TEMA 5: INSTALACIÓN Y CONFIGURACIÓN DE REDES DE ÁREA LOCAL

1. INTRODUCCIÓN

Una LAN consta tanto de hardware como de software.

En el hardware se incluyen: estaciones de trabajo, servidores, tarjeta de interfaz de red, medio de transmisión (cableado o inalámbrico) y equipo de conectividad (hub, switch, puentes,...).

En el software se encuentra el sistema operativo de red (Network Operating System, NOS).

2. COMPONENTES HARDWARE DE UNA LAN

2.1 ESTACIONES DE TRABAJO

Una estación de trabajo o workstation es un nodo de red desde el que actúa un usuario. Su misión principal es la de proporcionar a los usuarios el acceso a los servicios de la red.

Una estación de trabajo no comparte sus propios recursos con otras computadoras.

Hay estaciones de trabajo con disco duro y sin él. Si no lo tienen, su S.O. debe ser descargado desde algún servidor a través de la red.

2.2 SERVIDORES DE RED

Son nodos de la red especializados en ofrecer servicios al resto de nodos de la red.

Los servicios que ofrecen son muy variados, pero los más comunes suelen ser los de impresoras, unidades de disco y ficheros, y comunicaciones.

Un servidor **queda definido** por el tipo de servicio que ofrece (por ej. un servidor Web). No hay que asociar un hardware servidor con un servicio concreto, puesto que el mismo hardware servidor puede ocuparse de distintos tipos de servicios. Así, un servidor de red, puede brindar servicios de disco e impresoras a la vez.

Características que debe tener un servidor de red:

- Potencia de proceso: Los servidores tienen una exigencia alta de velocidad de proceso. Deben tener procesadores centrales de alto rendimiento, con varias CPUs y capacidad de multiproceso.
- Memoria RAM: Un servidor consume mucha memoria. Los factores que influyen a la hora de decidirse por una cantidad de memoria u otra son:
  - En función de los servicios (qué servicios y qué nº de ellos) que vaya a proveer se necesitará más o menos memoria
  - En función de la cantidad de protocolos de red que implemente
  - En función del S.O. de red que vaya a ejecutar y del nº de usuarios que se conecten a él simultáneamente.
- Capacidad de almacenamiento en disco: Un servidor de discos o ficheros y de impresoras debe tener una gran capacidad de almacenamiento. Puesto que todos los usuarios de la red podrán conectarse a sus servicios, compartiendo sus discos, es necesario que la *velocidad de acceso a los discos* sea lo más elevada posible, así como *el bus al que se conectan.* También son necesarios mecanismos de seguridad en los discos, bien por duplicación automática de la información, bien por un sistema de redundancia. Una tecnología muy usada para esto es RAID (*Redundant Arrays of Inexpensive Disk).*
- Conexión a la red: El sistema de conexión a la red en un servidor debe ser muy eficaz, puesto que soportará todo el tráfico generado entre él y

sus clientes. Lo normal es hacer conexiones con fibra óptica de alta velocidad.

Clasificación de los servidores de red:

- En función de los servicios prestados: los servidores se caracterizan por el tipo de servicio prestado:
  - servidores de discos
  - servidores de impresoras
  - servidores gráficos
  - servidores web
  - servidores DNS
  - ...
- En función de la red a que se conectan: los servidores se pueden conectar a una red LAN (servidor LAN), o a una red de área extendida WAN (servidor WAN) o a ambas (servidor LAN-WAN). Según estén conectados a un tipo de red u otra, los tipos de servicios que ofrecerán serán diferentes. Así, un servidor WAN brinda servicios de páginas WEB para Internet, resolución de direcciones, de control y seguridad de la red,...
- En función del sistema operativo de red usado

2.3 TARJETA DE INTERFAZ DE RED

Como ya se vió un adaptador o tarjeta de red (NIC = Network Interface Card) es un interfaz hardware entre el sistema informático (por ej. un ordenador) y el medio de transmisión físico de la red.

El adaptador puede venir incorporado o no en la plataforma hardware del sistema. Así, actualmente en los PC suele venir incluido en su placa base. En otros casos, la tarjeta se adapta en la ranura de expansión del ordenador. Otras tarjetas son unidades externas que se conectan a través de USB.

