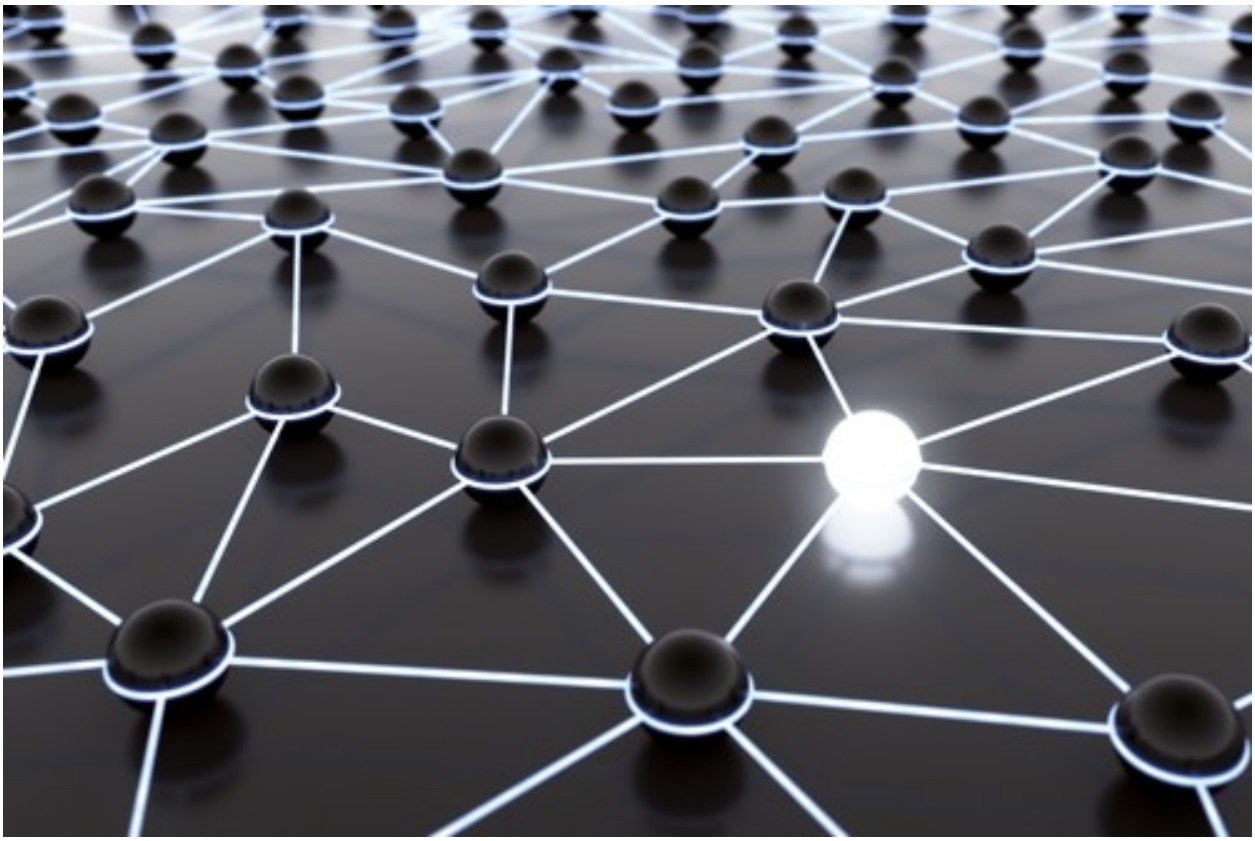
10.1 Introducción

Encaminamiento (o enrutamiento, ruteo) es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad. Dado que se trata de encontrar la mejor ruta posible, lo primero será definir qué se entiende por **mejor ruta** y en consecuencia cuál es la **métrica** que se debe utilizar para

medirla.

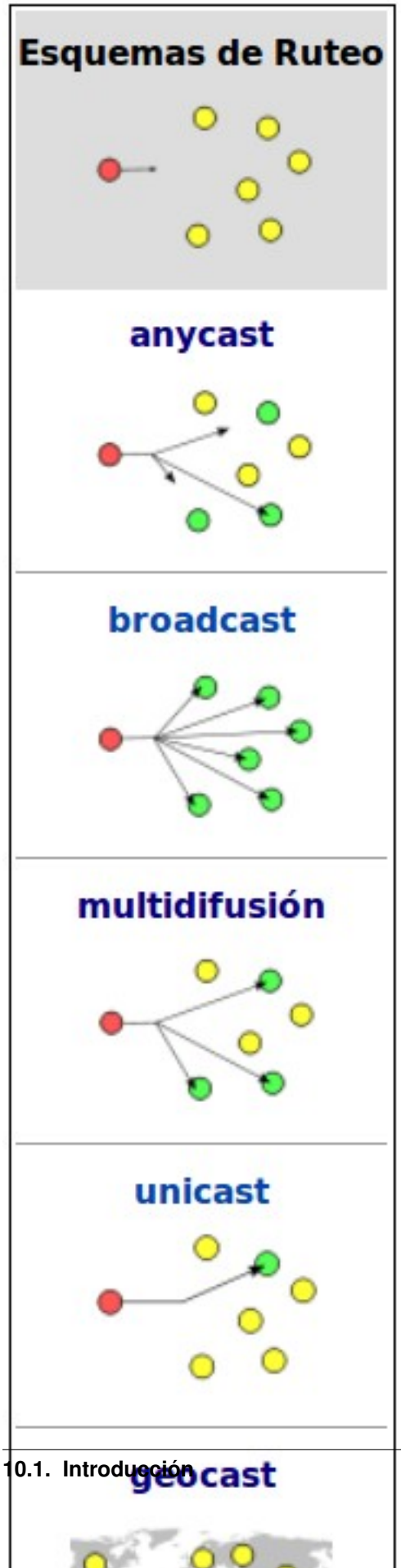
La métrica de la red puede ser por ejemplo de saltos necesarios para ir de un nodo a otro. Aunque ésta no se trata de una métrica óptima ya que supone "1" para todos los enlaces, es sencilla y suele ofrecer buenos resultados.

Otro tipo es la medición del retardo de tránsito entre nodos vecinos, en la que la métrica se expresa en unidades de tiempo y sus valores no son constantes sino que dependen del tráfico de la red.



Atendiendo al número de equipos a los que va destinado un datagrama, la comunicación se considera:

- Unicast
- Multicast
- Anycast
- Broadcast
- Geocast


Esquemas de Ruteo
anycast
broadcast
multidifusión
unicast
geocast

Unicast es el envío de información desde un único emisor a un único receptor. Se contrapone a multicast (envío a ciertos destinatarios específicos, más de uno), broadcast (radiado o difusión, donde los destinatarios son todas las estaciones en la red) y anycast (el destinatario es único, uno cualquiera no especificado).

Broadcast, difusión en español, es una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

Multicast, multidifusión en español, es el envío de la información en múltiples redes a múltiples destinos simultáneamente. Antes del envío de la información, deben establecerse una serie de parámetros. Para poder recibirla, es necesario establecer lo que se denomina «grupo multicast». Ese grupo multicast tiene asociado una dirección de internet. La versión actual del protocolo de internet, conocida como IPv4, reserva las direcciones de tipo D para la multidifusión.

Anycast es una forma de direccionamiento en la que la información es enrutada al mejor destino desde el punto de vista de la topología de la red. En la red internet, una dirección IP se puede anunciar desde varios puntos diferentes. Los routers intermedios encaminan el paquete hasta el destino más cercano. Un paquete enviado a una dirección anycast es entregado a la máquina más próxima desde el punto de vista del tiempo de latencia.

Geocast se refiere a la entrega de información a un grupo de destinos en una red identificada por su ubicación geográfica. Es una forma especializada de direccionamiento de multidifusión utilizado por algunos protocolos de enrutamiento para redes móviles ad hoc.

10.2 Clasificación

Los métodos de encaminamiento los podemos clasificar en función de:

- El procedimiento de encaminamiento.
- Las tablas de encaminamiento empleadas.

10.2.1 En función del procedimiento.

Los procedimientos de encaminamiento pueden ser:

Determinísticos o Estáticos

En los encaminamientos estático y cuasi-estático **la información necesaria se recoge y envía mediante gestión (al crear la red y en operaciones de mantenimiento)**.

Estático Las tablas de encaminamiento de los nodos se configuran de forma manual y permanecen inalterables hasta que no se vuelve a actuar sobre ellas. La adaptación a cambios es nula. Tanto la recogida como la distribución de información se realiza por gestión (se realiza de manera externa a la red), sin ocupar capacidad de red. El calculo de ruta se realiza off-line (en una maquina especifica),y las rutas pueden ser las óptimas al no estar sometido al requisito de tiempo real.

Este tipo de encaminamiento es el óptimo para topologías en los que solo hay una posibilidad de encaminamiento (topología en estrella).

Cuasiestático Este encaminamiento, es igual que el estático pero en vez de dar una sola ruta fija, se dan además varias alternativas en caso de que la principal no funcione, de ahí que tenga una adaptabilidad reducida.

Este tipo de encaminamiento puede dar lugar a situaciones incoherentes, ya que no se enteran todos los nodos de los problemas de la red, sino sólo los adyacentes a los problemas.

Adaptativos o Dinámicos

En este tipo de procedimientos de encaminamiento **la información se recoge y envía de forma periódica con el fin de detectar cambios en la red**.

Centralizado En este tipo de encaminamiento, todos los nodos son iguales salvo el nodo central, que recoge la información de control de todos los nodos y calcula la FIB (tabla de encaminamiento) para cada nodo, es decir, el nodo central decide la tabla de encaminamiento de cada nodo en función de la información de control que éstos le mandan. El inconveniente de este método es que consumimos recursos de la red, y se harían necesaria rutas alternativas para comunicarse con el nodo central. La adaptación a cambios es perfecta siempre y cuando las notificaciones de los cambios lleguen antes de iniciar los cálculos de las rutas.

Aislado Se basa en que cada vez que un nodo recibe un paquete que tiene que reenviar (porque no es para él) lo reenvía por todos los enlaces salvo por el que le llegó.

Distribuido En este tipo de encaminamiento todos los nodos son iguales, todos envían y reciben información de control y todos calculan, a partir de su RIB (base de información de encaminamiento) sus tablas de encaminamiento. La adaptación a cambios es optima siempre y cuando estos sean notificados.

Hay **dos familias de procedimientos distribuidos**:

1. **Vector de distancias**

Cada nodo informa a sus nodos vecinos de todas las distancias conocidas por él, mediante vectores de distancias (de longitud variable según los nodos conocidos). El vector de distancias es un vector de longitud variable que contiene un par (nodo:distancia al nodo) por cada nodo conocido por el nodo que lo envía, por ejemplo (A:0;B:1;D:1) que dice que el nodo que lo manda dista «0» de A,»1» de B y «1» de D, y de los demás no sabe nada (ésta es la forma en la que un nodo dice lo que sabe en cada momento). El nodo solo conoce la distancia a los distintos nodos de la red pero no conoce la topología.

Con todos los vectores recibidos, cada nodo monta su tabla de encaminamiento ya que al final conoce qué nodo vecino tiene la menor distancia al destino del paquete, pues se lo han dicho con el vector de distancias.

2. **Estado de enlaces**

Cada nodo difunde a todos los demás nodos de la red sus distancias con sus enlaces vecinos, es decir, cada nodo comunica su entorno local a todos los nodos. Así cada nodo es capaz de conocer la topología de la red. La clave y dificultad de este método es la difusión.

A continuación se muestra una tabla comparativa de todos los tipos de encaminamiento vistos.

Clasificación de los métodos de encaminamiento

Tipos de encaminamiento	Recepción de información de control	Envío de información de control	Decisión de encaminamiento	Adaptación a los cambios
Estático	NO	NO	OFF-LINE	NO
Cuasi - estático	NO	NO	OFF-LINE	Reducida
Centralizado	Nodos-Nodo central	Nodo central-Nodos	Nodo central	SI
Aislado	NO	NO	Inundación, por ejemplo	SI
Distribuido	Todos los nodos	Todos los nodos	Todos los nodos	SI

Comparación Vector de distancias – Estado del Enlaces

Haremos una comparación entre los algortitmos de vector de distancias y de estado de enlaces, ambos del tipo distribuido:

- Consumo de capacidad.

  Lo ideal es que el tráfico de control sea lo más pequeño posible. Con vectores de distancia se transmiten vectores cuyo tamaño es del orden del número de nodos de la red pues cada nodo comunica a su vecino todas las distancias que conoce; con procedimientos de estado de enlace, el tamaño del tráfico enviado es siempre el mismo independientemente del tamaño de la red. En consecuencia, **consume más capacidad un vector de distancias**.

- Consumo de memoria

  El encaminamiento basado en estado de enlace hace que cada nodo almacene toda la topología de la red, sin embargo con vectores de distancias sólo ha de almacenar distancias con el resto de los nodos. Luego **consume más memoria en los nodos un procedimiento basado en estado de enlace**.

- Adaptabilidad a los cambios

  El método de vector de distancia es más sencillo, pero se adapta peor a los cambios que el de estado de enlace. Esto es porque mientras que este último tiene información de toda la red, el primero sólo sabe a quién tiene que reenviar un paquete, pero no tiene información de la topología. Luego **se adapta mejor un encaminamiento de estado de enlaces**.

No obstante, el encaminamiento basado en vector de distancias es mucho menos complejo que el de estado de enlaces, cosa que en algunos casos prácticos puede llegar a ser muy importante.

10.2.2 En función de las tablas de encaminamiento empleadas.

Los nodos manejan **tablas de encaminamiento**, en las que aparece la ruta que deben seguir los paquetes con destino a un nodo determinado de la red.

Podemos distinguir entre encaminamiento salto a salto y encaminamiento fijado en origen. Nosotros veremos con detalle sólo el primer tipo (salto a salto).

Encaminamiento salto a salto

En la literatura inglesa, este tipo de encaminamiento se denomina como hop by hop. Se basa en que cada nodo no tiene que conocer la ruta completa hasta el destino, sino que sólo debe saber cuál es el siguiente nodo al que tiene que mandar el paquete: las tablas dan el nodo siguiente en función del destino. Como ejemplo, tomemos la siguiente red:

Las tablas de encaminamiento de los nodos A y B serán:

Tabla de encaminamiento del nodo A		Tabla de encaminamiento del nodo B	
Destino	Siguiente nodo	Destino	Siguiente nodo
B	B	A	A
C	B	C	C
D	B	D	C
E	H	E	C
F	H	F	C
G	H	G	G
H	H	H	A

En la tabla de encaminamiento de cada nodo deberá aparecer una entrada en el campo destino por cada nodo que se pueda alcanzar desde el citado nodo, y en el campo siguiente nodo aparecerá el nodo vecino al que se deberá enviar los datos para alcanzar el citado nodo destino. Las soluciones propuestas no son únicas, pudiendo elegir otros caminos que minimicen el tiempo de retardo, el número de saltos, etc. La única condición que se impone es que debe haber consistencia: si, por ejemplo, para ir de A a B pasamos por C, entonces para ir de B a C no podremos pasar por A,

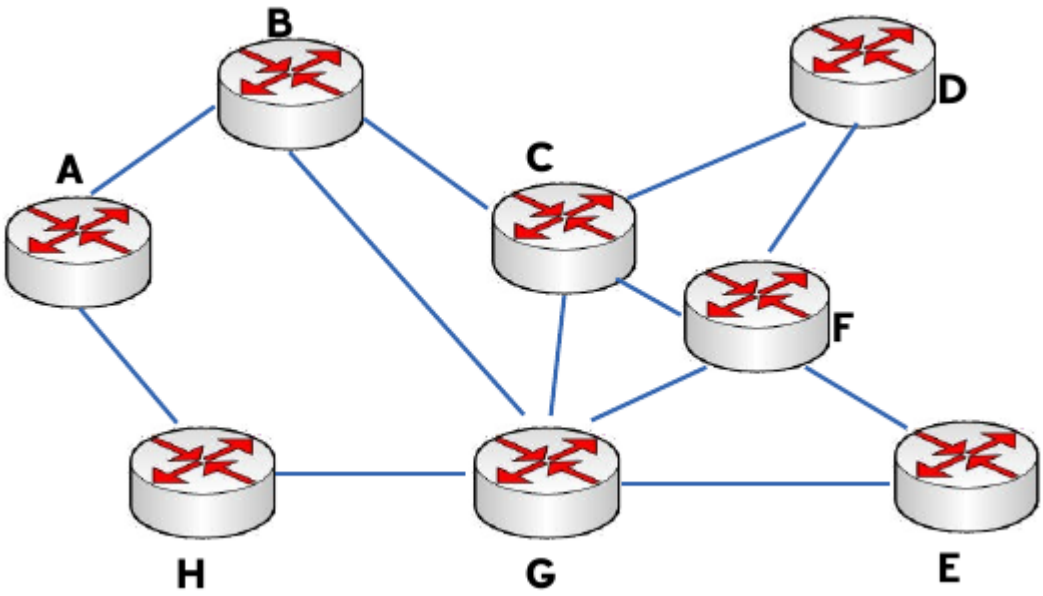


Figura 1: Red de ejemplo

porque entonces se formaría un bucle y el paquete mandado estaría continuamente viajando entre los nodos B y A, como puede comprobarse fácilmente.

Encaminamiento fijado en origen

En inglés este encaminamiento se llama source routing. En él, son los sistemas finales los que fijan la ruta que ha de seguir cada paquete. Para ello, cada paquete lleva un campo que especifica su ruta(campo RI: Routing Information), y los nodos sólo se dedican a reenviar los paquetes por esas rutas ya especificadas. Así pues, son los sistemas finales los que tienen las tablas de encaminamiento y no se hace necesaria la consulta o existencia de tablas de encaminamiento en los nodos intermedios. Este tipo de encaminamiento suele ser típico de las redes de IBM.

Tabla de encaminamiento del nodo A		Tabla de encaminamiento del nodo B	
Destino	Ruta a seguir	Destino	Ruta a seguir
B	B	A	A
C	B-C	C	C
D	B-C-D	D	C-D
E	H-G-E	E	C-F-E
F	H-G-F	F	C-F
G	H-G	G	G
H	H	H	A-H

Comparación entre ambos tipos de encaminamiento

Lo veremos por medio de la siguiente tabla:

■	Fijado en Origen	Salto a Salto
Conocimiento	Los sistemas finales han de tener un conocimiento completo de la red	SIMPLICIDAD: Los nodos han de tener un conocimiento parcial de la red (saber qué rutas son las mejores)
Complejidad	Recae toda en los sistemas finales	En los sistemas intermedios ya que son los que tienen que encaminar
Problemas de Bucles	No hay bucles: el sistema final fija la ruta (ROBUSTEZ)	Sí pueden ocurrir: no se tiene una visión completa de la red (INCONSISTENCIA)

Los **bucles** (situación que se da cuando los paquetes pasan más de una vez por un nodo) ocurren porque los criterios de los nodos no son coherentes, generalmente debido a que los criterios de encaminamiento o no han convergido después de un cambio en la ruta de un paquete; cuando por cualquier causa un paquete sufre un cambio de encaminamiento, la red tarda en adaptarse a ese cambio pues la noticia del cambio tiene que llegar a todos los nodos. Es en ese transitorio cuando se pueden dar los bucles, ya que unos nodos se han adaptado y otros no. El objetivo de los algoritmos de encaminamiento es detener el curso de los paquetes antes de que se produzcan bucles. Esto es importante sobre todo cuando se envían los paquete s por varias rutas simultáneamente (técnicas de inundación, etc. . .).

10.3 Aplicación práctica

Una red de redes está formada por redes interconectadas mediante routers o encaminadores. Cuando enviamos un datagrama desde un ordenador hasta otro, éste tiene que ser capaz de encontrar la ruta más adecuada para llegar a su destino. Esto es lo que se conoce como encaminamiento.

Los routers (encaminadores) son los encargados de elegir las mejores rutas. Estas máquinas pueden ser ordenadores con varias direcciones IP o bien, aparatos específicos.

Los routers deben conocer, al menos parcialmente, la estructura de la red que les permita encaminar de forma correcta cada mensaje hacia su destino. Esta información se almacena en las llamadas tablas de encaminamiento.

Observemos que debido al sistema de direccionamiento IP esta misión no es tan complicada. Lo único que necesitamos almacenar en las tablas son los prefijos de las direcciones (que nos indican la red). Por ejemplo, si el destino es la máquina 149.33.19.4 con máscara 255.255.0.0, nos basta con conocer el encaminamiento de la red 149.33.0.0 ya que todas las que empiecen por 149.33 se enviarán hacia el mismo sitio.

La orden **route** muestra y modifica la tabla de encaminamiento de un host. Todos los hosts (y no sólo los routers) tienen tablas de encaminamientos. A continuación se muestra una tabla sencilla para un host con IP 192.168.0.2 / 255.255.255.0 y puerta de salida 192.168.0.1.

```
C:\> route print

Rutas activas:

Dirección de red Máscara de red    Puerta de enlace  Interfaz      Métrica
0.0.0.0          0.0.0.0           192.168.0.1       192.168.0.2   1    (7)
127.0.0.0        255.0.0.0         127.0.0.1         127.0.0.1     1    (6)
192.168.0.0      255.255.255.0     192.168.0.2       192.168.0.2   1    (5)
192.168.0.2      255.255.255.255   127.0.0.1         127.0.0.1     1    (4)
192.168.0.255    255.255.255.255   192.168.0.2       192.168.0.2   1    (3)
224.0.0.0        224.0.0.0         192.168.0.2       192.168.0.2   1    (2)
255.255.255.255  255.255.255.255   192.168.0.2       0.0.0.0       1    (1)
```

Estas tabla se lee de abajo a arriba. La línea (1) indica que los datagramas con destino «255.255.255.255» (dirección de difusión a la red del host) deben ser aceptados. La línea (2) representa un grupo de multidifusión (multicasting). La dirección «224.0.0.0» es una dirección de clase D que se utiliza para enviar mensajes a una colección de hosts registrados previamente. Estas dos líneas se suelen pasar por alto: aparecen en todas las tablas de rutas.

La línea (3) indica que todos los mensajes cuyo destinatario sea «192.168.0.255» deben ser aceptados (es la dirección de difusión a la red del host). La línea (4) se encarga de aceptar todos los mensajes que vayan destinados a la dirección del host «192.168.0.2».

La línea (5) indica que los mensajes cuyo destinatario sea una dirección de la red del host «192.168.0.0 / 255.255.255.0» deben salir del host por su tarjeta de red para que se entreguen directamente en su subred. La línea (6) es la dirección de loopback: todos los paquetes con destino «127.0.0.0 / 255.0.0.0» serán aceptados por el propio host.

Finalmente, **la línea (7) representa a «todas las demás direcciones que no se hayan indicado anteriormente»**. En concreto son aquellas direcciones remotas que no pertenecen a la red del host. ¿A dónde se enviarán? Se enviarán a la **puerta de salida (gateway) de la red** «192.168.0.1».

Nótese que la tabla de rutas es la traducción de la configuración IP del host que habitualmente se escribe en las ventanas de Windows.

10.3.1 Gestión del encaminamiento IP

No existe un único protocolo para actualizar las tablas de encaminamiento IP, pudiendo elegirse el más adecuado dependiendo de los requisitos internos de las redes a interconectar y las preferencias de cada administrador.

A lo largo del tiempo, se han impuesto distintas soluciones, tanto abiertas como propietarias. Todas ellas operan con estrategias **Adaptativas Salto a Salto**.

¿Cómo pueden convivir todas ellas? Mediante los Dominios de Encaminamiento o **Sistemas Autónomos** (SA). **Un SA es un conjunto de redes gestionadas por una administración común y que comparten una estrategia de encaminamiento común**. En inglés sus siglas son AS.

Cada sistema autónomo:

- Elige su arquitectura y protocolos de encaminamiento internos.
- Es responsable de la consistencia de sus rutas internas.
- Debe recolectar información sobre todas sus redes y designar uno a más routers para pasar la información a otros sistemas autónomos.

Será por tanto necesario definir dos tipos de encaminamiento:

- Intradominio o IGP (Internal Gateway Protocol): Es el utilizado dentro del SA. Ejemplos: RIP, OSPF, IGRP, EIGRP, . . .
- Interdominio o EGP (External Gateway Protocol): Encamina entre Sistemas Autónomos. Ejemplos: BGP, IDPR, . . .

Los routers frontera ejecutan el encaminamiento EGP para cambiar información con routers de otros sistemas autónomos, y el IGP para cambiar información con otros routers de su SA:

10.3.2 Sistemas participantes

La función de encaminamiento se realiza principalmente en los routers, aunque en algunas situaciones los hosts también deben participar en la toma de decisiones (para seleccionar el router de su red al que envía el datagrama):

Estrategia básica de envío:

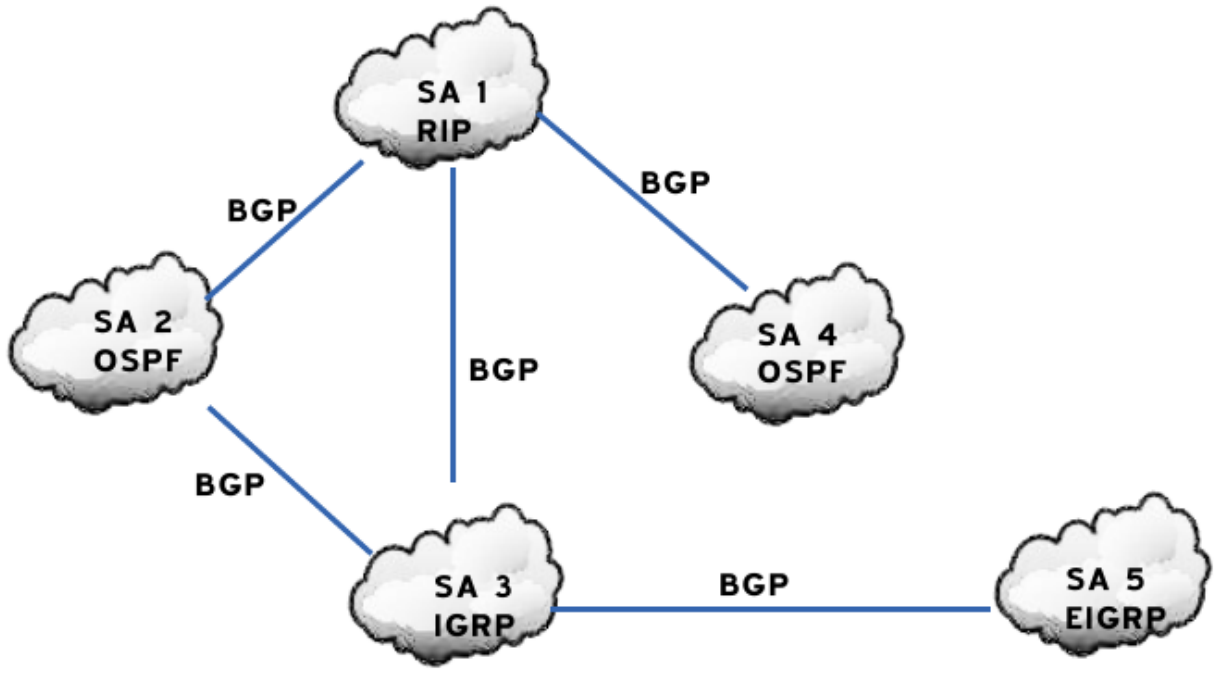


Figura 2: Interconexión de redes mediante BGP y distintos protocolos interiores

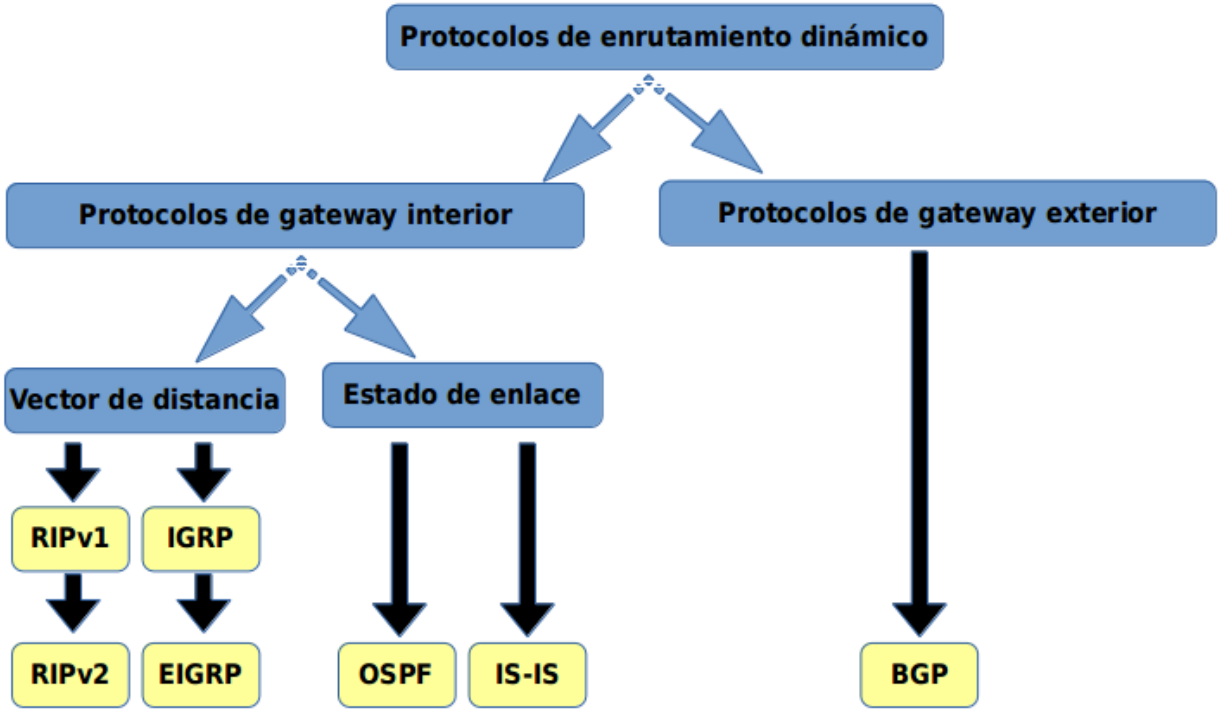


Figura 3: Clasificación de los protocolos de enrutamiento

- Si el host destino se encuentra en la misma red, se encapsula el datagrama IP en una trama de subred, se obtiene la dirección física (mediante ARP) y se envía (entrega directa)
- Si no está en la misma subred, se envía el datagrama a un router, éste lo reenvía al siguiente, y así sucesivamente, hasta alcanzar un router conectado a la misma subred que la máquina destino (entrega indirecta)

Para conocer si el host destino se encuentra en la misma subred que el origen, éste compara el prefijo de red de ambas direcciones. Si coinciden, se encuentran en la misma subred.

Para los envíos será necesario llevar a cabo la conversión entre direcciones IP y de subred (física) del destinatario (host o router). Esta función puede desempeñarla el protocolo ARP.

El encaminador sólo modifica los campos TTL y checksum del datagrama, no las direcciones IP origen o destino. Aunque debe obtener la dirección IP del siguiente salto y, a partir de ella, la de subred donde enviará el datagrama.

10.3.3 Tablas de encaminamiento

El encaminamiento IP hace uso de tablas de encaminamiento que se encuentran en cada máquina (hosts y routers, puesto que ambos encaminan datagramas) y almacenan información sobre los posibles destinos y cómo alcanzarlos.

La estrategia es siempre salto a salto (next-hop routing): las tablas almacenan el siguiente salto para las direcciones IP destino. Las direcciones son siempre IP, no físicas, debido a que se facilita su gestión y se ocultan los detalles de las subredes.

Para acelerar el proceso y reducir el consumo de recursos, las tablas sólo necesitan los prefijos de subred de las direcciones IP y no la dirección IP completa.

