# Configuración básica de redes TCP/IP

## 1. MODELO OSI

| Tecnologías y protocolos de red según el Modelo OSI | |
|---|---|
| **Nivel de aplicación** | DNS, FTP, HTTP, IMAP, IRC, NFS, NNTP, NTP, POP3, SMB/CIFS, SMTP, SNMP, SSH, Telnet, SIP |
| **Nivel de presentación** | ASN.1, MIME, SSL/TLS, XML |
| **Nivel de sesión** | NetBIOS |
| **Nivel de transporte** | SCTP, SPX, TCP, UDP |
| **Nivel de red** | AppleTalk, IP, IPX, NetBEUI, X.25 |
| **Nivel de enlace** | ATM, Ethernet, Frame Relay, HDLC, PPP, Token Ring, Wi-Fi, STP |
| **Nivel físico** | Cable coaxial, Cable de fibra óptica, Cable de par trenzado, Microondas, Radio, RS-232 |

El modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconection) lanzado en 1984 fue el modelo de red descriptivo creado por ISO.

### Historia

En sus inicios, el desarrollo de redes sucedió con desorden en muchos sentidos. A principios de la década de 1980 se produjo un enorme crecimiento en la cantidad y el tamaño de las redes. A medida que las empresas tomaron conciencia de las ventajas de usar tecnología de networking, las redes se agregaban o expandían a casi la misma velocidad a la que se introducían las nuevas tecnologías de red.

Para mediados de la década de 1980, estas empresas comenzaron a sufrir las consecuencias de la rápida expansión. De la misma forma en que las personas que no hablan un mismo idioma tienen dificultades para comunicarse, las redes que utilizaban diferentes especificaciones e implementaciones tenían dificultades para intercambiar información. El mismo problema surgía con las empresas que desarrollaban tecnologías de networking privadas o propietarias. "Propietario" significa que una sola empresa o un pequeño grupo de empresas controlan todo uso de la tecnología. Las tecnologías de networking que respetaban reglas propietarias en forma estricta no podían comunicarse con tecnologías que usaban reglas propietarias diferentes.

Para enfrentar el problema de incompatibilidad de redes, la Organización Internacional para la Estandarización (ISO) investigó modelos de networking como la red de Digital Equipment Corporation (DECnet), la Arquitectura de Sistemas de Red (SNA) y TCP/IP a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. Con base en esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes.

## Modelo de referencia OSI

Siguiendo el esquema de este modelo se crearon numerosos protocolos, como por ejemplo X.25, que durante muchos años ocuparon el centro de la escena de las comunicaciones informáticas. El advenimiento de protocolos más flexibles donde las capas no están tan demarcadas y la correspondencia con los niveles no era tan clara puso a este esquema en un segundo plano. Sin embargo sigue siendo muy usado en la enseñanza como una manera de mostrar como puede estructurarse una "pila" de protocolos de comunicaciones (sin importar su poca correspondencia con la realidad).

El modelo en sí mismo no puede ser considerado una arquitectura, ya que no especifica el protocolo que debe ser usado en cada capa, sino que suele hablarse de modelo de referencia. Este modelo está dividido en siete capas:

Capa Física (Capa 1)

La Capa Física del modelo de referencia OSI es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico (medios guiados: cable coaxial, cable de par trenzado, fibra óptica y otros tipos de cables; medios no guiado: radio, infrarrojos, microondas, láser y otras redes inalámbricas); características del medio (p.e. tipo de cable o calidad del mismo; tipo de conectores normalizados o en su caso tipo de antena; etc.) y la forma en la que se transmite la información (codificación de señal, niveles de tensión/intensidad de corriente eléctrica, modulación, tasa binaria, etc.)

Es la encargada de transmitir los bits de información a través del medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si esta es uni o bidireccional (simplex, dúplex o full-duplex). También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas/electromagnéticas.

Se encarga de transformar una trama de datos proveniente del nivel de enlace en una señal adecuada al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable); o electromagnéticos. Estos últimos, dependiendo de la frecuencia /longitud de onda de la señal pueden ser ópticos, de micro-ondas o de radio. Cuando actúa en modo recepción el trabajo es inverso; se encarga de transformar la señal transmitida en tramas de datos binarios que serán entregados al nivel de enlace.

Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados (o no, como en RS232/EIA232), coaxial, guías de onda, aire, fibra óptica.

- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.

- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).

- Transmitir el flujo de bits a través del medio.

- Manejar las señales eléctricas/electromagnéticas

- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de ésta).

Codificación de la señal

El nivel físico recibe una trama binaria que debe convertir a una señal eléctrica, electro magnética, óptica u otra dependiendo del medio, de tal forma que a pesar de la degradación que pueda sufrir en el medio de transmisión vuelva a ser interpretable correctamente en el receptor.

En el caso más sencillo el medio es directamente digital, como en el caso de las fibras ópticas, dado que por ellas se transmiten pulsos de luz.

Cuando el medio no es digital hay que codificar la señal, en los casos más sencillos la codificación puede ser por pulsos de tensión (PCM o *Pulse Code Modulatión*) (por ejemplo 5 V para los "unos" y 0 V para los "ceros"), es lo que se llaman codificación unipolar NRZ. Otros medios se codifican mediante presencia o ausencia de corriente. En general estas codificaciones son muy simples y no apuran bien la capacidad de medio. Cuando se quiere sacar más partido al medio se usan técnicas de modulación más complejas, y suelen ser muy dependientes de las características del medio concreto.

En los casos más complejos, como suelen ser las comunicaciones inalámbricas, se pueden dar modulaciones muy sofisticadas, este es el caso de los estándares Wi-Fi, con técnicas de modulación complejas de espectro ensanchado

Topología y medios compartidos

Indirectamente el tipo de conexión que se haga en la capa física puede influir en el diseño de la capa de Enlace. Atendiendo al número de equipos que comparten un medio hay dos posibilidades:

- Conexiones punto a punto: que se establecen entre dos equipos y que no admiten ser compartidas por terceros
- Conexiones multipunto: en las que dos o más equipos pueden usar el medio.

Así por ejemplo la fibra óptica no permite fácilmente conexiones multipunto (sin embargo, véase FDDI) y por el contrario las conexiones inalámbricas son inherentemente multipunto (sin embargo, véanse los enlaces infrarrojos). Hay topologías como el anillo, que permiten conectar muchas máquinas a partir de una serie de conexiones punto a punto.

Equipos adicionales

A la hora de diseñar una red hay equipos adicionales que pueden funcionar a nivel físico, se trata de los repetidores, en esencia se trata de equipos que amplifican la señal,

pudiendo también regenerarla. En las redes Ethernet con la opción de cableado de par trenzado (la más común hoy por hoy) se emplean unos equipos de interconexión llamados concentradores (repetidores en las redes 10Base-2) más conocidos por su nombre en inglés (hubs) que convierten una topología física en estrella en un bus lógico y que actúan exclusivamente a nivel físico, a diferencia de los conmutadores (switches) que actúan a nivel de enlace.

Capa de enlace de datos (Capa 2)

Cualquier medio de transmisión debe ser capaz de proporcionar una transmisión sin errores, es decir, un tránsito de datos fiable a través de un enlace físico. Debe crear y reconocer los límites de las tramas, así como resolver los problemas derivados del deterioro, pérdida o duplicidad de las tramas. También puede incluir algún mecanismo de regulación del tráfico que evite la saturación de un receptor que sea más lento que el emisor.

La capa de enlace de datos se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

Ejemplos: Ethernet, Token Ring, ATM, FDDI.

Capa de red (Capa 3)

El cometido de la capa de red es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Es decir que se encarga de encontrar un camino manteniendo una tabla de enrutamiento y atravesando los equipos que sea necesario, para hacer llevar los datos al destino. Los equipos encargados de realizar este encaminamiento se denominan en castellano encaminadores, aunque es más frecuente encontrar el nombre inglés *routers* y, en ocasiones enrutadores.

Adicionalmente la capa de red debe gestionar la congestión de red, que es el fenómeno que se produce cuando una saturación de un nodo tira abajo toda la red (similar a un atasco en un cruce importante en una ciudad grande). La PDU de la capa 3 es Paquetes.

Ejemplos: IP, IPX

Capa de transporte (Capa 4)

Su función básica es aceptar los datos enviados por las capas superiores, dividirlos en pequeñas partes si es necesario, y pasarlos a la capa de red. En el caso del modelo OSI, también se asegura que lleguen correctamente al otro lado de la comunicación. Otra característica a destacar es que debe aislar a las capas superiores de las distintas posibles implementaciones de tecnologías de red en las capas inferiores, lo que la convierte en el corazón de la comunicación. En esta capa se proveen servicios de conexión para la capa de sesión que serán utilizados finalmente por los usuarios de la red al enviar y recibir paquetes. Estos servicios estarán asociados al tipo de comunicación empleada, la cual puede ser diferente según el requerimiento que se le haga a la capa de transporte. Por ejemplo, la comunicación puede ser manejada para

que los paquetes sean entregados en el orden exacto en que se enviaron, asegurando una comunicación punto a punto libre de errores, o sin tener en cuenta el orden de envío. Una de las dos modalidades debe establecerse antes de comenzar la comunicación para que una sesión determinada envíe paquetes, y ése será el tipo de servicio brindado por la capa de transporte hasta que la sesión finalice. De la explicación del funcionamiento de esta capa se desprende que no está tan encadenada a capas inferiores como en el caso de las capas 1 a 3, sino que el servicio a prestar se determina cada vez que una sesión desea establecer una comunicación. Todo el servicio que presta la capa está gestionado por las cabeceras que agrega al paquete a transmitir.

Para finalizar, podemos definir a la capa de transporte como:

Capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la destino, independizándolo del tipo de red física que se esté utilizando. La PDU de la capa 4 se llama Segmentos.

Ejemplos: TCP, UDP

Capa de sesión (Capa 5)

Esta capa ofrece varios servicios que son cruciales para la comunicación, como son: 1 Control de la sesión a establecer entre el emisor y el receptor (quién transmite, quién escucha y seguimiento de ésta). 2 Control de la concurrencia (que dos comunicaciones a la misma operación crítica no se efectúen al mismo tiempo). 3 Mantener puntos de verificación (checkpoints), que sirven para que, ante una interrupción de transmisión por cualquier causa, la misma se pueda reanudar desde el último punto de verificación en lugar de repetirla desde el principio. Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción.

Capa de presentación (Capa 6)

El objetivo de la capa de presentación es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC), números (little-endian tipo Intel, big-endian tipo Motorola), sonido o imágenes, los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Por lo tanto, podemos resumir definiendo a esta capa como la encargada de manejar las estructuras de datos abstractas y realizar las conversiones de representación de datos necesarias para la correcta interpretación de los mismos.

Esta capa también permite cifrar los datos y comprimirlos.

Capa de aplicación (Capa 7)

Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente. Así por ejemplo un usuario no manda una petición "HTTP/1.0 GET index.html" para conseguir una página en html, ni lee directamente el código html/xml.

Entre los protocolos (refiriéndose a protocolos genéricos, no a protocolos de la capa de aplicación de OSI) más conocidos destacan:

- HTTP (HyperText Transfer Protocol) el protocolo bajo la www
- FTP (File Transfer Protocol) ( FTAM, fuera de TCP/IP) transferencia de ficheros
- SMTP (Simple Mail Transfer Protocol) (X.400 fuera de tcp/ip) envío y distribución de correo electrónico
- POP (Post Office Protocol)/IMAP: reparto de correo al usuario final
- SSH (Secure SHell) principalmente terminal remoto, aunque en realidad cifra casi cualquier tipo de transmisión.
- Telnet otro terminal remoto, ha caído en desuso por su inseguridad intrínseca, ya que las claves viajan sin cifrar por la red.

Hay otros protocolos de nivel de aplicación que facilitan el uso y administración de la red:

- SNMP (Simple Network Management Protocol)
- DNS (Domain Name System)

## Unidades de datos

El intercambio de información entre dos capas OSI consiste en que cada capa en el sistema fuente la agrega información de control a los datos, y cada capa en el sistema de destino analiza y remueve la información de control de los datos como sigue:

Si un ordenador (host A) desea enviar datos a otro (host B), en primer término los datos deben empaquetarse a través de un proceso denominado encapsulamiento, es decir, a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados, información final y otros tipos de información.