Un equipo informático puede tener una o más tarjetas de red instaladas para permitir distintas configuraciones o poder unirse con el mismo equipo a diferentes redes.

Cada tarjeta necesita un controlador software (driver) especial para cada sistema operativo. Al adquirir una tarjeta de red se debe asegurar de que existirán los drivers apropiados para esa tarjeta y para el sistema operativo del host donde se vaya a instalar.

No todos los adaptadores de red sirven para todas las redes. Según la tecnología de red que tengamos (Ethernet, Token Ring,...) necesitaremos un adaptador de red u otro. Además, dentro de una misma tecnología de red, puede haber parámetros que condicionen también el uso de una u otra tarjeta. Por ejemplo en la tecnología Ethernet existen tarjetas de 10Mbps, 100 Mbps,...Según el tipo de medio de transmisión empleado habrá diferentes tarjetas: inalámbricas para Ethernet, 10Base2 (para Ethernet con cable coaxial delgado),...

¿Cómo funciona una tarjeta de red?

La tarjeta de red obtiene la información del PC, la convierte al formato adecuado y la envía a través del medio de transmisión a otra tarjeta de interfaz de la red que estará en el destinatario. Esta última tarjeta recoge la información del medio de transmisión y la pasa a las capas superiores para que el usuario destinatario la entienda.

2.4 MEDIO DE TRANSMISIÓN

Los medios de transmisión de una red son los medios físicos que se usan para conectar todos los componentes de la red. A través de los medios de transmisión viajan las señales de unos equipos a otros.

BANDA BASE: Una transmisión es en banda base cuando toda la capacidad del canal la utiliza una única seña de transmisión.

BANDA ANCHA: Una transmisión es en banda ancha cuando la capacidad (ancho de banda) del canal se reparte entre varias señales de transmisión (cada una irá en un determinado rango de frecuencias).

Los medios de transmisión pueden ser de 2 tipos:

1) Medios guiados: usan un medio sólido para la transmisión (cable).
2) Medios no guiados: usan el aire para transportar señales. Son inalámbricos.

Cada medio de transmisión tiene ventajas e inconvenientes. En todo caso, hay una serie de **factores que deben tenerse en cuenta a la hora de elegir un medio de transmisión:**

- Tipo de instalación en la que el medio es más adecuado.
- Topología que soporta.
- Requisitos en cuanto a distancia
- Velocidad de transferencia de datos
- Costes de cableado y de componentes necesarios
- Equipos de red adicionales que son necesarios
- Posibilidad de ampliación.
- Influencia de las interferencias provocadas por fuentes externas.
- Economía y facilidad de instalación.
- Seguridad. Facilidad para intervenir el medio.

Todos los medios están ***vistos en el tema 2.*** Recordar únicamente que los más usados en redes eran:

- **Cable coaxial (fino o RG-58 y grueso o RG-8)**
- **Cable par trenzado (sin apantallar o UTP, de pantalla global o FTP, y apantallado o STP)**
- **Cable de fibra óptica**
- **Medios inalámbricos (ondas de radio** *(desde 30Mhz a 1 Ghz),* **frecuencias microondas** *(desde 2Ghz a 40 Ghz)* **e infrarrojos**

*(desde más de 40Ghz)***).**

2.5 EQUIPO DE CONECTIVIDAD

Por lo general, para redes pequeñas, la longitud del cable no es limitante para su desempeño; pero si la red crece, tal vez llegue a necesitarse una mayor extensión de la longitud de cable o exceder la cantidad de nodos especificada. Existen varios dispositivos que extienden la longitud de la red, donde cada uno tiene un propósito específico. Sin embargo, muchos dispositivos incorporan las características de otro tipo de dispositivo para aumentar la flexibilidad y el valor. Los dispositivos más utilizados son los repetidores, hubs, switch y router:

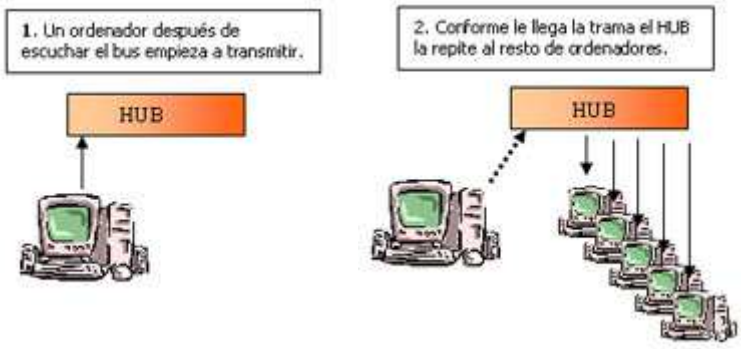
Repetidores

Un repetidor es un dispositivo de capa física que permite extender la longitud de la red; amplifica y retransmite la señal de red.