En un entorno de interconexión total, como el de Internet, no es posible que las tablas contengan la información sobre todas las posibles direcciones destino; se utiliza el principio de información oculta, que permite tomar decisiones de encaminamiento con la información mínima necesaria:

- Se aísla la información de hosts dentro del entorno local (subred) donde se encuentran; un host remoto puede enviar datagramas sin conocer al detalle la subred. El esquema de direccionamiento IP está diseñado para ayudar a conseguir éste objetivo.
- Se agrupan múltiples entradas de la tabla en una sola, la ruta por defecto.

Nota: Todos los routers listados en la tabla de encaminamiento de un nodo deben de encontrarse en subredes a las que dicho nodo esté conectado directamente (estrategia salto a salto).

10.3.4 Métricas

Una métrica es un valor utilizado por los protocolos de enrutamiento para asignar costos a fin de alcanzar las redes remotas.

La identificación de la mejor ruta de un router implica la evaluación de múltiples rutas hacia la misma red de destino y la selección de la ruta óptima o «la más corta» para llegar a esa red. Cuando existen múltiples rutas para llegar a la misma red, cada ruta usa una interfaz de salida diferente en el router para llegar a esa red. La mejor ruta es elegida por un protocolo de enrutamiento en función del valor o la métrica que usa para determinar la distancia para llegar a esa red.

Las métricas utilizadas en los protocolos de enrutamiento IP incluyen:

- Conteo de saltos: una métrica simple que cuenta la cantidad de routers que un paquete tiene que atravesar
- Ancho de banda: influye en la selección de rutas al preferir la ruta con el ancho de banda más alto
- Carga: considera la utilización de tráfico de un enlace determinado

- Retardo: considera el tiempo que tarda un paquete en atravesar una ruta
- Confiabilidad: evalúa la probabilidad de una falla de enlace calculada a partir del conteo de errores de la interfaz o las fallas de enlace previas
- Costo: un valor determinado ya sea por el IOS o por el administrador de red para indicar la preferencia hacia una ruta. El costo puede representar una métrica, una combinación de las mismas o una política.

Algunos protocolos de enrutamiento, como RIP, usan un conteo de saltos simple, que consiste en el número de routers entre un router y la red de destino. Otros protocolos de enrutamiento, como OSPF, determinan la ruta más corta al analizar el ancho de banda de los enlaces y al utilizar dichos enlaces con el ancho de banda más rápido desde un router hacia la red de destino. Los protocolos de enrutamiento dinámico generalmente usan sus propias reglas y métricas para construir y actualizar las tablas de enrutamiento. Una métrica es un valor cuantitativo que se usa para medir la distancia hacia una ruta determinada. La mejor ruta a una red es la ruta con la métrica más baja. Por ejemplo, un router preferirá una ruta que se encuentra a 5 saltos antes que una ruta que se encuentra a 10 saltos.

El objetivo principal del protocolo de enrutamiento es determinar las mejores trayectorias para cada ruta a fin de incluirlas en la tabla de enrutamiento. El algoritmo de enrutamiento genera un valor, o una métrica, para cada ruta a través de la red. Las métricas se pueden calcular sobre la base de una sola característica o de varias características de una ruta. Algunos protocolos de enrutamiento pueden basar la elección de la ruta en varias métricas, combinándolas en un único valor métrico. Cuanto menor es el valor de la métrica, mejor es la ruta.

Cuando un router tiene múltiples rutas hacia una red de destino y el valor de esa métrica (conteo de saltos, ancho de banda, etc.) es el mismo, esto se conoce como métrica de mismo costo, y el router realizará un balanceo de carga de mismo costo.

La métrica para cada protocolo de enrutamiento es:

- RIP: conteo de saltos: la mejor ruta se elige según la ruta con el menor conteo de saltos.
- IGRP e EIGRP: ancho de banda, retardo, confiabilidad y carga; la mejor ruta se elige según la ruta con el valor de métrica compuesto más bajo calculado a partir de estos múltiples parámetros. Por defecto, sólo se usan el ancho de banda y el retardo.
- IS-IS y OSPF: costo; la mejor ruta se elige según la ruta con el costo más bajo. . La implementación de OSPF de Cisco usa el ancho de banda

10.3.5 Distancia administrativa

Aunque es menos común, puede implementarse más de un protocolo de enrutamiento dinámico en la misma red. **En algunas situaciones, posiblemente sea necesario enrutar la misma dirección de red utilizando múltiples protocolos de enrutamiento** como RIP y OSPF. Debido a que diferentes protocolos de enrutamiento usan diferentes métricas, RIP usa el conteo de saltos y OSPF usa el ancho de banda, no es posible comparar las métricas para determinar la mejor ruta.

La distancia administrativa (AD) define la preferencia de un origen de enrutamiento. A cada origen de enrutamiento, entre ellas protocolos de enrutamiento específicos, rutas estáticas e incluso redes conectadas directamente, se le asigna un orden de preferencia de la más preferible a la menos preferible utilizando el valor de distancia administrativa. Los routers Cisco usan la función de AD para seleccionar la mejor ruta cuando aprende sobre la misma red de destino desde dos o más orígenes de enrutamiento diferentes.

La distancia administrativa es un valor entero entre 0 y 255. Cuanto menor es el valor, mayor es la preferencia del origen de ruta. **Una distancia administrativa de 0 es la más preferida**. Solamente una red conectada directamente tiene una distancia administrativa igual a 0 que no puede cambiarse. Cada protocolo tiene AD predeterminada: OSPF 110, EIGRP 90, IGRP 100, RIP 120 que aparecen en las tablas de enrutamiento precediendo a la métrica. **La AD de 0 se reserva para las redes conectadas directamente y la de 1 para las redes estáticas**.

Advertencia: Ojo, si agregamos una ruta estática que también haya sido aprendida por un protocolo dinámico, la ruta estática tendrá preferencia al tener una distancia administrativa de 1.

10.3.6 Protocolos de enrutamiento con clase y sin clase

Los protocolos de enrutamiento con clase no envían información de la máscara de subred en las actualizaciones de enrutamiento. Los primeros protocolos de enrutamiento tales como el RIP, fueron con clase. En aquel momento, las direcciones de red se asignaban en función de las clases; clase A, B o C. No era necesario que un protocolo de enrutamiento incluyera una máscara de subred en la actualización de enrutamiento porque la máscara de red podía determinarse en función del primer octeto de la dirección de red. Los protocolos de enrutamiento con clase no pueden usarse cuando una red se divide en subredes utilizando más de una máscara de subred; en otras palabras, los protocolos de enrutamiento con clase no admiten máscaras de subred de longitud variable (VLSM).

Los protocolos de enrutamiento sin clase incluyen la máscara de subred con la dirección de red en las actualizaciones de enrutamiento. Las redes de la actualidad ya no se asignan en función de las clases y la máscara de subred no puede determinarse según el valor del primer octeto. La mayoría de las redes de la actualidad requieren protocolos de enrutamiento sin clase porque admiten VLSM, redes no contiguas y otras funciones. **Los protocolos de enrutamiento sin clase son RIPv2, EIGRP, OSPF, IS-IS y BGP**.

10.3.7 Resumen de rutas

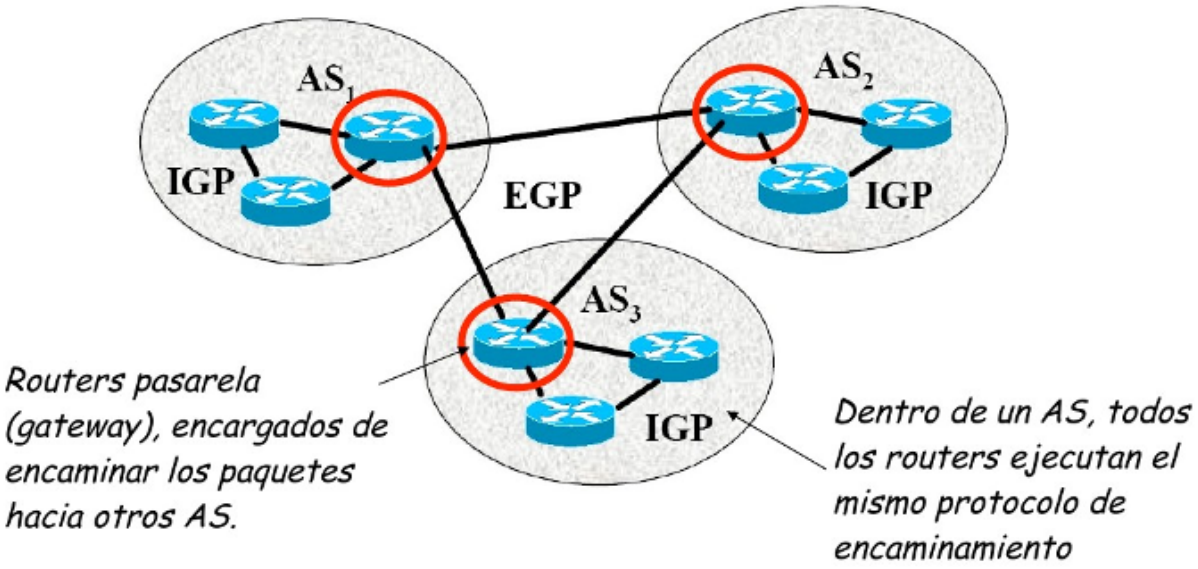
La creación de tablas de enrutamiento más pequeñas hace que el proceso de búsqueda en la tabla de enrutamiento sea más eficiente ya que existen menos rutas para buscar. Si se puede utilizar una ruta estática en lugar de múltiples rutas estáticas, el tamaño de la tabla de enrutamiento se reducirá. En muchos casos, una sola ruta estática puede utilizarse para representar docenas, cientos o incluso miles de rutas.

Podemos utilizar una sola dirección de red para representar múltiples subredes. Por ejemplo, las redes 10.0.0.0/16, 10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16, 10.4.0.0/16, 10.5.0.0/16, hasta 10.255.0.0/16, pueden representarse con una sola dirección de red: 10.0.0.0/8.

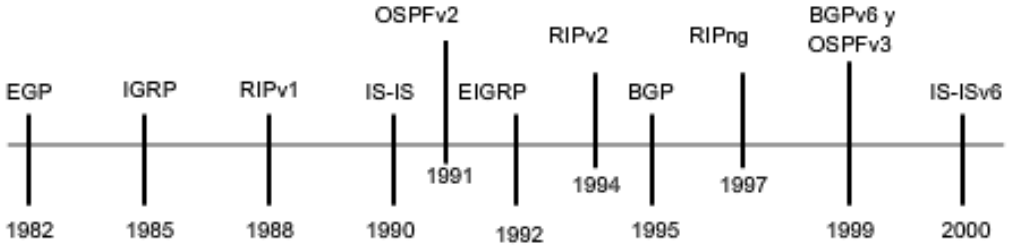
Las múltiples rutas estáticas pueden resumirse en una sola ruta estática si:

- las redes de destino pueden resumirse en una sola dirección de red, y
- todas las múltiples rutas estáticas utilizan la misma interfaz de salida o dirección IP del siguiente salto.

10.4 Protocolos interiores y exteriores



Clasificación y evolución de los protocolos de enrutamiento



	Protocolos de gateway interior				Protocolos de gateway exterior
	Protocolos de enrutamiento por vector de distancia		Protocolos de enrutamiento de estado de enlace		Vector de ruta
Con clase	RIP	IGRP			EGP
Sin clase	RIPv2	EIGRP	OSPFv2	IS-IS	BGPv4
IPv6	RIPng	EIGRP para IPv6	OSPFv3	IS-IS para IPv6	BGPv4 para IPv6

10.4.1 Protocolos interiores (IGP)

Routing Information Protocol (RIP)

Protocolo IGP. RFC 1095. Muy simple y extendido, gracias a que fue incluido en la distribución UNIX BSD (routed)

Características generales:

- Vector distancia.
- Métrica = número de saltos (de 1 a 15). 16 es infinito.
- Dos tipos de participantes: activos (sólo pueden ser routers) y pasivos.
- Cada 30 segundos los participantes activos difunden su vector de distancias: duplas de (prefijo IP, distancia).
- Utiliza UDP como protocolo de transporte (puerto 520).
- Todos los participantes (activos y pasivos) escuchan los mensajes RIP y actualizan sus tablas.
- Existe un proceso de borrado de rutas (cada 180 segundos), para mantener las tablas fiables y para recuperarse ante caídas de routers, por ejemplo.
- Dos tipos de paquetes. REQUEST: enviados por los routers o hosts que acaban de conectarse o su información ha caducado. RESPONSE: enviados periódicamente, en respuesta a un REQUEST o cuando cambia algún coste.
- Actualmente existen dos versiones del protocolo: RIPv1 y RIPv2 (aporta subnetting y autenticación).

Limitaciones:

- Existen diferencias entre implementaciones debido a que la RFC tardó un poco en aparecer.
- Convergencia lenta (inconsistencias transitorias provocan bucles de encaminamiento). Se han propuesto algunas soluciones, pero son parciales o no sirven para todas las topologías.
- Carga las redes innecesariamente. Todos los routers hacen broadcast periódicamente.
- Permite 15 saltos como máximo.
- Métrica de saltos. No contempla otras posibilidades (caudal, probabilidad de error, etc.)

Open Shortest Path First (OSPF)

Primero el Camino Abierto más Corto. Protocolo IGP. RFC 1247. Presentado en 1990 como sustituto de RIP. Recomendado por la IETF para redes IP.

Características generales:

- Escalable: admite redes con miles de encaminadores
- Estado de Enlaces
- Soporta subnetting: prefijos + máscaras.
- Los mensajes OSPF se encapsulan directamente dentro de datagramas IP: no utilizan ningún protocolo de transporte.
- Encaminamiento multimétrica. Distinto camino dependiendo del campo TOS de la cabecera IP. También soporta balanceado de carga entre rutas de igual coste.
- Encaminamiento jerárquico. Divide el sistema autónomo en áreas. Cada área esconde su topología. El encaminador OSPF sólo necesita conocer la topología de su área.
- Tipos de encaminadores: Internal, Area Border, Backbone y AS Boundary.

- Tipos de Redes: Point to Point, Broadcast y Non-Broadcast
- Inyección de rutas externas: uno o varios encaminadores aprenden rutas externas y las propagan.
- Descubrimiento dinámico de encaminadores.
- Adaptación a redes locales: aprovecha las redes con difusión hardware para disminuir el número de mensajes OSPF.
- Soporte para autentificación, lo que proporciona mayor seguridad y evita ataques.

10.4.2 Protocolos exteriores (EGP)

BGP

Border Gateway Protocol es un protocolo mediante el cual se **intercambia información de encaminamiento entre sistemas autónomos**.

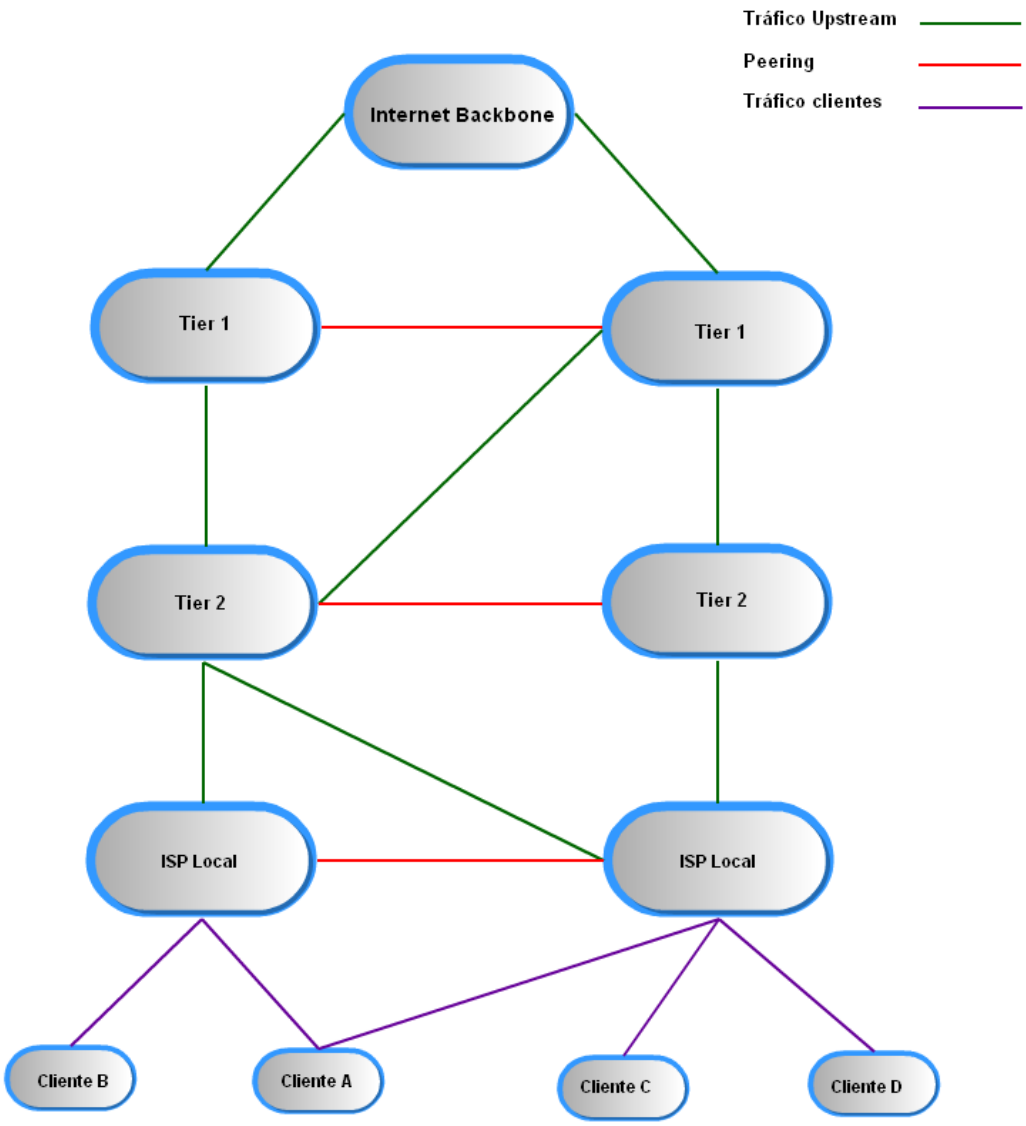
Entre los sistemas autónomos de los ISP se intercambian sus tablas de rutas a través del protocolo BGP. Este intercambio de información de encaminamiento **se hace entre los routers externos de cada sistema autónomo**. Estos routers deben soportar BGP. Se trata del protocolo más utilizado para redes con intención de configurar un EGP (external gateway protocol)

Es el protocolo principal de publicación de rutas utilizado por las compañías más importantes de ISP en Internet. BGP4 es la primera versión que admite encaminamiento entre dominios sin clase (CIDR) y agregado de rutas. A diferencia de los protocolos de Gateway internos (IGP), como RIP, OSPF y EIGRP, no usa métricas como número de saltos, ancho de banda, o retardo. En cambio, **BGP toma decisiones de encaminamiento basándose en políticas de la red, o reglas que utilizan varios atributos de ruta BGP**.

Con BGP los encaminadores en la frontera de un sistema autónomo intercambian prefijos de redes hacia las que saben encaminar. Las rutas aprendidas son inyectadas en el IGP para distribuirlas entre los encaminadores interiores al AS.

Relaciones entre Sistemas Autónomos

Las relaciones que existen entre distintos sistemas autónomos son principalmente de **peering** y de **tránsito**. Básicamente **una relación de tránsito es la que existe entre un proveedor y un cliente**, de modo que **el cliente pague** por los recursos de Internet que le puede suministrar su proveedor. **Las relaciones de peering no suelen se pagadas y consisten en un enlace para comunicar dos sistemas autónomos** con el fin de reducir costes, latencia, pérdida de paquetes y obtener caminos redundantes. Se suele hacer peering con sistemas autónomos potencialmente similares, es decir, no se hace peering con un cliente potencial ya que saldría uno de los dos sistemas autónomos beneficiado.

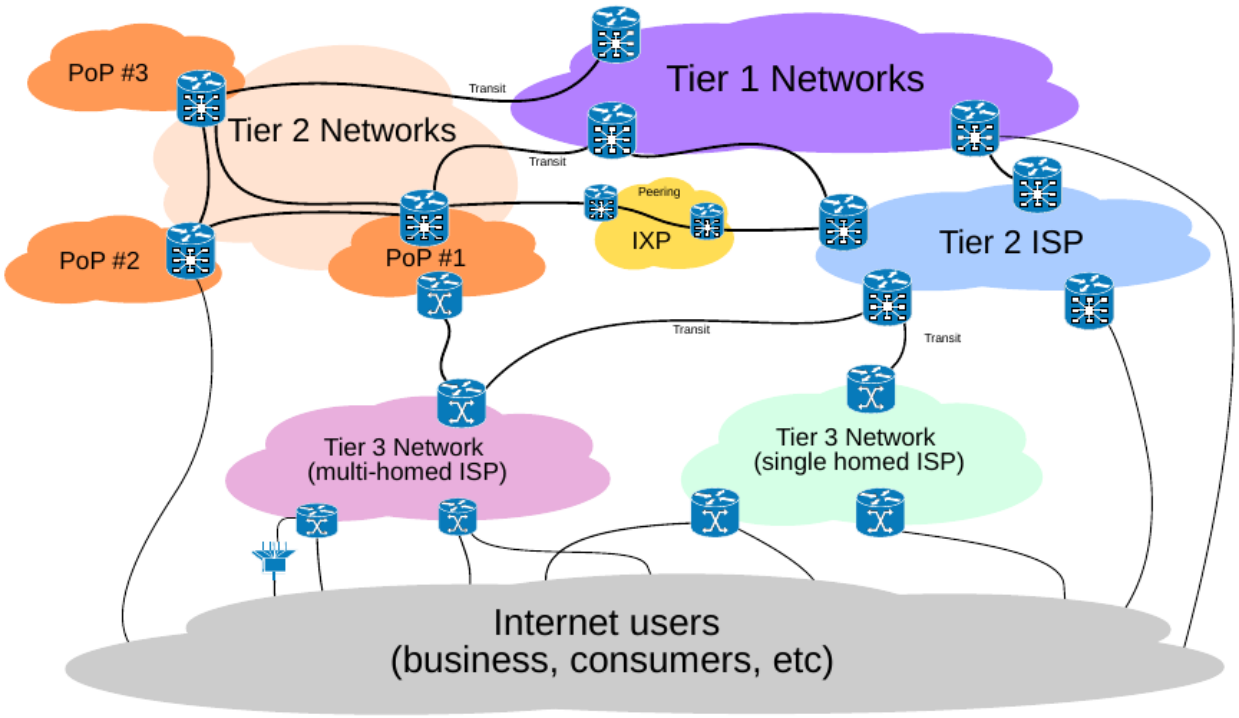


Curiosidad

Durante las protestas de Egipto de 2011 el gobierno de Hosni Mubarak ordenó a todos los proveedores de acceso que operan en el país árabe el corte de las conexiones internacionales. Como consecuencia de los cortes y bloqueos en la noche del 27 al 28 de enero los enrutadores egipcios dejaron de anunciar hasta 3.500 rutas de BGP, dejando al resto de enrutadores sin la información necesaria para intercambiar tráfico con los servidores egipcios.

Fuente y más información: http://internacional.elpais.com/internacional/2011/01/28/actualidad/1296169207_850215.html

10.5 Estructura jerárquica de internet



Nota: Tier es una palabra inglesa que puede traducirse por nivel.

Una red **Tier 1** (Tier 1 ISPs o Internet backbone networks) es capaz de alcanzar cualquier red de Internet sin tener que pagar por tránsito (por enviar sus bits a través de otras redes.)

- Grandes proveedores internacionales (AT&T, Deutsche Telekom,
- AOL, Telefónica y algunos más)
- Conectados directamente a cada uno de los demás Tier 1 ISPs
- Conectados a un gran número de Tier 2 ISPs
- Cobertura internacional

Los **Tier 2** ISPs suelen ser regionales o nacionales y son los ISPs más comunes.

- Se conectan sólo a algunos Tier 1 ISPs (pagando por el uso de sus redes).
- También se conectan a muchos otros Tier 2 ISPs (mediante acuerdos de peering), de forma que el tráfico fluye entre ambas redes sin necesidad de usar una red Tier 1.
- Pero para alcanzar una gran cantidad de redes necesitan encaminar su tráfico a través de los ISP de nivel 1 a los que están conectados (ellos son los clientes y el Tier 1 el proveedor de tránsito).

Los **Tier 3** ISPs son ISPs locales de acceso

- Para alcanzar internet solamente contratan tránsito IP (normalmente a ISPs Tier2) ¿Cómo se conectan los ISPs?
- Point of Presence (PoP): es un interfaz entre dos ISPs. Pueden estar en las propias instalaciones de un ISP o en un IX.

- Internet eXchange point: infraestructura en la que los ISPs intercambian tráfico entre sus redes.
  - Reducen la cantidad de tráfico que deben enviar a los ISPs superiores → reducción de costes
  - Aprenden nuevas rutas → mayor eficiencia y tolerancia a fallos
  - Mantienen el tráfico local → mejor latencia

10.6 Referencias

- Como funciona la Red: peering & transit (en inglés)

10.7 Actividades

10.7.1 Actividades de teoría

1. Atendiendo al número de receptores de un paquete, ¿qué tipos de encaminamiento existen? Explicar.
2. ¿En qué se diferencian el encaminamiento estático del encaminamiento dinámico?
3. ¿Qué comando utilizamos para ver la tabla de rutas en un equipo terminal Windows? ¿Y en Linux?
4. En Windows, desde un terminal de texto, elimina la ruta por defecto con el comando route. Prueba a hacer un ping al equipo 8.8.8.8. Vuelve a añadir la ruta. Vuelve a probar el ping. (Realiza dos capturas de pantalla)
5. En Linux, desde un terminal de texto, elimina la ruta por defecto con el comando route. Prueba a hacer un ping al equipo 8.8.8.8. Vuelve a añadir la ruta. Vuelve a probar el ping. (Realiza dos capturas de pantalla)
6. En un equipo terminal, ¿por qué es tan importante la puerta de enlace o ruta por defecto?
7. Haz un esquema de los distintos protocolos de encaminamiento dinámico que existen, atendiendo a externos o internos. Y en estos últimos según se basen en el vector de distancia o en el estado del enlace.
8. ¿Qué protocolos admiten encaminamiento sin clase?
9. ¿Qué es la distancia administrativa y cuándo es necesaria?
10. De los protocolos de encaminamiento, ¿cuáles son propietarios?
11. ¿Cómo está organizada Internet? ¿Qué niveles existen?
12. ¿Qué son y por qué son importantes los Internet eXchange points?

10.7.2 Actividades de Packet Tracer

Inicio (comandos básicos)

```
Router>  ping IP
Router>  show ip route
Router>  enable
Router#  configure terminal
Router(config)#  no ip domain-lookup

<Aquí ponemos los comandos de enrutamiento>

Fin
Router0(config-router)#  exit
```

(continues on next page)

(proviene de la página anterior)

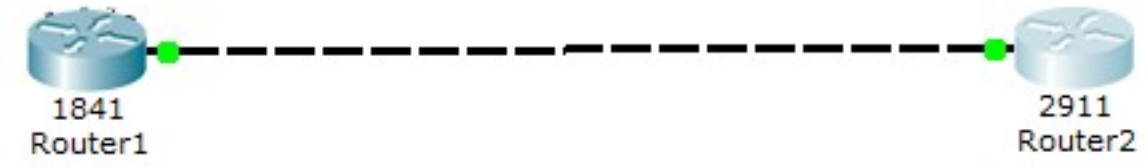
```
Router0(config)#  exit
Router0#  copy running-config startup-config
```

Enrutamiento estático

Añadimos rutas estáticas

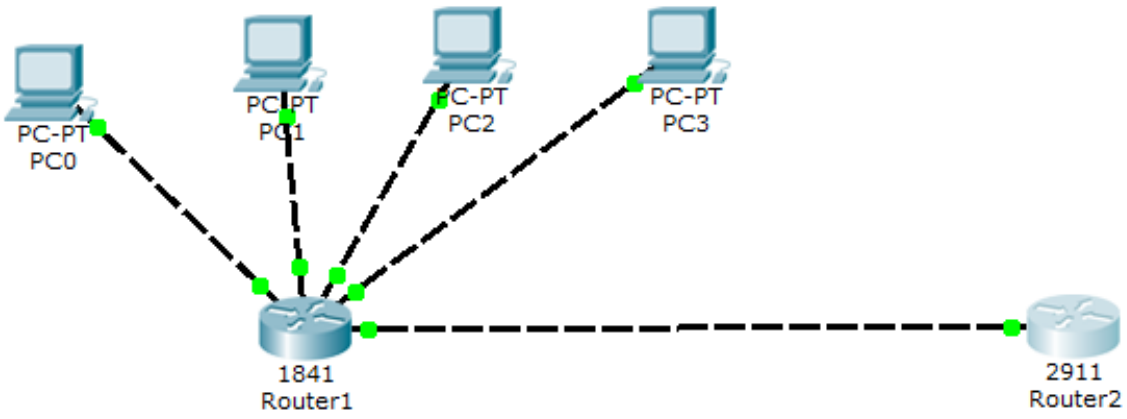
```
Router(config)#  ip route   RED   MASCARA    SIGUIENTE_SALTO
Router(config)#  ip route ...
```

1. Conecta 2 routers entre sí y comprueba que tienen comunicación entre ellos (utiliza el comando ping). Router1 (11.0.0.1/30), Router2 (11.0.0.2/30). ¿Es necesario configurar tablas de rutas? ¿Por qué? Muestra la tabla de rutas con el comando show ip route.