N-PDU (Unidad de datos de servicio)

Es la información intercambiada entre entidades pares utilizando una conexión(N-1).
Esta compuesta por:
N-SDU (Unidad de datos del servicio)
Son los datos que se necesitan la entidades(N) para realizar funciones del servicio pedido por la entidad(N+1).
N-PCI (Información de control del protocolo)
Información intercambiada entre entidades (N) utilizando una conexión (N-1) para coordinar su operación conjunta.

N-IDU (Unidad de datos del interface)

Es la información transferida entre dos niveles adyacentes.
Esta compuesta por:
N-ICI (Información de control del interface)
Información intercambiada entre una entidad (N+1) y una entidad (N) para coordinar su operación conjunta.
Datos de Interface-(N)
Información transferida ente una entidad-(N+1) y una entidad-(N) y que normalmente coincide con la (N+1)-PDU.

## Transmisión de los datos

La capa de aplicación recibe el mensaje del usuario y le añade una cabecera constituyendo así la PDU de la capa de aplicación. La PDU se transfiere a la capa de aplicación del nodo destino, este elimina la cabecera y entrega el mensaje al usuario.

Para ello ha sido necesario todo este proceso:

1-Ahora hay que entregar la PDU a la capa de presentación para ello hay que añadirla la correspondiente cabecera ICI y transformarla así en una IDU, la cual se transmite a dicha capa.

2-La capa de presentación recibe la IDU, le quita la cabecera y extrae la información, es decir, la SDU, a esta le añade su propia cabecera (PCI) constituyendo así la PDU de la capa de presentación.

3- Esta PDU es transferida a su vez a la capa de sesión mediante el mismo proceso, repitiéndose así para todas las capas.

4-Al llegar al nivel físico se envían los datos que son recibidos por la capa física del receptor.

5-Cada capa del receptor se ocupa de extraer la cabecera, que anteriormente había añadido su capa homóloga, interpretarla y entregar la PDU a la capa superior.

6-Finalmente llegará a la capa de aplicación la cual entregará el mensaje al usuario.

## Formato de los datos

Estos datos reciben una serie de nombres y formatos específicos en función de la capa en la que se encuentren, debido a como se describió anteriormente la adhesión de una serie de encabezados e información final. Los formatos de información son los siguientes:

APDU

Unidad de datos en la Capa de aplicación.

PPDU

Unidad de datos en la Capa de presentación.

SPDU

Unidad de datos en la capa de sesión.

TPDU

Unidad de datos en la capa de transporte.

Paquete

Unidad de datos en el Nivel de red.

Trama

Unidad de datos en la capa de enlace.

Bits

Unidad de datos en la capa física.

Operaciones sobre los datos

En determinadas situaciones es necesario realizar una serie de operaciones sobre las PDU para facilitar su transporte, bien debido a que son demasiado grandes o bien porque son demasiado pequeñas y estaríamos desaprovechando la capacidad del enlace.

SEGMENTACIÓN Y REENSAMBLAJE

Hace corresponder a una (N)-SDU sobre varias (N)-PDU.

El reensamblaje hace corresponder a varias (N)-PDUs en una (N)-SDU.

BLOQUEO Y DESBLOQUEO

El bloqueo hace corresponder varias (N)-SDUs en una (N)-PDU.

El desbloqueo identifica varias (N)-SDUs que están contenidas en una (N)-PDU.

CONCATENACIÓN Y SEPARACIÓN

La concatenación es una función-(N) que realiza el nivel-(N) y que hace corresponder varias (N)-PDUs en una sola (N-1)-SDU.

La separación identifica varias (N)-PDUs que están contenidas en una sola (N-1)-SDU.

## 2. FAMILIA DE PROTOCOLOS DE INTERNET

La familia de protocolos de Internet es un conjunto de protocolos de red que implementa la pila de protocolos en la que se basa Internet y que permiten la transmisión de datos entre redes de computadoras. En ocasiones se la denomina *conjunto de protocolos TCP/IP*, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse, y que son los más utilizados de la familia. Existen tantos protocolos en este conjunto que llegan a ser más de 100 diferentes, entre ellos se encuentra el popular HTTP (HyperText Transfer Protocol), que es el que se utiliza para acceder a las páginas web, además de otros como el ARP (Address Resolution Protocol) para la resolución de direcciones, el FTP (File Transfer Protocol) para transferencia de archivos, y el SMTP (Simple Mail Transfer Protocol) y el POP (Post Office Protocol) para correo electrónico, TELNET para acceder a equipos remotos, entre otros.

El TCP/IP es la base de Internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN). TCP/IP fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en ARPANET, una red de área extensa del departamento de defensa.

La familia de protocolos de internet puede describirse por analogía con el modelo OSI, que describe los niveles o capas de la pila de protocolos, aunque en la práctica no corresponde exactamente con el modelo en Internet. En una pila de protocolos, cada nivel soluciona una serie de problemas relacionados con la transmisión de datos, y proporciona un servicio bien definido a los niveles más altos. Los niveles superiores son los más cercanos al usuario y tratan con datos más abstractos, dejando a los niveles más bajos la labor de traducir los datos de forma que sean físicamente manipulables.

El modelo de Internet fue diseñado como la solución a un problema práctico de ingeniería. El modelo OSI, en cambio, fue propuesto como una aproximación teórica y también como una primera fase en la evolución de las redes de ordenadores. Por lo tanto, el modelo OSI es más fácil de entender, pero el modelo TCP/IP es el que realmente se usa. Sirve de ayuda entender el modelo OSI antes de conocer TCP/IP, ya que se aplican los mismos principios, pero son más fáciles de entender en el modelo OSI.

Niveles en la pila TCP/IP

Hay algunas discusiones sobre como encaja el modelo TCP/IP dentro del modelo OSI. Como TCP/IP y OSI no están delimitados con precisión no hay una respuesta que sea la correcta.

El modelo OSI no está lo suficientemente dotado en los niveles inferiores como para detallar la auténtica estratificación en niveles: necesitaría tener una capa extra (el nivel de Interred) entre los niveles de transporte y red. Protocolos específicos de un tipo concreto de red, que se sitúan por encima del marco de hardware básico, pertenecen al nivel de red, pero sin serlo. Ejemplos de estos protocolos son el ARP (Protocolo de resolución de direcciones) y el STP (Spanning Tree Protocol). De todas formas, estos son protocolos locales, y trabajan por debajo de las capas de Intered. Cierto es que situar ambos grupos (sin mencionar los protocolos que forman parte del nivel de Interred pero se sitúan por encima de los protocolos de Interred, como ICMP) todos en la misma capa puede producir confusión, pero el modelo OSI no llega a ese nivel de complejidad para ser más útil como modelo de referencia.

El siguiente diagrama intenta mostrar la pila TCP/IP y otros protocolos relacionados con el modelo OSI original:

| | | |
|---|---|---|
| 7 | Aplicación | ej. HTTP, DNS, SMTP, SNMP, FTP, Telnet, SSH y SCP, NFS, RTSP, Feed, Webcal |
| 6 | Presentación | ej. XDR, ASN.1, SMB, AFP |
| 5 | Sesión | ej. TLS, SSH, ISO 8327 / CCITT X.225, RPC, NetBIOS |
| 4 | Transporte | ej. TCP, UDP, RTP, SCTP, SPX |
| 3 | Red | ej. IP, ICMP, IGMP, X.25, CLNP, ARP, RARP, BGP, OSPF, RIP, IGRP, EIGRP, IPX, DDP |
| 2 | Enlace de datos | ej. Ethernet, Token Ring, PPP, HDLC, Frame Relay, RDSI, ATM, IEEE 802.11, FDDI |
| 1 | Físico | ej. cable, radio, fibra óptica |

Normalmente, los tres niveles superiores del modelo OSI (Aplicación, Presentación y Sesión) son considerados simplemente como el nivel de aplicación en el conjunto TCP/IP. Como TCP/IP no tiene un nivel de sesión unificado sobre el que los niveles superiores se sostengan, estas funciones son típicamente desempeñadas (o ignoradas) por las aplicaciones de usuario. La diferencia más notable entre los modelos de TCP/IP y OSI es el nivel de Aplicación, en TCP/IP se integran algunos niveles del modelo OSI en su nivel de Aplicación. Una interpretación simplificada de la pila se muestra debajo:

| | | |
|---|---|---|
| 5 | Aplicación | ej. HTTP, FTP, DNS *(protocolos de enrutamiento como BGP y RIP, que por varias razones funcionen sobre TCP y UDP respectivamente, son considerados parte del nivel de red)* |
| 4 | Transporte | ej. TCP, UDP, RTP, SCTP *(protocolos de enrutamiento como OSPF, que funcionen sobre IP, son considerados parte del nivel de red)* |
| 3 | Interred | Para TCP/IP este es el Protocolo de Internet (IP) *(protocolos requeridos como ICMP e IGMP funcionan sobre IP, pero todavía se pueden considerar parte del nivel de red; ARP no funciona sobre IP* |
| 2 | Enlace | ej. Ethernet, Token Ring, etc. |
| 1 | Físico | ej. medio físico, y técnicas de codificación, T1, E1 |

**El nivel Físico**

El nivel físico describe las características físicas de la comunicación, como las convenciones sobre la naturaleza del medio usado para la comunicación (como las comunicaciones por cable, fibra óptica o radio), y todo lo relativo a los detalles como los conectores, código de canales y modulación, potencias de señal, longitudes de onda, sincronización y temporización y distancias máximas. La familia de protocolos de Internet no cubre el nivel físico de ninguna red; véanse los artículos de tecnologías específicas de red para los detalles del nivel físico de cada tecnología particular.

**El nivel de Enlace de datos**

El nivel de enlace de datos especifica como son transportados los paquetes sobre el nivel físico, incluido los delimitadores (patrones de bits concretos que marcan el comienzo y el fin de cada trama). Ethernet, por ejemplo, incluye campos en la cabecera de la trama que especifican que máquina o máquinas de la red son las destinatarias de la trama. Ejemplos de protocolos de nivel de red de datos son Ethernet, Wireless Ethernet, SLIP, Token Ring y ATM.

PPP es un poco más complejo y originalmente fue diseñado como un protocolo separado que funcionaba sobre otro nivel de enlace, HDLC/SDLC.

Este nivel es a veces subdividido en Control de enlace lógico (Logical Link Control) y Control de acceso al medio (Media Access Control).

**El nivel de Interred**

Como fue definido originalmente, el nivel de red soluciona el problema de conseguir transportar paquetes a través de una red sencilla. Ejemplos de protocolos son X.25 y *Host/IMP Protocol* de ARPANET.

Con la llegada del concepto de Interred, nuevas funcionalidades fueron añadidas a este nivel, basadas en el intercambio de datos entre una red origen y una red destino. Generalmente esto incluye un enrutamiento de paquetes a través de una red de redes, conocida como Internet.

En la familia de protocolos de Internet, IP realiza las tareas básicas para conseguir transportar datos desde un origen a un destino. IP puede pasar los datos a una serie de protocolos superiores; cada uno de esos protocolos es identificado con un único "Número de protocolo IP". ICMP y IGMP son los protocolos 1 y 2, respectivamente.

Algunos de los protocolos por encima de IP como ICMP (usado para transmitir información de diagnóstico sobre transmisiones IP) e IGMP (usado para dirigir tráfico multicast) van en niveles superiores a IP pero realizan funciones del nivel de red e ilustran una incompatibilidad entre los modelos de Internet y OSI. Todos los protocolos de enrutamiento, como BGP, OSPF, y RIP son realmente también parte del nivel de red, aunque ellos parecen pertenecer a niveles más altos en la pila.

**El nivel de Transporte**

Los protocolos del nivel de transporte pueden solucionar problemas como la fiabilidad ("¿alcanzan los datos su destino?") y la seguridad de que los datos llegan en el orden correcto. En el conjunto de protocolos TCP/IP, los protocolos de transporte también determinan a que aplicación van destinados los datos.

Los protocolos de enrutamiento dinámico que técnicamente encajan en el conjunto de protocolos TCP/IP (ya que funcionan sobre IP) son generalmente considerados parte del nivel de red; un ejemplo es OSPF (protocolo IP número 89).