Hubs o concentradores

El concentrador o hub es un dispositivo de capa física que interconecta físicamente otros dispositivos (por ejemplo: ordenadores, impresoras, servidores, switchs, etc) en topología estrella. Los hubs son cajas (ver figura) con un número determinado de conectores, habitualmente RJ45 más otro conector adicional de tipo diferente para enlazar con otro tipo de red.

Un HUB simplemente une conexiones y no altera las tramas que le llegan. Para entender como funciona veamos paso a paso lo que sucede (aproximadamente) cuando llega una trama.



Visto lo anterior podemos sacar las siguientes conclusiones:

1 - El HUB envía información a ordenadores que no están interesados. A este nivel sólo hay un destinatario de la información, pero para asegurarse de que la recibe el HUB envía la información a todos los ordenadores que están conectados a él, así seguro que acierta.

2 - Este tráfico añadido genera más probabilidades de colisión. Al chocar los dos mensajes se pierden y es necesario retransmitir. Además, a medida que añadimos ordenadores a la red también aumentan las probabilidades de colisión.

3 - Un HUB funciona a la velocidad del dispositivo más lento de la red. Si observamos cómo funciona vemos que el HUB no tiene capacidad de almacenar nada. Por lo tanto si un ordenador que emite a 100 Mbps le trasmitiera a otro de 10 Mbps algo se perdería el mensaje.

Switch

Un switch es un dispositivo parecido al hub, pero opera a nivel de la capa de enlace de datos. Veamos cómo funciona un switch.

1 - El switch conoce los ordenadores que tiene conectados a cada uno de sus puertos. Un switch cuando se enciende no conoce las direcciones de los ordenadores de sus puertos, las aprende a medida que circula información a través de él. Por cierto, cuando un switch no conoce la dirección MAC de destino envía la trama por todos sus puertos, al igual que un HUB. Cuando hay más de un ordenador conectado a un puerto de un switch este aprende

sus direcciones MAC y cuando se envían información entre ellos no la propaga al resto de la red, a esto se llama filtrado.

2 - El switch almacena la trama antes de reenviarla. A este método se llama **store forward** es decir: **almacenar y enviar**. Hay otros métodos como por ejemplo **Cut-through** que consiste en recibir los 6 primeros bytes de una trama que contienen la dirección MAC y a partir de aquí ya empezar a enviar al destinatario. **Cut-through** no permite descartar paquetes defectuosos.

Un switch de tipo **store & forward** controla el CRC de las tramas para comprobar que no tengan error, en caso de ser una trama defectuosa la descarta y ahorra tráfico innecesario. El store & forward también permite adaptar velocidades de distintos dispositivos de una forma más cómoda, ya que la memoria interna del switch sirve de buffer. Obviamente si se envía mucha información de un dispositivo rápido a otro lento otra capa superior se encargará de reducir la velocidad. Así pues cuando vemos que un switch tiene 512KB de RAM es para realizar el store & forward. Esta RAM suele estar compartida entre todos los puertos, aunque hay modelos que dedican un trozo a cada puerto.

Finalmente comentar que hay otro método llamado **Fragment-free** que consiste en recibir los primeros 64 bytes de una trama porque es en estos donde se producen la mayoría de colisiones y errores.

3 – Un switch moderno también suele tener lo que se llama **Auto-Negotation**, es decir, negocia con los dispositivos que se conectan a él la velocidad de funcionamiento, así como si se funcionara en modo ;full-duplex o half-duplex.

4 - Velocidad de proceso: todo lo anterior explicado requiere que el switch tenga un procesador y claro, debe ser lo más rápido posible.