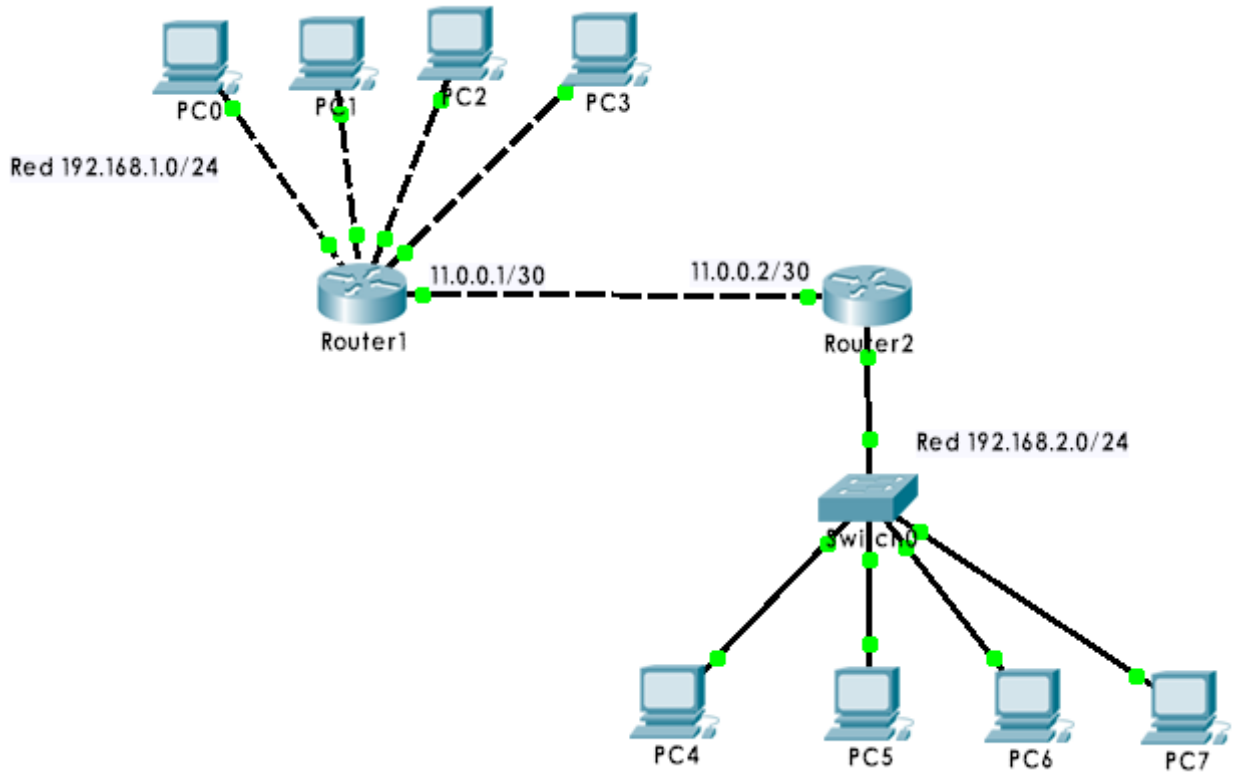
2. Añade al Router1 un módulo HWIC-4ESW (4 ports switch). Configura el módulo HWIC-4ESW como se vio en el tema anterior. Añade 4 PC y configura una red diferente para ellos (192.168.1.0/24). Configura la puerta de enlace de cada uno de los PC. Añade una entrada a la tabla de rutas en el Router2 para alcanzar la red 192.168.1.0. Comprueba que hay comunicación entre los PC y el Router2. Muestra la tabla de rutas del Router2 con el comando show ip route.

```
Router2(config)#  ip route 192.168.1.0   255.255.255.0   11.0.0.1
```



3. Añade un switch y 4 PC más en otra red. Configura Router1 para alcanzar la red2 (192.168.2.0). Configura Router2 para alcanzar la red1 (192.168.1.0). Comprueba que hay comunicación entre los PC del Router1 y los del Router2. Muestra la tabla de rutas del Router1 con el comando show ip route.

```
Router1(config)#  ip route 192.168.2.0   255.255.255.0   11.0.0.2
Router2(config)#  ip route 192.168.1.0   255.255.255.0   11.0.0.1
```

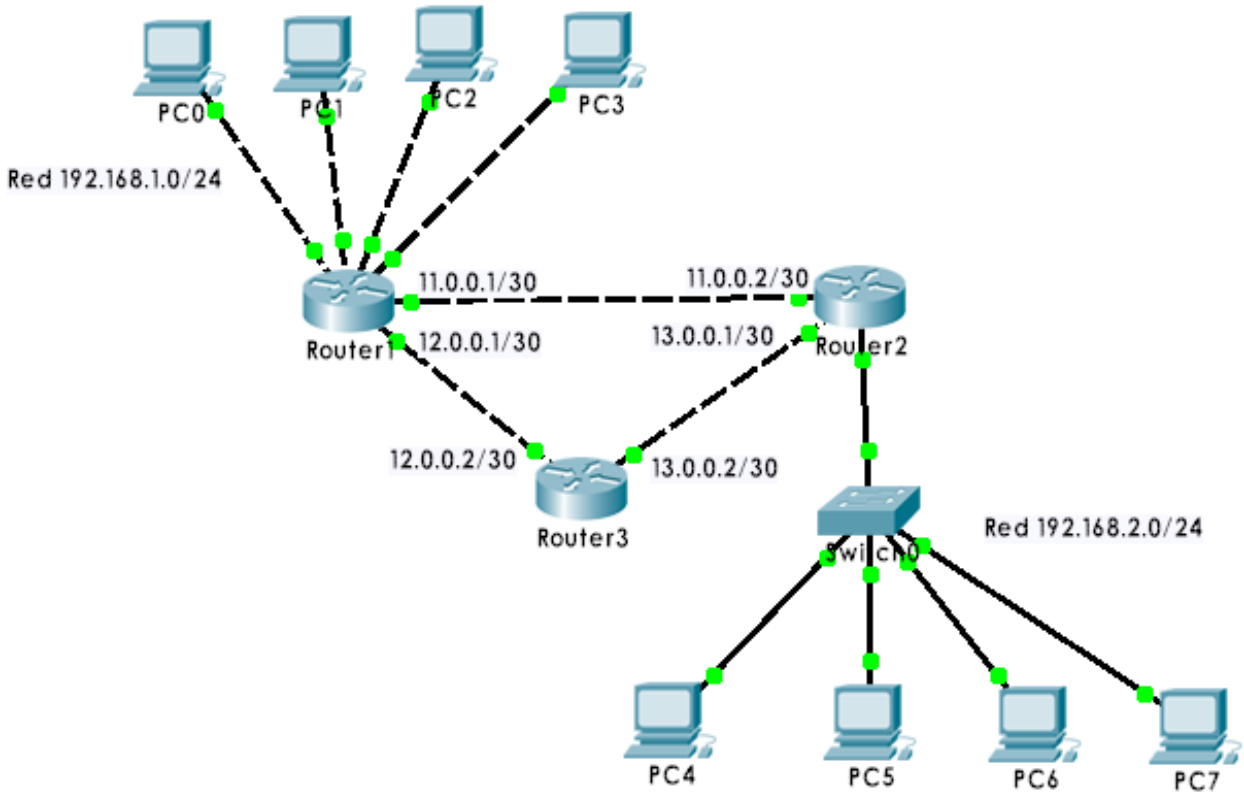


4. Añade el Router3 (12.0.0.0/30 hacia Router1; 13.0.0.0/30 hacia Router2). Configura su tabla de rutas. Modifica la tabla de rutas del Router2 para que los envíos que vayan a la red local del Router1 pasen por el Router3. Configura el Router3. Muestra las tablas de rutas de los Router2 y Router3 con el comando show ip route.

```
Router1(config)#  ip route 192.168.2.0   255.255.255.0   12.0.0.2
Router2(config)#  ip route 192.168.1.0   255.255.255.0   13.0.0.2
Router3(config)#  ip route 192.168.1.0   255.255.255.0   12.0.0.1
Router3(config)#  ip route 192.168.2.0   255.255.255.0   13.0.0.1
```

Nota: Las siguientes rutas deben ser eliminadas:

- `Router1(config)# ip route 192.168.2.0 255.255.255.0 11.0.0.2`
- `Router2(config)# ip route 192.168.1.0 255.255.255.0 11.0.0.1`

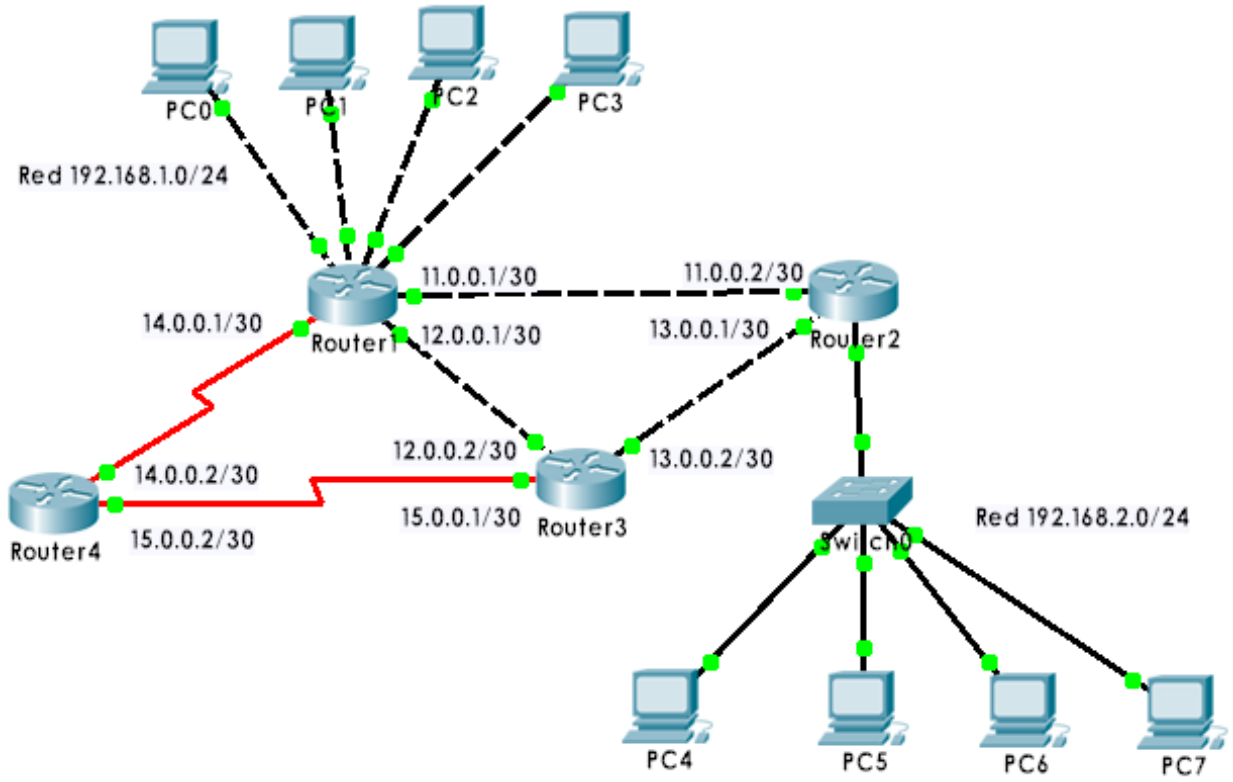


5. Añade un Router4 (con IP 14.0.0.0/30 y 15.0.0.0/30, por ejemplo) con un módulo HWIC-2T para 2 líneas serie. Añade a los Router3 y Router1 otro módulo HWIC-2T. Recuerda Guardar la configuración en ejecución a la NVRAM (Save Running Configuration to NVRAM) antes de apagar los routers si no quieres perderla. Modifica la tabla de rutas de Router3 para que los paquetes que vayan a la red local del Router1 pasen por Router4. Muestra las tablas de rutas de los Router3 y Router4 con el comando show ip route.

```
Router3(config)#  ip route 192.168.1.0   255.255.255.0   15.0.0.2
Router4(config)#  ip route 192.168.1.0   255.255.255.0   14.0.0.1
Router4(config)#  ip route 192.168.2.0   255.255.255.0   15.0.0.1
```

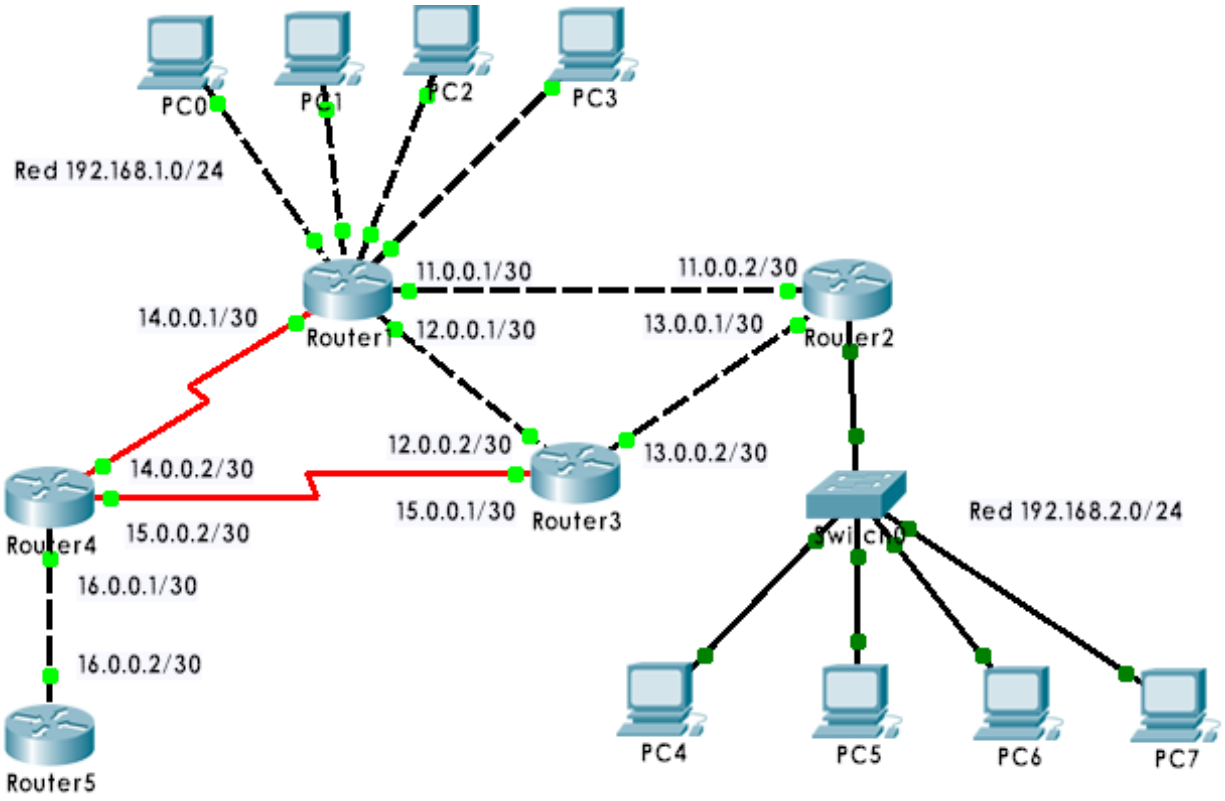
Nota: Las siguientes rutas deben ser eliminadas:

- `Router3(config)# ip route 192.168.1.0 255.255.255.0 12.0.0.1`



6. Añade un Router5 (16.0.0.0/30). Elimina todas las entradas de las tablas de rutas de los Router1 y Router2. Añade a Router1 una entrada para alcanzar la red2 a través del Router2. Añade a Router2 una entrada para alcanzar la red1 a través del Router1. Añade a ambos routers, una ruta por defecto (para enviar datos a cualquier otra red) a través de Router3. Configura Router3 y Router4 para que sus rutas por defecto se encaminen hacia Router5. Muestra las tablas de rutas de los Router3 y Router4 con el comando show ip route.

```
Router1(config)#  ip route 192.168.2.0   255.255.255.0 11.0.0.2
Router1(config)#  ip route 0.0.0.0       0.0.0.0       12.0.0.2
Router2(config)#  ip route 192.168.1.0   255.255.255.0 11.0.0.1
Router2(config)#  ip route 0.0.0.0       0.0.0.0       13.0.0.2
.
.
.
Router5(config)#  ip route 0.0.0.0       0.0.0.0       16.0.0.1
```



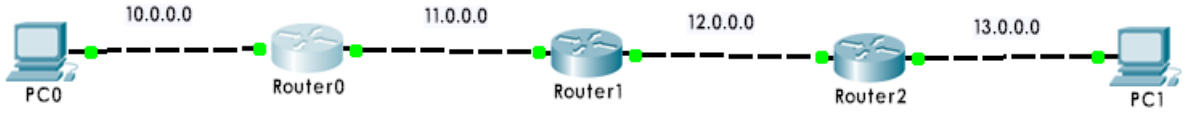
Enrutamiento dinámico (RIP)

Habilitamos RIP 2 y publicamos rutas adyacentes

```
Router0(config)#  router rip
Router0(config-router)#  version 2
Router0(config-router)#  network  RED
Router0(config-router)#  network  RED
```

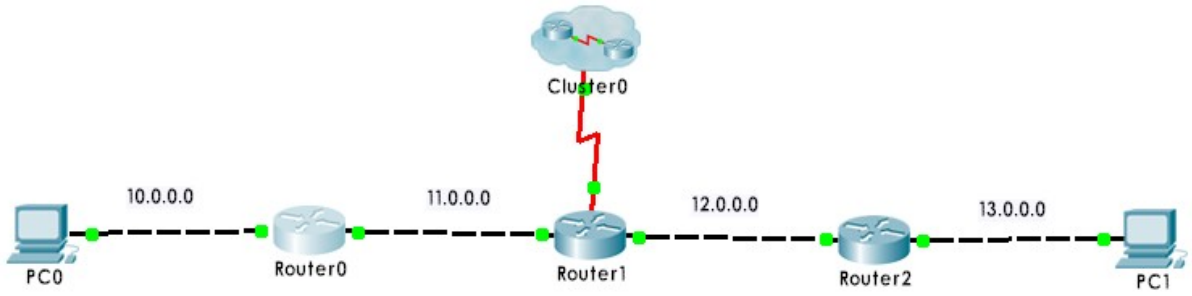
1. Crea un esquema con 3 routers tal como se muestra. Configura RIP versión 2 en cada uno de ellos. Comprueba que hay comunicación entre PC0 y PC1. ¿Cuáles son las tablas de rutas de Router0 y Router2?

```
Router0(config)#  router rip
Router0(config-router)#  version 2
Router0(config-router)#  network 10.0.0.0
Router0(config-router)#  network 11.0.0.0
```



2. Haz que Router1 se publique como ruta por defecto. Cualquier paquete con IP destino que no se halle en las redes mostradas se enviará a Router1, que a su vez lo enviará hacia fuera. Mostrar tabla de rutas de Router0.

```
Router1(config-router)#  default-information originate
```



Enrutamiento dinámico (OSPF)

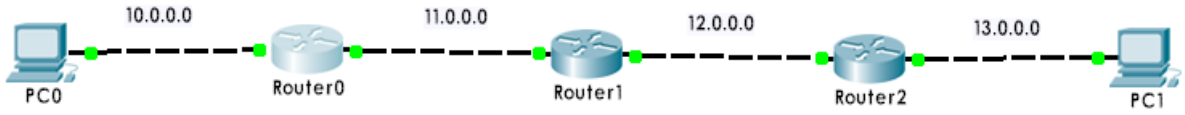
Habilitamos OSPF y publicamos rutas adyacentes

```
Router(config)#  router ospf x
Router(config-router)#  network  RED   WILDCARD  area 0
Router(config-router)#  network  RED   WILDCARD  area 0
```

```
x:        número de proceso (puede tomar un valor entre 1 y 65535)
WILDCARD: inverso binario de la máscara de red.
area 0:   núm. área (aconsejable poner 0 para área única en todos los routers de la␣
↪misma)
```

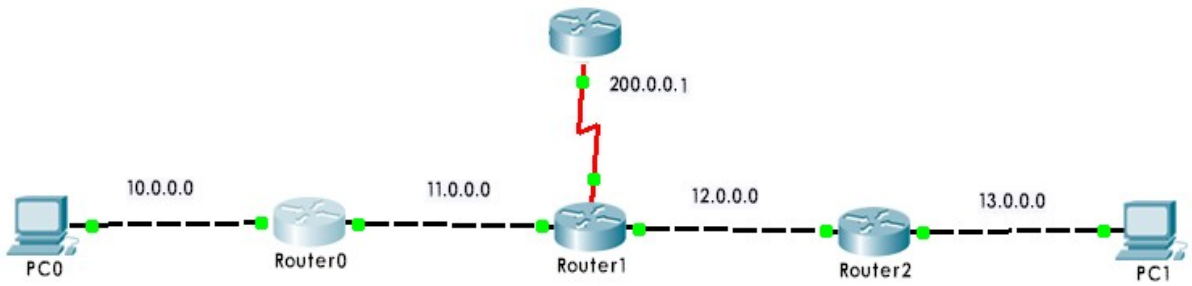
1. Crea un esquema con 3 routers tal como se muestra. Configura OSPF en cada uno de ellos. Comprueba que hay comunicación entre PC0 y PC1. ¿Cuáles son las tablas de rutas de Router0 y Router2?

```
Router0(config-router)#  network  10.0.0.0   0.255.255.255   area 0
Router0(config-router)#  network  11.0.0.0   0.255.255.255   area 0
```



2. Haz que Router1 se publique como ruta por defecto. Cualquier paquete con IP destino que no se halle en las redes mostradas se enviará a Router1, que a su vez lo enviará hacia fuera. Mostrar tabla de rutas de Router0.

```
Router1(config-router)#  ip route   0.0.0.0   0.0.0.0   200.0.0.1
Router1(config-router)#  default-information originate
```



Enrutamiento dinámico (BGP)

Habilitamos BGP

```
Router(config)#  router bgp  x
Router(config-router)#  neighbor   IP   remote-as  y
```

Redes detrás del router BGP

```
Router(config-router)#  network  RED  mask MASK
Router(config-router)#  network  RED  mask MASK
Router(config-router)#  network  RED  mask MASK
...
```

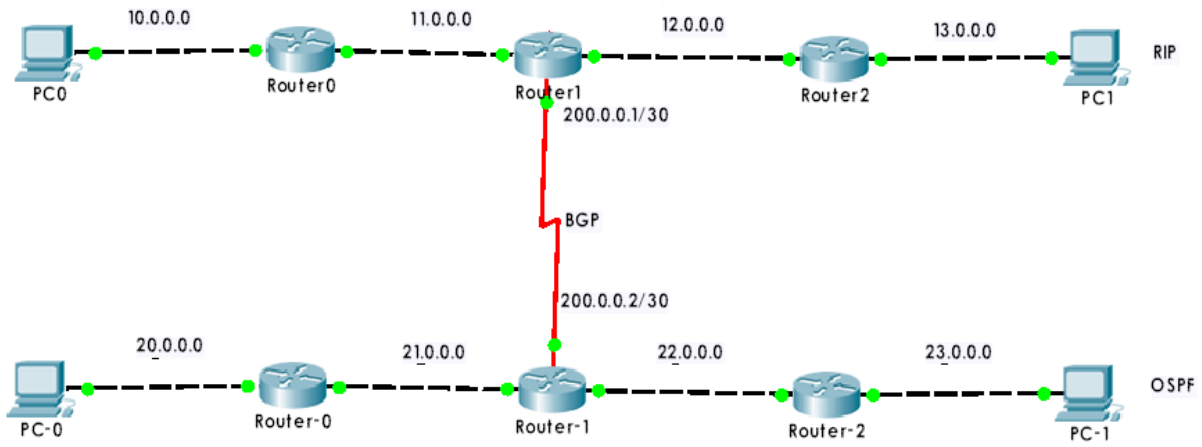
```
x, y: números de sistemas autónomos.
```

1. Crear el siguiente esquema. Tenemos 2 sistemas autónomos (AS): uno funcionando internamente con RIP (AS=10) y otro con OSPF (AS=20). Como routers frontera tenemos Router1 y Router-1. Configurar BGP en Router1 y Router-1. Mostrar ambas tablas de rutas.

```
Router-1(config)#  router bgp 20
Router-1(config-router)#  neighbor  200.0.0.1   remote-as 10
Router-1(config-router)#  network   20.0.0.0    mask 255.0.0.0
Router-1(config-router)#  network   21.0.0.0    mask 255.0.0.0
Router-1(config-router)#  network   22.0.0.0    mask 255.0.0.0
Router-1(config-router)#  network   23.0.0.0    mask 255.0.0.0
```

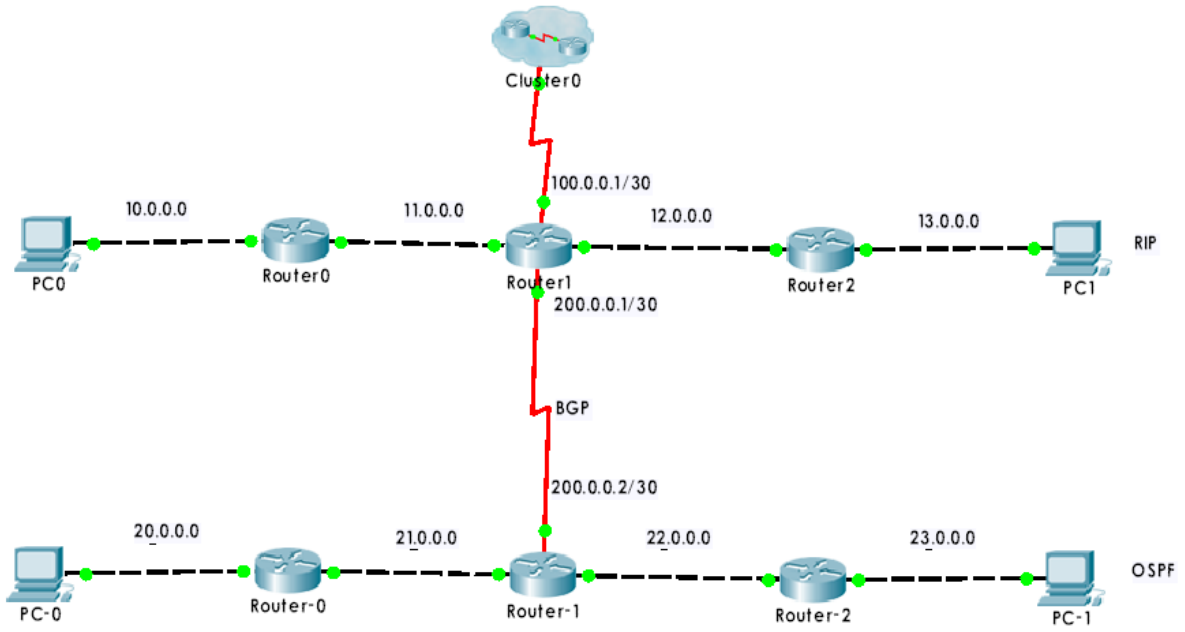
No olvides crear las rutas por defecto, tanto en Router1 como en Router-1

```
Router1(config-router)#  default-information originate
Router-1(config-router)#  ip route   0.0.0.0   0.0.0.0   200.0.0.1
Router-1(config-router)#  default-information originate
```



2. Añadir a Router1 una red exterior. Configurar la ruta BGP por defecto en Router1. Debes configurar además el equipo exterior 100.0.0.2 con soporte de BGP. Mostrar tablas de rutas de Router-1.

```
Router1(config-router)#  neighbor 100.0.0.2   default-originate
```



10.7.3 Actividad práctica (Opcional)

1. Instalar en el ordenador de casa los servicios:

- XAMPP (servidor de páginas web)
- VNC (servidor de acceso remoto gráfico)

En el router hacer DNAT estático (es decir, abrir y redirigir puertos o port forwarding):

- 80 (a ordenador de casa)
- 5800-5810, 5900-5910 (a ordenador de casa)

Hacer DDNS (DNS dinámico), es decir, registrar un nombre de dominio en dyndns, no-ip, o similar.

CAPÍTULO 11

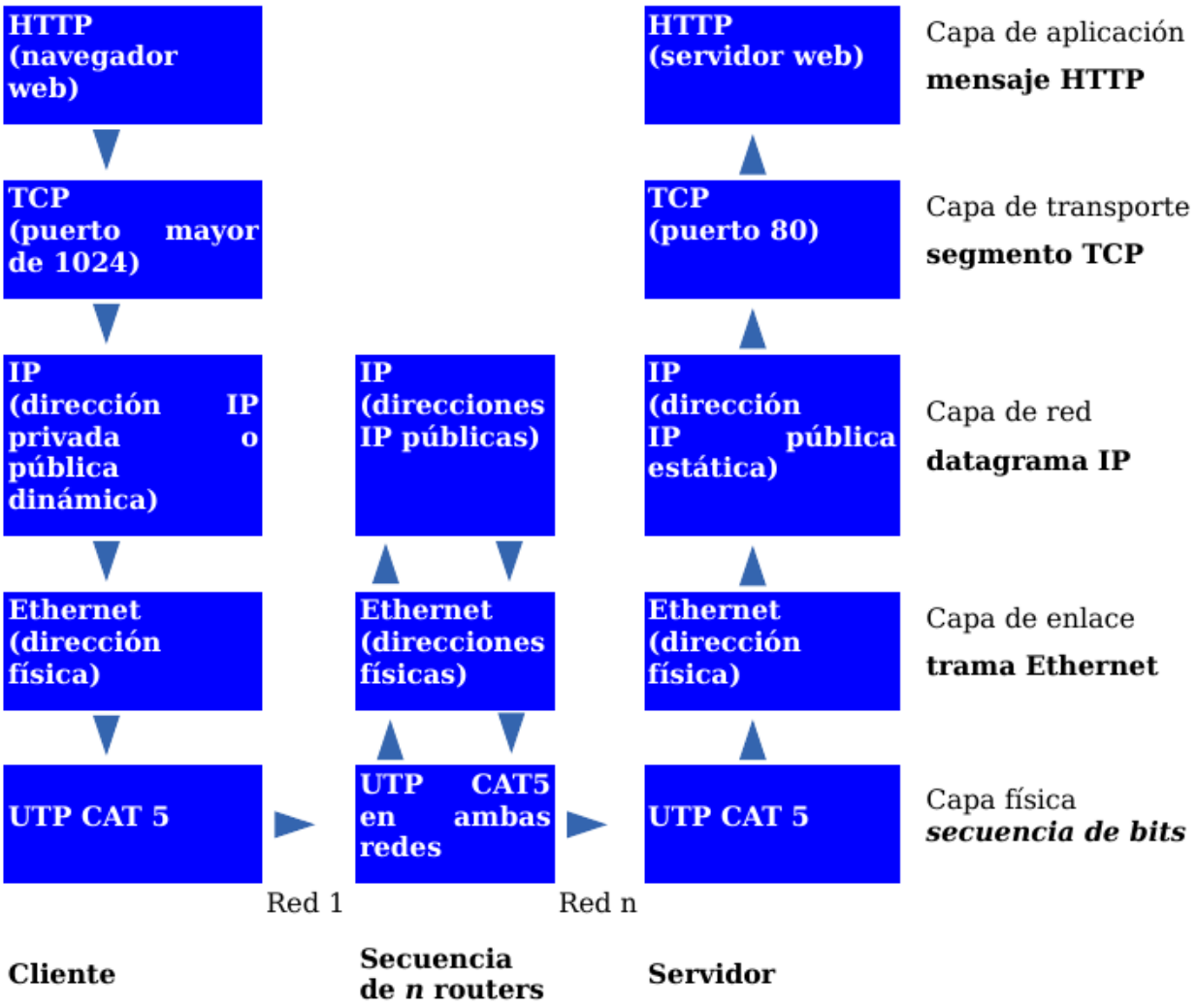
LA CAPA DE TRANSPORTE

11.1 Conceptos generales

La capa de red transfiere datagramas entre dos ordenadores a través de la red utilizando como identificadores las direcciones IP. La capa de transporte añade la noción de puerto para distinguir entre los muchos destinos dentro de un mismo host. No es suficiente con indicar la dirección IP del destino, además hay que especificar la aplicación que recogerá el mensaje. Cada aplicación que esté esperando un mensaje utiliza un número de puerto distinto; más concretamente, la aplicación está a la espera de un mensaje en un puerto determinado (escuchando un puerto).

Pero no sólo se utilizan los puertos para la recepción de mensajes, también para el envío: todos los mensajes que envíe un ordenador debe hacerlo a través de uno de sus puertos. El siguiente diagrama representa una transmisión entre el ordenador 194.35.133.5 y el 135.22.8.165. El primero utiliza su puerto 1256 y el segundo, el 80.

La capa de transporte transmite mensajes entre las aplicaciones de dos ordenadores. Por ejemplo, entre nuestro navegador de páginas web y un servidor de páginas web, o entre nuestro programa de correo electrónico y un servidor de correo.



11.1.1 Puertos

Un ordenador puede estar conectado con distintos servidores a la vez; por ejemplo, con un servidor de noticias y un servidor de correo. Para distinguir las distintas conexiones dentro de un mismo ordenador se utilizan los puertos.

Un puerto es un número de 16 bits, por lo que existen 65536 puertos en cada ordenador. Las aplicaciones utilizan estos puertos para recibir y transmitir mensajes.

La asignación de puertos puede obtenerse desde el IANA

Se pueden clasificar en:

- **Puertos bien conocidos** (Known Ports: **0 hasta 1023**).
- **Puertos registrados** (Registered Ports: **2024 hasta 49151**)
- **Puertos dinámicos y/o privados** (Dynamic and/or Private Ports: **49152 hasta 65535**)

A continuación se muestra una lista de los **puertos más importantes**.