TCP (protocolo IP número 6) es un mecanismo de transporte fiable y orientado a conexión, que proporciona un flujo fiable de bytes, que asegura que los datos llegan completos, sin daños y en orden. TCP realiza continuamente medidas sobre el estado de la red para evitar sobrecargarla con demasiado tráfico. Además, TCP trata de enviar todos los datos correctamente en la secuencia especificada. Esta es una de las principales diferencias con UDP, y puede convertirse en una desventaja en flujos en tiempo real (muy sensibles a la variación del retardo) o aplicaciones de enrutamiento con porcentajes altos de pérdida en el nivel de interred.

Más reciente es SCTP, también un mecanismo fiable y orientado a conexión. Está relacionado con la orientación a byte, y proporciona múltiples sub-flujos multiplexados sobre la misma conexión. También proporciona soporte de *multihoming*, donde una conexión puede ser representada por múltiples direcciones IP (representando múltiples interfaces físicas), así si una falla la conexión no se interrumpe. Fue desarrollado inicialmente para aplicaciones telefónicas (para transportar SS7 sobre IP), pero también fue usado para otras aplicaciones.

UDP (protocolo IP número 17) es un protocolo de datagramas sin conexión. Es un protocolo no fiable (*best effort* al igual que IP) - no porque sea particularmente malo, sino porque no verifica que los paquetes lleguen a su destino, y no da garantías de que lleguen en orden. Si una aplicación requiere estas características, debe llevarlas a cabo por sí misma o usar TCP.

UDP es usado normalmente para aplicaciones de streaming (audio, video, etc) donde la llegada a tiempo de los paquetes es más importante que la fiabilidad, o para aplicaciones simples de tipo petición/respuesta como el servicio DNS, donde la sobrecarga de las cabeceras que aportan la fiabilidad es desproporcionada para el tamaño de los paquetes.

DCCP está actualmente bajo desarrollo por el IETF. Proporciona semántica de control para flujos TCP, mientras de cara al usuario se da un servicio de datagramas UDP..

TCP y UDP son usados para dar servicio a una serie de aplicaciones de alto nivel. Las aplicaciones con una dirección de red dada son distinguibles entre sí por su número de puerto TCP o UDP. Por convención, los puertos bien conocidos (*well-known ports*) son asociados con aplicaciones específicas.

RTP es un protocolo de datagramas que ha sido diseñado para datos en tiempo real como el streaming de audio y video que se monta sobre UDP.

**El nivel de Aplicación**

El nivel de aplicación es el nivel que los programas más comunes utilizan para comunicarse a través de una red con otros programas. Los procesos que acontecen en este nivel son aplicaciones específicas que pasan los datos al nivel de aplicación en el formato que internamente use el programa y es codificado de acuerdo con un protocolo estándar.

Algunos programas específicos se considera que se ejecutan en este nivel. Proporcionan servicios que directamente trabajan con las aplicaciones de usuario. Estos programas y sus correspondientes protocolos incluyen a HTTP (*HyperText Transfer Protocol*), FTP (Transferencia de archivos), SMTP (correo electrónico), SSH (login remoto seguro), DNS (Resolución de nombres de dominio) y a muchos otros.

Una vez que los datos de la aplicación han sido codificados en un protocolo estándar del nivel de aplicación son pasados *hacia abajo* al siguiente nivel de la pila de protocolos TCP/IP.

En el nivel de transporte, las aplicaciones normalmente hacen uso de TCP y UDP, y son habitualmente asociados a un número de puerto bien conocido (*well-known port*). Los puertos fueron asignados originalmente por la IANA.

**Ventajas e inconvenientes**

El conjunto TCP/IP está diseñado para enrutar y tiene un grado muy elevado de fiabilidad, es adecuado para redes grandes y medianas, así como en redes empresariales. Se utiliza a nivel mundial para conectarse a Internet y a los servidores web. Es compatible con las herramientas estándar para analizar el funcionamiento de la red.

Un inconveniente de TCP/IP es que es más difícil de configurar y de mantener que NetBEUI o IPX/SPX; además es algo más lento en redes con un volumen de tráfico medio bajo. Sin embargo, puede ser más rápido en redes con un volumen de tráfico grande donde haya que enrutar un gran número de tramas.

El conjunto TCP/IP se utiliza tanto en redes empresariales como por ejemplo en campus universitarios o en complejos empresariales, en donde utilizan muchos enrutadores y conexiones a mainframe o a ordenadores UNIX, como así también en redes pequeñas o domésticas, y hasta en teléfonos móviles y en domótica.

# Realización de cables y verificación para LAN´s

## 1. SISTEMAS DE CABLEADO ESTRUCTURADO

### Introducción

Tradicionalmente hemos visto que a los edificios se les ha ido dotando distintos servicios de mayor o menor nivel tecnológico. Así se les ha dotado de calefacción, aire acondicionado, suministro eléctrico, megafonía, seguridad, etc, características que no implican dificultad, y que permiten obtener un edificio automatizado.

Cuando a estos edificios se les dota de un sistema de gestión centralizado, con posibilidad de interconexión entre ellos, y se le otra de una infraestructura de comunicaciones (voz, datos, textos, imágenes), empezamos a hablar de edificios inteligentes o racionalizados.

El desarrollo actual de las comunicaciones, vídeo conferencia, telefax, servicios multimedia, redes de ordenadores, hace necesario el empleo de un sistema de cableado estructurado avanzado capaz de soportar todas las necesidades de comunicación.

Estas tecnologías se están utilizando en: Hospitales, Hoteles, Recintos feriales y de exposiciones, áreas comerciales, edificios industriales, viviendas, etc.

### Ventajas

En la actualidad, numerosas empresas poseen una infraestructura de voz y datos principalmente, disgregada, según las diferentes aplicaciones y entornos y dependiendo de las modificaciones y ampliaciones que se ha ido realizando. Por ello es posible que coexistan multitud de hilos, cada uno para su aplicación, y algunos en desuso después de las reformas. Esto pone a los responsables de mantenimiento en serios apuros cada vez que se quiere ampliar las líneas o es necesario su reparación o revisión.

Todo ello se puede resumir en los siguientes puntos:

Convivencia de cable de varios tipos diferentes, telefónico, coaxial, pares apantallados, pares si apantallar con diferente número de conductores, etc.

Deficiente o nulo etiquetado del cable, lo que impide su uso para una nueva función incluso dentro del mismo sistema.

Imposibilidad de aprovechar el mismo tipo de cable para equipos diferentes.

Peligro de interferencias, averías y daños personales, al convivir en muchos casos los cables de transmisión con los de suministro eléctrico.

Coexistencia de diferentes tipos de conectores.

Trazados diversos de los cables a través del edificio. Según el tipo de conexión hay fabricantes que eligen la estrella, otros el bus, el anillo o diferentes combinaciones de estas topologías.

Posibilidad de accidentes. En diversos casos la acumulación de cables en el falso techo ha provocado su derrumbamiento.

Recableado por cada traslado de un terminal, con el subsiguiente coste de materiales y sobre todo de mano de obra.

Nuevo recableado al efectuar un cambio de equipo informático o telefónico.

Saturación de conducciones.

Dificultades en el mantenimiento en trazados y accesibilidad de los mismos.

Ante esta problemática parece imposible encontrar una solución que satisfaga los requerimientos técnicos de los fabricantes y las necesidades actuales y futuras de los mismos.

Sin embargo entran en juego varios factores que permiten modificar este panorama:

Tendencia a la estandarización de Interfases por parte de gran número de fabricantes.

Estándares internacionalmente reconocidos para RDSI (Red Digital de Servicios Integrados).

Evolución de grandes sistemas informáticos hacia sistemas distribuidos y redes locales.

Generalización del PC o compatible en el puesto de trabajo como terminal conectado a una red.

Tecnologías de fabricación de cables de cobre de alta calidad que permite mayores velocidades y distancias.

Aparición de la fibra óptica y progresivo abaratamiento del coste de la electrónica asociada.

Además de todo ello algunas compañías han tenido la iniciativa de racionalizar dichos sistemas, así como dar soluciones comunes.

## Aplicaciones

Las técnicas de cableado estructurado se aplican en:

Edificios donde la densidad de puestos informáticos y teléfonos es muy alta: oficinas, centros de enseñanza, tiendas, etc.

Donde se necesite gran calidad de conexionado así como una rápida y efectiva gestión de la red: Hospitales, Fábricas automatizadas, Centros Oficiales, edificios alquilados por plantas, aeropuertos, terminales y estaciones de autobuses, etc.

Donde a las instalaciones se les exija fiabilidad debido a condiciones extremas: barcos, aviones, estructuras móviles, fábricas que exijan mayor seguridad ante agentes externos.

## Topología

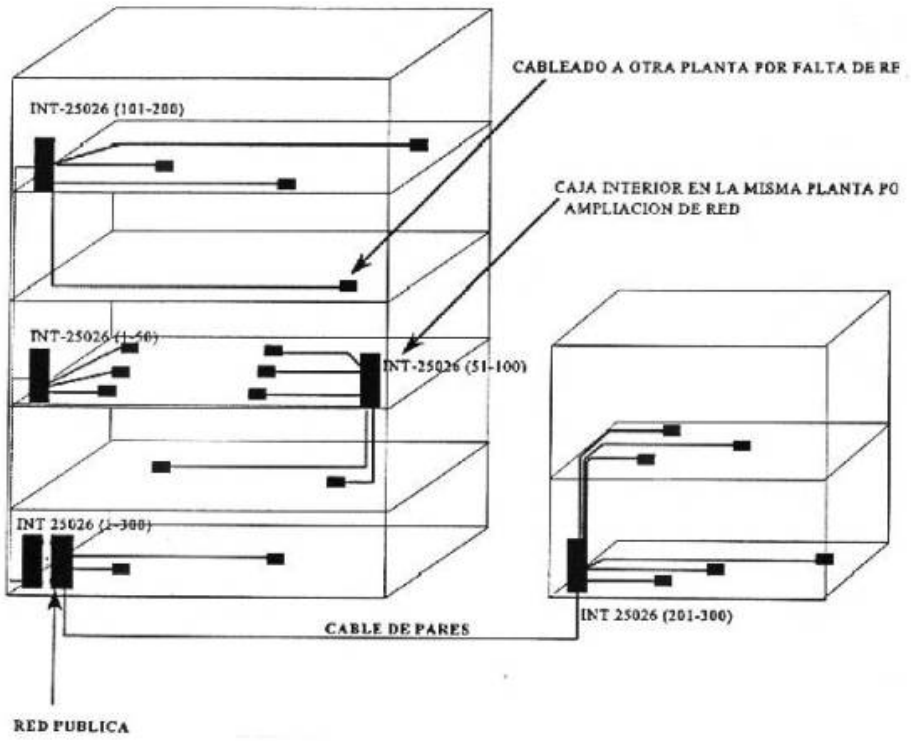
Para ver las diferencias entre redes estructuradas y las redes convencionales comentaremos ambas:

**Redes convencionales**

Como se puede observar en la figura en las redes interiores actuales, el diseño de la red se hace al construir el edificio y según hagan falta modificaciones se harán colocando cajas interiores, según lo crea oportuno el proyectista y sin ninguna estructura definida. Todo ello tiene el inconveniente de que no siempre tenemos una caja cerca y el cableado hasta la caja, cada instalador la hace por donde lo cree más conveniente, teniendo así el edificio infinidad de diferentes trazados para el cableado.

Además de todo ello para cada traslado de un solo teléfono tenemos que recablear de nuevo y normalmente dejar el cable que se da de baja sin desmontar, siendo este inutilizable de nuevo muchas veces por no saber *y* otras por la incompatibilidad de distintos sistemas con un cable.

Pero el mayor problema lo encontramos cuando queremos integrar varios sistemas en el mismo edificio. En este caso tendremos además de la red telefónica la red informática así como la de seguridad o de control de servicios técnicos. Todo ello con el gran inconveniente de no poder usar el mismo cable para varios sistemas distintos bien por interferencias entre los mismos o bien por no saber utilizarlo los instaladores. Los cables están por lo general sin identificar y sin etiquetar.



**Desventajas**

Diferentes trazados de cableado.

Reinstalación para cada traslado.

Cable viejo acumulado y no reutilizable.

Incompatibilidad de sistemas.