Router

Un router es un dispositivo de **CAPA 3 (capa de red) que i**nterconecta redes **en el nivel de red** y **encamina paquetes** entre ellas.

Los "routers" son capaces de elegir las mejores rutas de transmisión así como tamaños óptimos para los paquetes.

El router tomará decisiones basándose en grupos de **direcciones de red** a diferencia de las **direcciones MAC** individuales, que es lo que se hace en la capa 2.

3. COMPONENTES SOFTWARE DE UNA LAN

3.1 CONTROLADORES DE LOS ADAPTADORES DE RED

Como cualquier tarjeta, las de red también necesitan un **software controlador o driver** que controle sus operaciones desde el sistema operativo. Este software es específico para cada adaptador.

Sobre este controlador pueden establecerse otros programas de más alto nivel y que tienen funciones específicas relacionadas con los protocolos de la red en la que se vaya a instalar el sistema.

3.2 ACCESO DE LAS APLICACIONES A LOS RECURSOS DE LA RED

Para que las aplicaciones de usuario o del sistema operativo de red accedan a los recursos de la red se establecen unos interfaces software entre la capa de aplicación y la de transporte de datos, de modo que las unidades de disco remotas se vean, por ejemplo, como locales, al igual que las impresoras y demás dispositivos de red compartidos. El encargado de realizar esta transparencia entre servicios remotos y locales es lo que se

denomina **REDIRECTOR DE LA RED** y que suele estar incorporado en el Sistema Operativo de Red.

3.3 SISTEMA OPERATIVO DE RED

Por definición, un **sistema operativo** es un conjunto de programas que funcionan sobre un ordenador y que se encargan de administrar de forma eficiente los recursos de él.

Al igual que un equipo no puede trabajar sin un sistema operativo, una red de equipos no puede funcionar sin un sistema operativo de red. Si no se dispone de ningún sistema operativo de red, los equipos no pueden compartir recursos y los usuarios no pueden utilizar estos recursos.

Un **sistema operativo de red** se define como aquel que tiene la capacidad de interactuar con S.O. en otras máquinas por medio de un medio de transmisión y con el objeto de intercambiar información, transferir archivos, ejecutar comandos remotos, ...

Antiguamente, los S.O. y los N.O.S. (Network Operating System) eran software diferente, es decir, los S.O. no incluían software de red. Si se quería que un S.O. funcionase en una red, había que incluir software de terceros. Hoy en día, todos los S.O. actuales vienen con todo el software de red que necesitan para permitir al sistema compartir recursos y acceder a recursos compartidos. La cantidad de seguridad proporcionada a usuarios y datos es la cuestión principal que diferencia un N.O.S. de otro.

3.3.1. Tipos de Sistemas Operativos de Red

Un servidor siempre ejecuta software de servidor. Pero un servidor es capaz de ejecutar más de un programa servidor diferente.

Un cliente ejecuta software de cliente.

Algunos N.O.S. llevan incorporado en el mismo S.O. software de servidor y de cliente.

Teniendo en cuenta esto, los NOS se dividen en:

a) **Sistemas para redes cliente/servidor**

En las redes cliente/servidor existe un nodo **servidor dedicado** y el resto de nodos son **clientes.**

Un **servidor dedicado** es un equipo que sólo realiza la función prevista para él (por ej. servir páginas Web, servir correo,...) y es incapaz de ejecutar aplicaciones de usuario desde su consola. Es decir, nadie podría sentarse en su teclado y usarlo para cualquier otra tarea. Estos servidores ejecutan potentes S.O. de servidor de red que ofrecen ficheros, carpetas, páginas Web y demás a los sistemas clientes de la red.

Por el contrario, **los sistemas clientes** en una red cliente/servidor nunca pueden funcionar como servidores. Es decir, un sistema cliente nunca puede acceder a recursos compartidos de otro sistema cliente.

El ejemplo clásico para este tipo de NOS es el popular y potente **NOVELL NETWARE.**

Los servidores NOVELL son verdaderos servidores dedicados. No tienen windows ni aplicaciones de usuario. Lo único que saben hacer es compartir sus recursos. El SO Novell es totalmente distinto de Windows. Requiere aprender comandos totalmente distintos de instalación, configuración y administración.

b) **Sistemas para redes entre iguales o peer to peer**

En este tipo de sistemas, cada nodo puede ser **cliente** respecto de un servicio que le provee otro nodo y **servidor** respecto de otros clientes de la red que se benefician de sus servicios.