Puertos bien conocidos

Puerto/Protocolo	Descripción
0/udp	Reservado
20/tcp	FTP File Transfer Protocol (Protocolo de Transferencia de Ficheros) - datos
21/tcp	FTP File Transfer Protocol (Protocolo de Transferencia de Ficheros) - control
22/tcp	SSH, scp, SFTP
23/tcp	Telnet manejo remoto de equipo, inseguro
25/tcp	SMTP Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correo)
53/tcp	DNS Domain Name System (Sistema de Nombres de Dominio)
53/udp	DNS Domain Name System (Sistema de Nombres de Dominio)
67/udp	BOOTP BootStrap Protocol (Server), también usado por DHCP
68/udp	BOOTP BootStrap Protocol (Client), también usado por DHCP
69/udp	TFTP Trivial File Transfer Protocol (Protocolo Trivial de Transferencia de Ficheros)
80/tcp	HTTP HyperText Transfer Protocol (Protocolo de Transferencia de HiperTexto) (WWW)
88/tcp	Kerberos Agente de autenticación
110/tcp	POP3 Post Office Protocol (E-mail)
123/udp	NTP Protocolo de sincronización de tiempo
123/tcp	NTP Protocolo de sincronización de tiempo
137/tcp	NetBIOS Servicio de nombres
137/udp	NetBIOS Servicio de nombres
138/tcp	NetBIOS Servicio de envío de datagramas
138/udp	NetBIOS Servicio de envío de datagramas
139/tcp	NetBIOS Servicio de sesiones
139/udp	NetBIOS Servicio de sesiones
143/tcp	IMAP4 Internet Message Access Protocol (E-mail)
161/tcp	SNMP Simple Network Management Protocol
161/udp	SNMP Simple Network Management Protocol
389/tcp	LDAP Protocolo de acceso ligero a Bases de Datos
389/udp	LDAP Protocolo de acceso ligero a Bases de Datos
443/tcp	HTTPS/SSL para la transferencia segura de páginas web
445/tcp	Microsoft-DS (Active Directory, compartición en Windows, gusano Sasser, Agobot)
445/udp	Microsoft-DS compartición de ficheros
465/tcp	SMTP Sobre SSL. Envío de correo electrónico (E-mail)
631/tcp	CUPS sistema de impresión de Unix
993/tcp	IMAP4 sobre SSL (E-mail)
995/tcp	POP3 sobre SSL (E-mail)
1023/tcp	Reservado
1023/udp	Reservado

Puertos registrados

Puerto/Protocolo	Descripción
1024/tcp	Reservado
1024/udp	Reservado
1433/tcp	Microsoft-SQL-Server
1512/tcp	WINS Windows Internet Naming Service
2049/tcp	NFS Archivos del sistema de red
3128/tcp	HTTP web cache y por defecto en Squid cache
3306/tcp	MySQL sistema de gestión de bases de datos
3389/tcp	RDP (Remote Desktop Protocol) Terminal Server
4662/tcp	eMule (aplicación de compartición de ficheros)
4672/udp	eMule (aplicación de compartición de ficheros)
4899/tcp	RAdmin (Remote Administrator), herramienta de administración remota (normalmente troyanos)
5432/tcp	PostgreSQL sistema de gestión de bases de datos
5631/tcp	PC-Anywhere protocolo de escritorio remoto
5632/udp	PC-Anywhere protocolo de escritorio remoto
5400/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5500/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5600/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5700/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5800/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5900/tcp	VNC protocolo de escritorio remoto (conexión normal)
6881/tcp	BitTorrent puerto por defecto
6969/tcp	BitTorrent puerto de tracker
8080/tcp	HTTP alternativo. Proxy Web el servidor de almacenamiento en caché. Tomcat.
8118/tcp	privoxy
10000/tcp	Webmin (Administración remota web)
31337/tcp	Back Orifice herramienta de administración remota (por lo general troyanos)
49151/tcp	Reservado
49151/udp	Reservado

Puede encontrarse las lista completa con el servicio asociado en http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

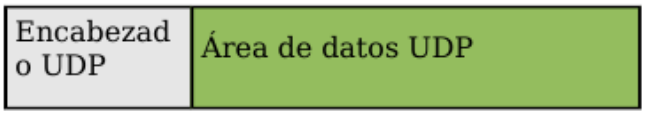
11.2 Estándares

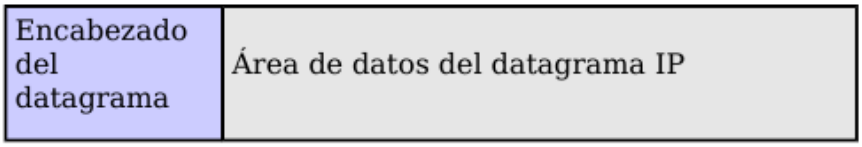
11.2.1 Protocolo UDP

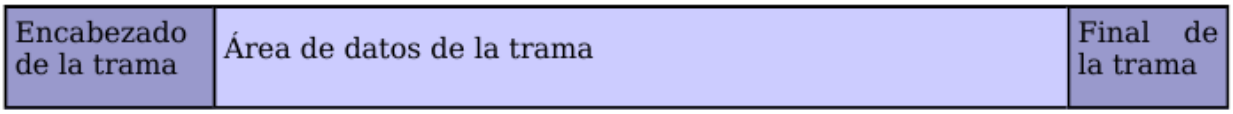
El protocolo UDP (User Datagram Protocol, protocolo de datagrama de usuario) proporciona una comunicación muy sencilla entre las aplicaciones de dos ordenadores. Al igual que el protocolo IP, UDP es:

- **No orientado a conexión**. No se establece una conexión previa con el otro extremo para transmitir un mensaje UDP. Los mensajes se envían sin más y éstos pueden duplicarse o llegar desordenados al destino.
- **No fiable**. Los mensajes UDP se pueden perder o llegar dañados.

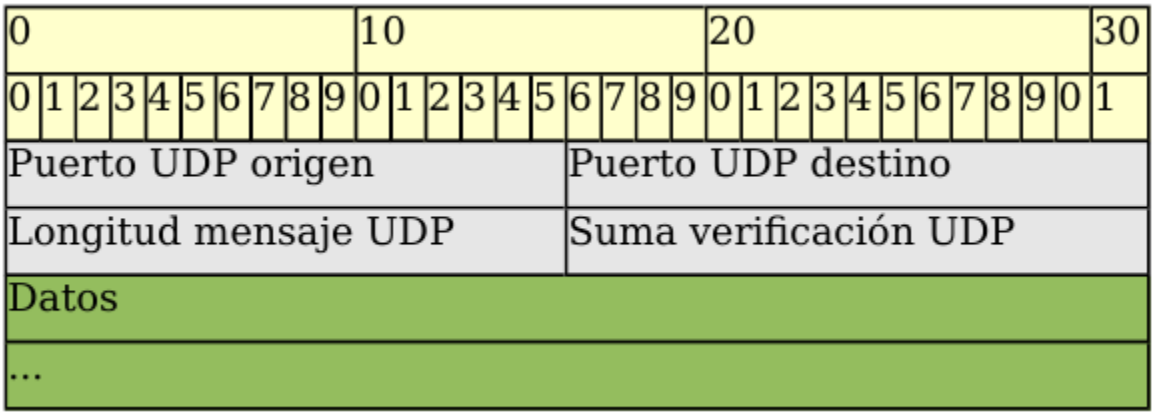
UDP utiliza el protocolo IP para transportar sus mensajes. Como vemos, no añade ninguna mejora en la calidad de la transferencia; aunque sí incorpora los puertos origen y destino en su formato de mensaje. Las aplicaciones (y no el protocolo UDP) deberán programarse teniendo en cuenta que la información puede no llegar de forma correcta.







Formato de un mensaje UDP



- **Puerto UDP de origen** (16 bits, opcional). Número de puerto de la máquina origen.
- **Puerto UDP de destino** (16 bits). Número de puerto de la máquina destino.
- **Longitud del mensaje UDP** (16 bits). Especifica la longitud medida en bytes del mensaje UDP incluyendo la cabecera. La longitud mínima es de 8 bytes.
- **Suma de verificación UDP** (16 bits, opcional). Suma de comprobación de errores del mensaje. Para su cálculo se utiliza una pseudo-cabecera que también incluye las direcciones IP origen y destino. Para conocer estos datos, el protocolo UDP debe interactuar con el protocolo IP.
- **Datos**. Aquí viajan los datos que se envían las aplicaciones. Los mismos datos que envía la aplicación origen son recibidos por la aplicación destino después de atravesar toda la Red de redes.

11.2.2 Protocolo TCP

El protocolo TCP (Transmission Control Protocol, protocolo de control de transmisión) está basado en IP que es no fiable y no orientado a conexión, y sin embargo es:

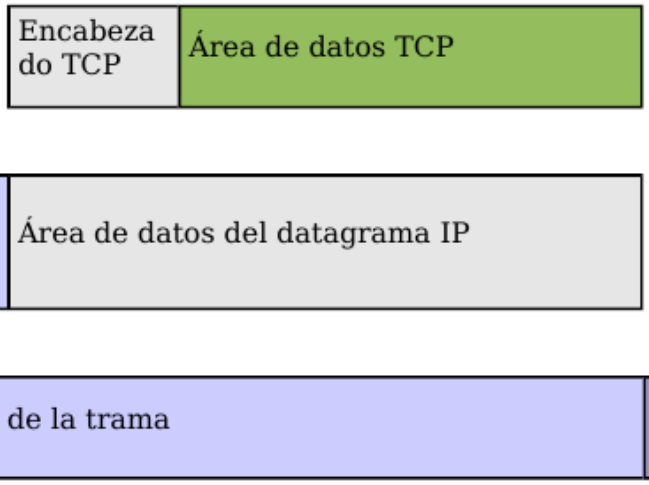
- **Orientado a conexión**. Es necesario establecer una conexión previa entre las dos máquinas antes de poder transmitir ningún dato. A través de esta conexión los datos llegarán siempre a la aplicación destino de forma ordenada y sin duplicados. Finalmente, es necesario cerrar la conexión.

- **Fiable**. La información que envía el emisor llega de forma correcta al destino.

El protocolo TCP permite una comunicación fiable entre dos aplicaciones. De esta forma, las aplicaciones que lo utilicen no tienen que preocuparse de la integridad de la información: dan por hecho que todo lo que reciben es correcto.

El flujo de datos entre una aplicación y otra viajan por un circuito virtual. Sabemos que los datagramas IP pueden seguir rutas distintas, dependiendo del estado de los encaminadores intermedios, para llegar a un mismo sitio. Esto significa que los datagramas IP que transportan los mensajes siguen rutas diferentes aunque el protocolo TCP logré la ilusión de que existe un único circuito por el que viajan todos los bytes uno detrás de otro (algo así como una tubería entre el origen y el destino). Para que esta comunicación pueda ser posible es necesario abrir previamente una conexión. Esta conexión garantiza que los todos los datos lleguen correctamente de forma ordenada y sin duplicados. La unidad de datos del protocolo es el byte, de tal forma que la aplicación origen envía bytes y la aplicación destino recibe estos bytes.

Sin embargo, cada byte no se envía inmediatamente después de ser generado por la aplicación, sino que se espera a que haya una cierta cantidad de bytes, se agrupan en un segmento y se envía el segmento completo. Para ello son necesarias unas memorias intermedias o buffers. Cada uno de estos segmentos viaja en el campo de datos de un datagrama IP. Si el segmento es muy grande será necesario fragmentar el datagrama, con la consiguiente pérdida de rendimiento; y si es muy pequeño, se estarán enviando más cabeceras que datos. Por consiguiente, es importante elegir el mayor tamaño de segmento posible que no provoque fragmentación.

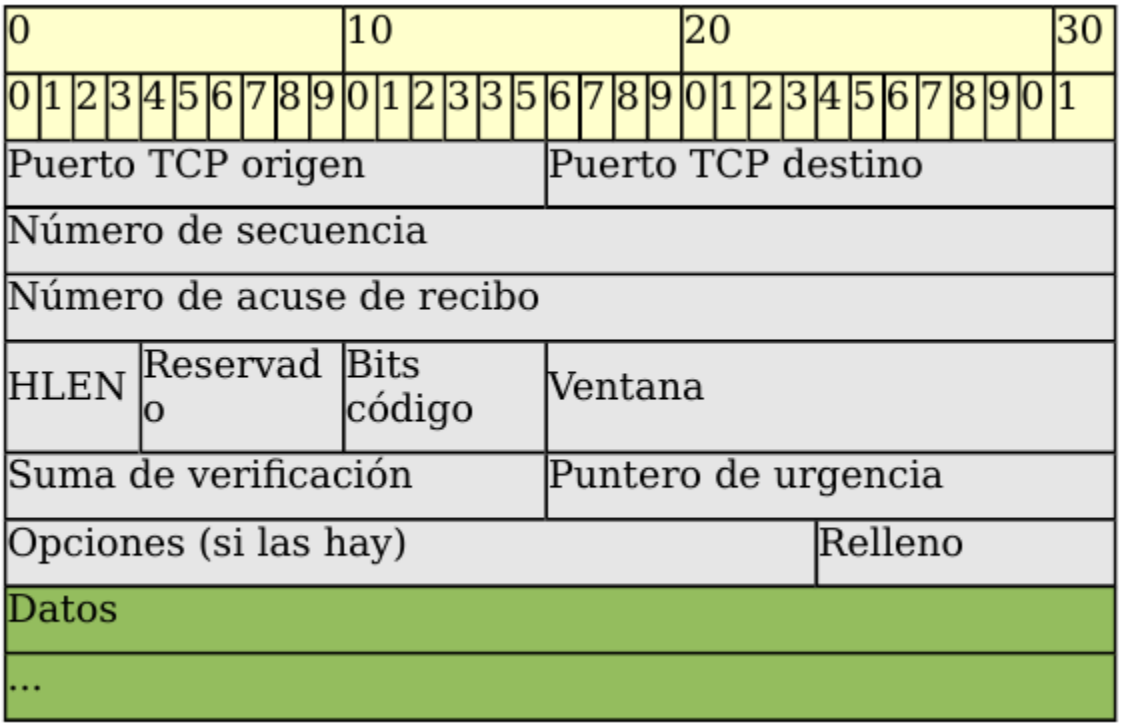


El protocolo TCP envía un flujo de información no estructurado. Esto significa que los datos no tienen ningún formato, son únicamente los bytes que una aplicación envía a otra. Ambas aplicaciones deberán ponerse de acuerdo para comprender la información que se están enviando.

Cada vez que se abre una conexión, se crea un canal de comunicación bidireccional en el que ambas aplicaciones pueden enviar y recibir información, es decir, una conexión es full-dúplex.

Formato del segmento TCP

Ya hemos comentado que el flujo de bytes que produce una determinada aplicación se divide en uno o más segmentos TCP para su transmisión. Cada uno de estos segmentos viaja en el campo de datos de un datagrama IP. Para facilitar el control de flujo de la información los bytes de la aplicación se numeran. De esta manera, cada segmento indica en su cabecera el primer byte que transporta. Las confirmaciones o acuses de recibo (ACK) representan el siguiente byte que se espera recibir (y no el número de segmento recibido, ya que éste no existe).



- **Puerto fuente** (16 bits). Puerto de la máquina origen. Al igual que el puerto destino es necesario para identificar la conexión actual.
- **Puerto destino** (16 bits). Puerto de la máquina destino.
- **Número de secuencia** (32 bits). Indica el número de secuencia del primer byte que trasporta el segmento.
- **Número de acuse de recibo** (32 bits). Indica el número de secuencia del siguiente byte que se espera recibir. Con este campo se indica al otro extremo de la conexión que los bytes anteriores se han recibido correctamente.
- **HLEN** (4 bits). Longitud de la cabecera medida en múltiplos de 32 bits (4 bytes). El valor mínimo de este campo es 5, que corresponde a un segmento sin datos (20 bytes).
- **Reservado** (6 bits). Bits reservados para un posible uso futuro.
- **Bits de código o indicadores** (6 bits). Los bits de código determinan el propósito y contenido del segmento. A continuación se explica el significado de cada uno de estos bits (mostrados de izquierda a derecha) si está a 1.
  - **URG**. El campo Puntero de urgencia contiene información válida.
  - **ACK**. El campo Número de acuse de recibo contiene información válida, es decir, el segmento actual lleva un ACK. Observemos que un mismo segmento puede transportar los datos de un sentido y las confirmaciones del otro sentido de la comunicación.
  - **PSH**. La aplicación ha solicitado una operación push (enviar los datos existentes en la memoria temporal sin esperar a completar el segmento).
  - **RST**. Interrupción de la conexión actual.
  - **SYN**. Sincronización de los números de secuencia. Se utiliza al crear una conexión para indicar al otro extremo cual va a ser el primer número de secuencia con el que va a comenzar a transmitir (veremos que no tiene porqué ser el cero).
  - **FIN**. Indica al otro extremo que la aplicación ya no tiene más datos para enviar. Se utiliza para solicitar el cierre de la conexión actual.
- **Ventana** (16 bits). Número de bytes que el emisor del segmento está dispuesto a aceptar por parte del destino.

- **Suma de verificación** (24 bits). Suma de comprobación de errores del segmento actual. Para su cálculo se utiliza una pseudo-cabecera que también incluye las direcciones IP origen y destino.
- **Puntero de urgencia** (8 bits). Se utiliza cuando se están enviando datos urgentes que tienen preferencia sobre todos los demás e indica el siguiente byte del campo Datos que sigue a los datos urgentes. Esto le permite al destino identificar donde terminan los datos urgentes. Nótese que un mismo segmento puede contener tanto datos urgentes (al principio) como normales (después de los urgentes).
- **Opciones** (variable). Si está presente únicamente se define una opción: el tamaño máximo de segmento que será aceptado.
- **Relleno**. Se utiliza para que la longitud de la cabecera sea múltiplo de 32 bits.
- **Datos**. Información que envía la aplicación.

Fiabilidad

¿Cómo es posible enviar información fiable basándose en un protocolo no fiable? Es decir, si los datagramas que transportan los segmentos TCP se pueden perder, ¿cómo pueden llegar los datos de las aplicaciones de forma correcta al destino?

La respuesta a esta pregunta es sencilla: cada vez que llega un mensaje se devuelve una confirmación (acknowledgement) para que el emisor sepa que ha llegado correctamente. Si no le llega esta confirmación pasado un cierto tiempo, el emisor reenvía el mensaje.

Veamos a continuación la manera más sencilla (aunque ineficiente) de proporcionar una comunicación fiable. El emisor envía un dato, arranca su temporizador y espera su confirmación (ACK). Si recibe su ACK antes de agotar el temporizador, envía el siguiente dato. Si se agota el temporizador antes de recibir el ACK, reenvía el mensaje. Los siguientes esquemas representan este comportamiento:

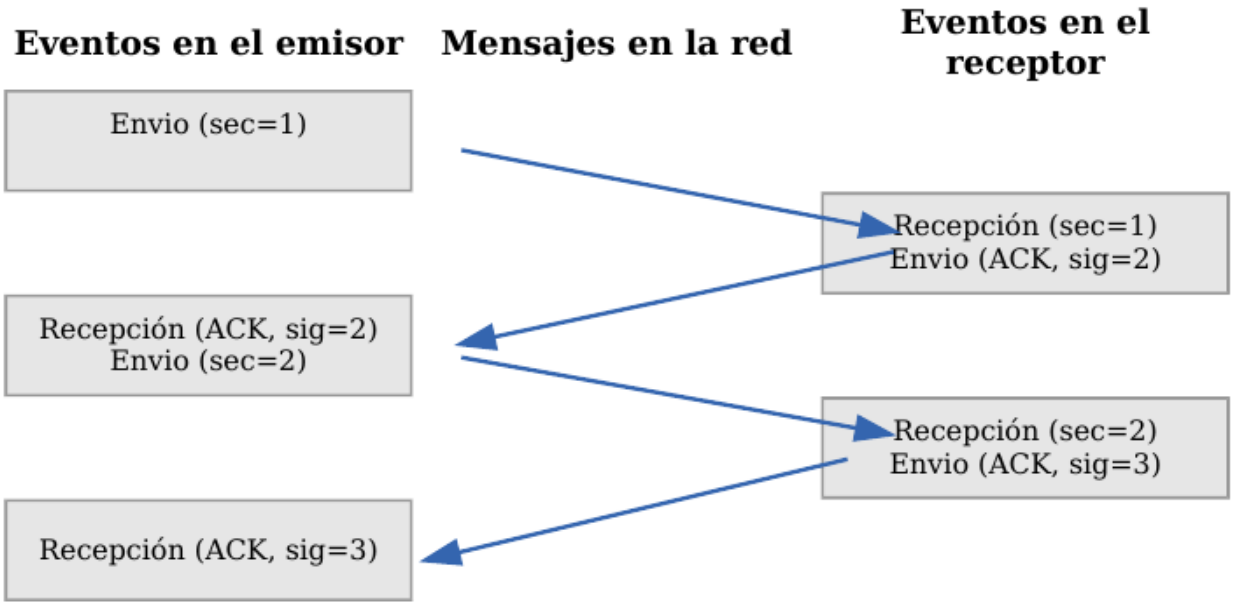


Figura 1: TCP - Confirmaciones positivas (ACK)

Este esquema es perfectamente válido aunque muy ineficiente debido a que sólo se utiliza un sentido de la comunicación a la vez y el canal está desaprovechado la mayor parte del tiempo. Para solucionar este problema se utiliza un protocolo de ventana deslizante, que se resume en el siguiente esquema. Los mensajes y las confirmaciones van numerados y el emisor puede enviar más de un mensaje antes de haber recibido todas las confirmaciones anteriores.

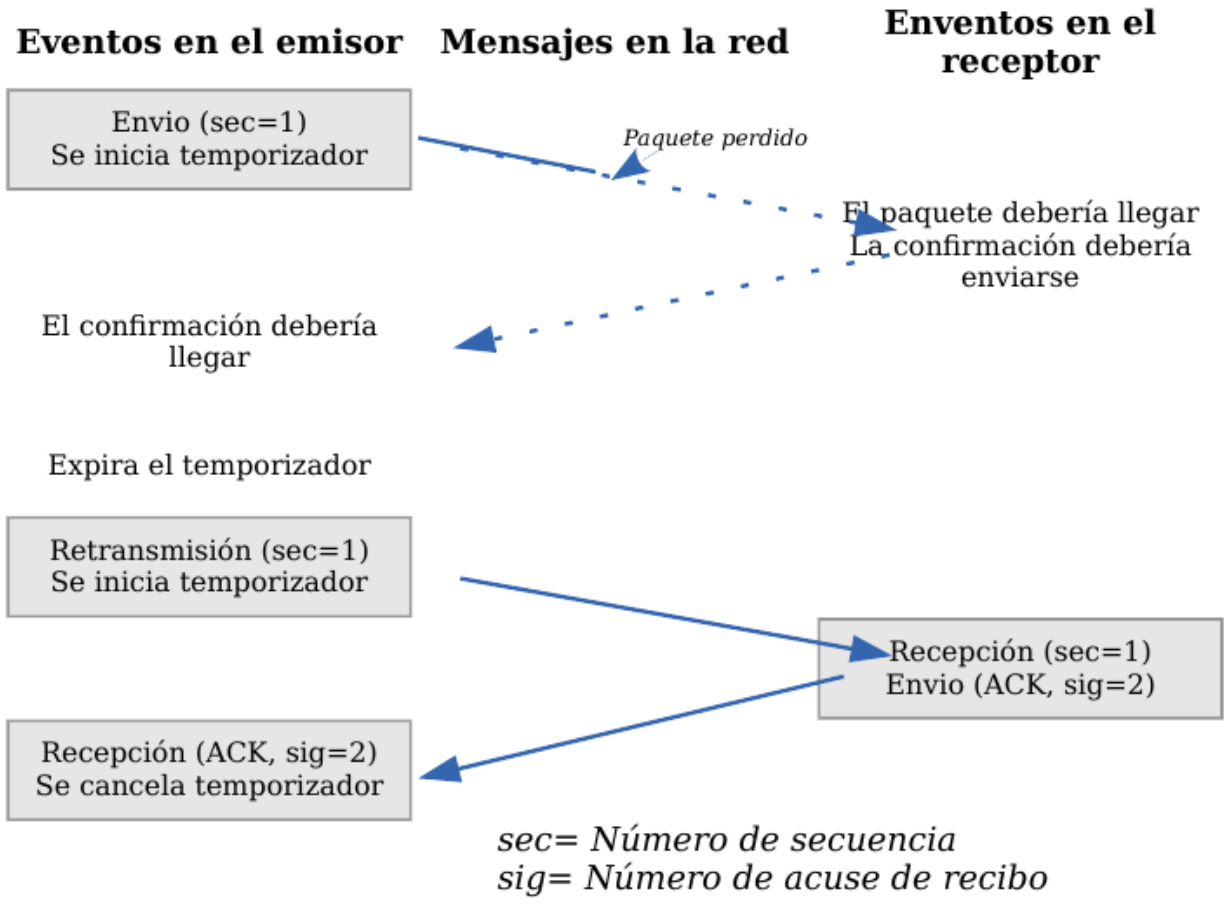


Figura 2: TCP - Temporizador

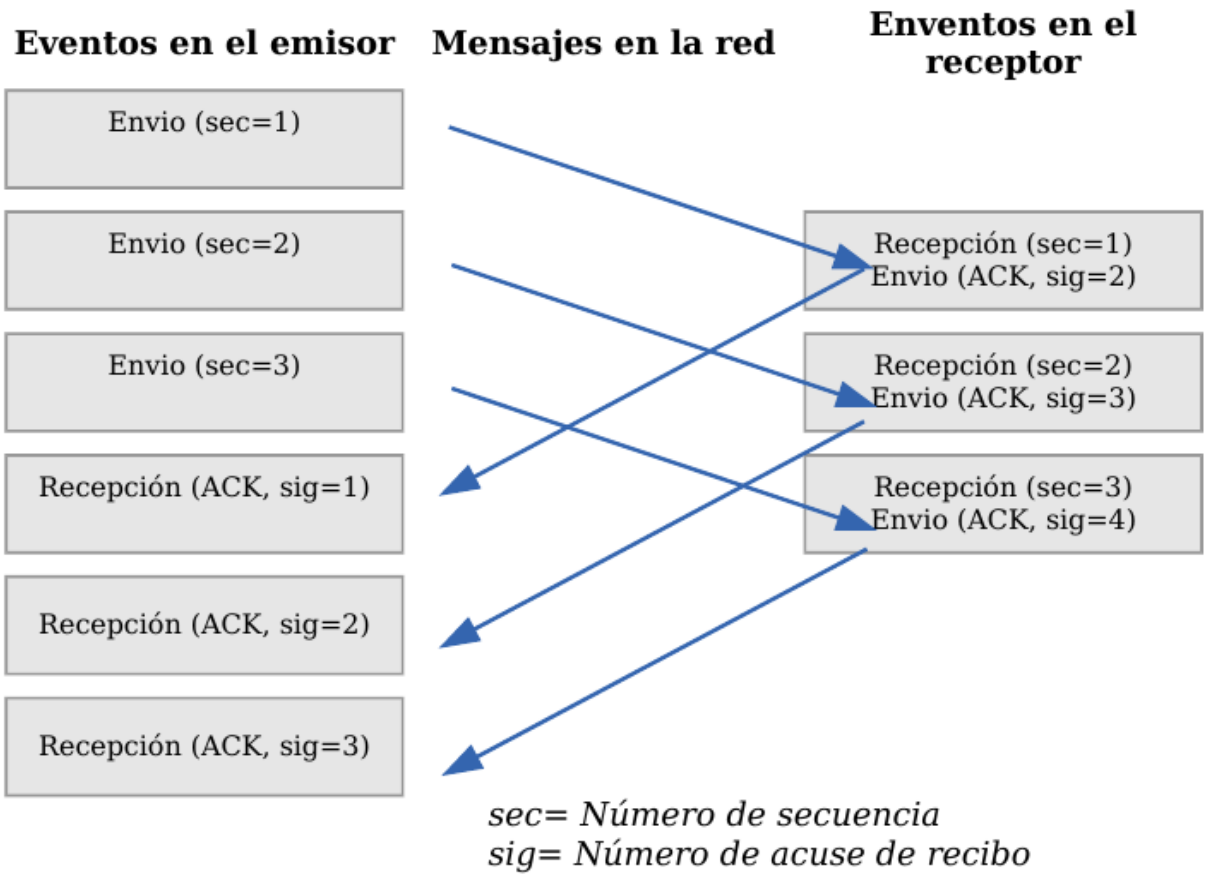
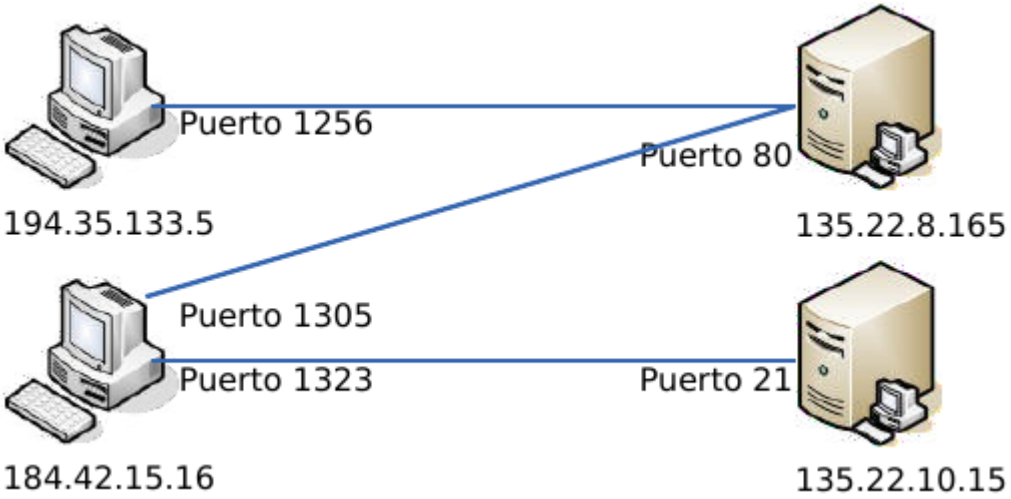


Figura 3: TCP - Ventana deslizante

Conexiones

Una conexión son dos pares dirección IP:puerto. No puede haber dos conexiones iguales en un mismo instante en toda la Red. Aunque bien es posible que un mismo ordenador tenga dos conexiones distintas y simultáneas utilizando un mismo puerto. El protocolo TCP utiliza el concepto de conexión para identificar las transmisiones. En el siguiente ejemplo se han creado tres conexiones. Las dos primeras son al mismo servidor Web (puerto 80) y la tercera a un servidor de FTP (puerto 21).

Host 1	Host 2
194.35.133.5:1256	135.22.8.165:80
184.42.15.16:1305	135.22.8.165:80
184.42.15.16:1323	135.22.10.15:21



Para que se pueda crear una conexión, el extremo del servidor debe hacer una apertura pasiva del puerto (escuchar su puerto y quedar a la espera de conexiones) y el cliente, una apertura activa en el puerto del servidor (conectarse con el puerto de un determinado servidor).

Nota: El comando **NetStat** muestra las conexiones abiertas en un ordenador, así como estadísticas de los distintos protocolos de Internet.

Establecimiento de una conexión

Antes de transmitir cualquier información utilizando el protocolo TCP es necesario abrir una conexión. Un extremo hace una apertura pasiva y el otro, una apertura activa. El mecanismo utilizado para establecer una conexión consta de tres vías.

1. La máquina que quiere iniciar la conexión hace una apertura activa enviando al otro extremo un mensaje que tenga el bit SYN activado. Le informa además del primer número de secuencia que utilizará para enviar sus mensajes.
2. La máquina receptora (un servidor generalmente) recibe el segmento con el bit SYN activado y devuelve la correspondiente confirmación. Si desea abrir la conexión, activa el bit SYN del segmento e informa de su primer número de secuencia. Deja abierta la conexión por su extremo.