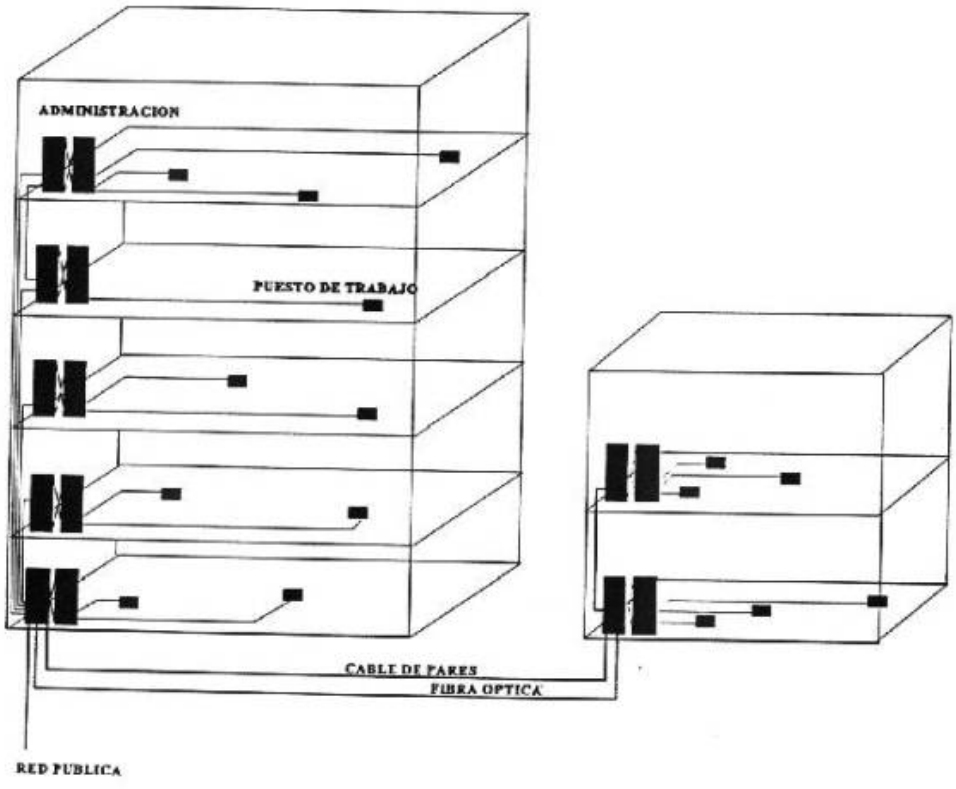
Interferencias por los distintos tipos de cables.

Mayor dificultad para localización de averías.

## Redes estructuradas

A diferencia de una red convencional, en el cableado estructurado, como su mismo nombre indica, la red se estructura (o divide en tramos), para estudiar cada tramo por separado y dar soluciones a cada tramo independientemente sin que se afecten entre sí.

En el tipo de cableado estructurado se han dado solución a muchos de los problemas citados en el apartado anterior, como por ejemplo el poder reutilizar el cable para distintos sistemas así como poder compartirlo entre si sin interferencias. También tenemos que al tratarse de un mismo tipo de cable se instala todo por el mismo trazado (dentro de lo posible) no hace falta una nueva instalación para efectuar un traslado de equipo, siempre que se haya sobredimensionado bien la red, lo cual trae como consecuencia que no existan cables viejos inutilizables.



**Ventajas**

Trazados homogéneos.

Fácil traslados de equipos.

Convivencia de distintos sistemas sobre el mismo soporte físico.

Transmisión a altas velocidades para redes.

Mantenimiento mucho más rápido y sencillo.

## Conceptos básicos sobre categorías

En los sistemas de cableado estructurado, entran en juego nuevos conceptos que antes no se daban. Para entenderlo, pondremos un ejemplo.

No podremos reutilizar la línea existente entre dos teléfonos para una conexión punto a punto entre dos ordenadores, debido a que no sabemos las características de los cables montados y además, si quisiéramos medirlas, nos saldría más caro ( en tiempo y equipo necesario para cada tipo de cable).

Por ello aparece el concepto de Categoría. Esto significa predefinir varios anchos de banda, y darles a cada una un nombre.

| CATEGORÍA | VELOCIDAD MÁXIMA | DISTANCIA MÁXIMA |
|---|---|---|
| 3 | 10Mbps | 100 m |
| 4 | 20 Mbps | 100 m |
| 5 | 100Mbps | 100 m |

Lo que esta tabla quiere decir es que por ejemplo para una categoría 3 la velocidad máxima de transmisión por ella es de 10 Mbps a una distancia de 100 m. Como se puede observar lo que se vende a los clientes es una velocidad máxima de transmisión a una distancia máxima, pero en esto hay que hacer una salvedad, como siempre en una línea si la velocidad de transmisión la bajamos por supuesto la distancia donde llega la señal aumentará. De todas formas todo ello tendría que ser calculado por el técnico que diseñe la red, quién será el que determinará la distancia máxima (en la práctica). No olvidemos que la tabla es el estándar definido internacionalmente y es lo que en los folletos comerciales se les ofrece a los clientes.

Las categorías inferiores no se tratan porque son de características de muy baja calidad para el mercado actual por lo que no se venden.

Debido a las tecnologías de fabricación se pueden conseguir pares sin apantallar para estas velocidades de transmisión. Estos cables se pueden conseguir debido a la calidad del cobre y del trenzado que se construyen mediante tecnología láser.

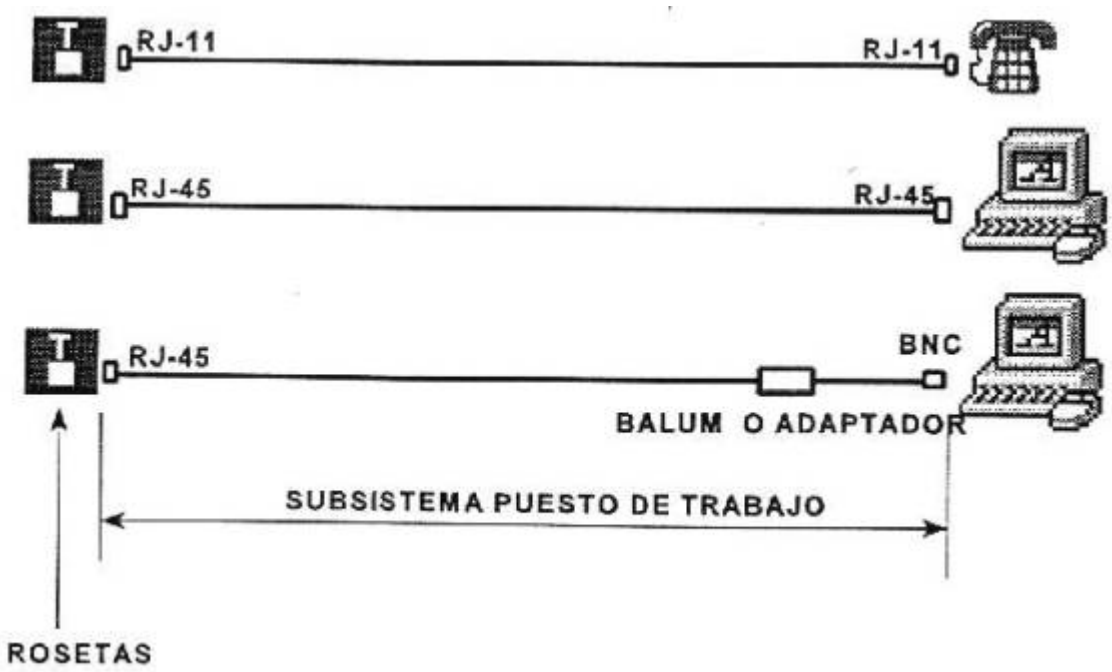
## 2. COMPONENTES DE UN SISTEMA

En conjunto, a todo el cableado de un edificio se llama SISTEMA y a cada parte en la que se subdivide se llama SUBSISTEMA. Se llama estructurado porque obedece a esta estructura definida.

Existen varios tipos de cableado estructurados según la aplicación en que se usen, aunque por lo general se les denomina a todas P.D.S. Las variaciones de unas a otras son, el tipo de componentes utilizados según el ambiente donde se usen, como por ejemplo cables y elementos especiales para ambientes ácidos o húmedos.

Los componentes de un sistema son:

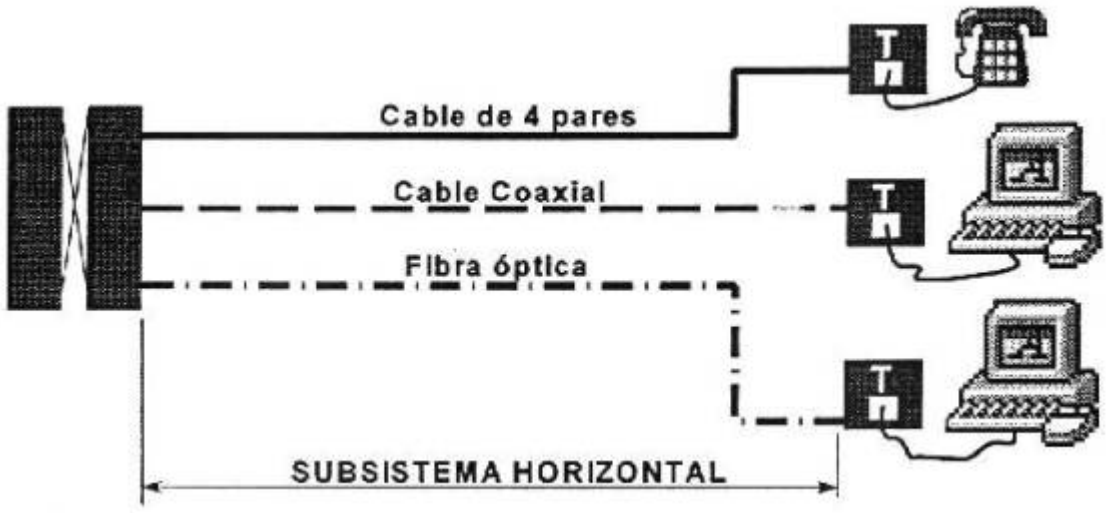
Puesto de Trabajo.- Son los elementos que conectan la toma de usuario al terminal telefónico o de datos. Puede ser un simple cable con los conectores adecuados o un adaptador par convertir o amplificar la señal.




Horizontal.- Este subsistema comprende el conjunto de medios de transmisión (cables, fibras, coaxiales, etc) que unen los puntos de distribución de planta con el conector o conectores del puesto de trabajo.
Ésta es una de las partes más importantes a la hora del diseño debido a la distribución de los puntos de conexión en la planta, que no se parece a una red convencional.

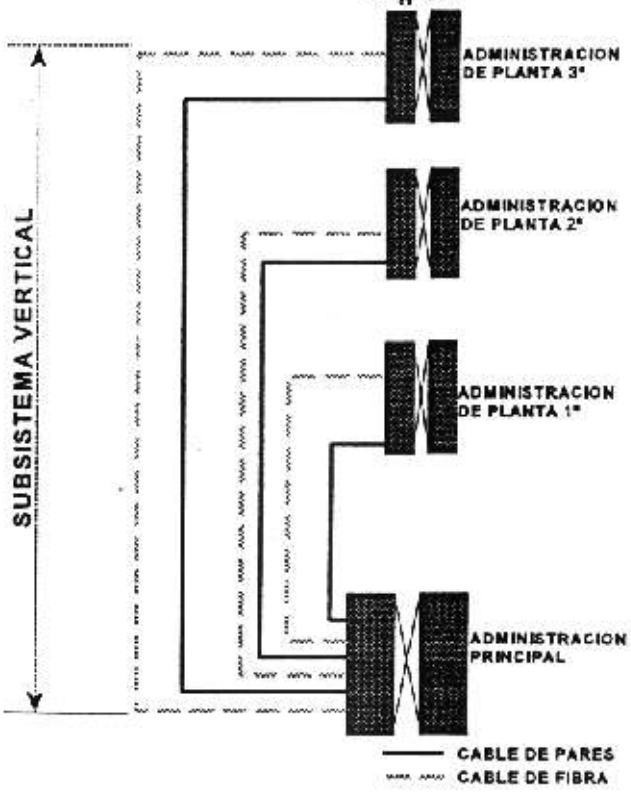
En una red convencional los puntos de conexión los colocamos donde el cliente nos dice en el momento de la instalación del equipo y cableamos por donde mejor nos conviene. El cableado estructurado no se monta en el momento de la instalación del equipo, sino que se hace un proyecto de ingeniería sobre el edificio y se estudian de antemano donde se pondrán las tomas.