Los S.O. para redes entre iguales permiten que cualquier sistema pueda actuar como servidor o cliente o de las dos formas, dependiendo de cómo se configure.

El ejemplo típico de NOS entre iguales es Windows 9x.

c) **Sistemas híbridos cliente/servidor-entre iguales**

Durante años hemos dividido los NOS en cliente/servidor o entre iguales. Pero desde que apareció Windows NT y posteriormente Windows 2000/2003, XP,...todo se lió pues **un sistema NT puede formar parte de una red cliente/servidor y una red entre iguales al mismo tiempo.**

Por eso, actualmente para distinguir **qué NOS es mejor que otro para una determinada red** nos basamos en más en el concepto de **SEGURIDAD QUE OFRECE A LA RED.**

3.3.2. Seguridad en la Red

La seguridad en la Red implica proteger a los usuarios de la red de sus **dos mayores enemigos: "los malos" y ellos mismos**. Proteger una red de los usuarios e impedir que éstos *accidentalmente* destruyan datos o concedan acceso a individuos no autorizados es una parte fundamental de la seguridad de una red. También hay que limitar el control que los usuarios tienen sobre los recursos compartidos (no todos los usuario tendrán permiso para modificar un recurso compartido, algunos sólo podrán leerlo, otros modificarlo,...). Es decir, el nivel de control que pueden ejercitar los usuarios sobre los recursos se llama **permisos o derechos**, según la marca de NOS que se use.

Modelos de seguridad

Estos modelos nos permiten separar los NOS según cómo aseguren los recursos de la red.

Existen 3 modelos de seguridad diferentes según qué parte del NOS maneja la seguridad: Recursos, Servidor y Organización.

Pensad en esto: alguna parte del NOS debe hacer el seguimiento de quién puede hacer qué en la red. En algún sitio de la red debe estar almacenado qué recursos se comparten y cómo se comparten. Alguna parte del NOS debe comprobar esta información siempre que un cliente intenta acceder a un recurso compartido para garantizar que esa persona tiene permiso para hacer lo que está intentando hacer con ese recurso.

a) Modelo de seguridad basada en recursos:

Este modelo de seguridad lo usan los NOS más simples.

En los NOS basados en recursos, **los propios recursos individuales** almacenan la información sobre quién puede acceder al recurso y qué puede hacer (ej. la ficha compartir de windows 98 nos permite elegir entre compartir sólo para lectura, completo o según la contraseña). Esta información suele almacenarse dentro de alguna estructura de datos que es parte del propio recurso compartido, aunque también puede estar almacenada en alguna parte arbitraria del NOS. Lo importante es que **no hay una instalación de almacenamiento central para esa información: *cada recurso está a cargo del almacenamiento de su propia seguridad***.

El ejemplo más común de un NOS basado en recurso es la **serie de S.O. Microsoft Windows 9x. La mayoría de los sistemas operativos de red llamados entre iguales pertenece a este modelo de seguridad**.

Inconvenientes:

Los permisos se dan sobre las carpetas,..., los recursos a compartir. Podemos elegir si compartimos ese recurso para lectura o para todo. Pero, salvo que pongamos contraseña no podemos decirle que el usuario Pepe lo comparta para lectura y Juan para acceso total.

Es un control de seguridad muy simple. Pensad por ejemplo, que quiero que algunas personas tengan acceso completo y otras de sólo lectura. A no ser que ponga contraseñas para cada tipo de acceso, no lo puedo hacer. Pero de esta forma, todos los que tengan el mismo nivel de acceso tienen la misma contraseña. Supongamos que quiero cambiar sólo el acceso de una persona: tengo que cambiar la contraseña y después dar la nueva contraseña a todos los que necesitan acceder a este recurso. Esto no sólo es pesado para el Administrador, sino que, además hay que confiar en que ninguno de los que conoce la contraseña común se la diga nunca a nadie.

Pensad también que haya 30 o 40 recursos compartidos. Cada recurso tendrá su propia contraseña. Esto es impensable, ya que un sólo sistema puede llegar a tener entre 60 y 70 contraseñas diferentes.