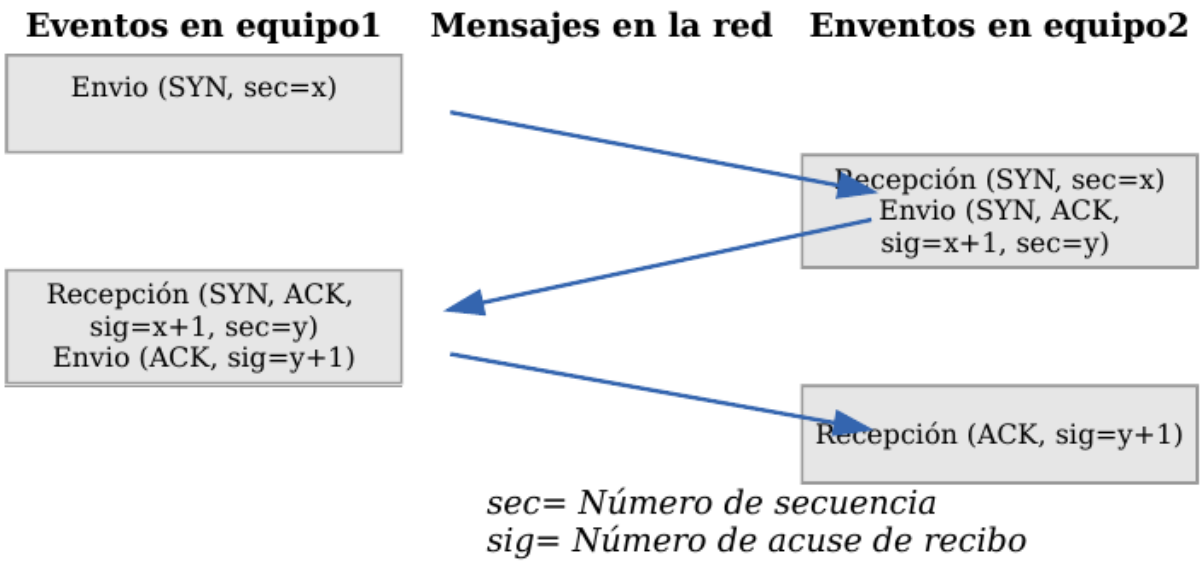


Figura 4: TCP - Establecimiento de una conexión

3. La primera máquina recibe el segmento y envía su confirmación. A partir de este momento puede enviar datos al otro extremo. Abre la conexión por su extremo.
4. La máquina receptora recibe la confirmación y entiende que el otro extremo ha abierto ya su conexión. A partir de este momento puede enviar ella también datos. La conexión ha quedado abierta en los dos sentidos.

Observamos que son necesarios 3 segmentos para que ambas máquinas abran sus conexiones y sepan que la otra también está preparada.

Números de secuencia

Se utilizan números de secuencia distintos para cada sentido de la comunicación. Como hemos visto el primer número para cada sentido se acuerda al establecer la comunicación. Cada extremo se inventa un número aleatorio y envía éste como inicio de secuencia. Observamos que los números de secuencia no comienzan entonces en el cero. ¿Por qué se procede así? Uno de los motivos es para evitar conflictos: supongamos que la conexión en un ordenador se interrumpe nada más empezar y se crea una nueva. Si ambas han empezado en el cero es posible que el receptor entienda que la segunda conexión es una continuación de la primera (si utilizan los mismos puertos).

Cierre de una conexión

Cuando una aplicación ya no tiene más datos que transferir, el procedimiento normal es cerrar la conexión utilizando una variación del mecanismo de 3 vías explicado anteriormente.

El mecanismo de cierre es algo más complicado que el de establecimiento de conexión debido a que las conexiones son full-duplex y es necesario cerrar cada uno de los dos sentidos de forma independiente.

1. La máquina que ya no tiene más datos que transferir, envía un segmento con el bit FIN activado y cierra el sentido de envío. Sin embargo, el sentido de recepción de la conexión sigue todavía abierto.
2. La máquina receptora recibe el segmento con el bit FIN activado y devuelve la correspondiente confirmación. Pero no cierra inmediatamente el otro sentido de la conexión sino que informa a la aplicación de la petición de cierre. Aquí se produce un lapso de tiempo hasta que la aplicación decide cerrar el otro sentido de la conexión.

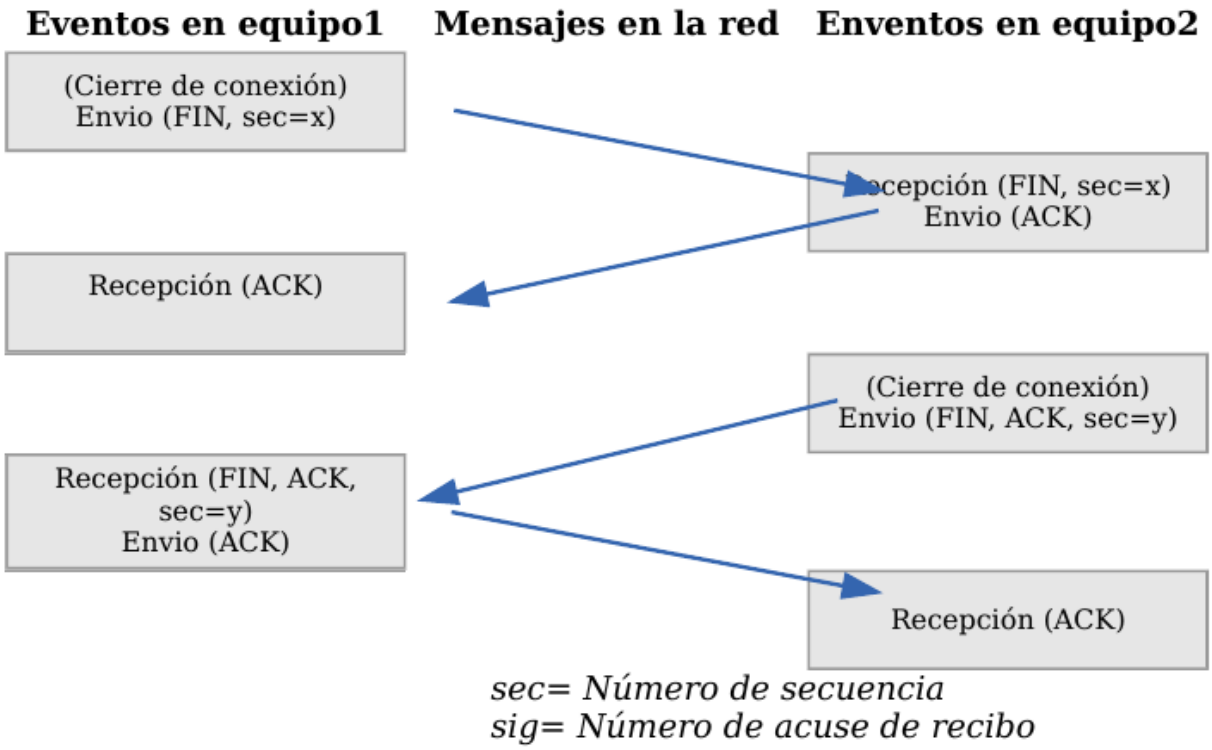


Figura 5: TCP - Cierre de una conexión

3. La primera máquina recibe el segmento ACK.
4. Cuando la máquina receptora toma la decisión de cerrar el otro sentido de la comunicación, envía un segmento con el bit FIN activado y cierra la conexión.
5. La primera máquina recibe el segmento FIN y envía el correspondiente ACK. Observemos que aunque haya cerrado su sentido de la conexión sigue devolviendo las confirmaciones.
6. La máquina receptora recibe el segmento ACK.

11.3 Técnicas

11.3.1 NAT (Network Address Translation)

Es un estándar creado por la Internet Engineering Task Force (IETF) el cual utiliza una o más direcciones IP para conectar varios computadores a otra red (normalmente a Internet), los cuales tiene una dirección IP completamente distinta (normalmente una IP no válida de Internet). Por lo tanto, se puede utilizar para dar salida a redes públicas a computadores que se encuentran con direccionamiento privado o para proteger máquinas públicas.

Fue inicialmente propuesto como otra solución para la extinción de direcciones IP. Como ya sabemos para poder comunicarse en Internet se requieren direcciones IP públicas únicas (“legales”) para cada host. La idea en la que se basa NAT es que sólo una pequeña parte de la red de una organización está conectada con el exterior simultáneamente, es decir, sólo se asigna una dirección IP pública oficial a un host cuando va a comunicarse con el exterior, por tanto, solo es necesario un pequeño número de direcciones públicas. Los hosts internos pueden utilizar direcciones IP privadas (o direcciones IP no oficiales) y para los paquetes de salida el dispositivo NAT cambia la dirección origen privada por

una dirección pública oficial. Igualmente para los paquetes de entrada el dispositivo NAT cambia la dirección pública por otra privada.

Funcionamiento

El protocolo TCP/IP tiene la capacidad de generar varias conexiones simultáneas con un dispositivo remoto. Para realizar esto, dentro de la cabecera de un paquete IP, existen campos en los que se indica la dirección fuente y destino con sus respectivos puertos. Esta combinación de números define una única conexión.

Un encaminador NAT cambia la dirección fuente (lo que se conoce como SNAT, **Source NAT**) en cada paquete de salida y, dependiendo del método, también el puerto de fuente para que sea único. Estas traducciones de dirección se almacenan en una tabla, para recordar que dirección y puerto le corresponde a cada dispositivo cliente y así saber donde deben regresar los paquetes de respuesta. Si un paquete que intente ingresar a la red interna no existe en la **tabla de traducciones**, entonces es descartado. Por ello las conexiones que se inicien en el exterior (Internet) hacia el interior (Intranet) no están permitidas, lo que hace que dicho encaminador NAT tenga el "efecto secundario" de servir de cortafuegos.

Debido a este comportamiento, si queremos ofrecer al exterior (Internet) un servicio, se puede definir en la tabla que en un determinado puerto y dirección, se pueda acceder a un determinado dispositivo, como por ejemplo un servidor web, lo que se denomina NAT inverso o DNAT (**Destination NAT**).

Resumiendo:

- **SNAT - Source NAT** es cuando alteramos el origen del primer paquete: esto es, estamos cambiando el lugar de donde viene la conexión. Source NAT siempre se hace después del encaminamiento, justo antes de que el paquete salga por el cable. El enmascaramiento es una forma especializada de SNAT.
- **DNAT - Destination NAT** es cuando alteramos la dirección de destino del primer paquete: esto es, cambiamos la dirección a donde se dirige la conexión. DNAT siempre se hace antes del encaminamiento, cuando el paquete entra por el cable. El port forwarding (reenvío de puerto), el balanceo de carga y el proxy transparente son formas de DNAT.

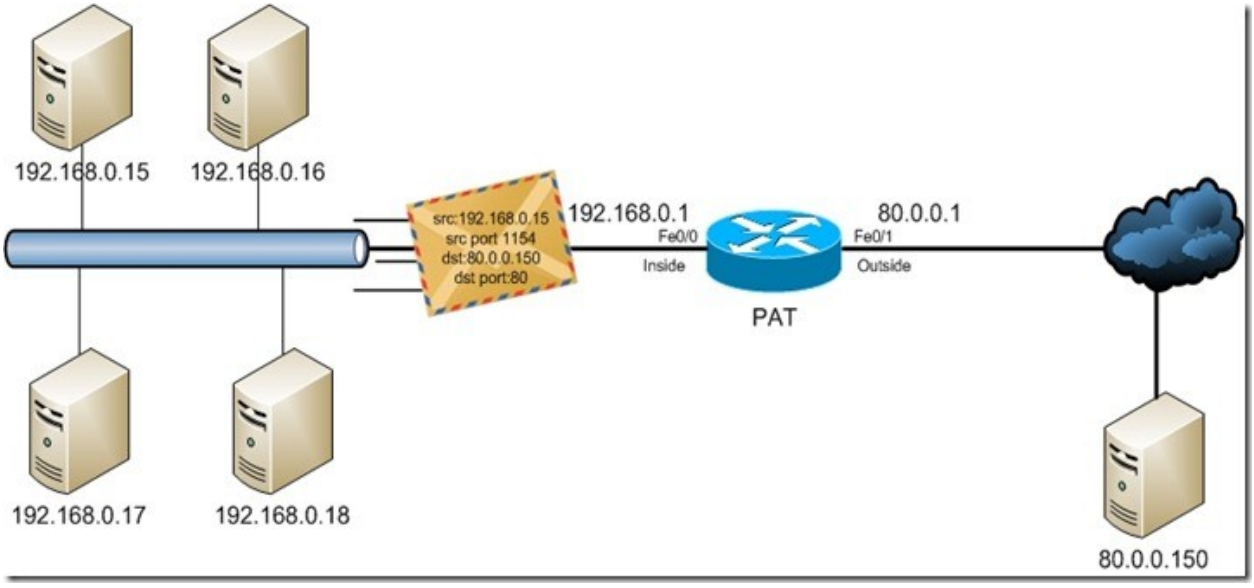
Tipos de NAT

NAT tiene muchas formas de funcionamiento, entre las que destaca:

- **NAT estático (Static NAT)**: Realiza un mapeo en la que una dirección IP privada se traduce a una correspondiente dirección IP pública de forma unívoca. Normalmente se utiliza cuando un dispositivo necesita ser accesible desde fuera de la red privada.
- **NAT dinámico (Dynamic NAT)**: Varias direcciones IP privadas se traducen a una dirección pública. Por ejemplo, si un router posee la IP pública 194.68.10.10, esta dirección se utiliza para representar todo un rango de direcciones privadas como puede ser 192.168.1.x. Implementando esta forma de NAT se genera automáticamente un firewall entre la red pública y la privada, ya que sólo se permite la conexión que se origina desde ésta última.

Sobrecarga

La forma más utilizada de NAT, proviene del NAT dinámico ya que toma múltiples direcciones IP privadas (normalmente entregadas mediante DHCP) y las traduce a una única dirección IP pública utilizando diferentes puertos. Esto se conoce también como **PAT (Port Address Translation - Traducción de Direcciones por Puerto)**, NAT de única dirección o NAT multiplexado a nivel de puerto. Otra denominación es Network Address Port Translation (NAPT).


192.168.0.15
192.168.0.16
src:192.168.0.15
src port 1154
dst:80.0.0.150
dst port:80
192.168.0.1
Fe0/0
Inside
PAT
80.0.0.1
Fe0/1
Outside
192.168.0.17
192.168.0.18
80.0.0.150

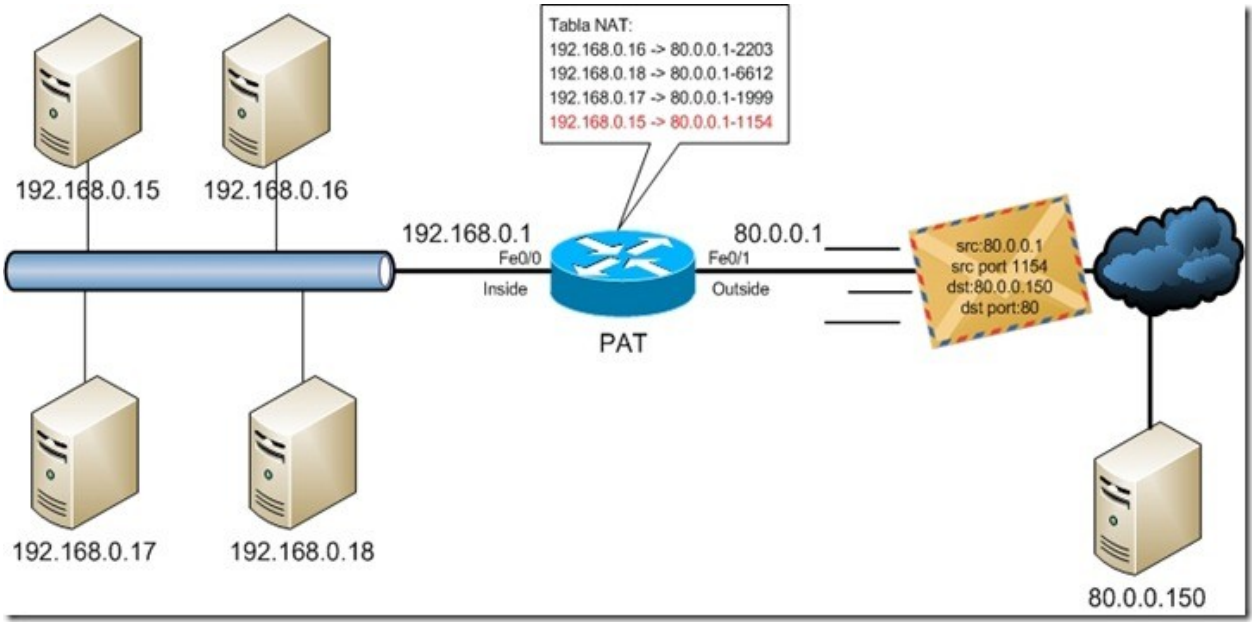


Tabla NAT:
192.168.0.16 -> 80.0.0.1-2203
192.168.0.18 -> 80.0.0.1-6612
192.168.0.17 -> 80.0.0.1-1999
192.168.0.15 -> 80.0.0.1-1154
192.168.0.15
192.168.0.16
192.168.0.1
Fe0/0
Inside
PAT
80.0.0.1
Fe0/1
Outside
src:80.0.0.1
src port 1154
dst:80.0.0.150
dst port:80
192.168.0.17
192.168.0.18
80.0.0.150

11.4 Herramientas

11.4.1 netstat

Es una herramienta que se ejecuta en modo terminal y que permite ver **los puertos que nuestro equipo tiene abiertos**.

Está disponible tanto en Windows como en Linux. A menudo se utiliza con opciones, de las cuales las más frecuentes son:

```
-a:  Muestra todas las conexiones
-n:  Muestra números de puerto
-p:  Muestra programa o aplicación que está usando el puerto
-t:  Puertos TCP (sólo Linux)
-u:  Puertos UDP(sólo Linux)
-l:  Sólo puertos en modo escucha.
```

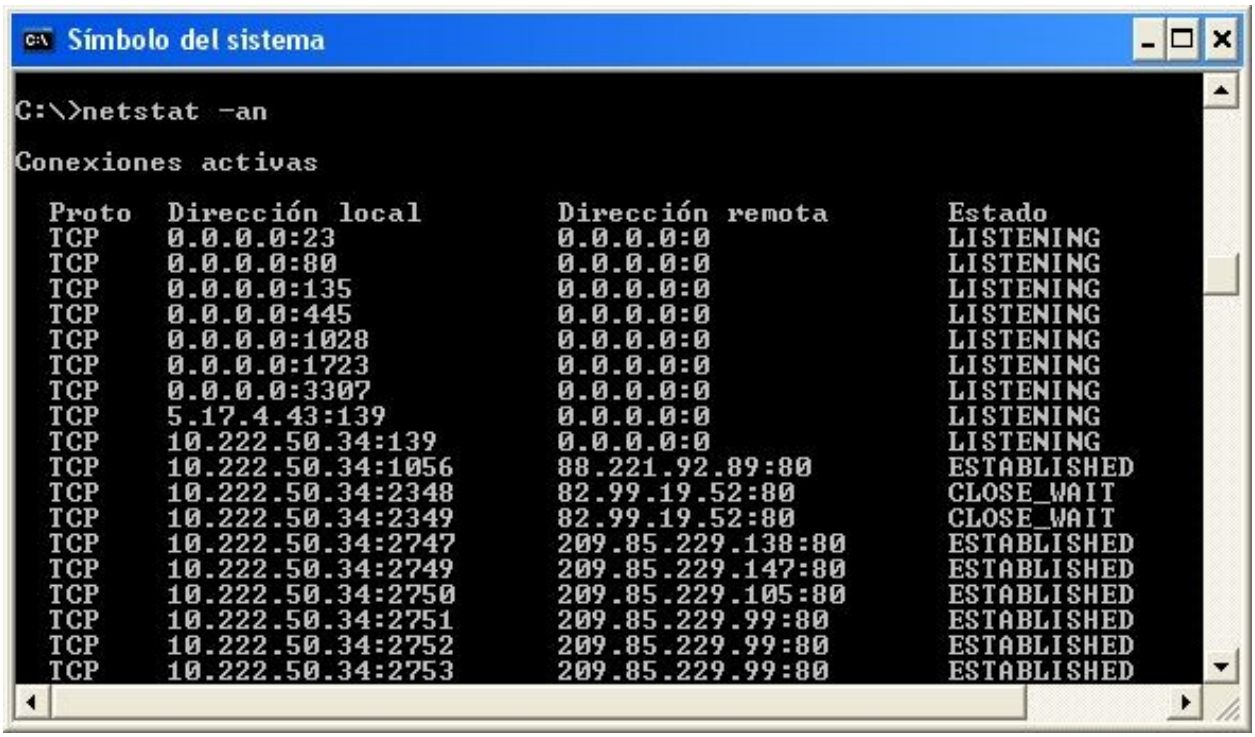


Figura 6: Windows: netstat -na

11.4.2 nmap

Es una herramienta que se ejecuta en modo terminal y que permite ver **los puertos que otro equipo tiene abiertos**. Es una herramienta disponible para Windows y Linux, aunque no viene instalada por defecto. Es necesario instalarla.

Nmap es extremadamente potente y dispone de numerosas opciones para realizar distintos tipos de sondeos o escaneos. Dichas opciones pueden consultarse en la página de manual propia.

Existe un front-end gráfico conocido como **zenmap**.

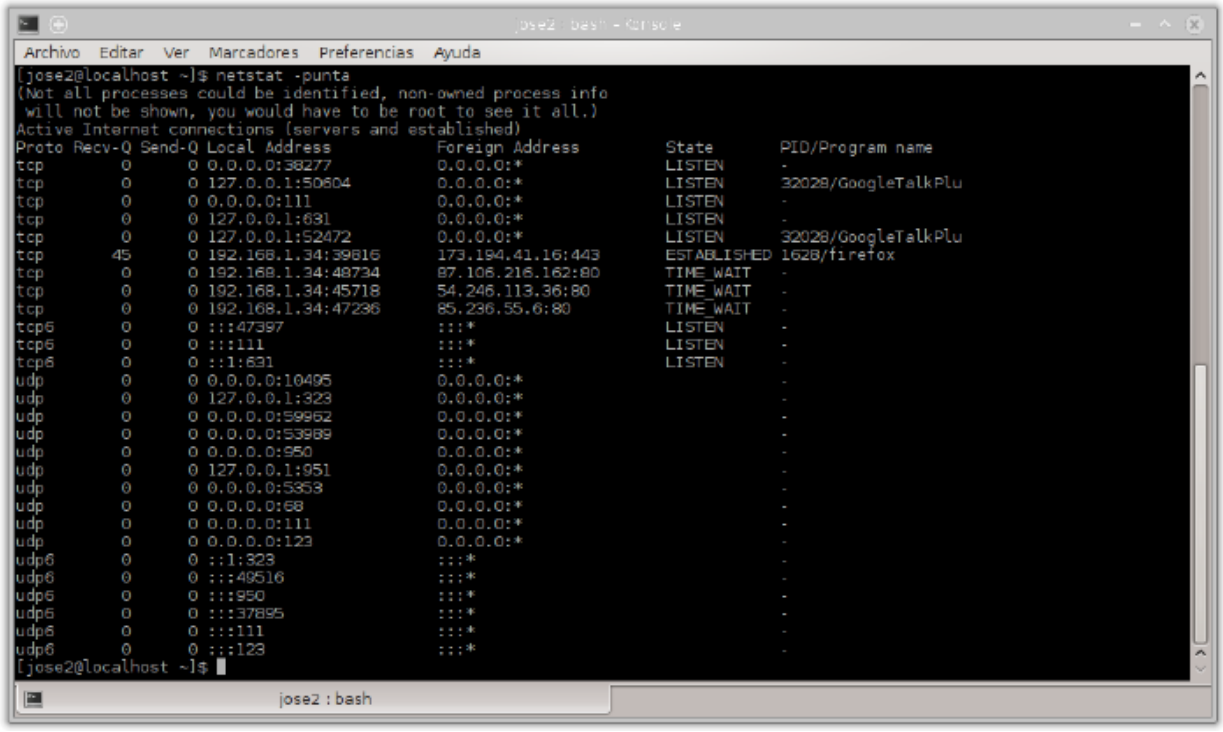


Figura 7: Linux: netstat -punta

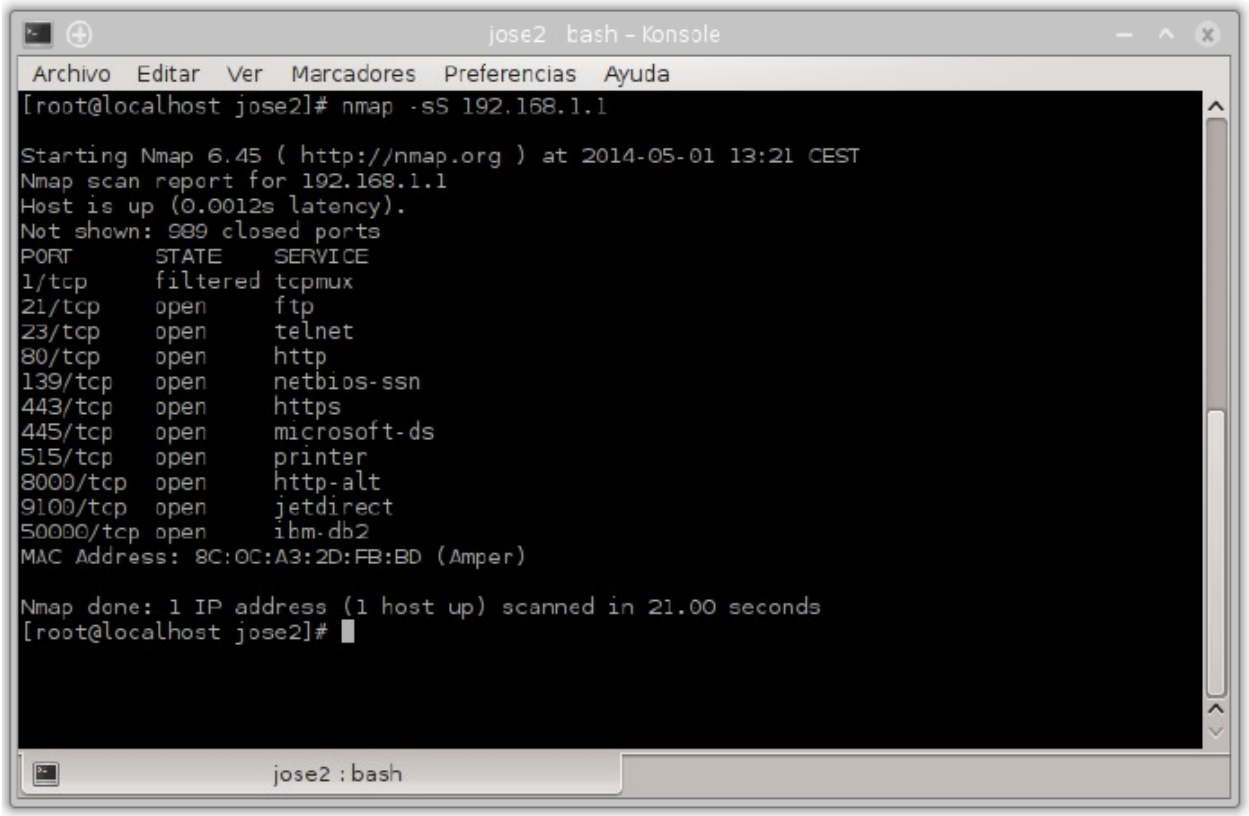


Figura 8: Sondeo de puertos abiertos en 192.168.1.1

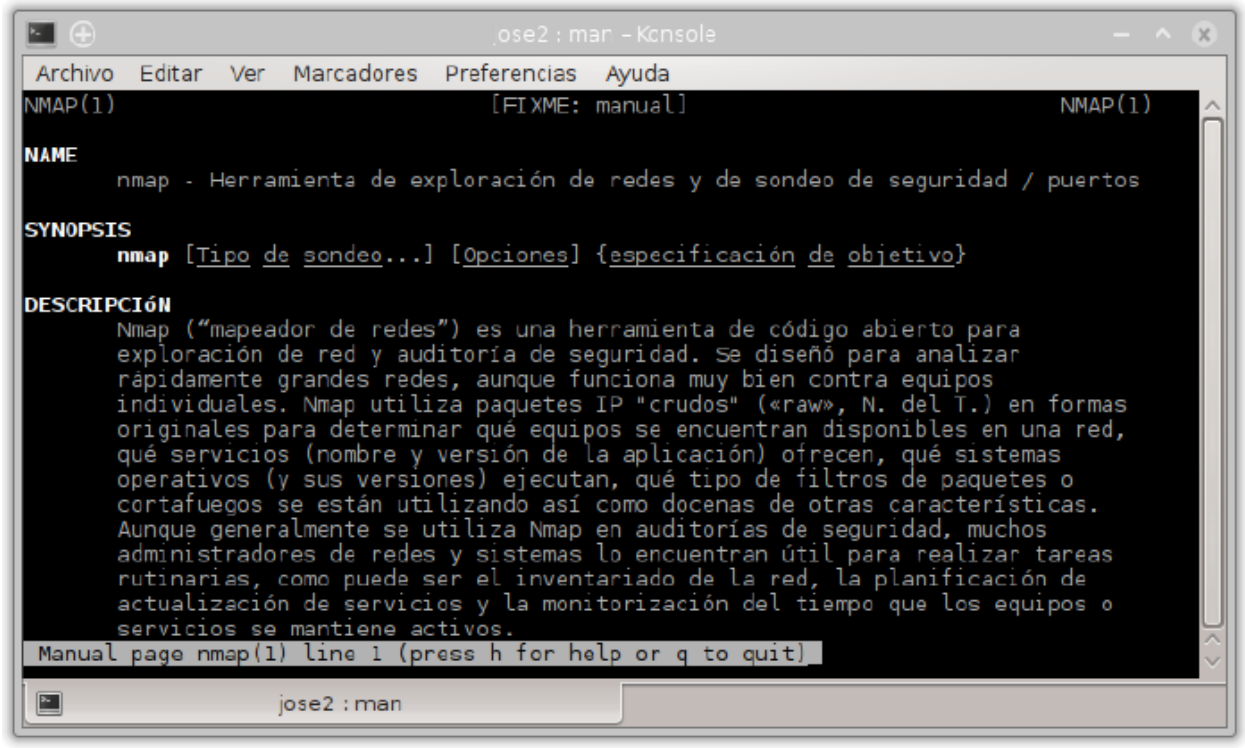


Figura 9: Ayuda de nmap en Linux: man nmap

11.4.3 Cortafuegos

Un cortafuegos (**firewall** en inglés) es una parte de un sistema o una red que está diseñada para **bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas**.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Existen 2 tipos de cortafuegos:

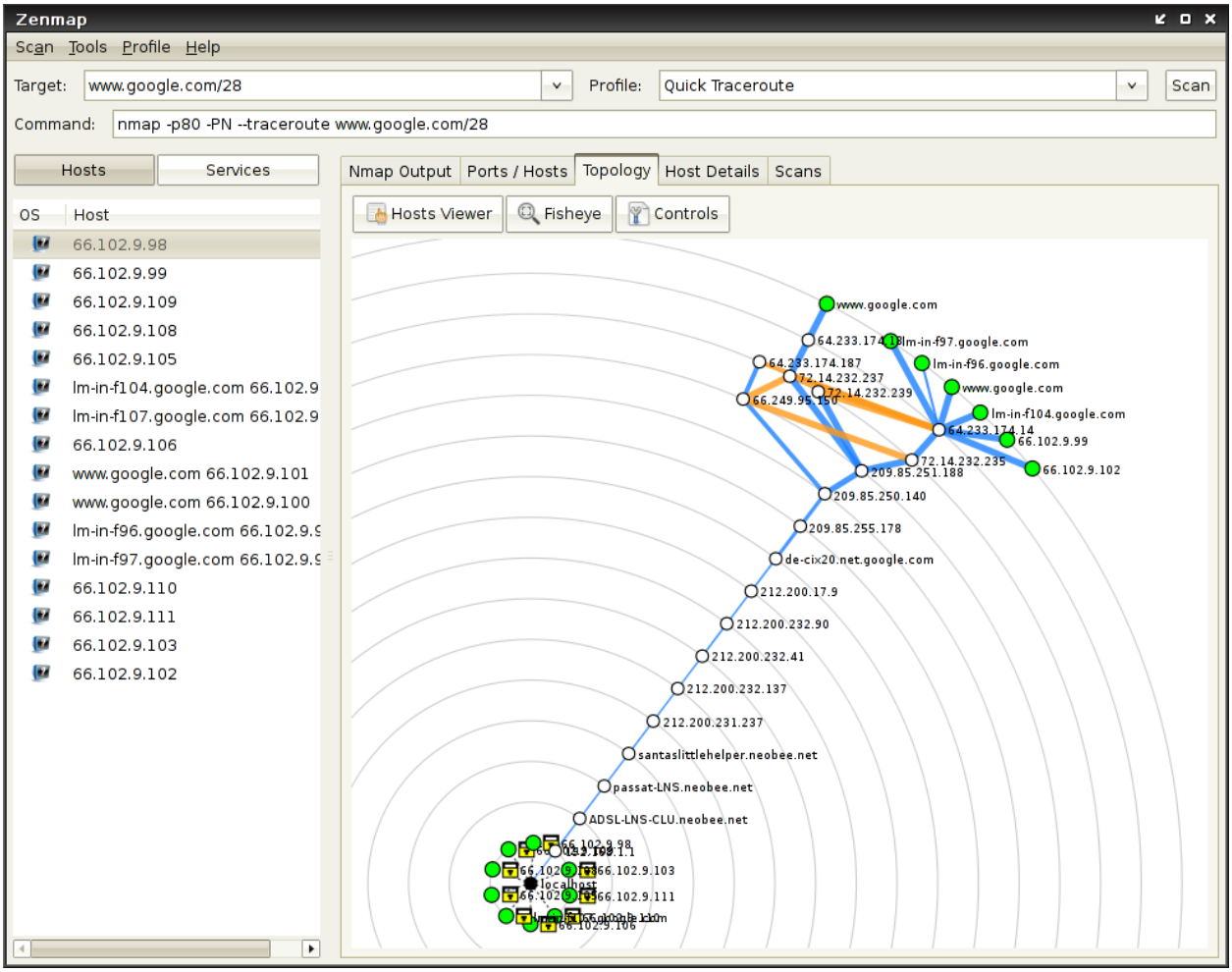
- **Personales**
- **De red**

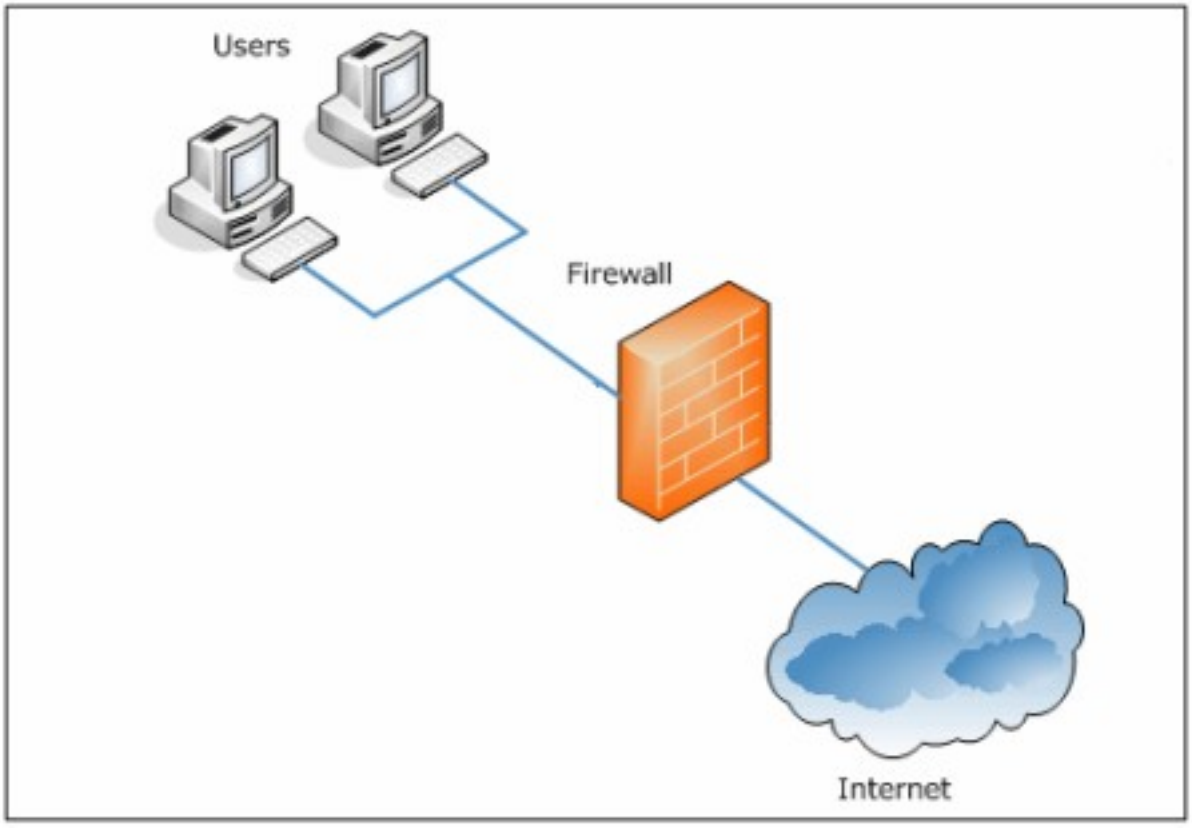
Los cortafuegos personales son los que el usuario final instala en su equipo con el fin de proteger dicho equipo.

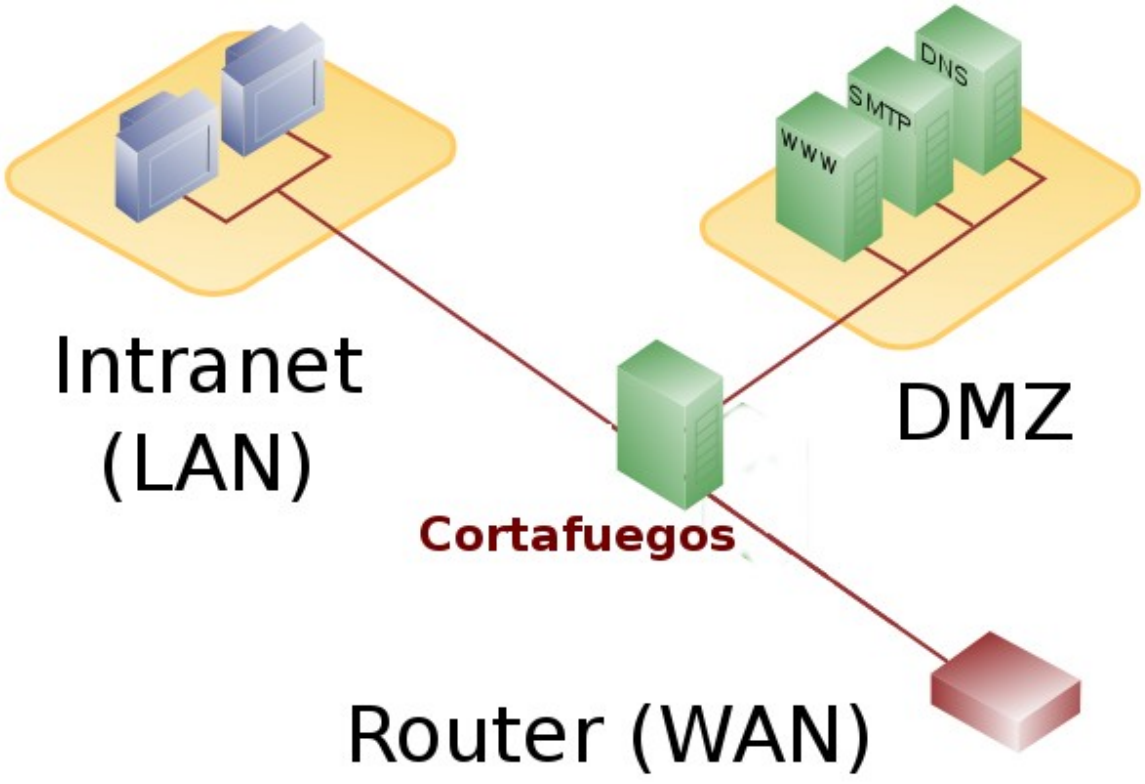
Los cortafuegos de red son los que se instalan en una Intranet con el fin de proteger todos los equipos que se hallen detrás de él. Una variante de los cortafuegos de red son los cortafuegos de nivel de aplicación de tráfico HTTP, que suelen conocerse mayormente como **proxy** o **proxy-caché** (si este dispone de cacheo de páginas web), y permite que los ordenadores de una organización entren a Internet de una forma controlada.

De ahora en adelante nos ocuparemos de los cortafuegos de red.

Los cortafuegos **pueden ser implementados en hardware o software, o una combinación de ambos**. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuegos a **una tercera red, llamada «zona desmilitarizada» o DMZ**, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.


Zenmap
Scan Tools Profile Help
Target: www.google.com/28
Profile: Quick Traceroute
Scan
Command: nmap -p80 -PN --traceroute www.google.com/28
Hosts
Services
OS Host
66.102.9.98
66.102.9.99
66.102.9.109
66.102.9.108
66.102.9.105
lm-in-f104.google.com 66.102.9
lm-in-f107.google.com 66.102.9
66.102.9.106
www.google.com 66.102.9.101
www.google.com 66.102.9.100
lm-in-f96.google.com 66.102.9.9
lm-in-f97.google.com 66.102.9.9
66.102.9.110
66.102.9.111
66.102.9.103
66.102.9.102
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
www.google.com
64.233.174.1
lm-in-f97.google.com
64.233.174.187
lm-in-f96.google.com
72.14.232.237
www.google.com
72.14.232.239
66.249.95.150
lm-in-f104.google.com
64.233.174.14
66.102.9.99
72.14.232.235
66.102.9.102
209.85.251.188
209.85.250.140
209.85.255.178
de-cix20.net.google.com
212.200.17.9
212.200.232.90
212.200.232.41
212.200.232.137
212.200.231.237
santaslittlehelper.neobee.net
passat-LNS.neobee.net
ADSL-LNS-CLU.neobee.net
66.102.9.98
66.102.9.103
localhost
66.102.9.111
66.102.9.106


Users
Firewall
Internet


DNS
SMTP
WWW
Intranet
(LAN)
DMZ
Cortafuegos
Router (WAN)

Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

Políticas del cortafuegos

Hay dos políticas básicas en la configuración de un cortafuegos que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

- **Política restrictiva**: Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuegos obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten. Esta aproximación es la que suelen utilizar la empresas y organismos gubernamentales.
- **Política permisiva**: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado. Esta aproximación la suelen utilizar universidades, centros de investigación y servicios públicos de acceso a Internet.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por omisión.

Ejemplos de cortarfuegos para Linux

- **iptables** (su sucesor será nftables)
- IPCop
- Shorewall
- SmoothWall
- UFW – Uncomplicated Firewall

11.4.4 Proxy-caché

El término proxy significa intermediario. Un proxy es un equipo o software intermediario que hace peticiones a distintos servidores en representación del equipo que se halla detrás de proxy haciendo uso de él. Las peticiones más frecuentes son aquellas que se realizan a páginas web aunque pueden ser de otro tipo. Pueden ser peticiones HTTP(páginas web), FTP(transferencia de archivos), DNS(resolución de nombres), ...

Cuando un proxy hace una petición a un servidor aparece como origen de la petición el mismo proxy ocultando de esta forma el equipo que realizó la petición original detrás del proxy.

Los proxies suelen disponer de una memoria denominada caché donde se van almacenando el resultado de todas las peticiones por si en un futuro próximo otro equipo detrás del proxy realizase la misma petición. Esto tiene dos ventajas:

- **Aumenta la velocidad de obtención de respuesta puesto que está almacenada en la caché**.
- **Ahorra ancho de banda puesto que dicha petición no tiene que volver a hacerse al servidor**.

Debido a que la mayoría de los proxies disponen de una caché, el término empleado para referirse a ellos es el de proxy-caché. En algún caso particular un proxy podría no disponer de caché pero, entonces, no dispondría de las ventajas indicadas anteriormente. Soló proporcionaría cierto anonimato al equipo que realiza peticiones detrás del proxy.

Resumiendo, un proxy, o servidor proxy, en una red informática, es un servidor (un programa o sistema informático), que sirve de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C). Por ejemplo, si una hipotética máquina A solicita un recurso a C, lo hará mediante una petición a B, que a su vez trasladará la

petición a C; de esta forma C no sabrá que la petición procedió originalmente de A. Esta situación estratégica de punto intermedio suele ser aprovechada para soportar una serie de funcionalidades: control de acceso, registro del tráfico, prohibir cierto tipo de tráfico, mejorar el rendimiento, mantener el anonimato, proporcionar Caché web, etc; este último sirve para acelerar y mejorar la experiencia del usuario.

Tipos de proxy-caché según localización

- **Proxy local**

  En este caso el que quiere implementar la política es el mismo que hace la petición. Por eso se le llama local. Suelen estar en la misma máquina que el cliente que hace las peticiones. Son muy usados para que el cliente pueda controlar el tráfico y pueda establecer reglas de filtrado que por ejemplo pueden asegurar que no se revela información privada (Proxys de filtrado para mejora de la privacidad).

- **Proxy externo**

  El que quiere implementar la política del proxy es una entidad externa. Por eso se le llama externo. Se suelen usar para implementar cacheos, bloquear contenidos, control del tráfico, compartir IP, etc.

Tipos de proxy según su uso

Los proxies que veremos a continuación son todos ellos externos.

- **Proxy HTTP, FTP, . . .**

  Es el tipo de proxy más conocido. Es utilizado ampliamente como intermediario y memoria caché entre una red local e Internet. El tipo de tráfico cacheado principalmente es HTTP y FTP. A menudo se le añade un filtro de contenido con listas negras para bloqueo de determinados sitios. Puede además estar complementado con algún tipo de antivirus que comprobará todo el tráfico destinado a los equipos de la red local, con lo cual, en principio, no sería necesario de disponer de antivirus en cada PC de red, aunque si aconsejable.

  Un software muy popular para proxy-caché http es **Squid**.

- **Caché DNS**

  Un servidor de nombres (DNS) en nuestra red local no tiene porque tener configurado un dominio. La configuración más simple es aquella en la cual únicamente actúa como caché DNS (el término proxy no se suele utilizar en este caso). Una caché DNS permite a un navegador web adquirir información de DNS de dicha caché, siempre que esta información se haya almacenado en caché peticiones anteriores, sin la necesidad de acceder a los servidores DNS públicos, lo que resulta en la navegación web más rápida.

  El software más utilizado tanto de servidor DNS como caché DNS es **Bind**. Un software más ligero es **dnsmasq**.

- **Proxy inverso**

  Un servidor proxy inverso es un dispositivo de seguridad que suele desplegarse en la DMZ de una red para proteger a los servidores HTTP de una intranet corporativa, realizando funciones de seguridad que protegen a los servidores internos de ataques de usuarios en Internet.

  El servidor proxy inverso protege a los servidores HTTP internos proporcionando un punto de acceso único a la red interna.

  El administrador puede utilizar las características de autenticación y control de acceso del servidor proxy inverso para controlar quién puede acceder a los servidores internos y controlar a qué servidores puede acceder cada usuario individual.

  Todo el tráfico hacia los servidores de la intranet parece dirigido a una única dirección de red (la dirección del servidor proxy inverso).

El administrador realiza configuraciones de correlación de URL en el servidor proxy inverso que hace esta redirección posible. Todo el tráfico enviado a los usuarios de Internet desde los servidores internos parece proceder de una única dirección de red.

Finalmente, con algoritmos perfeccionados, el proxy inverso puede distribuir la carga de trabajo mediante la redirección de las solicitudes a otros servidores similares. Este proceso se denomina balanceo de carga. Un software muy utilizado para esto es **HAProxy**.

- **Proxy web**

  Los proxy web se utilizan para navegación anónima.

  Los equipos de una red local que disponga de un proxy-caché y filtro de contenido, pueden saltárselo mediante el uso de un proxy web. Este último, normalmente funciona sobre HTTPS puesto que dicho tipo de tráfico no es "cacheable" por el proxy de la red local. El administrador del proxy-caché de la red local, a menudo, no puede bloquear el tráfico HTTPS puesto que muchas webs (de correo, compras, administración pública, bancos, ...) utilizan dicho protocolo. La solución es elaborar una lista negra con los proxies web más conocidos y activarla en el filtro de contenido.

11.4.5 Cortafuegos y Proxy-caché en un sólo equipo

Proxies transparentes

Muchas organizaciones (incluyendo empresas, colegios y familias) usan los proxies para reforzar las políticas de uso de la red o para proporcionar seguridad y servicios de caché. Normalmente, un proxy Web o NAT no es transparente a la aplicación cliente: debe ser configurada para usar el proxy, manualmente. Por lo tanto, el usuario puede evadir el proxy cambiando simplemente la configuración.

Un proxy transparente combina un servidor proxy con un cortafuegos de manera que las conexiones son interceptadas y desviadas hacia el proxy sin necesidad de configuración en el cliente, y habitualmente sin que el propio usuario conozca de su existencia.

Además, suele ser frecuente en el proxy-caché la instalación de un servicio de control de acceso a la web y algún antivirus de red. El control de acceso a la web normalmente se implementa mediante algún tipo de software de **filtrado por contenido** (además de URL e IP, puede bloquear accesos a páginas web según el contenido de estás (palabras desagradables, obscenas o similares e incluso por imágenes -aunque esté último método suele dar peores resultados-). Un software libre muy utilizado para ello es **Dansguardian** y sus listas negras asociadas.

A continuación se muestra un ejemplo de script Linux para cortafuegos con reglas activadas para habilitar un proxy-transparente. Básicamente lo que hace es dirigir todas las petición a puertos destino 80 (web), 3128 (cliente despistado con configuración manual de proxy) y algunos otros puertos que nos interesen al puerto 8080 (dansguardian) donde tenemos el filtro de contenido.

```
#!/bin/sh
### BEGIN INIT INFO
# Provides:          cortafuegos
# Required-Start:    balanceo-de-carga
# Required-Stop:
# Should-Start:
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: Cortafuegos para IES Guadalpeña - Dpto. Informática
# Description:       Cortafuegos contiene las reglas de iptables que se aplicarán
#                    después de la configuración del soporte de red o networking
#                    y del balanceo de carga (si está habilitado).
#                    Proporciona redirección de puertos en el canal PREROUTING
#                    para dar soporte a un proxy transparente.
```

(continues on next page)

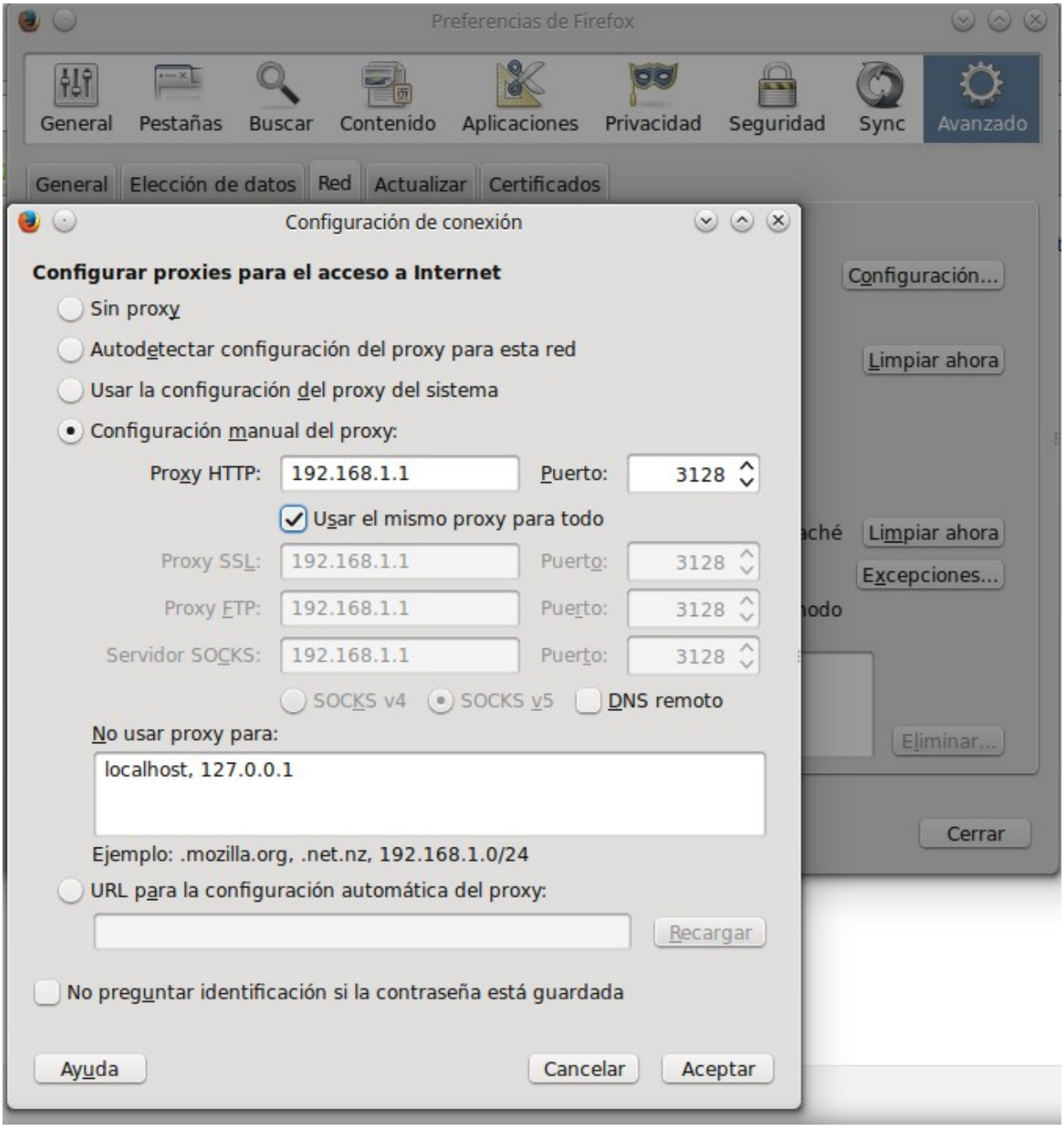


Figura 10: Configuración de proxy en Firefox

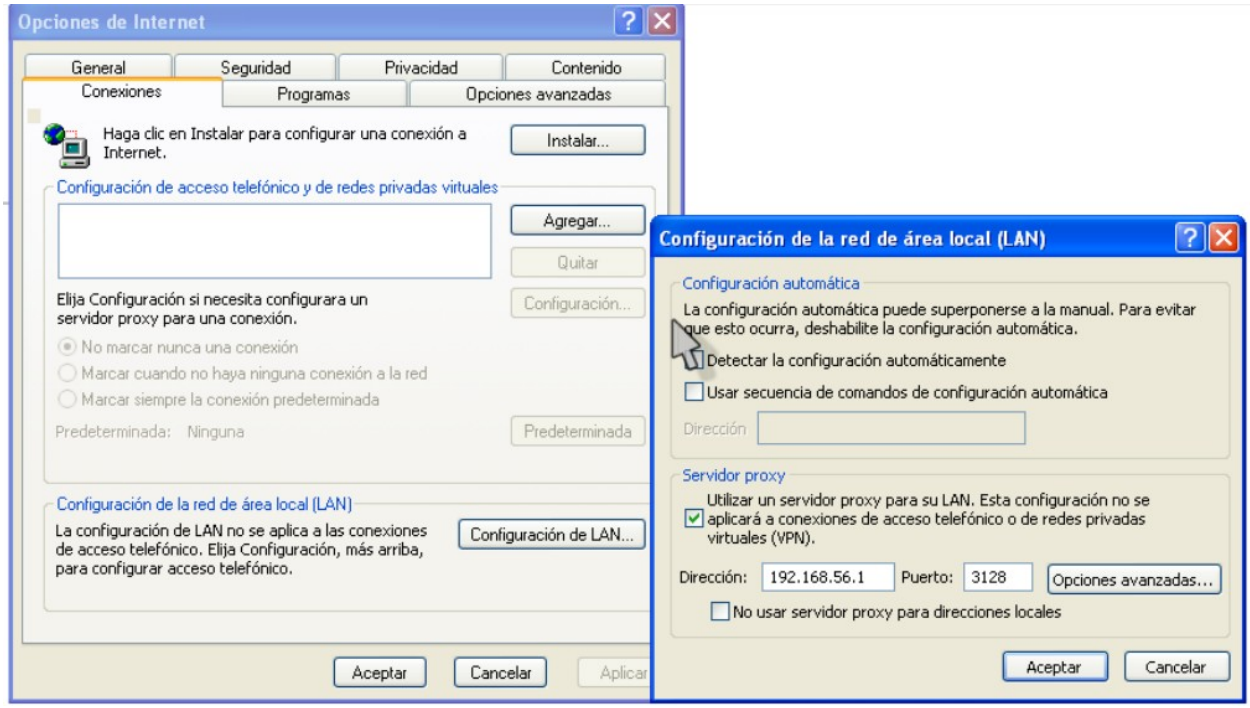


Figura 11: Configuración de proxy en Internet Explorer

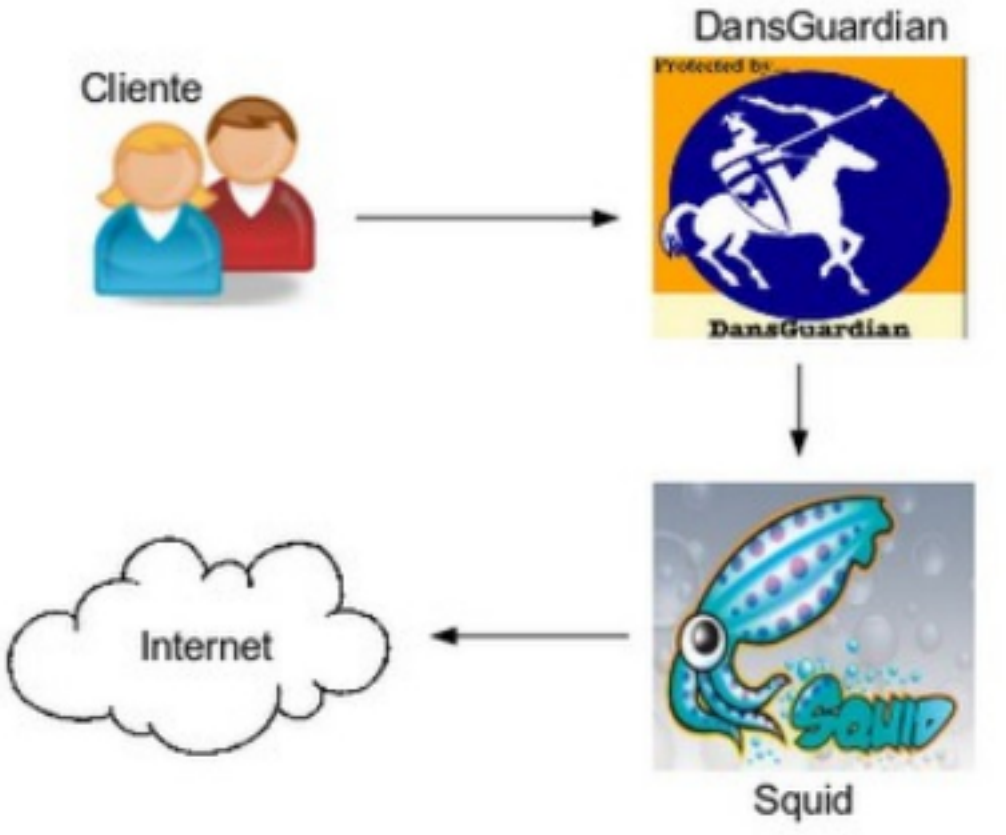


Figura 12: Squid + Dansguardian.png

(proviene de la página anterior)

```
### END INIT INFO


# Variables generales
PATH=/sbin:/usr/sbin:/bin:/usr/bin
NAME=cortafuegos
PIDFILE=/var/run/$NAME.pid

# Variables de red
IF_ADSL1="p1p1"             # Interface conectada a ADSL1
IF_ADSL2="p4p1"             # Interface conectada a ADSL2
IF_LOCAL="p2p1"             # Interface conectada a la LAN
IP_ADSL1="192.168.1.2"      # IP de la IF_ADSL1
IP_ADSL2="192.168.2.2"      # IP de la IF_ADLS2
IP_LOCAL="10.0.0.1"         # IP de la IF_LOCAL, Gateway Local
NET_ADSL1="192.168.1.0/24" # Red para IF_ADSL1
NET_ADSL2="192.168.2.0/24" # Red para IF_ADLS2
NET_LOCAL="10.0.0.0/8"      # Red para IF_LOCAL
GW_ADSL1="192.168.1.1"      # Gateway para ADSL1
GW_ADSL2="192.168.2.1"      # Gateway para ADSL2


###### START
do_start () {
  # Reglas de iptables
  echo "Limpiando Reglas Anteriores..."
  iptables -F
  iptables -X
  iptables -Z
  iptables -t nat -F
  iptables -t mangle -F

  # Ahora hago el NAT
  echo "Activando NAT ..."
  echo 1 > /proc/sys/net/ipv4/ip_forward
  # iptables -t nat -A POSTROUTING -s ${NET_LOCAL} -o ${IF_ADSL1} -j MASQUERADE
  # iptables -t nat -A POSTROUTING -s ${NET_LOCAL} -o ${IF_ADSL2} -j MASQUERADE
  iptables -t nat -A POSTROUTING -o ${IF_ADSL1} -j SNAT --to-source ${IP_ADSL1}
  iptables -t nat -A POSTROUTING -o ${IF_ADSL2} -j SNAT --to-source ${IP_ADSL2}

  # Redirecciono al Proxy
  echo "Creando reglas para proxy transparente..."
  iptables -t nat -A PREROUTING -i ${IF_LOCAL} -p tcp --dport http      -j DNAT --to $
↪{IP_LOCAL}":8080"
  iptables -t nat -A PREROUTING -i ${IF_LOCAL} -p tcp --dport 81        -j DNAT --to $
↪{IP_LOCAL}":8080"
  iptables -t nat -A PREROUTING -i ${IF_LOCAL} -p tcp --dport 8080:8099 -j DNAT --to $
↪{IP_LOCAL}":8080"
  iptables -t nat -A PREROUTING -i ${IF_LOCAL} -p tcp --dport 3128:3130 -j DNAT --to $
↪{IP_LOCAL}":8080"

  #echo "Reglas Aplicadas"
}


###### STATUS
do_status () {
```

(continues on next page)

(proviene de la página anterior)

```
  echo "Listado de Reglas activas"
  iptables -L -n -v
  iptables -t nat -L -n -v
  iptables -t mangle -L -n -v
}


###### STOP
do_stop () {
  echo "Limpiando Reglas anteriores..."
  iptables -F
  iptables -X
  iptables -Z
  iptables -t nat -F
  iptables -t mangle -F
}


case "$1" in
  start|"")
        do_start
        ;;
  restart)
        do_stop
        do_start
        ;;
  reload|force-reload)
        echo "Error: el argumento '$1' no está soportado" >&2
        exit 3
        ;;
  stop)
        do_stop
        ;;
  status)
        do_status
        ;;
  *)
        echo "Uso: cortafuegos [start|stop|restart|status]" >&2
        exit 3
        ;;
esac
:
```

11.4.6 Balanceadores de carga de red

En informática, el balanceo de carga distribuye las cargas de trabajo a través de múltiples recursos informáticos, como procesadores (balanceo de cómputo), enlaces de red (balanceo de red), ordenadores, cluster de ordenadores o unidades de disco. El balanceo de carga tiene como objetivo optimizar el uso de recursos, maximizar el rendimiento, minimizar el tiempo de respuesta y evitar la sobrecarga de cualquier recurso individual. El uso de varios componentes con el equilibrio de carga en lugar de un solo componente puede aumentar la confiabilidad mediante redundancia. El equilibrio de carga por lo general implica software o hardware dedicado, tal como un switch multicapa o un proceso DNS .

El balanceo de carga difiere del channel bonding en que el primero se realiza en la capa 4 del modelo OSI, mientras que el channel bonding hace la división del tráfico en un nivel inferior, ya en la capa 3 del modelo OSI o en el enlace

de datos capa 2 del modelo OSI).