Por ello, la distribución que se aconseja e por metros cuadrados, siendo la densidad aconsejada 2 tomas cada 5 u 6 $m^2$ .




Vertical.-

*Subsistema Vertical*
*Fig 2.3*




Está constituido por el conjunto de cables que interconectan las diferentes planta y zonas ente los puntos de distribución y administración (llamado también troncal).

Administración (Repartidores).-

Son los puntos de distribución o repartidores donde se interconectan los diferentes subsistemas. Mediante la unión con puentes móviles, es posible configurar la conexión entre dos subsistemas, dotando al conjunto de una gran capacidad de asignación y modificación de los conductores. Este subsistema se divide en dos:

<u>Administración principal.-</u>

Éste subsistema sería el repartidor principal del edificio en cuestión, que normalmente está ubicado en el sótano o planta baja y es donde suele llegar el cable de la red pública ay donde se instalan la centralita y todos los equipos servidores.

Administración de planta.- Los componen los pequeños repartidores que se ubican por las distintas plantas del edificio.

Campus (entre edificios diferentes).-

Lo forman los elementos de interconexión entre un grupo de edificios que posean una infraestructura común (fibras ópticas, cables de pares, sistemas de radioenlace, etc.

Sala de equipos.-

Este subsistema lo constituye el conjunto de conexiones que se realizan entre el o los repartidores principales y el equipamiento común como puede se la centralita, ordenadores centrales, equipos de seguridad, etc. Ubicados todos en esta sala común.

## FÍSICA DEL SISTEMA

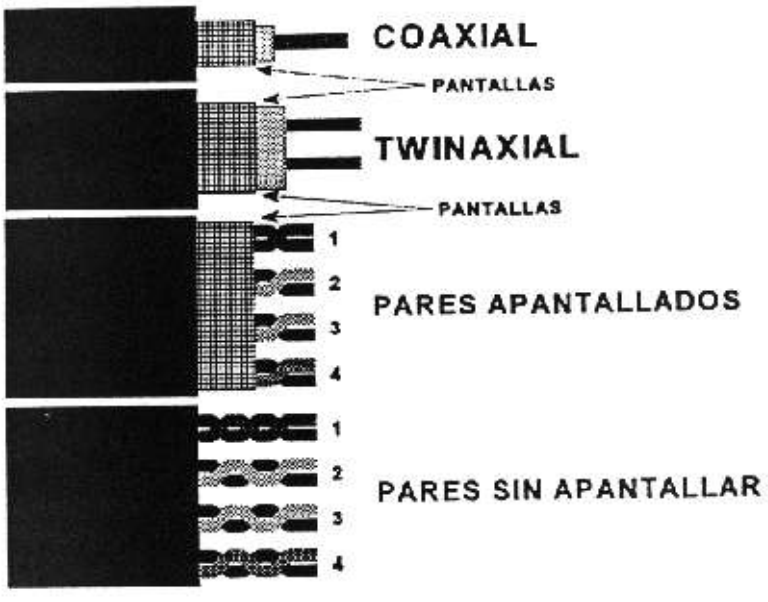
Ahora estudiaremos los distintos componentes de cada subsistema.

Horizontal.-

En la figura podemos observar lo que incluye el subsistema horizontal desde el repartidor de planta hasta la roseta o conector de puesto de trabajo. Esta es una de las partes más importantes.

Ya que en el 99% de las instalaciones se montará pares trenzados sin apantallar, es por ello que se estudiará este tipo de instalaciones principalmente.

Tendremos en cuenta que las tendencias del mercado es a la instalaciones de RDSI (ó ADSL) en la actualidad, lo que quiere decir que se tiende al RJ-45 y por lo tanto el tipo de cable usado tiene que ser de 8 hilos (4 pares), pudiéndose alcanzar velocidades de 100 MHz.




Cables.- Para el cableado de los puestos de trabajo se usará cable de 4 pares sin apantallar, preferiblemente el de categoría 5, pues su precio que muy económico nos lo permite.

Estos cables constan de unos hilos perfectamente identificables con colores, y bajo ningún concepto se cambiará el orden de cableado de estos hilos.

Conectores RJ.- El conector RJ se ha diseñado en varios estándares distintos, cada uno con una nomenclatura. Los más usuales son el RJ-11 y RJ-45.

RJ-11.-

Puede albergar como máximo un total de 6 pines, aunque podemos encontrarlo en el mercado con los formatos de 2, 4 ó 6 pines según la aplicación a la cual estén destinados.

RJ-45.-

Puede albergar como máximo un total de 8 pines aunque al igual que el anterior lo podemos encontrar en diferentes formatos según nuestras necesidades. El más usual es el de 8 pines, el cual se usa en el estándar RDSI.

Para manejar estos conectores se usarán herramientas diseñadas para tal efecto, recomendándose una de tipo universal para RJ, que es válida para todo tipo de conectores RJ en el mercado.

Norma de conexión de RJ para P.D.S..-

Para conectar el cable al RJ-45 se hace de la misma manera en todas las instalaciones de P.D.S., ya que esta es una de las normas del cableado estructurado. Como se puede ver hay dos formas de hacerlo, pero se elegirá la forma europea, ya que es el estándar R.D.S.I.

Cada hilo tiene su posición, por lo que las conexiones no se pueden trastocar bajo ningún concepto, ni en caso de avería en el cableado (en tal caso se cambiará la manguera completa, aunque solo tenga mal un par). En el otro extremo se conectará un repartidor (panel de parcheado) y desde éste se gestionará toda la red de puestos de trabajo.

Impedancia característica.-

Es una de las características más importantes de un cable así como para todos los elementos de la red, que indica la resistencia a la corriente alterna entre hilos que ofrece el cable a las distintas frecuencias. En este caso es de 100 □ a 1-16 MHz, variando con la frecuencia.

Atenuación.-

Esta característica nos indica la pérdida en dB/m que tiene el cable que puede estar en 7dB/305 m a una frecuencia de 1MHz y 35 dB/305 m a 16 MHz.

Resistencia a la corriente continua.-

Esto como su nombre indica nos da la resistencia por metros a la c.c. que suele estar alrededor de los 10 / 100 m.

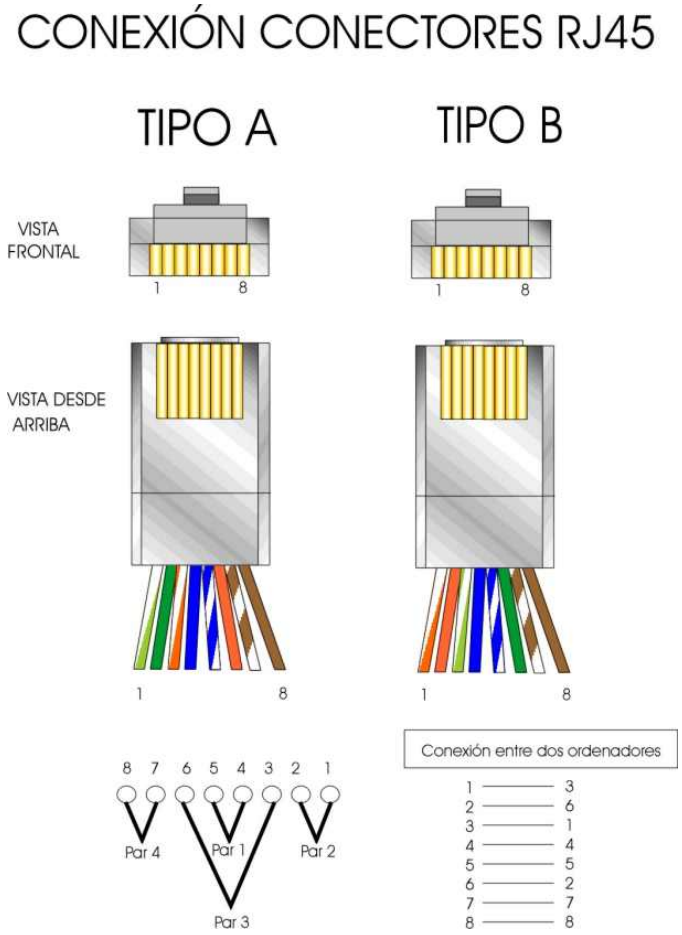
Calculo de una red.-

Para calcular la distancia máxima que podremos dar a una tirada de cable para el horizontal se calculará de la siguiente manera.

Supongamos que queremos montar una red local de las características siguientes:

- Frecuencia de transmisión por la red 100 MHz.
- Nivel de salida de la tarjeta 10 dB.
- Nivel mínimo de entrada –10 dB.

Si usamos un cable que tiene una atenuación de 47,5 dB /305 m entonces aplicando una regla de tres: de 10 dB a –10 dB hay una caída de 20 dB que es lo máximo permitido.




x = 128,4 m es la distancia máx. que permite una tirada.

Administración (Repartidores o paneles de parcheado).-

Para el subsistema de administración se usarán paneles de parcheado para cables de par trenzado sin apantallar o fibra óptica.

Estas regletas puedes ser de 19 ", lo que facilita la instalación en armarios metálicos para tal fin. Estos armarios permiten albergar distintos dispositivos, y los hay de diferentes unidades de altura.

Para realizar las conexiones en los paneles de parcheado se necesita una herramienta de inserción o llave de impacto, que permite introducir el hilo en su alojamiento y seguidamente lo corta.

Se deberán identificar correctamente todos los cables con etiquetadotas especiales.

Será necesario realizar puentes con latiguillos prefabricados con categoría adecuada a la instalación que se lleve a cabo.

Vertical.-

Para este subsistema se emplearán los medios que se han visto para los anteriores, salvo pequeñas modificaciones:

Para circuitos de ancho de banda vocal usaremos hilos de pares de teléfono.

Para uniones de datos entre plantas cercanas sin mucha demanda, cable de categoría.

Cable de fibra óptica par la comunicación de datos entre plantas lejanas o con mucha densidad.

El tipo de fibra óptica que se suele utilizar en redes interiores es fibra multimodo que es más barata y la pérdidas no son muy grandes a ser recorridos cortos.

En los extremos de la fibra se colocarán conectores ST adecuados, y éstos irán a un equipo de comunicaciones, que adaptan la señal eléctrica/óptica. Para enviar varias señales por la fibra óptica se recurrirá a un concentrador. Sin embargo como es un sistema caro, la telefonía se montará sobre los enlaces de pares normales.

En definitiva, entre administradores de distintas plantas montaremos dos sistemas paralelos uno de pares y otro de fibra, así como enlaces con cable o mangueras de categoría 3 ó 5 según nuestras necesidades. Los cables de pares y pares trenzados terminarán en un repartidor o panel de parcheado.

Los cables de fibra óptica terminarán en un repartidor con conectores ST.

Campus (entre edificios diferentes).-

Para este subsistema se utilizarán los mismos medios que en el anterior ya que no habrá grandes distancias entre los distintos edificios, terminando cada fibra y en un repartidor principal así como los pares de cobre para telefonía.

Para este tipo de instalaciones no conviene utilizar ningún tipo de cable apantallado pues las corrientes que se pueden crear entre las tierras de distintos edificios pueden ser bastante fuertes, pudiendo producir más problemas que beneficios.

Puesto de trabajo.-

En este subsistema tendremos que prestar especial atención ya que tendremos que interconectar dos o más sistemas. Así podemos encontrarnos con diferentes sistemas que tengan que convivir con el mismo cable.

Para ello existen soluciones en el mercado, cables RJ45-RJ45, RJ45-BNC, RJ45-RS232, etc.

Los adaptadores pueden ser de dos tipos:

Adaptadores que conectan dos medios balanceados.

RJ45 a RJ45

RJ45 a RS232

Balunes (balun) que adaptan un medio balanceado a otro no balanceado.

RJ45 a BNC

RJ45 a TNC

RJ45 a Twinaxial.

Los conductores balanceados tiene ambos la mismas características eléctricas (pares trenzados) y los no balanceados son diferentes, haciendo normalmente de pantalla eléctrica o masa alguno de los conductores (coaxial).