Por tanto, para redes complejas **este tipo de seguridad no vale.**

b) Modelo de seguridad basada en servidor:

Una red que use este modelo de seguridad **emplea una BD central en cada servidor** para controlar quién obtiene qué nivel de acceso a los recursos que contiene ese servidor.

Ejemplo: **NOVELL NETWARE**

Para acceder a un recurso compartido en una servidor, hay que tener una **cuenta de usuario.** Una cuenta de usuario contiene listas de derechos de usuario que dicen a la red qué puede y qué no puede hacer el usuario en la red, incluyendo los derechos de sistema de ficheros que determinan a qué recursos compartidos puede acceder el usuario. Cada cuenta de usuario tiene también una contraseña.

Una persona que quiera acceder a los recursos compartidos en el servidor debe pasar por un proceso que se llama **iniciar la sesión** en el servidor (*log on)*.

Inconvenientes:

La seguridad basada en servidor es más fácil de configurar para el administrador. Pero aún así, en una organización grande, asignar derechos concretos a cada usuario individualmente es un trabajo muy laborioso. La solución: organizar a los usuarios que tienen necesidades similares en grupos. Y luego **asignar derechos concretos a grupos de usuarios** (asignar permiso al grupo de contabilidad para acceder a la BD de contabilidad,...)

Con este sistema de crear grupos y después asignar cuentas de usuario a grupos, se ahorra mucho tiempo y esfuerzo.

En la mayoría de los casos, los derechos de una cuenta de usuario son **acumulativos**, es decir, un usuario recibe la suma total de los derechos concedidos a su cuenta de usuario individual y los derechos concedidos a los grupos a que pertenece.

Las redes basadas en servidor funcionan **bien cuando sólo hay un servidor.** Para usar redes basadas en servidor con múltiples servidores, primero hay que tener una cuenta de usuario en cada servidor que se quiera usar y después hay que iniciar una sesión en cada uno para poder usar sus recursos. Si la red tiene pocos servidores, no es un problema, pero si hay muchos, vuelve a tener problemas el administrador.

c) Modelo de seguridad basada en organización:

Una red que use este modelo de seguridad, una **sola BD actúa como punto de inicio de sesión** para todos los recursos compartidos de la red. En este único lugar se almacena como mínimo todas las cuentas de usuario y grupos de la red. Esta BD puede residir en un solo ordenador, en un ordenador con uno o más ordenadores que actúan como copia de seguridad o en varios ordenadores que comparten copias completas de la BD que se sincronizan continuamente a través de un proceso llamado **replicación.**

Las redes con modelo de seguridad basada en organización simplifican la administración de la red, puesto que con un solo inicio de sesión vale para todos los servidores de la red.

Todos los NOS modernos usan alguna forma del modelo de seguridad basada en organización. De hecho, Microsoft y Novell usan incluso un sistema de BD **más avanzado** llamado **DIRECTORIO**. Un directorio describe cada sistema (no solo las cuentas de usuario), cada impresora, cada usuario y cada grupo de su red, proporcionando un depósito central de todo lo que forma la red en una gran base de datos.

Cada fabricante de S.O. de red usa nombres diferentes para esta BD, pero básicamente funcionan todos igual. Así, Novell lo llama **eDirectory** y Microsoft **Active Directory.**

3.3.3 Sistemas Operativos de Red COMERCIALES

Los principales fabricantes de NOS son: **Microsoft, Novell, Apple y Unix.**

Microsoft Windows domina el mercado de los **clientes.**

Microsoft, Novell, Apple y Unix compiten por el mercado de **NOS de servidor**.

3.3.3.1.-MICROSOFT WINDOWS

- Existen 2 líneas de productos Windows:
  - **Familia Windows 9x** (Windows 95,98, 98 SE y Me)
  - **Familia Windows NT** (Windows NT, Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003 y Windows Server 2008)

- **Familia Windows 9x:**

  Proporcionan funciones básicas de compartir impresoras y ficheros, pero poca seguridad.