Existen distintos tipos de balanceo de carga según el elemento equilibrado siendo los más frecuentes:

- Balanceo de carga entre procesadores (Operaciones de cómputo)
- Balanceo de carga entre líneas de red (Tráfico de red)

Aquí se tratará el balanceo de carga de red y en concreto los dos tipos existentes:

- Balanceo de carga en el lado cliente
- Balanceo de carga en el lado servidor

Balanceo en el lado cliente (Multihoming)

El Multihoming (comúnmente conocido como ruta de doble WAN) es la capacidad de equilibrar el tráfico a través de dos o más enlaces WAN sin necesidad de utilizar protocolos de enrutamiento complejos como BGP.

Esta técnica equilibra sesiones de red como web, correo electrónico, etc a través de múltiples conexiones con el fin de extender la cantidad de ancho de banda utilizado por los usuarios de la LAN, lo que aumenta la cantidad total de ancho de banda disponible. Por ejemplo, un usuario tiene una única conexión a la WAN a 10 Mbit/s. Desea añadir una segunda línea de banda ancha (cable, DSL, inalámbrico, etc.) a 20 Mbit/s. Esto les proporcionará un total de 30 Mbits/s de ancho de banda para balancear sesiones.

El balanceo de sesión no sólo eso, equilibra sesiones a través de cada enlace WAN. Cuando los navegadores Web se conectan a Internet, que comúnmente se abren varias sesiones, una para el texto, otra para una imagen, otro por alguna otra imagen, etc. Cada una de estas sesiones pueden ser equilibradas a través de las conexiones disponibles. Una aplicación FTP sólo utiliza una sola sesión por lo que no está equilibrada; sin embargo, si se realiza una conexión FTP secundaria, entonces puede ser equilibrada por lo que, en conjunto, el tráfico se distribuye uniformemente a través de las diversas conexiones y por lo tanto proporciona un aumento global en el rendimiento.

A continuación se muestra un esquema de red donde se puede realizar “balanceo de carga” con 2 líneas de salida a internet.

Balanceo de carga en el lado servidor

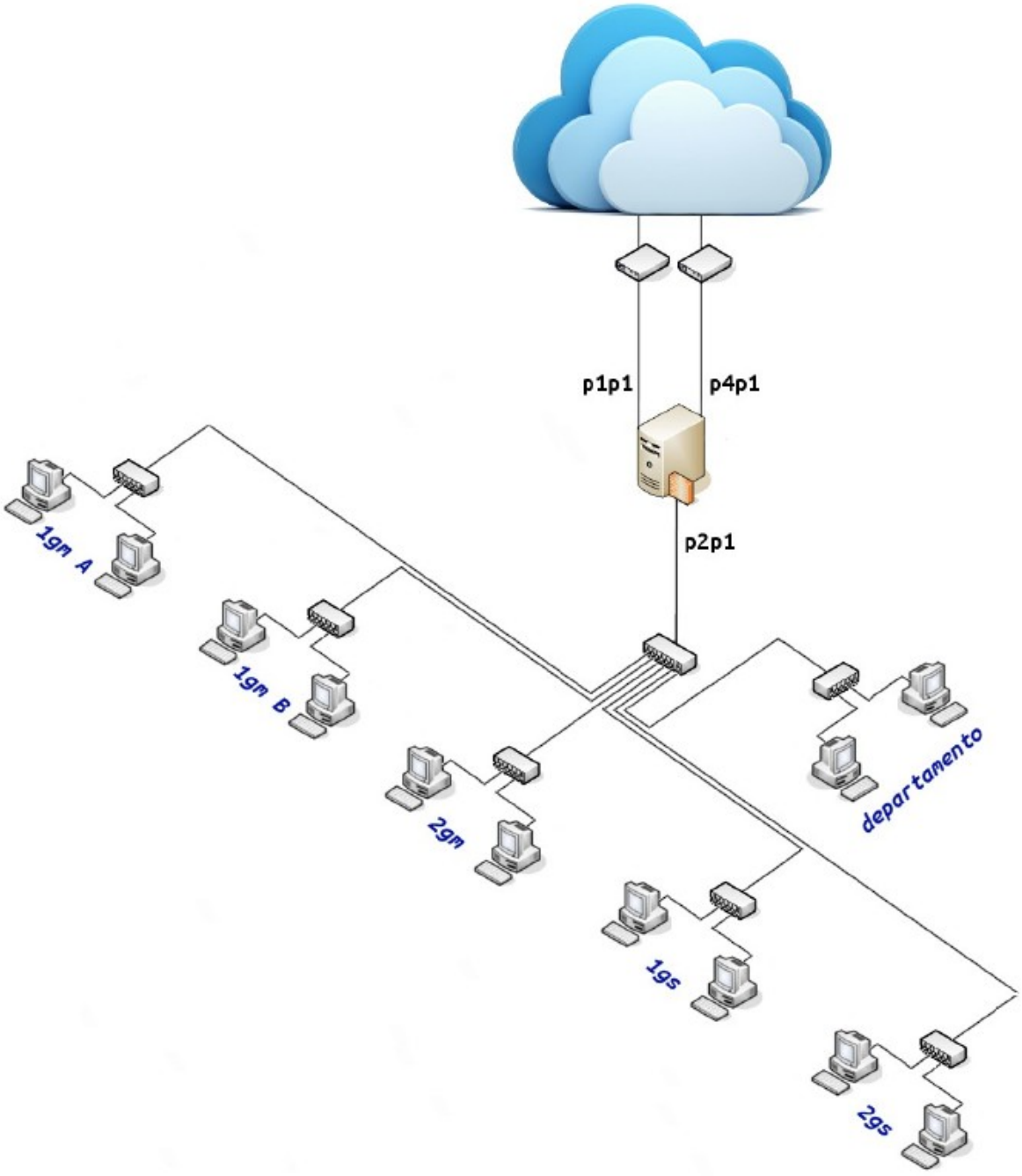
El problema a solucionar es la sobrecarga de los servidores. Se puede balancear cualquier protocolo, pero dado que este sitio se centra en las tecnologías web, el artículo trata exclusivamente de **balancear servidores HTTP**.

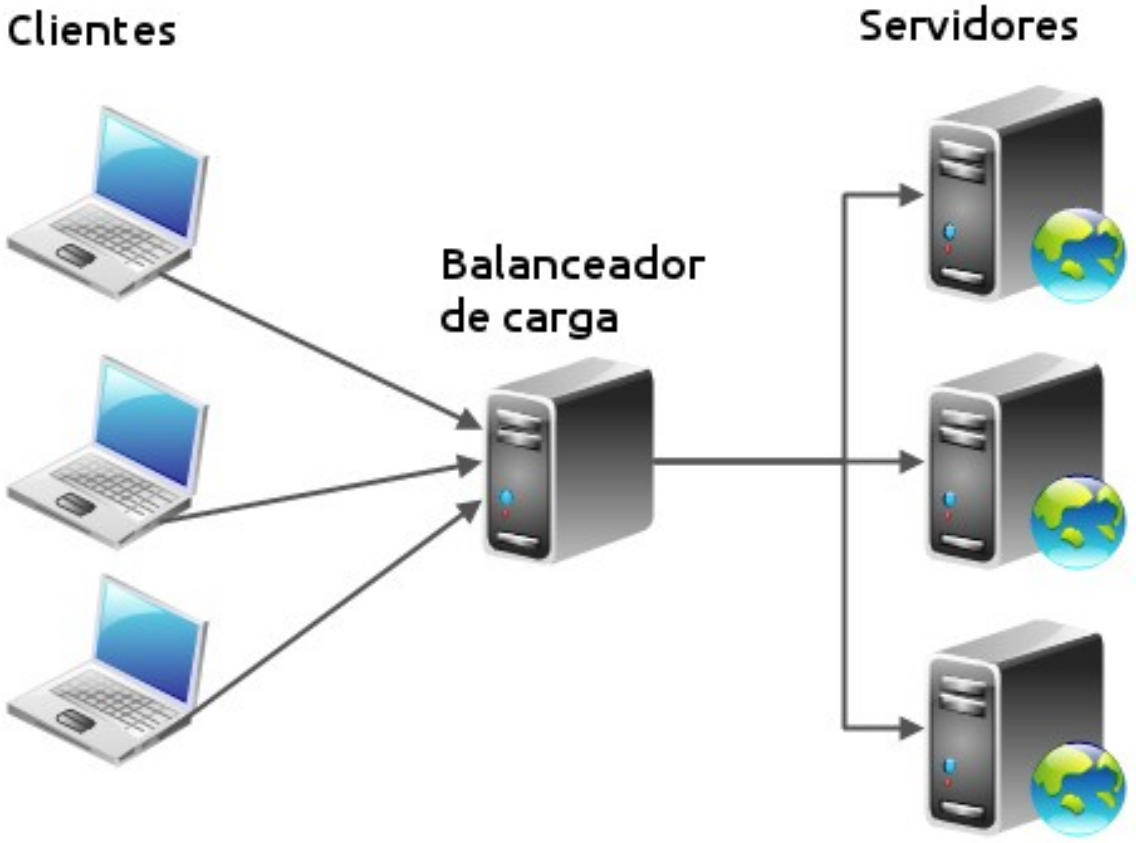
Al mismo tiempo, si el balanceador detecta la caída de uno de los servidores web, puede optar por no enviarle más peticiones. De esta forma, si uno de los servidores web se cae, las peticiones del cliente no se dirigen al servidor caído.

Vemos que el balance de carga también contribuye a una infraestructura redundante y de alta disponibilidad (aunque no la asegura, el balance de carga por sí mismo no alcanza para tener HA1). En este punto creo conveniente introducir los conceptos básicos que se manejarán a lo largo del artículo:

- **Balanceador**: es un sistema, software o hardware, que distribuye las peticiones de los clientes de forma equitativa entre distintos servidores de “backend”.
- **Servidor de backend**: es un servidor (web en este caso), que responde la petición del usuario.

Así el balanceador distribuye las peticiones y son los servidores de backend, quienes arman la respuesta efectiva al cliente. Para balancear la carga entre varios servidores es deseable que el mismo balanceador sea justo (fair), y que detecte servidores sobrecargados para dejar de enviarle peticiones hasta que no baje su carga. Este mismo mecanismo sirve para que un balanceador no envíe peticiones a un servidor caído.


p1p1
p4p1
p2p1
1gm A
1gm B
2gm
1gs
2gs
departamento


Clientes
Servidores
Balanceador
de carga

Balanceo mediante DNS

La forma más elemental de balancear la carga entre varios servidores esa utilizando el DNS. Por ejemplo, buscando la IP de **yahoo.com** con el comando dig he obtenido el siguiente resultado. En este caso responden 3 servidores: 206.190.36.45, 98.139.183.24 y 98.138.253.109.

```
jose@portatil:~ > dig yahoo.com

; <<>> DiG 9.9.5-3ubuntu0.2-Ubuntu <<>> yahoo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7865
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;yahoo.com.                     IN      A

;; ANSWER SECTION:
yahoo.com.              289     IN      A       206.190.36.45
yahoo.com.              289     IN      A       98.139.183.24
yahoo.com.              289     IN      A       98.138.253.109

;; Query time: 81 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Sat Apr 18 13:45:30 CEST 2015
;; MSG SIZE  rcvd: 86
```

Figura 13: Balanceo mediante DNS

Este es el tipo de balanceo más elemental que se puede hacer, y tiene una ventaja muy importante: **simplicidad y eficiencia**; ya que en principio lo único que se necesitan son varios servidores con distintas IPs, por lo que es barato, simple y fácil de mantener. Sin embargo, el balance de carga por DNS tiene algunos inconvenientes:

- El balanceo mediante DNS no tiene en cuenta la carga de cada servidor.
- El balanceo mediante DNS no detecta si un servidor ha caído.

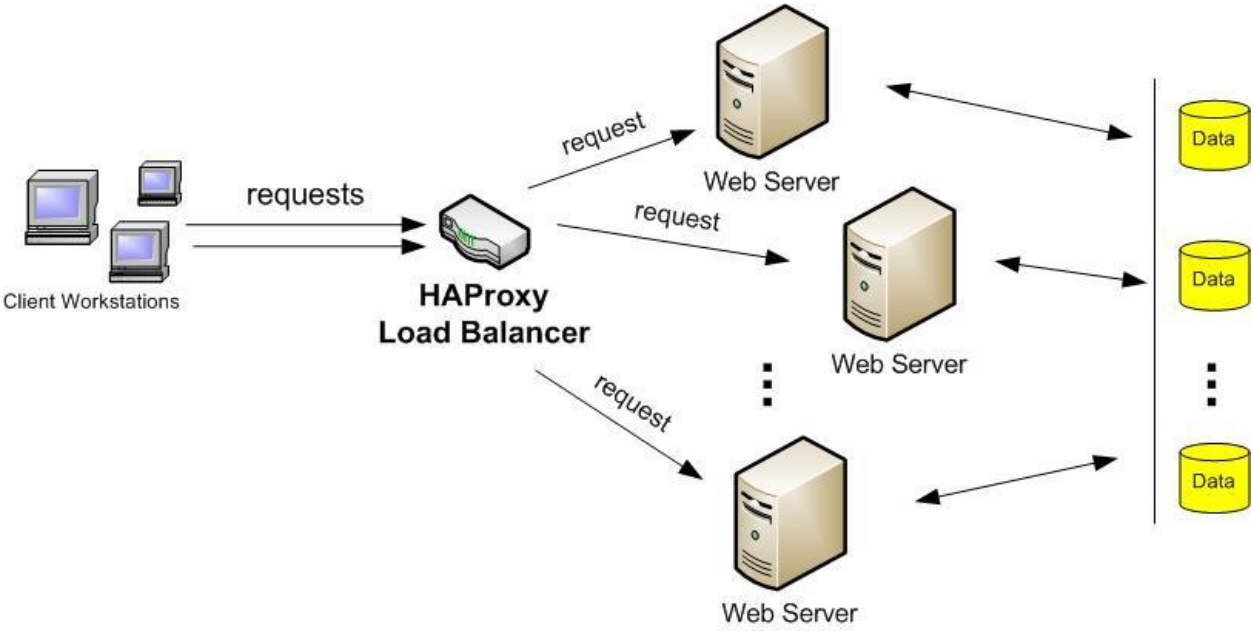
Balanceo mediante balanceador

Una solución menos simple pero más adecuada es utilizar un hardware o software balanceador de carga. Debemos tener en cuenta que un balanceador de este tipo es por definición un proxy inverso. Actualmente un software muy utilizado es HAProxy.

Los balanceadores de carga tienen varias ventajas sobre el balanceado mediante DNS:

- Un balanceador puede tener en cuenta la carga de cada equipo y distribuir las peticiones según esas cargas.
- Si un servidor queda fuera de línea, el balanceador de carga lo detecta y redirige las peticiones web a los otros servidores..

- Por último, la mayoría de los balanceadores pueden mantener las sesiones de los usuarios, de forma que un usuario que inicia sesión en el servidor "**A**" siempre sea dirigido por el balanceador al mismo servidor "**A**" (de no hacerlo el usuario perdería la sesión). Sin embargo, el balance de carga por DNS es del tipo "**Round Robin**", por lo que es casi seguro que el usuario pierda la sesión.



11.4.7 VPN

Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

El protocolo estándar de facto es el **IPSEC**, pero también están PPTP, L2F, L2TP, **SSL/TLS**, SSH, etc. Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados.

Aplicaciones software muy conocidas son **Hamachi** para uso doméstico y **OpenVPN** para uso en empresas.

Básicamente existen 2 tipos de conexión VPN:

- **VPN de acceso remoto**

  Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

- **VPN punto a punto**

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.

Tunneling

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU (unidades de datos de protocolo) determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

11.5 Referencias

- RFC 2663
- Listados de puertos más frecuentemente usados
- Explicación de la técnica NAT
- Explicación de todos los tipos de NAT (en inglés)
- Forwardind o Redirección de puertos
- Manual práctico de IPTABLES
- Documentación de IPROUTE2
- Balanceo de carga en el lado cliente con iptables e iproute2
- Instalación y configuración básica de HAProxy
- HAproxy configuration and Load balancing Part 1
- HAproxy configuration and Load balancing Part 2

11.6 Actividades

1. En términos informáticos, referido a redes, ¿qué es un puerto?
2. Atendiendo al número de puerto, ¿cómo se clasifican?
3. ¿Qué número de puerto y tipo (TCP, UDP) utilizan los siguientes servidores?

- HTTP
- HTTPS
- DHCP
- DNS

- SSH
- FTP
- SMB (Compartición de archivos e impresoras)
- MySQL
- NTP (Tiempo de red)
- BitTorrent
- POP3 (Recepción de correo)
- IMAP4 (Recepción de correo)
- SMTP (Envío de correo)

4. ¿Cuáles son los principales protocolos de la capa de transporte?
5. Características de UDP.
6. Características de TCP.
7. Campos de un segmento TCP. Bits SYN, ACK y FIN.
8. Cuando abrimos un puerto, ¿qué es una apertura pasiva y qué es una apertura activa?
9. Proceso de inicio de una conexión TCP.
10. Proceso de cierre de una conexión TCP.
11. Cuando se utiliza traducción de direcciones, la traducción de la dirección IP origen se denomina _____
12. Cuando se utiliza traducción de direcciones, la traducción estática de direcciones se denomina _____
13. Cuando se utiliza traducción de direcciones, la traducción de la dirección IP destino se denomina _____
14. Cuando se utiliza traducción de direcciones, la traducción dinámica de direcciones se denomina _____
15. Si tenemos un router NAT, ¿es posible iniciar una conexión desde Internet a nuestra Intranet a través de él? ¿Por qué? En el caso de que no sea posible, ¿qué debemos hacer para que lo sea?
16. Tipos de cortafuegos dependiendo del lugar de la red donde se colocan.
17. Tipos de políticas de los cortafuegos.
18. ¿Qué es el SNAT? ¿Y el enmascaramiento?
19. ¿Qué es el DNAT? Explica cada uno de los siguientes tipos de DNAT:

1. Port forwarding (redirección de puertos)
2. Balanceo de carga
3. Proxy transparente

IPTABLES

Uso de iptables

```
iptables -t TABLA -L                        # Listado de reglas
iptables -t TABLA -F                        # Flush de reglas (borrado total)

iptables -t TABLA -P CANAL ACCEPT           # Política por defecto permisiva
iptables -t TABLA -P CANAL DROP             # Política por defecto restrictiva

iptables -t TABLA -A CANAL REGLA            # Añadir regla
iptables -t TABLA -D CANAL REGLA            # Borrar regla
```

TABLAS	CANALES o CADENAS
filter	INPUT, FORWARD, OUTPUT
nat	PREROUTING, POSTROUTING
mangle	

.

REGLAS	SIGNIFICADO
-s IP	Dirección IP origen
-d IP	Dirección IP destino
-i INTERFAZ	Tarjeta de red de entrada. Input
-o INTERFAZ	Tarjeta de red de salida. Output
-p PROTOCOLO	Protocolo (tcp, udp, icmp, . . .)
–sport PUERTO	Puerto de origen. Source port
–dport PUERTO	Puerto de destino. Dest. port
-j ACCEPT	Aceptar paquetes
-j DROP	Ignorar paquetes

Nota: Deberemos sustituir las palabras *TABLA*, *CANAL*, *REGLA*, *IP*, *INTERFAZ*, *PROTOCOLO* y *PUERTO* por los valores adecuados.

EJEMPLOS DE REGLAS:

Aceptamos paquetes TCP al puerto 80 desde cualquier IP

```
iptables -t filter -A INPUT -s 0.0.0.0/0 -p tcp --dport 80 -j ACCEPT
```

Bloqueamos paquetes al servidor MySQL

```
iptables -t filter -A INPUT -p tcp --dport 3306 -j DROP
```

Permitimos salida a peticiones HTTPS

```
iptables -t filter -A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT
```

Permitimos que los equipos de la red 192.168.10.0 conectados a mi tarjeta eth1 puedan ver páginas web

```
iptables -t filter -A FORWARD -s 192.168.10.0/24 -i eth1 -p tcp --dport 80 -
↪j ACCEPT
```

Política de preenrutamiento

```
iptables -t nat -P PREROUTING ACCEPT
```

Política de preenrutamiento

```
iptables -t nat -P POSTROUTING ACCEPT
```

Todo lo que venga por la tarjeta eth0 y vaya al puerto 80 lo redirigimos a una maquina interna

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 192.168.
↪10.12:80
```

Todo lo que salga de nuestra red 192.168.10.0 por la tarjeta eth0 se enmascara (es un tipo de SNAT)