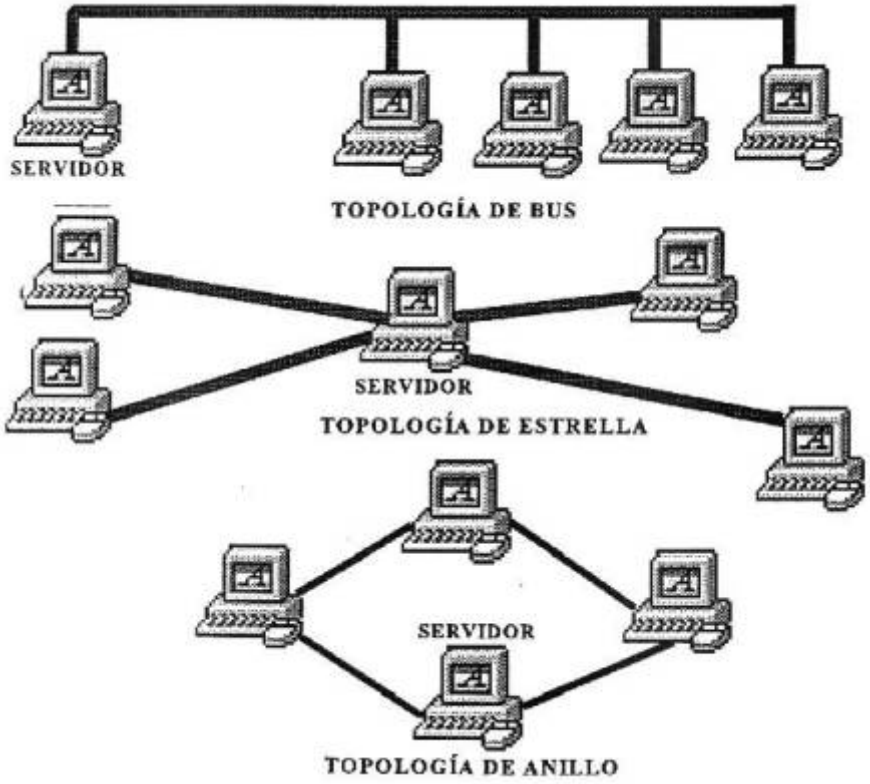
Cuando queremos conectar además de un ordenador un teléfono a la misma toma, existen adaptadores especiales para ello. Tendremos en cuenta que el teléfono viene cableado en los pines 3 y 4 del RJ11 o lo que es lo mismo, en los pines centrales o también en el par 1 del RJ 45. De hecho se puede conectar un macho RJ11 en una base RJ45, y tendremos señal en el teléfono.

## CONEXIÓN DE SISTEMAS

Sistema de telefonía.-

Para esto únicamente tendremos en cuenta que el teléfono utiliza dos hilos de línea coincidentes con el par 1 de P.D.S., y prácticamente puede convivir con casi cualquier tipo de redes.

Redes locales.-




Tenemos básicamente tres tipos de topología de red, que son: en estrella, en BUS, en Anillo, o bien alguna combinación de alguna de ellas.

En los últimos años estamos asistiendo a un auge en el montaje de redes locales, con todas las ventajas que ello conlleva.

Los concentradores se suelen instalar en el RAC 19" de la red P.D.S., debido a su pequeño tamaño y facilita las conexiones.

## 3. INFRAESTRUCTURA NECESARIA PARA LA INSTALACIÓN

CANALIZACIONES DE EDIFICIOS.-

Para La instalación de un sistema de cableado estructurado se puede usar toda la canalización de comunicaciones del edificio, siempre que permita su instalación el diámetro de los conductores. Por esto, es preferible realizar el proyecto del edifico teniendo en cuenta las instalaciones que necesitará en cuanto voz, datos, seguridad de robo e incendios, etc.

Las canalizaciones pueden ser del tipo ackermann (bandeja metálica y registros incrustados bajo el cemento del suelo, tubo corrugado, tubo de PVC, falso techo, falso suelo, etc.

Falso suelo.-

La instalación en este medio es una de las más fáciles ya que sólo tendremos que levantar las baldosas para realizar el tendido del cable y para sacarlo a la superficie, será suficiente con un taladro y si el mecanismo va empotrado hay que mecanizar la baldosa. La ventaja es que no tenemos que usar canalizaciones ni escaleras.

Canalizaciones.-

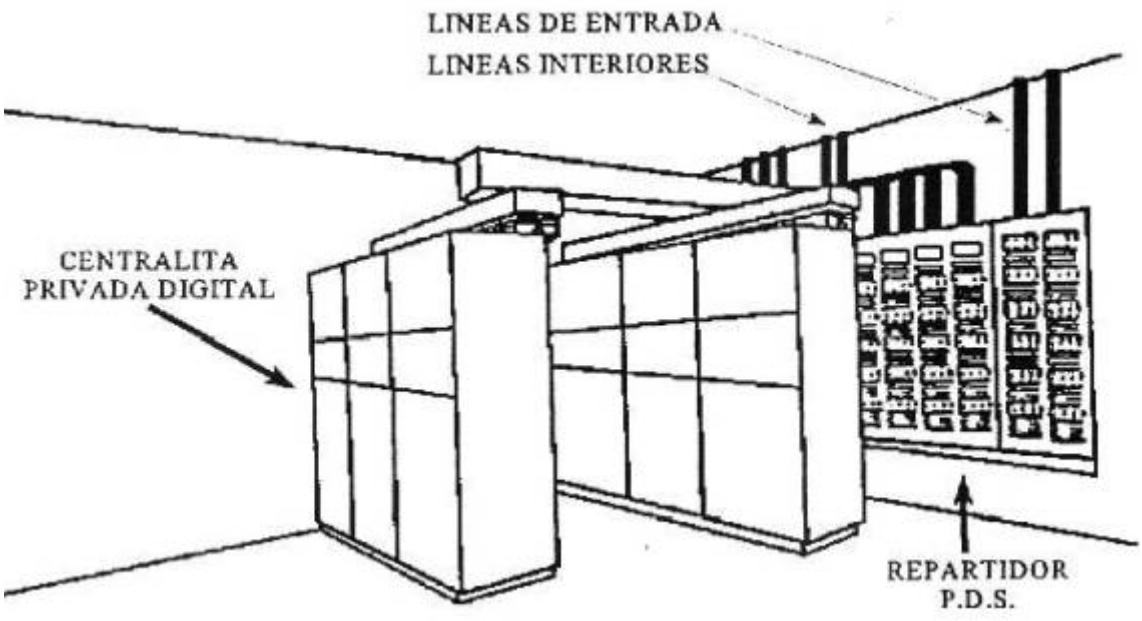
También se puede usar la canalización existente en el edificio para lo cual tiene que tener suficiente sección para albergar las mangueras y repartidores de planta. Esas podrán ir a la altura del suelo, por el rodapié, o por las paredes.

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. Este tipo de columna es aluminio prefabricado y viene con unas guías para su sujeción de mecanismos pero tendremos que mecanizarla (hacer los taladros o ranuras necesarias) para poder instalar los mecanismos.

Sala de equipos.-

En la sala de equipos, donde se encuentra las centrales de abonados así como servidores, se ubicarán todos los elementos necesarios distribuidos sobre una pared, o preferiblemente en un armario o armarios de 19". Se podrán añadir elementos que mejoren el servicio como SAI's, etc.




Repartidores de planta.-

Para ubicar en las distintas planta las regletas de parcheado, se pueden usar cajas metálicas de 19" de superficie o empotradas en la pared. Si la planta es demasiado grande, se pueden colocar concentradores.

# Configuración Redes LAN´S-WAN´s

## 1. ELEMENTOS DE RED

### Switch

Un switch (en castellano "conmutador") es un dispositivo electrónico de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (*Open Systems Interconection*). Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

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 LANs (*Local Area Network*- Red de Área Local).

Interconexión de conmutadores y puentes

Los puentes (bridges) y conmutadores (switches) pueden ser conectados unos a los otros, pero existe una regla que dice que sólo puede existir un único camino entre dos puntos de la red. En caso de que no se siga esta regla, se forma un bucle en la red, lo que tiene como resultado la transmisión infinita de datagramas de una red a otra.

Sin embargo, esos dispositivos utilizan el algoritmo de spanning tree para evitar bucles, haciendo la transmisión de datos de forma segura.

Introducción al funcionamiento de los conmutadores


Conexiones en un *switch* Ethernet

Los conmutadores poseen la capacidad de aprender y almacenar las direcciones de red de nivel 2 (direcciones MAC) de los dispositivos alcanzables a través de cada uno de sus puertos. Por ejemplo, un equipo conectado directamente a un puerto de un conmutador provoca que el conmutador almacene su dirección MAC. Esto permite que, a diferencia de los concentradores o hubs, la información dirigida a un dispositivo se dirija únicamente desde el puerto origen al puerto que permite alcanzar el dispositivo destino. En el caso de conectar dos conmutadores o un conmutador y un concentrador, cada conmutador aprenderá las direcciones MAC de los dispositivos accesibles por sus puertos, por tanto en el puerto de interconexión se almacenan las MAC de los dispositivos del otro conmutador.

Bucles de red e inundaciones de tráfico

Como anteriormente se comentaba, uno de los puntos críticos de estos equipos son los bucles (ciclos) que consisten en habilitar dos caminos diferentes para llegar de un equipo a otro a través de un conjunto de conmutadores. Los bucles se producen porque los conmutadores que detectan que un dispositivo es accesible a través de dos puertos emiten la trama por ambos. Al llegar esta trama al conmutador siguiente, este vuelve a enviar la trama por los puertos que permiten alcanzar el equipo. Este proceso provoca que cada trama se multiplique de forma exponencial, llegando a producir las denominadas inundaciones de la red, provocando en consecuencia el fallo o caída de las comunicaciones.

Como se ha comentado se emplea el protocolo spanning tree para evitar este tipo de fallos.

Conmutadores de nivel 3

Aunque los conmutadores o switches son los elementos que fundamentalmente se encargan de encaminar las tramas de nivel 2 entre los diferentes puertos, existen los denominados conmutadores de nivel 3 o superior, que permiten crear en un mismo dispositivo múltiples redes de nivel 3 (ver VLANs) y encaminar los paquetes (de nivel 3) entre las redes, realizado por tanto las funciones de encaminamiento o routing (ver router).

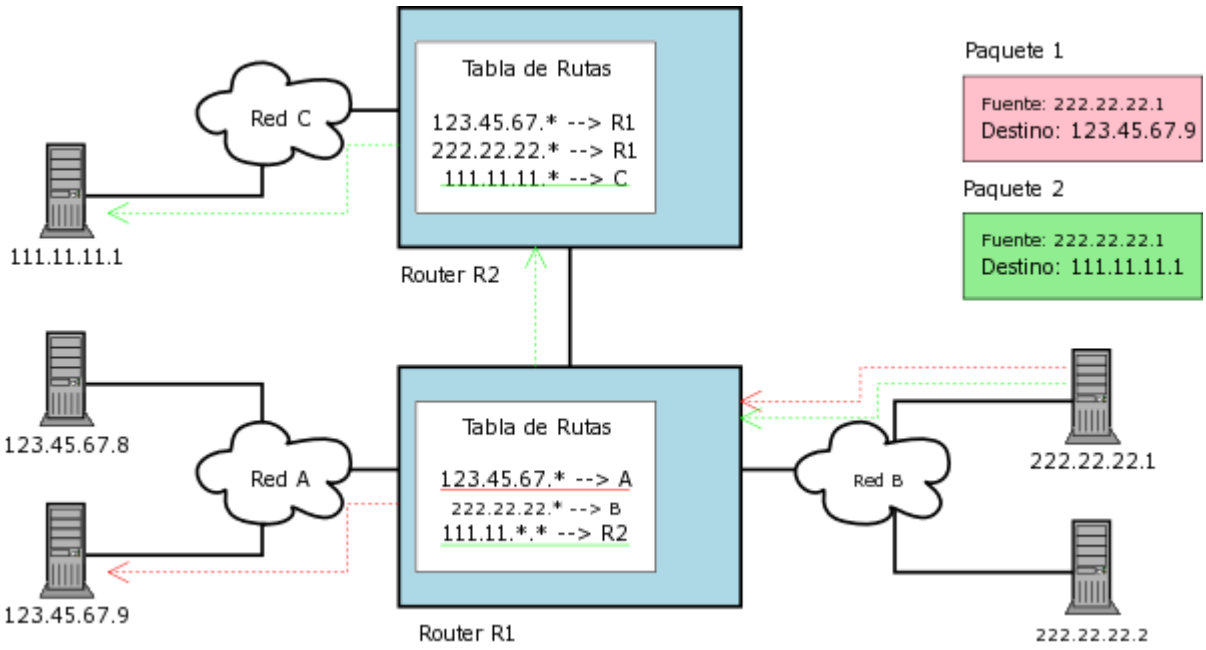
**Router**

Enrutador, encaminador. Dispositivo de hardware o software para interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI.