```
iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o eth0 -j MASQUERADE
```

20 Haciendo uso del resumen que aparece arriba y de los ejemplos que aparecen en http://www.pello.info/filez/firewall/iptables.html, ¿cómo escribirías las siguientes reglas?

1. Hacer un listado de reglas de la tabla filter.
2. Hacer un listado de reglas de la tabla nat.
3. Hacer un borrado total (flush) de reglas de la tabla filter.
4. Hacer un borrado total (flush) de reglas de la tabla nat.
5. No permitir entrada del equipo 10.0.5.200 al servidor web de nuestro equipo
6. No permitir entrada del equipo 10.0.5.200 al servidor web 20.20.20.20.
7. Poner política por defecto ACCEPT para los canales INPUT, FORWARD y OUTPUT.
8. Poner política por defecto ACCEPT para los canales PREROUTING y POSTROUTING.
9. Hacer un enmascaramiento de los paquetes de nuestra red 10.0.5.0/24 que salen por eth2. (SNAT)
10. Todo lo que venga por la tarjeta eth0 destinado al puerto 80 se manda a 10.0.5.222 y puerto 8080. (DNAT)
21. Ejecuta **netstat -na** en tu equipo Windows. Muestra una captura de los puertos abiertos.
22. Ejecuta **netstat -punta** en un equipo Linux. Muestra una captura de los puertos abiertos.
23. Ejecuta **Zenmap** desde un equipo (Windows o Linux). Realiza las siguientes operaciones:
    1. Ver puertos abiertos del equipo 10.0.5.1.
    2. Ver lista de equipos en nuestra subred 10.0.5.0/24.
    3. Ver puertos abiertos de los equipos www.google.es y 8.8.8.8
    4. Hacer un trazado de ruta a los equipos anteriores. Hacer una captura de pantalla donde se muestre la topología.
    5. Hacer un trazado de ruta a www.google.es/30. Hacer una captura de pantalla donde se muestre la topología.
24. Hacer un pequeño tutorial de configuración de un punto de acceso. (Opcional)
    1. Estado del AP.
    2. Claves de acceso.
    3. Modos de funcionamiento (Repetidor, Bridge, Punto de Acceso, . . .)
    4. Configuración de la red Wi-Fi (SSID, Seguridad).
25. Hacer un pequeño tutorial de configuración de un router.
    1. Estado del router.

2. Claves de acceso al router.
3. Configuración de IP Interna / Máscara.
4. Configuración del DHCP.
5. Configuración de la red Wi-Fi (SSID, Seguridad) si es un router inalámbrico.
6. Filtrado de MAC si está disponible.
7. NAT. Port forwarding. Apertura de puertos.

26. Hacer un pequeño tutorial de configuración de un switch gestionable si está disponible. (Opcional)

1. Estado del switch.
2. Claves de acceso.
3. Configuración de IP Interna / Máscara.
4. Configuración de VLANs si está disponible.

27. ¿Qué es y para que sirve un proxy? Ventajas de su uso.
28. ¿Qué diferencias existen entre un proxy normal y uno inverso?
29. Si tenemos 3 líneas ADSL de distintos ISP y queremos utilizarlas a la vez para nuestra red local para tener una conexión a Internet tolerante a fallos y mayor ancho de banda, ¿qué técnica podemos utilizar?
30. Tenemos 4 servidores web con el mismo contenido y queremos balancear las peticiones de los clientes entre los 4 servidores. Explica las 2 formas principales de hacerlo.

CAPÍTULO 12

CONEXIÓN A REDES DE ÁREA EXTENSA

12.1 Introducción

Los métodos de acceso a Internet más frecuentes son:

- Tecnologías de cable:
  - Módem telefónico
  - Módem de cable
  - PLC
  - RDSI
  - **ADSL / VDSL**
  - **FTTH**
- Tecnologías inalámbricas
  - LMDS
  - MMDS
  - Wi-Fi
  - WiMAX
  - **4G**

12.2 Módem telefónico

Módem (del inglés modem, acrónimo de modulator demodulator; pl. módems)1 es el dispositivo que convierte las señales digitales en analógicas (modulación) y viceversa (demodulación), permitiendo la comunicación entre computadoras a través de la línea telefónica.

Es cierto que se suelen oír expresiones como módem ADSL o incluso módem RDSI, aunque esto no es cierto en estos casos, ya que estas líneas de tipo digital no necesitan de ningún tipo de conversión de digital a analógico, y su función en este caso es más parecida a la de una tarjeta de red que a la de un módem.

Uno de los primeros parámetros que lo definen es su velocidad. El estándar más habitual y uno de los últimos está basado en la norma V.90 de la UIT-T cuya velocidad máxima está en los 56 Kbps (Kilobits por segundo). Esta norma se caracteriza por un funcionamiento asimétrico, puesto que la mayor velocidad sólo es alcanzable «en bajada», ya que en el envío de datos está limitada a 33,6 Kbps.

En el año 2000 la UIT-T aprobo la norma V.92 titulada «Mejoras a la Recomendación V.90» («Enhancements to Recommendation V.90»). Esta norma establece un estándar para módems que permite transmisiones de hasta 56 Kbit/s en el canal de bajada y 48 Kbit/s en el canal de subida. Esta norma mejora la velocidad de conexión, además les permite aceptar llamadas mientras navegan, aumenta la velocidad de descarga y permite el manejo más fácil de las llamadas. No alcanzó demasiado éxito debido a la proliferación del acceso a internet de banda ancha.

Otra consideración importante es que para poder llegar a esta velocidad máxima se deben dar una serie de circunstancias que no siempre están presentes y que dependen totalmente de la compañía telefónica que nos presta sus servicios, pudiendo ser en algunos casos bastante inferiores.

Evidentemente, el módem que se encuentre al otro lado de la línea telefónica, sea nuestro proveedor de Internet o el de nuestra oficina debe ser capaz de trabajar a la misma velocidad y con la misma norma que el nuestro, ya que sino la velocidad que se establecerá será la máxima que aquel soporte.

Otras normas habitualmente utilizadas son:

Norma	Velocidad máxima
V.90 y X2[1]	56.000 bps
V.34+	33.600 bps
V.34	28.800 bps
V.32bis	14.400 bps
V.32	9.600 bps
V.23	4.800 bps
V.22bis	2.400 bps
V.22 y Bell 212A	1.200 bps
V.21 y Bell 103	300 bps

Otra funcionalidad ya considerada como obligatoria en cualquier módem es el soporte de funciones de FAX. Lo estándares son los siguientes:

Norma	Velocidad máxima
V.17	14.400 bps
V.29	9.600 bps
V.27ter	4.800 bps
V.21	300 bps

Otros estándares considerados como imprescindibles son los de control de errores y compresión de datos. Los más habituales son: V.42, V.42bis y MNP 2-5.

No podemos dejar de comentar otros aspectos igualmente importantes como el de contar con una memoria de tipo flash que nos permita la actualización del firmware al igual que ocurre con las BIOS de las placas base.

Este detalle ha sido extremadamente importante en los módem que utilizaban los distintos estándares de 56K anteriores a la norma V.90, ya que gracias a ello y mediante una simple actualización ha sido posible no quedarse con un modelo desfasado.Igualmente algunos modelos que funcionaban a 33,6 Kbps han podido ser actualizados y funcionar a 56 Kbps con el mismo método y sin necesidad de actualizar el hardware.

[1] protocolo propietario de 3Com, es decir, no estándar.

12.2.1 Tipos de modems

Internos

Consisten en una tarjeta de expansión sobre la cual están dispuestos los diferentes componentes que forman el módem. Existen para diversos tipos de conectores:

- ISA. Hoy en día en desuso.
- PCI.
- AMR. Baratos pero poco recomendables por su bajo rendimiento.

Externos

Similares a los anteriores, pero externos al ordenador. La ventaja de estos módems reside en su fácil transportabilidad entre ordenadores diferentes.

- Puerto serie (RS-232). La conexión de los módems telefónicos con el ordenador se realiza generalmente mediante uno de los puertos serie tradicionales o COM, por lo que se usa la UART del ordenador, que deberá ser capaz de proporcionar la suficiente velocidad de comunicación. La UART debe ser de 16550 o superior para que el rendimiento de un módem de 28.800 bps o más sea el adecuado.
- Modems PC Card (PCMCIA). Son módems en forma de tarjeta, que se utilizaban en portátiles, antes de la llegada del USB, que puede ser utilizado tanto en los ordenadores de sobremesa como en los portátiles. Su tamaño es similar al de una tarjeta de crédito algo más gruesa.
- Puerto USB, de conexión y configuración aún más sencillas.

Modems software, HSP o Winmodems

Son modems generalmente internos, en los cuales se han eliminado varias piezas electrónicas (por ejemplo, chips especializados), de manera que el microprocesador del ordenador debe suplir su función mediante un programa. Lo normal es que utilicen como conexión una ranura PCI (o una AMR), aunque no todos los módems PCI son de este tipo. El uso de la CPU entorpece el funcionamiento del resto de aplicaciones del usuario. A pesar de su bajo coste, resultan poco o nada recomendables.

12.3 Módem de cable (cablemódem)

Un cablemódem o cable módem es un tipo especial de módem diseñado para modular la señal de datos sobre una infraestructura de televisión por cable. El término Internet por cable (o simplemente cable) se refiere a la distribución de un servicio de conectividad a Internet sobre esta infraestructura de telecomunicaciones.

Los cablemodems no deben confundirse con antiguos sistemas LAN como 10base2 o 10base5 que utilizaban cables coaxiales – y especialmente con 10base36, el cual realmente utiliza el mismo tipo de cable que los sistemas CATV.

Los cablemodems se utilizan principalmente para distribuir el acceso a Internet de banda ancha, aprovechando el ancho de banda que no se utiliza en la red de TV por cable.

La televisión por cable utiliza cables coaxiales en las residencias familiares que tienen un ancho de banda de hasta 862 MHz (750 MHz en América). El ancho de banda completo se reparte de la siguiente forma:

- 5 - 55 MHz para el canal de retorno
- 87,5 – 108 MHz para canales de radiodifusión sonora
- 118 – 606 MHz para canales de televisión analógica

- 606 – 862 MHz para canales de televisión digital

Las redes en sí hacen uso de HFC (Hibrido Fibra-Coaxial), fibra óptica en las trocales y coaxial en el tramo final hacia el abonado. Se suelen distribuir entre 20 y 100 canales utilizando FDM (Multiplexación por División de Frecuencias). Cada canal de TV analógica ocupa 8 MHz (6 MHz en el estándar americano). Se pueden dedicar 2 canales o bandas para permitir al usuario cargar y descargar información de Internet.

La velocidades de transmisión son:

Descarga de datos

64-QAM –> 6 MHz * 6 = 36 Mbps (En la práctica de 3 a 10 Mbps)

Carga de datos

4-PSK –> 6 MHz * 2 = 12 Mbps (En la practica de 0,5 a 1 Mbps)

12.4 PLC

PLC (**Power Line Comunications**) es una tecnología basada en la transmisión de datos utilizando como infraestructura la red eléctrica.

Hay dos tipos principales de Power Line Communications:

- PLOC (Power Line Outdoors Telecoms o comunicaciones extrahogareñas utilizando la red eléctrica). Esto es, la comunicación entre la subestación eléctrica y la red doméstica (electro-módem). El estándar es ETSI
- PLIC (Power Line Indoors Telecoms o comunicaciones intrahogareñas utilizando la red eléctrica). Esto es, utilizando la red eléctrica interior de la casa, para establecer comunicaciones internas. Un ejemplo: PLIC es una de las vías utilizadas en domótica (otra que se suele utilizar también es la comunicación vía radio

El concepto técnico es sencillo, desde la estación de transformación hasta el usuario final se utiliza la red eléctrica y a partir de la estación de transformación se conecta con la red de telecomunicaciones convencional. Esto supone que se podrá tener acceso a Internet en cualquier punto de la geografía donde llegue la red eléctrica.

La señal utilizada para transmitir datos a través de la red eléctrica suele ser de 1,6 a 30 MHz.

Se consiguen velocidades de transmisión de hasta 200 Mbps en el tramo de la Media y Baja Tensión. Como desventaja, dependiendo de la frecuencia utilizada, se pueden producir interferencias en frecuencias correspondientes a las fuerzas de seguridad, frecuencias de emergencia de la aviación civil y bandas de radioaficionados.

12.5 RDSI

12.5.1 La interfaz del usuario

El usuario tiene acceso a la RDSI mediante un interfaz local a un flujo digital con una cierta velocidad binaria y un ancho de banda determinado.Hay disponibles flujos de varios tamaños para satisfacer diferentes necesidades. Por ejemplo un cliente residencial puede requerir sólo capacidad para gestionar un teléfono o un terminal de videotexto. Una oficina querrá sin duda conectarse a la a RDSI a través de una centralita (PBX) digital local, y requerirá un flujo de mucha más capacidad.

12.5.2 Canales RDSI

El flujo digital entre la central y el usuario RDSI se usa para llevar varios canales de comunicación. La capacidad del flujo, y por tanto el número de canales de comunicación, puede variar de un usuario a otro. Para la transferencia de información y señalización se han definido los siguientes canales:

- **Canal B**: es el canal básico de usuario. Es un canal a 64 kbps para transporte de la información generada por el terminal de usuario. Se puede usar para transferir datos digitales, voz digital codificada PCM, o una mezcla de tráfico de baja velocidad, incluyendo datos digitales y voz digitalizada descodificada a la velocidad antes mencionada de 64 kbps. Puede subdividirse en subcanales, en cuyo caso todos ellos deben establecerse entre los mismos extremos subcriptores. Puede soportar las siguientes clases de conexiones:
- **Conmutación de circuitos**: es el equivalente al servicio digital conmutado disponible en la RDI. El usuario hace una llamada y se establece una conexión de circuito conmutado con otro usuario de la red, con unos recursos dedicados. Cabe destacar que el diálogo de establecimiento de la llamada no tiene lugar en el canal B, sino en el D, que se define a continuación.
- **Conmutación de paquetes**: el usuario se conecta a un nodo de conmutación de paquetes y los datos se intercambian con otros usuarios vía X.25. Los recursos no son dedicados.
- **Permanentes**: no requiere un protocolo de establecimiento de llamada. Es equivalente a una línea alquilada. Se contrata un canal fijo, permanente.
- **Canal D**: es un canal de señalización a 16 ó 64 kbps. Sirve para dos fines. Primero, lleva información de señalización para controlar las llamadas de circuitos conmutados asociadas con los canales B. Además el canal D puede usarse para conmutación de paquetes de baja velocidad mientras no haya esperando información de señalización.
- **Canales H**: son canales destinados al transporte de flujos de información de usuario a altas velocidades, superiores a 64 kbps.

Los canales tipos B y D se agrupan, a su vez, en diferentes tipos o grupos, según el siguiente esquema:

Tipo	Función	Velocidad
B	Servicios básicos	64 Kbps.
D	Señalización	16 Kbps. (BRI)
▪	▪	64 Kbps. (PRI)
H0	6 canales B	384 Kbps. (PRI)
H1	todos los canales H0	▪
▪	H11 (24B)	1.536 Kbps.(PRI)
▪	H12 (30B)	1.920 Kbps. (PRI)
H2	RDSI de banda ancha	(propuesta actual)
▪	H21	32.768 Kbps.
▪	H22	43-45 Mbps.
H4	RDSI de banda ancha	132-138,240 Mbps.

Por tanto, las interfaces BRI y PRI tienen la siguiente estructura:

Interfaz	Estructura	Velocidad total	Velocidad disponible
BRI	2B + D16	192 Kbps.	144 Kbps.
PRI	23B + D64	1.544 Kbps.	1.536 Kbps. (EE.UU.)
PRI	30B + D64	2.048 Kbps.	1.984 Kbps. (Europa)

12.5.3 Tipos de contratación

Acceso Básico (BRI)

El acceso básico consiste en dos canales B full-duplex de 64 kbps y un canal D full-duplex de 16 kbps. Luego, la división en tramas, la sincronización, y otros bits adicionales dan una velocidad total a un punto de acceso básico de 192 kbps x segundo

- **2B+D+señalización+sincronización+mantenimiento**

Acceso Primario (PRI)

El acceso primario está destinado a usuarios con requisitos de capacidad mayores, tales como oficinas con centralita (PBX) digital o red local (LAN). Debido a las diferencias en las jerarquías de transmisión digital usadas en distintos países, no es posible lograr un acuerdo en una única velocidad de los datos.

Estados Unidos, Japón y Canadá usan una estructura de transmisión basada en 1.544 Mbps, mientras que en Europa la velocidad estándar es 2.048 Mbps. Típicamente, la estructura para el canal de 1.544 Mbps es 23 canales B más un canal D de 64 kbps y, para velocidades de 2.048 Mbps, 30 canales B más un canal D de 64 kbps.

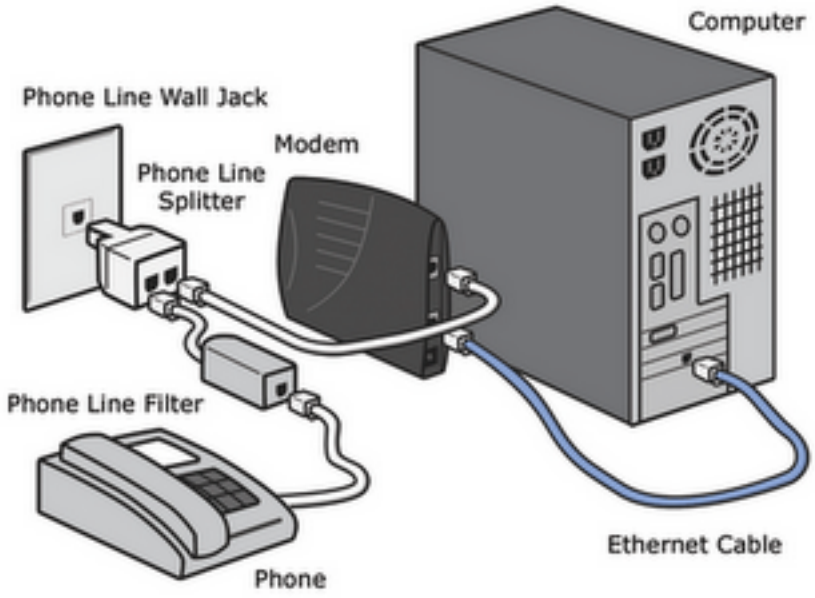
- 30B(64)+D(64)señalización+sincronización(64) **2048 Europa (E1)**
- 23B(64)+D(64)señalización+sincronización(8) **1544 Estados Unidos, Japón, Canadá (T1)**

12.6 ADSL-VDSL

12.6.1 Tecnologías xDSL

Nombre	Significado	Velocidad	Modo	Observaciones
ADSL	DSL asimétrico	▪ Hasta 12 Mbps ▪ Hasta 1.8 Mbps	▪ Descendente ▪ Ascendente	Utiliza un par de hilos. Hasta 5,5 km de distancia.
RADSL	DSL de velocidad adaptable	▪ De 1,5 a 8 Mbps ▪ De 16 a 640 kbps	▪ Descendente ▪ Ascendente	Utiliza un par de hilos. Adapta su velocidad de datos a la velocidad de la línea
CDSL	DSL de consumidor	▪ Hasta 1 Mbps ▪ De 16 a 128 kbps	▪ Descendente ▪ Ascendente	Utiliza un par de hilos. No necesita splitter en casa.
SDSL	DSL de par único	▪ 768 kbps	▪ Simétrico	Utiliza un par de hilos.
IDSL	DSL de RDSI	▪ Igual a BRI de RDSI	▪ Simétrico	Utiliza un par de hilos que se denomina Bri sin conmutador.
HDSL	DSL de alta velocidad	▪ 1,544 Mbps (EE.UU) ▪ 2,048 Mbps (Europa)	▪ Simétrico ▪ Simétrico	Utiliza 2 o 3 pares de hilos.
VDSL	DSL de altísima velocidad	▪ Máximo 52 o 26 Mbps ▪ Máximo 12 o 26 Mbps	▪ Descendente ▪ Ascendente	Necesita una red de fibra y ATM. De 300 a 1.500 metros.

El siguiente esquema muestra los elementos necesarios y su forma de conexión.



El PTR es un cajetín que hace de punto de conexión entre la red telefónica y el cableado telefónico de la casa. Permite descubrir si un problema está provocado por el cableado telefónico de la casa o si es de la red telefónica. PTR significa Punto Terminación de Red.

Normalmente para que la conexión a Internet con ADSL funcione es necesario instalar o usar un filtro que separe la conexión a Internet del servicio de teléfono para que puedan funcionar ambas cosas sobre el mismo cable. En el pasado, la compañía telefónica cambiaba el PTR por otro cajetín llamado Splitter, actuando este como un filtro centralizado.

Según se fueron popularizando las conexiones ADSL se opto por sustituir la instalación del Splitter por el uso de microfiltros en cada uno de los aparatos telefónicos que tuviésemos en la casa (incluido fax y datafonos), salvo en el router.

12.6.2 ADSL, ADSL2 y ADSL2+

ADSL es una tecnología de acceso a Internet de banda ancha. Esta tecnología permite el envio de voz y datos por una misma línea de forma simultánea. Esto se consigue mediante la utilización de una banda de frecuencias más alta que la utilizada en las conversaciones telefónicas convencionales (300-3.400 Hz). Para la transmisión de datos se emplean las frecuencias superiores a 25 KHz.

ADSL ha ido evolucionando con el paso del tiempo. La siguiente tabla muestra dicha evolución.

Tabla comparativa de velocidades en ADSL

■	ADSL	ADSL2	ADSL2+
Ancho de banda de descarga	0.5 MHz	1.1 MHz	2.2 MHz
Velocidad máxima de subida	1 Mbps	1 Mbps	1.2 Mbps
Velocidad máxima de descarga	8 Mbps	12 Mbps	24 Mbps
Distancia	2 Km	2.5 Km	2.5 Km
Tiempo de sincronización	10 a 30 segundos	3 segundos	3 segundos
Corrección de errores	No	Sí	Sí

El rango de frecuencias utilizado (en este caso para ADSL2+) es:

- 0 - 4 KHz para el canal de voz
- 25 - 500 KHz para el canal de subida de datos.
- 550 KHz - 2,2 MHz para el canal de bajada de datos.

12.6.3 VDSL y VDSL2

VDSL (o VHDSL) son las siglas de Very high bit-rate Digital Subscriber Line (DSL de muy alta tasa de transferencia). Se trata de una tecnología de acceso a internet de Banda Ancha, perteneciente a la familia de tecnologías xDSL que transmiten los impulsos sobre pares de cobre.

Se trata de una evolución del ADSL, que puede suministrarse de manera asimétrica (**52 Mbit/s de descarga y 12 Mbit/s de subida**) o de manera simétrica (**26 Mbit/s tanto en subida como en bajada**), en condiciones ideales sin resistencia de los pares de cobre y con una distancia nula a la central.

VDSL2 (Very-High-Bit-Rate Digital Subscriber Line 2) Línea digital de abonado de muy alta tasa de transferencia, que aprovecha la actual infraestructura telefónica de pares de cobre.

ITU-T G.993.2 VDSL2 es el estándar de comunicaciones DSL más reciente y avanzado. Está diseñado para soportar los servicios conocidos como «Triple Play», incluyendo voz, video, datos, televisión de alta definición (HDTV) y juegos interactivos.

ITU-T G.993.2 permite la transmisión simétrica o asimétrica de datos, llegando a anchos de bandas superiores a 200 Mbit/s (**100 Mbps para subida y 100 Mbps**, aunque pueden distribuirse de forma asimétrica). Este ancho de banda de transmisión depende de la distancia a la central. A medida que la longitud del bucle se acorta, sube la relación de simetría, llegando a más de 100 Mbit/s (tanto upstream como downstream), dadas las condiciones idóneas.

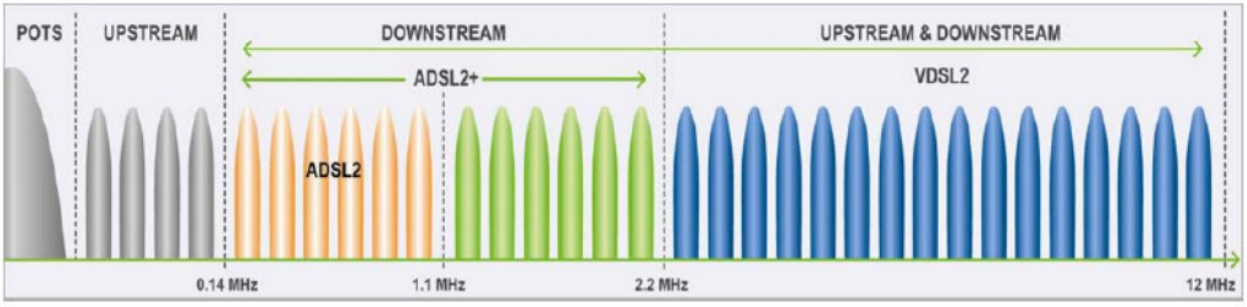


Figura 1: Espectro_de_asignación_VDSL2

12.6.4 ADSL-VDSL Estándares

Estándar	Nombre común	Velocidad de bajada máxima	Velocidad de subida máxima
ANSI T1.413-1998 Issue 2	**ADSL**	8 Mbit/s	1.0 Mbit/s
ITU G.992.1	**ADSL (G.DMT)**	12 Mbit/s	1.3 Mbit/s
ITU G.992.1 Annex A	**ADSL over POTS**	12 Mbit/s	1.3 MBit/s
ITU G.992.1 Annex B	**ADSL over ISDN**	12 Mbit/s	1.8 MBit/s
ITU G.992.2	**ADSL Lite (G.Lite)**	1.5 Mbit/s	0.5 Mbit/s
ITU G.992.3	**ADSL2**	12 Mbit/s	1.0 Mbit/s
ITU G.992.3 Annex J	**ADSL2**	12 Mbit/s	3.5 Mbit/s
ITU G.992.3 Annex L	**RE-ADSL2**	5 Mbit/s	0.8 Mbit/s
ITU G.992.4	**splitterless ADSL2**	1.5 Mbit/s	0.5 Mbit/s
ITU G.992.5	**ADSL2+**	24 Mbit/s	1.0 Mbit/s
ITU G.992.5 Annex M	**ADSL2+M**	24 Mbit/s	3.5 Mbit/s
ITU G.993.1	**VDSL**	52Mbit/s 26 Mbit/s	12 Mbit/s 26 Mbit/s
ITU G.993.2	**VDSL2**	100 Mbit/s	100 Mbit/s

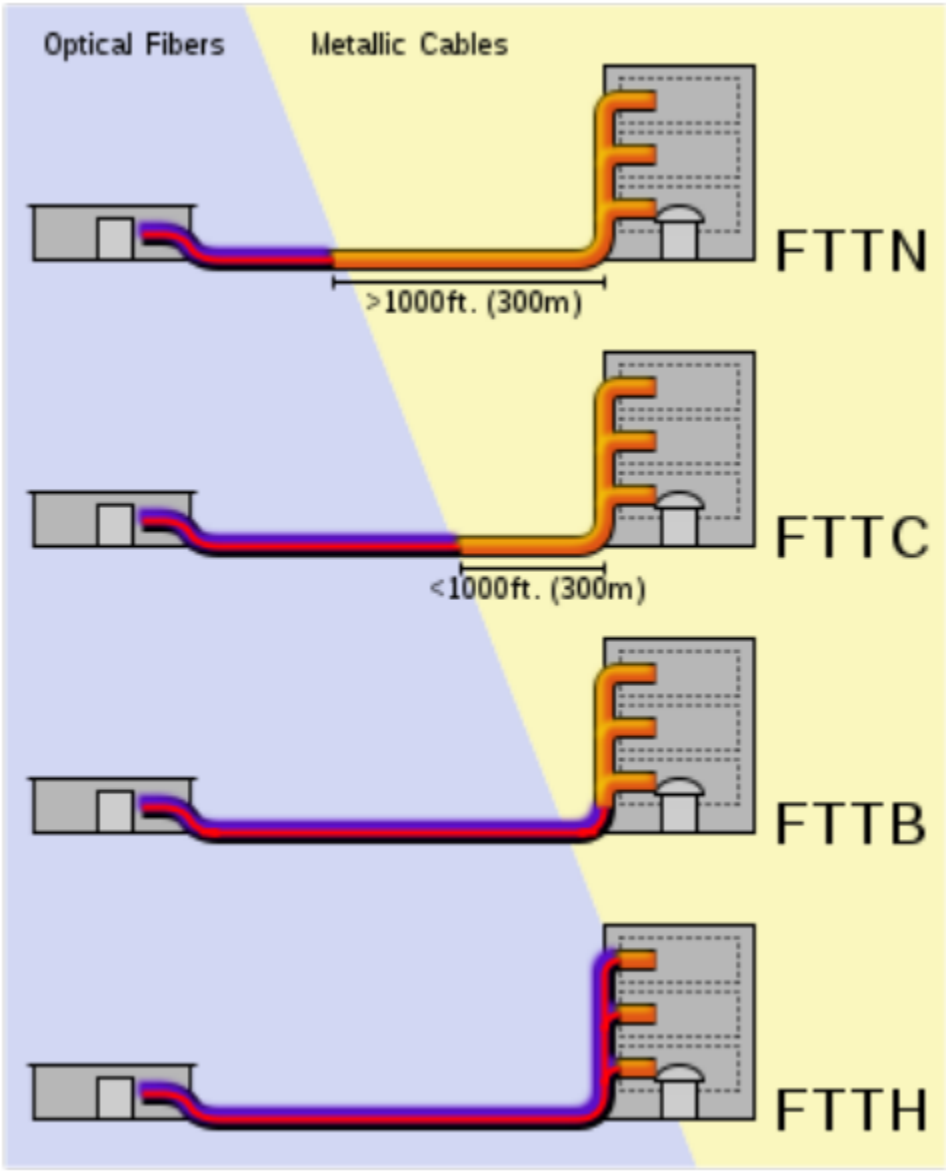
12.7 FTTH

12.7.1 Tecnologías FTTx

La tecnología de telecomunicaciones **FTTx** (del inglés **Fiber to the** x) es un término genérico para designar cualquier acceso de banda ancha sobre fibra óptica que sustituya total o parcialmente el cobre del bucle de acceso. El acrónimo FTTx se origina como generalización de las distintas configuraciones desplegadas (FTTN, FTTC, FTTB, FTTH...), diferenciándose por la última letra que denota los distintos destinos de la fibra (nodo, acera, edificio, hogar...).

La industria de las telecomunicaciones diferencia distintas arquitecturas dependiendo de la distancia entre la fibra óptica y el usuario final. Las más importantes en la actualidad son:

- **FTTN** (Fibra hasta el nodo - Fiber-to-the-node). La fibra óptica termina en una central del operador de telecomunicaciones que presta el servicio, suele estar más lejos de los abonados que en FTTH y FTTB, típicamente en las inmediaciones del barrio.
- **FTTC** (Fibra hasta la acera - Fiber-to-the-cabinet o fiber-to-the-curb). Similar a FTTN, pero la cabina o armario de telecomunicaciones está más cerca del usuario, normalmente a menos de 300 metros.
- **FTTB** (Fibra hasta el edificio - Fiber-to-the-building o Fiber-to-the-basement). La fibra óptica normalmente termina en un punto de distribución intermedio en el interior o inmediaciones del edificio de los abonados. Desde este punto de distribución intermedio, se accede a los abonados finales del edificio o de la casa mediante la tecnología VDSL2 (Very high bit-rate Digital Subscriber Line 2) sobre par de cobre o Gigabit Ethernet sobre par trenzado CAT5. De este modo, el tendido de fibra puede hacerse de forma progresiva, en menos tiempo y con menor coste, reutilizando la infraestructura del edificio del abonado.
- **FTTH** (Fibra hasta el hogar - Fiber-to-the-home). En FTTH o fibra hasta el hogar, la fibra óptica llega hasta el interior de la misma casa u oficina del abonado.


Optical Fibers
Metallic Cables
FTTN
>1000ft. (300m)
FTTC
<1000ft. (300m)
FTTB
FTTH

12.7.2 FTTH

La tecnología de telecomunicaciones FTTH (del inglés Fiber To The Home), también conocida como **fibra hasta la casa o fibra hasta el hogar**, enmarcada dentro de las tecnologías FTTx, se basa en la utilización de cables de fibra óptica y sistemas de distribución ópticos adaptados a esta tecnología para la distribución de servicios avanzados, como el **Triple Play: telefonía, Internet de banda ancha y televisión**, a los hogares y negocios de los abonados.

Para la instalación y/o mantenimiento de redes FTTH se utilizan instrumentos electrónicos de precisión denominados Analizadores FTTH que efectúan medidas sobre diferentes parámetros de las señales utilizadas en la tecnología de telecomunicaciones FTTH.

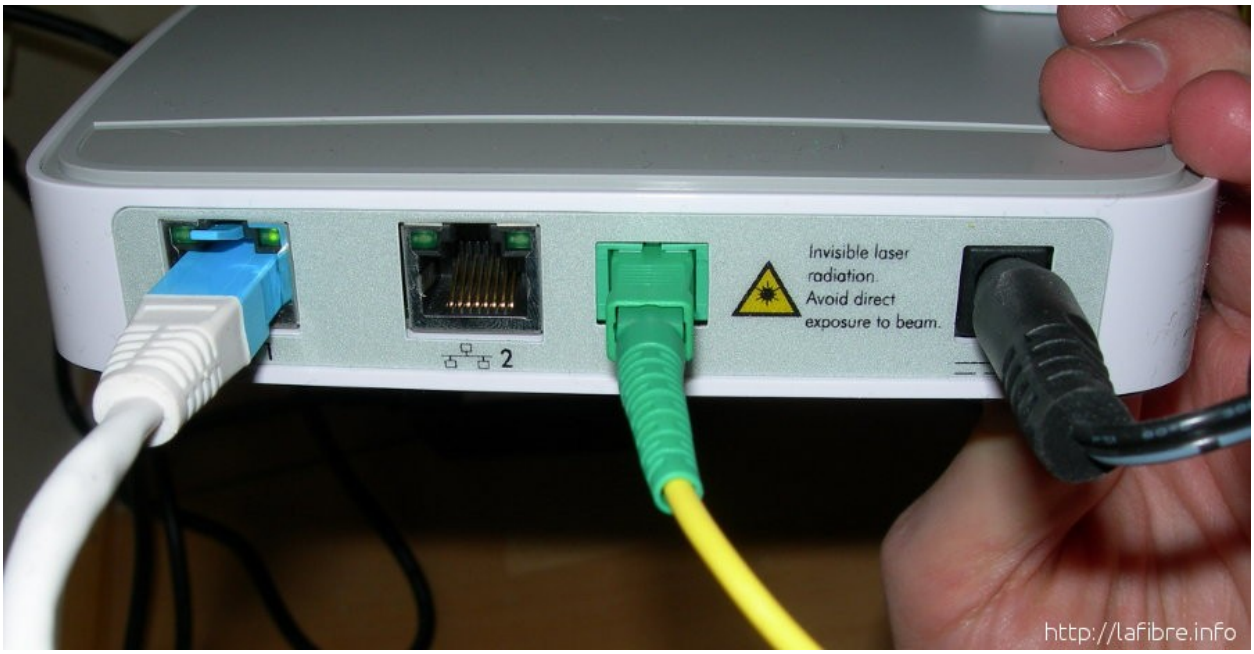


Figura 2: Terminal de Fibra Óptica para el usuario (ONT, en sus siglas en inglés)

12.8 LMDS

Sistema de Distribución Multipunto Local.

LDMS es un sistema de comunicación punto-multipunto inalámbrico para transmisión de banda ancha en **frecuencias entre 24 y 42 GHz** dependiendo del pais. También se utiliza la gama baja **de 3,4 a 3,6 GHz**.

El uso de microondas hace que sea **necesario una línea directa de visión** entre la estación base y la antena del abonado.

Proporciona una velocidad de **hasta 8 Mbps** y una distancia del enlace que va **desde 100 m a 35 Km** dependiendo de la sensibilidad de las unidades de abonado y la calidad de servicio a ofrecer. Los sistemas de comunicación LMDS en la banda de 3,5GHz tienen la ventaja de no verse afectados por la niebla, la lluvia o la nieve.

12.9 MMDS

Sistema de Distribución Multipunto Multicanal.

MMDS es un acrónimo de **Multichannel Multipoint Distribution Service**, e identifica a una tecnología inalámbriaca de telecomunicaciones, usada para el establecimiento de una red de banda ancha de uso general o, más comúnmente, como método alternativo de recepción de programación de televisión por cable.

Se utiliza generalmente en áreas rurales poco pobladas, en donde instalar redes de cable no es económicamente viable.

La banda de MMDS utiliza frecuencias microondas con rangos **de 2 GHz a 3 GHz** en gama. La recepción de las señales entregadas vía MMDS requiere una antena especial de microondas y un decodificador que se conecta al receptor de televisión

12.10 Wi-Fi

Wi-Fi (o Wi-fi, WiFi, Wifi, wifi) es un conjunto de estándares para redes inalámbricas basado en las especificaciones **IEEE 802.11**.

Los estándares IEEE 802.11b e IEEE 802.11g que 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 y 54 Mbps, respectivamente. Existe también el estándar IEEE 802.11n que trabaja a 2.4 GHz a una velocidad de 108 Mbps. Aunque estas velocidades de 108 Mbps son capaces de alcanzarse ya con el estandar 802.11g gracias a técnicas de aceleramiento que consiguen duplicar la transferencia teórica.

Wi-Fi se creó para ser utilizada en redes locales inalámbricas, pero es frecuente que en la actualidad también se utilice para acceder a Internet.

RedLibre es la primera comunidad inalámbrica (de redes libres) de habla hispana del mundo (2001). Los miembros de la comunidad crean una red de acceso libre y gratuíto. Varios años más tarde, a finales del 2005, Jazztel, en España, es el primer proveedor de acceso a Internet que abre sus redes a FON, la comunidad de usuarios que comparten sus accesos a Internet inalámbricos (Wi-Fi). La utilización de esta tecnología todavía no es masiva, con lo que la cobertura de una red que entrelace los distintos puntos de acceso Wi-Fi aún es muy limitada.

Otra red es guifi.net. Es una red de telecomunicaciones libre, abierta y neutral, mayoritariamente inalámbrica, con más de 31.701 nodos, de los cuales más de 20.332 están operativos (marzo 2013). La mayoría de éstos nodos se encuentran ubicados en Cataluña y la Comunidad Valenciana, aunque se están expandiendo a nuevas zonas en el resto del Mundo. Actualmente, guifi.net es la red libre más extensa de todo el Mundo.

12.11 WiMax

WiMAX (del inglés Worldwide Interoperability for Microwave Access, Interoperabilidad Mundial para Acceso por Microondas) es un estándar de transmisión inalámbrica de datos (802.MAN) proporcionando accesos concurrentes en áreas de hasta 48 kilómetros de radio y a velocidades de hasta 70 Mbps, utilizando tecnología que no requiere visión directa (NLOS).

El WiMAX Forum es un consorcio de empresas (inicialmente 67 y hoy en día más de 100) dedicadas a diseñar los parámetros y estándares de esta tecnología, y a estudiar, analizar y probar los desarrollos implementados. En principio se podría deducir que esta tecnología supone una grave amenaza para el negocio de tecnologías inalámbricas de acceso de corto alcance en que se basan muchas empresas, pero hay entidades muy importantes detrás del proyecto. Las principales firmas de telefonía móvil también están desarrollando terminales capaces de conectarse a estas nuevas redes. Después de la fase de pruebas y estudios cuya duración prevista es de unos dos años, se espera comenzar a ofrecer servicios de conexión a Internet a 4 Mbps a partir de 2007, incorporando WiMAX a los ordenadores portátiles y PDA.

El IEEE 802.16 el estándar con revisiones específicas se ocupa de dos modelos de uso:

- Fijo
- Móvil

El estándar inicial 802.16 era fijo y se encontraba en la banda de frecuencias de 10-66 GHz y requería torres LOS. La nueva versión 802.16a, ratificada en marzo de 2003, utiliza una banda del espectro más estrecha y baja, de 2-11 GHz, facilitando su regulación. Además, como ventaja añadida, no requiere de torres LOS sino únicamente del despliegue de estaciones base (BS) formadas por antenas emisoras/receptoras con capacidad de dar servicio a unas 200 estaciones suscriptoras (SS) que pueden dar cobertura y servicio a edificios completos

El pasado 7 de diciembre de 2005, el IEEE aprobó el estándar del WiMAX MÓVIL, el 802.16e, que permite utilizar este sistema de comunicaciones inalámbricas con terminales en movimiento. Muchos fabricantes de hardware y operadores estaban esperando a esta decisión para empezar a desplegar redes de wimax.

Tabla resumen de características del estándar 802.16 (WiMAX)

	802.16	802.16a	802.16e
Espectro	10 - 66 GHz	2 - 11 GHz	< 6 GHz
Funcionamiento	Solo con visión directa (LOS)	Sin visión directa (NLOS)	Sin visión directa (NLOS)
Tasa de bit	32 - 134 Mbit/s con canales de 28 MHz	Hasta 75 Mbit/s con canales de 20 MHz	Hasta 15 Mbit/s con canales de 5 MHz
Modulación	QPSK, 16QAM y 64 QAM	OFDM con 256 subportadoras QPSK, 16QAM, 64QAM	Igual que 802.16a
Movilidad	Sistema fijo	Sistema fijo	Sistema móvil
Anchos de banda	20, 25 y 28 MHz	Seleccionables entre 1,25 y 20 MHz	Igual que 802.16a con los canales de subida para ahorrar potencia
Radio de celda típico	2 - 5 km aprox.	5 - 10 km aprox. (alcance máx. de unos 50 km)	2 - 5 km aprox.

12.12 4G

En telecomunicaciones, 4G son las siglas utilizadas para referirse a la cuarta generación de tecnologías de telefonía móvil. Es la sucesora de las tecnologías 2G y 3G, y que precede a la próxima generación la 5G.

La 4G está **basada completamente en el protocolo IP**, siendo un sistema y una red, que se alcanza gracias a la convergencia entre las redes de cables e inalámbricas. Esta tecnología podrá ser usada por módems inalámbricos, móviles inteligentes y otros dispositivos móviles. La principal diferencia con las generaciones predecesoras será la capacidad para proveer velocidades de acceso mayores de **100 Mbit/s en movimiento y 1 Gbit/s en reposo**, manteniendo una calidad de servicio (QoS) de punta a punta de alta seguridad que permitirá ofrecer servicios de cualquier clase en cualquier momento, en cualquier lugar, con el mínimo coste posible. Esta tecnología podrá ser usada por módems inalámbricos, móviles inteligentes y otros dispositivos móviles.

12.13 Referencias

- Control de Acceso al Medio (MAC) de distintas tecnologías
- Antiguo módem analógico
- LMDS
- Blog francés acerca de la fibra óptica (fotos interesantes)

Figura 3: Modem 4G

Figura 4: TP-LINK MR3050, router WiFi 3G/4G con batería incorporada

- Proyecto Innovación sobre Fibra y Redes
- Despliegue de fibra óptica bajo el océano (Vídeo en Inglés)

12.14 Actividades

1. Crear 3 grupos. Cada grupo escogerá uno de los siguientes métodos de conexión a Internet:
   - VDSL
   - FTTH
   - 4G

   Buscar información y elaborar una presentación en PowerPoint o Impress acerca del método de conexión escogido. Dicha exposición deberá exponerse al resto de la clase. Para la elaboración de la presentación deberán abordarse al menos los siguientes puntos:
   - Dicha tecnología en el mundo
     - Empresas y países.
     - Grado de penetración de la tecnología.
   - Dicha tecnología en España
     - Empresas y regiones o ciudades.
     - Grado de penetración de la tecnología.
   - Productos y servicios disponibles en el mercado