El router interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

El router toma decisiones basadas en diversos parámetros con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego redirige los paquetes hacia el segmento y el puerto de salida adecuados. Sus decisiones se basan en diversos parámetros. Una de las más importantes es decidir la dirección de la red hacia la que va destinado el paquete (En el caso del protocolo *IP* esta sería la dirección IP). Otras

decisiones son la carga de tráfico de red en las distintas interfaces de red del router y establecer la velocidad de cada uno de ellos, dependiendo del protocolo que se utilice.




En el ejemplo del diagrama, se muestran 3 redes IP interconectadas por 2 routers. La computadora con el IP 222.22.22.1 envía 2 paquetes, uno para la computadora 123.45.67.9 y otro para 111.11.11.1 A través de sus tablas de enrutamiento configurados previamente, los routers pasan los paquetes para la red o router con el rango de direcciones que corresponde al destino del paquete. Nota: el contenido de las tablas de rutas está simplificado por motivos didácticos. En realidad se utilizan máscaras de red para definir las subredes interconectadas.

Los broadcast, o difusiones, se producen cuando una fuente envía datos a todos los dipositivos de una red. En el caso del protocolo IP, una dirección de broadcast es una dirección compuesta exclusivamente por números unos (1) en el campo del host (para la dirección ip en formato binario de modo que para una máscara de red 255.255.255.0 la dirección de broadcast para la dirección 192.168.0.1 seria la 192.168.0.255 o sea xxxxxxxx.xxxxxxxx.xxxxxxxx.11111111).

Los protocolos de enrutamiento son aquellos protocolos que utilizan los routers o encaminadores para comunicarse entre sí y compartir información que les permita tomar la decisión de cual es la ruta más adecuada en cada momento para enviar un paquete. Los protocolos más usados son RIP (v1 y v2), OSPF (v1, v2 y v3), y BGP (v4), que se encargan de gestionar las rutas de una forma dinámica. aunque no es estrictamente necesario que un router haga uso de estos protocolos, pudiéndosele indicar de forma estática las rutas (caminos a seguir) para las distintas subredes que estén conectadas al dispositivo.

Comúnmente los routers se implementan también como puertas de acceso a Internet (por ejemplo un router ADSL), usándose normalmente en casas y oficinas pequeñas. Es correcto utilizar el término router en este caso, ya que estos dispositivos unen dos redes (una red de área local con Internet).

**Enrutador**

Existe la posibilidad de no utilizar equipos dedicados, opción que puede ser la más adecuada para redes locales o redes con un tráfico limitado, y usar software que implemente los protocolos de red antes mencionados. Para dar funcionalidad de router a un PC u otros ordenadores embebidos con sistemas operativos unix-like como pueden ser GNU/Linux o BSD, es suficiente con añadirle al menos dos interfaces de red y activar el soporte de enrutamiento en el kernel. Si se desea propocionarle la funcionalidad de un router completo, y que soporte diversos protocolos de red, se pueden utilizar paquetes como:

- Quagga [1]
- Zebra [2]
- ZebOs

Otra forma de adquirir un router es ya contactando con fabricantes que se dedican a desarrollar su propio software no libre y con su hardware especialmente hecho para tal fin, este es el caso de fabricantes como:

- Cisco Systems
- Juniper Networks

**Routers inalámbricos**

A pesar de que tradicionalmente los routers solían tratar con redes fijas (Ethernet, ADSL, RDSI...), en los últimos tiempos han comenzado a aparecer routers que permiten realizar una interfaz entre redes fijas y móviles (Wi-Fi, GPRS, Edge, UMTS, WiMAX).

## 2. REDES PRIVADAS Y PÚBLICAS

Si tenemos que diseñar una red, lo normal es coger una ip pública, y el resto de la red deberá usar ips privadas.

Clases de redes Privadas

Existen direcciones IP reservadas para redes privadas, para usos internos, que se establecieron por convenio. Estas direcciones no son vistas desde el exterior, no son públicas, y sus rangos son:

- Clase A: 10.0.0.0
- Clase B: 172.16.0.0 a 172.31.0.0
- Clase C: 192.168.X.0 (con X variando).

Valores de las máscaras de subred: subneting

Dado que los bits en la máscara de subred han de ser contiguos, esto reduce la cantidad de máscaras de subred que se pueden crear.

Tabla Binario - Octeto

| BITS DEL OCTETO | DECIMAL |
|---|---|
| 00000000 | 0 |
| 10000000 | 128 |
| 11000000 | 192 |
| 11100000 | 224 |
| 11110000 | 240 |
| 11111000 | 248 |
| 11111100 | 252 |
| 11111110 | 254 |
| 11111111 | 255 |

La máscara por defecto de la clase A es 255.0.0.0

La máscara por defecto de la clase B es 255.255.0.0

La máscara por defecto de la clase C es 255.255.255.0

Una máscara de subred por si sola no nos dice nada. Tiene que ir siempre relacionada con una dirección IP, ya que por ejemplo la máscara 255.255.255.0 puede ser relacionada con una clase A o B, porque estamos haciendo Subnetting o con la clase C, sin hacer Subnetting.

Máscaras válidas para una red.

Máscaras válidas para una red de clase A

Aparecen los siguiente valores:

- MÁSCARA: MÁSCARA DE SUBRED
- BITS: NUMERO DE BITS DE RED
- REDES: NUMERO DE REDES
- MÁQUINAS: NUMERO DE MÁQUINAS.

Subnet Mask Networking Bits Number of Networks Number of Hosts. Class A

| MÁSCARA | BITS | REDES | MAQUINAS |
|---|---|---|---|
| 255.255.255.252 | /30 | 4,194,304 | 2 |
| 255.255.255.248 | /29 | 2,097,152 | 6 |
| 255.255.255.240 | /28 | 1,048,576 | 14 |
| 255.255.255.224 | /27 | 524,288 | 30 |
| 255.255.255.192 | /26 | 262,144 | 62 |
| 255.255.255.128 | /25 | 131,072 | 126 |
| 255.255.255.0 | /24 | 65,536 | 254 |
| 255.255.254.0 | /23 | 32,768 | 510 |
| 255.255.252.0 | /22 | 16,384 | 1,022 |
| 255.255.248.0 | /21 | 8,192 | 2,046 |
| 255.255.240.0 | /20 | 4,096 | 4,094 |
| 255.255.224.0 | /19 | 2,048 | 8,190 |
| 255.255.192.0 | /18 | 1,024 | 16,382 |
| 255.255.128.0 | /17 | 512 | 32,766 |
| 255.255.0.0 | /16 | 256 | 65,534 |
| 255.254.0.0 | /15 | 128 | 131,070 |
| 255.252.0.0 | /14 | 64 | 262,142 |
| 255.248.0.0 | /13 | 32 | 524,286 |
| 255.240.0.0 | /12 | 16 | 1,048,574 |
| 255.224.0.0 | /11 | 8 | 2,097,150 |
| 255.192.0.0 | /10 | 4 | 4,194,302 |
| 255.128.0.0 | /9 | 2 | 8,388,606 |
| 255.0.0.0 | /8 | 1 | 16,777,216 |

Máscaras válidas para una red de clase B

Subnet Mask Networking Bits Number of Networks Number of Hosts.Class B

| MÁSCARA | BITS | REDES | MAQUINAS |
|---|---|---|---|
| 255.255.255.252 | /30 | 32,768 | 2 |
| 255.255.255.248 | /29 | 8,192 | 6 |
| 255.255.255.240 | /28 | 4,096 | 14 |
| 255.255.255.224 | /27 | 2,048 | 30 |
| 255.255.255.192 | /26 | 1,024 | 62 |
| 255.255.255.128 | /25 | 512 | 126 |
| 255.255.255.0 | /24 | 256 | 254 |
| 255.255.254.0 | /23 | 128 | 510 |
| 255.255.252.0 | /22 | 64 | 1,022 |
| 255.255.248.0 | /21 | 32 | 2,046 |
| 255.255.240.0 | /20 | 16 | 4,094 |
| 255.255.224.0 | /19 | 8 | 8,190 |
| 255.255.192.0 | /18 | 4 | 16,382 |
| 255.255.128.0 | /17 | 2 | 32,764 |
| 255.255.0.0 | /16 | 1 | 65,534 |

Máscaras válidas para una red de clase C

Subnet Mask Networking Bits Number of Networks Number of Hosts. Class C

| MÁSCARA | BITS | REDES | MAQUINAS |
|---|---|---|---|
| 255.255.255.252 | /30 | 64 | 2 |
| 255.255.255.248 | /29 | 32 | 6 |
| 255.255.255.240 | /28 | 16 | 14 |
| 255.255.255.224 | /27 | 8 | 30 |
| 255.255.255.192 | /26 | 4 | 62 |
| 255.255.255.128 | /25 | 2 | 126 |
| 255.255.255.0 | /24 | 1 | 254 |

Firewalls (Cortafuegos - FW)

¿Qué es un firewall?

Básicamente, podrías asimilar un firewall a un router al que se le añade seguridad. Esa seguridad hace que para algunas conexiones o paquetes o aplicaciones que tu le defines en lo que se llama política de seguridad, el router se niegue a mandarlo al otro lado. Esto puede valer tanto para cosas que vienen de fuera hacia dentro (lo más habitual) como de cosas que van de dentro hacía afuera.

Si tu política de seguridad es ninguna, un firewall y un router es lo mismo. Si tienes algunas reglas que te interesa que cumpla tu router y que signifiquen que bajo ciertas circunstancias a algún tipo de tráfico debe impedirsele atravesarlo, tienes un firewall.

Un firewall es un dispositivo que filtra el tráfico entre redes, como mínimo dos. El firewall puede ser un dispositivo físico o un software sobre un sistema operativo. En general debemos verlo como una caja con DOS o mas interfaces de red en la que se establecen una reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no. Incluso puede ir más allá y realizar modificaciones sobre las comunicaciones, como el NAT.

Esa sería la definición genérica, hoy en dia un firewall es un hardware especifico con un sistema operativo o una IOS que filtra el tráfico TCP / UDP / ICMP / .. / IP y decide si un paquete pasa, se modifica, se convierte o se descarta. Para que un firewall entre redes funcione como tal debe tener al menos dos tarjetas de red. Esta sería la tipología clásica de un firewall:

En el figura se muestra un ejemplo de firewall entre internet y una red local.

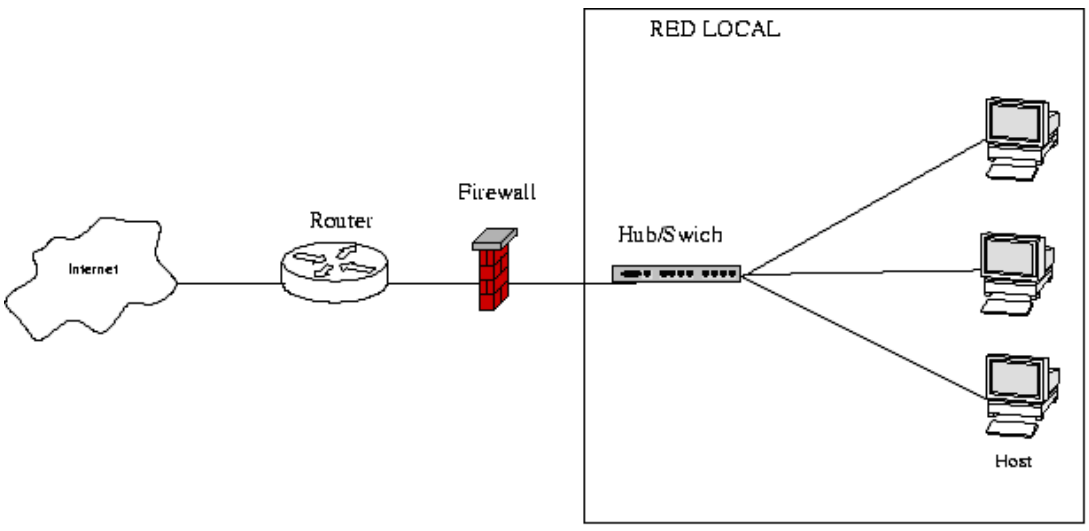


Figura: Firewall entre internet y una red local

Esquema típico de firewall para proteger una red local conectada a internet a través de un router. El firewall debe colocarse entre el router (con un único cable) y la red local (conectado al switch o al hub de la LAN)

Dependiendo de las necesidades de cada red, puede ponerse uno o más firewalls para establecer distintos perímetros de seguridad en torno a un sistema. Es frecuente también que se necesite exponer algún servidor a internet (como es el caso de un servidor web, un servidor de correo, etc..), y en esos casos obviamente en principio se debe aceptar cualquier conexión a ellos. Lo que se recomienda en esa situación es situar ese servidor en lugar aparte de la red, el que denominamos DMZ o zona desmilitarizada. El firewall tiene entonces tres entradas:

En el figura se  muestra un ejemplo de firewall entre internet y una red local, con zona dmz.

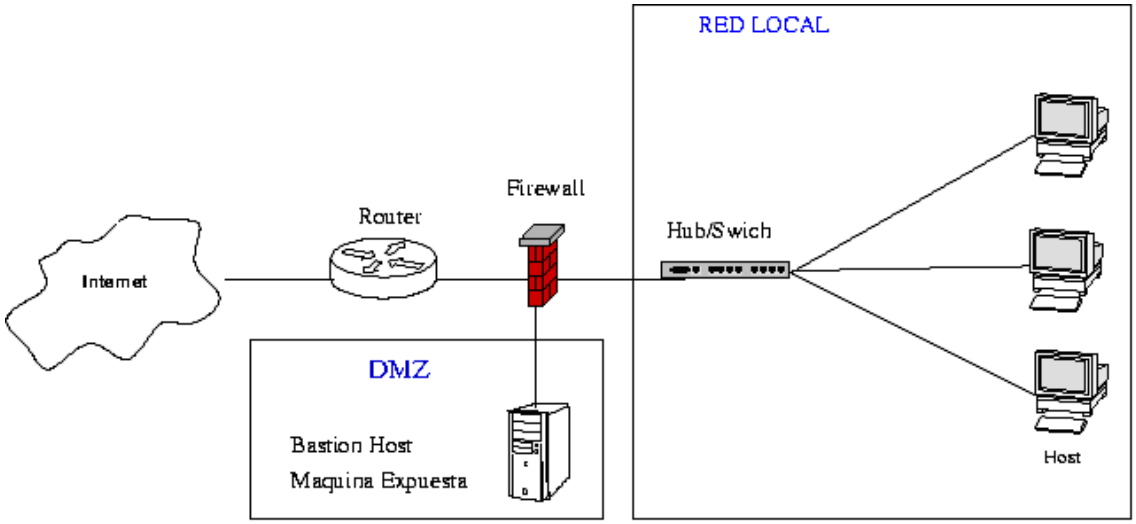



Figura: Firewall entre internet y una red local, con zona dmz

¿Por qué es necesaria la seguridad en las redes?

Actualmente, Internet se compone de decenas de miles de redes conectadas entre sí. La seguridad en las redes resulta esencial en este entorno, ya que toda red organizada es accesible desde cualquier computadora de la red y potencialmente es vulnerable a las amenazas de personas que no necesitan acceso físico a ella. En un sondeo reciente dirigido por el Computer Security Institute (CSI), el 70% de las organizaciones encuestadas declararon que las defensas de sus redes habían sido atacadas y el 60% afirmaba que los incidentes procedían desde dentro de las propias empresas.

Aunque sea difícil calcular el número de empresas que tiene problemas de seguridad relacionados con Internet y las pérdidas financieras debidas a tales problemas, queda

claro que los problemas existen. Definición del diseño de redes seguras Una internetwork se compone de muchas redes que están conectadas entre sí. Cuando se accede a información en un entorno de internetwork, hay que crear áreas seguras. El dispositivo que separa cada una de estas áreas se denomina firewall. Aunque un firewall suele separar una red privada de una red pública, esto no siempre es así. Lo normal es usar un firewall para separar los segmentos de una red privada.

NOTA: Un firewall, tal y como lo define el Dictionary of Internetworking Terms and Acronyms (Diccionario para términos y acrónimos de Internetworking), es un router o servidor de acceso, o varios routers o servidores de acceso, que actúan como búfer entre las redes públicas y una red privada.

Un router firewall utiliza listas de acceso y otros métodos para garantizar la seguridad de la red privada . Un firewall suele tener un mínimo de tres interfaces, aunque las primeras implementaciones sólo incluían dos.

Todavía resulta habitual instalar firewalls de dos interfaces.

Cuando se usa un firewall con tres interfaces, se crea un mínimo de tres redes. Las tres redes que crea el firewall se describen de este modo:

Interior

El interior es el área de confianza de la internetwork. Los dispositivos que están en el interior forman la red privada de la organización. Estos dispositivos comparten unas directivas de seguridad comunes con respecto a la red exterior (Internet). Sin embargo, resulta muy habitual que un firewall segmente el entorno de confianza. Si un departamento, como Recursos Humanos, tiene que ser protegido del resto de usuarios de confianza, se puede utilizar un firewall.

Exterior

El exterior es el área de no confianza de la internetwork. El firewall protege los dispositivos del interior y de la DMZ (Zona desmilitarizada) de los dispositivos del exterior. Para ofrecer servicios, ya sean Web, FTP publico u otros, las empresas suelen permitir el acceso a la DMZ desde el exterior. En ocasiones, es necesario configurar un firewall para el acceso selectivo desde el 2 exterior hasta los hosts y servicios de la DMZ. Si es inevitable, es posible configurar un firewall para permitir el acceso desde un dispositivo del exterior hasta un dispositivo de confianza del interior, siendo la razón principal para esto, el que no todas las empresas quieren invertir en tener varios servidores. Esto es mucho más arriesgado que permitir el acceso, desde el exterior hasta la DMZ aislada.

DMZ (Zona desmilitarizada)

La DMZ es una red aislada, a la que pueden acceder los usuarios del exterior. Es necesario configurar el firewall para permitir el acceso desde el exterior o el interior hasta la DMZ. La creación de una DMZ posibilita que una empresa ponga la información y los servicios a disposición de los usuarios del exterior dentro de un entorno seguro y controlado. Esto permite el acceso a los usuarios del exterior, sin permitir el acceso al interior. Los hosts o servidores que residen en la DMZ suelen

denominarse hosts bastión. En este caso, un host bastión es un host que está actualizado con respecto a su sistema operativo y las modificaciones experimentadas por este último. El hecho de que esté actualizado generalmente lo hará menos vulnerable a los ataques, ya que el fabricante habrá establecido o "parcheado" todos los defectos conocidos. El host bastión es un host que sólo ejecuta los servicios necesarios para realizar sus tareas de aplicación. Los servicios innecesarios (y a veces más vulnerables) son desactivados o eliminados.

En el figura ❑de la página ❑, muestra una red general.

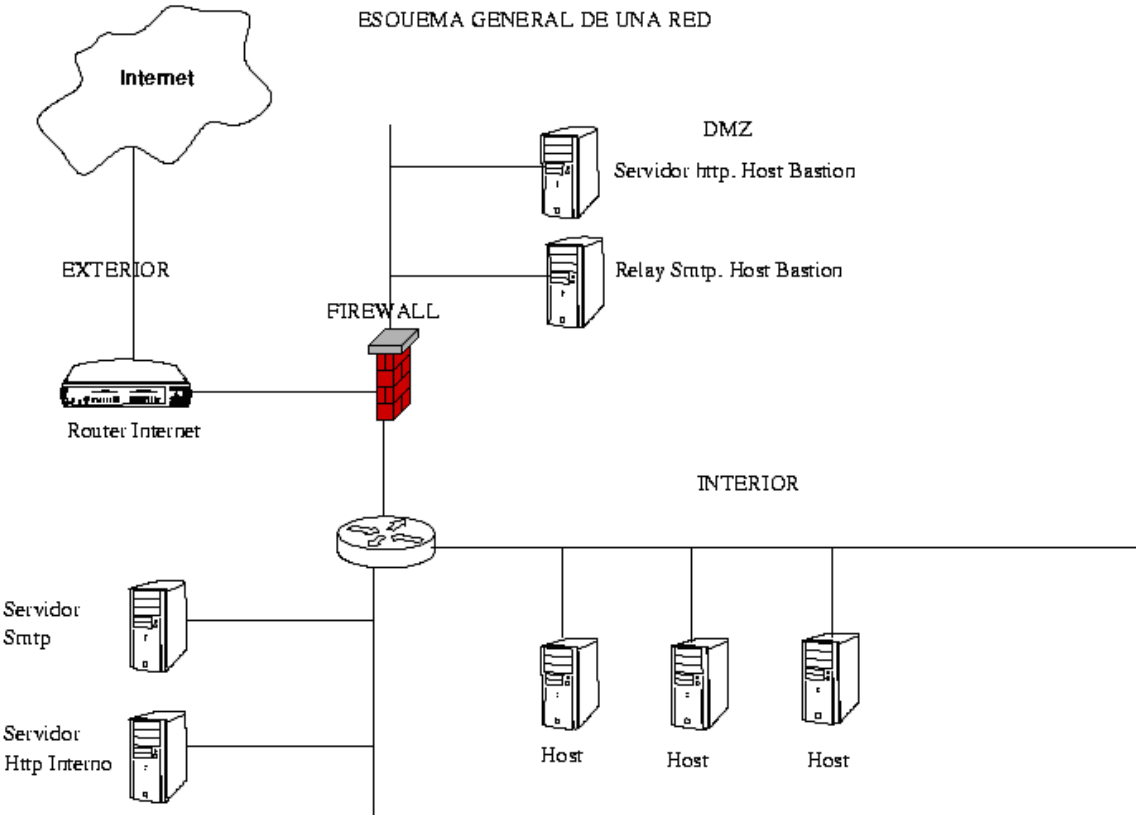


Figura: Red General

El cometido básico de un firewall consiste en llevar a cabo las siguientes funciones:

- No permitir acceso desde el exterior hasta el interior
- Permitir un acceso limitado desde el exterior hasta la DMZ
- Permitir todo el acceso desde el interior hasta el exterior
- Permitir un acceso limitado desde el interior hasta la DMZ

En muchos diseños de red existen excepciones a algunas de estas reglas (o a todas ellas). Por ejemplo, podría ser necesario permitir los mensajes SMTP desde el exterior hasta el interior. Si un entorno no tiene un servidor SMTP en la DMZ o carece de un host de relay de correo SMTP en la DMZ, sería necesario permitir acceder al servidor SMTP que resida físicamente en el interior. El hecho de permitir este tráfico incrementa considerablemente el riesgo en la red interna. Otra excepción podría ser que no se permitiera a la totalidad del tráfico pasar del interior al exterior. Potencialmente, una dirección IP, una subred, o la totalidad de la red del interior,

podrían estar limitadas a la hora de usar una determinada aplicación (puerto). Otra restricción podría ser el filtrado de los URL.

## Seguridad

En principio, el propósito genérico de un firewall es controlar y auditar los accesos a un servicio determinado. Su función es la de multiplexar los accesos a una red interna desde Internet; es una puerta entre una IntraNET 'A' e InterNET. La vigilancia que otra el firewall requiere unas normativas de seguridad impuestas por el propio administrador.

Una política bastante correcta y fiable, es la de hacer pasar siempre por el firewall el trafico que se necesite originar entre a e Internet y viceversa, de forma que se audite y controle todo lo que accede a A y/o sale de la misma. Esto nos permitirá sistemas de autentificación segura, detección de posibles intentos de acceso no autorizados, etc etc.

Una falacia es la idea que establece que un Firewall es inatacable. Esto es totalmente falso, existen métodos, con mayor o menor riesgo para el sistema, pero existen. Un ejemplo seria dar la oportunidad al atacante de restablecer las políticas de filtrado y selección. esto crearía un gran agujero de seguridad que posiblemente le permita acceder a cualquier host de la red interna que desee.

El firewall debe ser capaz de evaluar los posibles daños ofertados por un ataque e informar al administrador de ello. Tengamos en cuenta el bug propuesto antes. Una eliminación de políticas de auditoría podría darnos muchos dolores de cabeza.

Bajo GNU/LiNUX, tenemos a nuestra disposición numerosos programas capaces de convertir nuestro sistema en un potente firewall. El ejemplo mas conocido quizás sea iptables.