Todos los equipos con Windows 9x reciben un nombre cuando se instala el NOS. Ese nombre es el nombre **NETBIOS** y puede modificarse en la ficha *Identificación* del subprograma *Red* del *Panel de Control (o Botón Dcho en Mis Sitios de Red-Propiedades).*

La convención de nomenclatura de NetBios permite 16 caracteres en un nombre NetBIOS. Microsoft, sin embargo, limita los nombres NetBIOS a 15 caracteres y utiliza el carácter 16 como sufijo NetBios.

Un **sufijo NetBios** es el carácter 16 del nombre NetBIOS de 16 caracteres. El software Conexiones de red de Microsoft utiliza el sufijo NetBios para **identificar la funcionalidad instalada en el dispositivo registrado**. Los sufijos se enumeran en formato hexadecimal ya que, de lo contrario, muchos de ellos no podrían imprimirse.

Los sufijos Netbios <00>, <20>, etc significan lo siguiente:

Sufijo Servicio

<00> Estación de trabajo
<20> Servidor
<1C> Controlador de Dominio y/o IIS (serv. Web Microsoft)
<1B> Explorador Principal de Dominio
<1E> Elecciones del servicio del explorador
<1D> Explorador Principal
<01> Mensajería. Para mensajes enviados a esta máquina
<03> Mensajería

Existen muchos más sufijos, por ejemplo

Sufijo Servicio
<06> Servidor RAS
<21> Cliente RAS
Etc

¿Cómo ver el nombre NetBIOS de cualquier máquina?

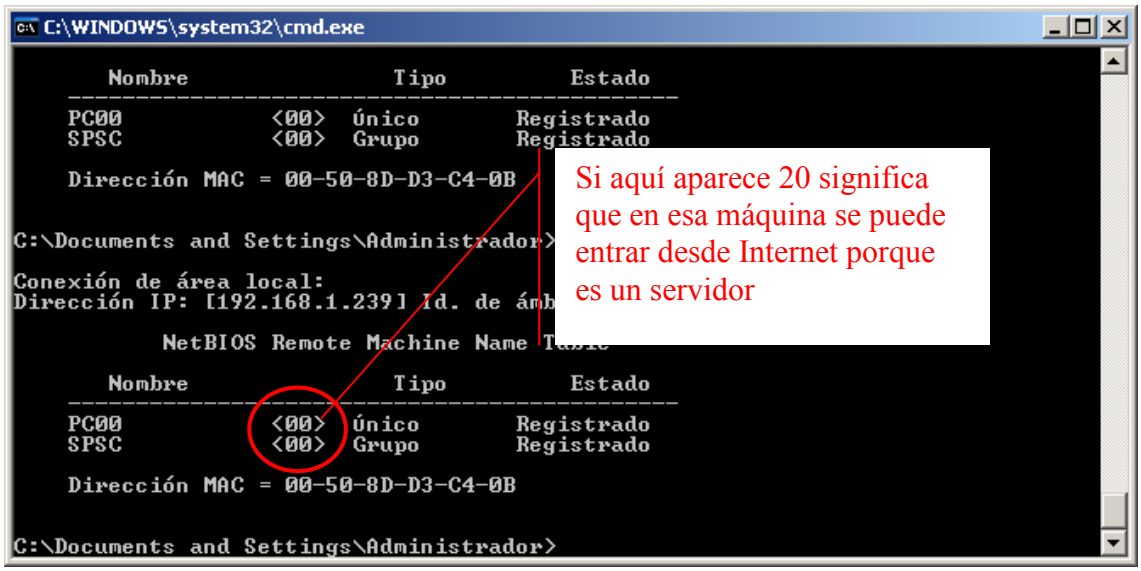
Con el comando **nbtstat.** Este comando sirve para obtener información de equipos remotos como:

nombre del host
IP
Puertos
estado

La sintaxis es:

nbtstat -a nombre del host [-modificadores] y también nbtstat -A dirección IP [-modificadores]

Ejemplo:



Antiguamente en el hacking, nbtstat era particularmente útil para introducirse vía internet dentro de otro equipo. Si en la columna del sufijo del nombre NetBIOS aparece <20> significa que ese equipo es un servidor de archivos.

También es interesante la columna *Tipo*, que puede ser:

Unique(U): El nombre tiene una única dirección IP asignada

Group (G): Un único nombre pero pueden tener asignadas muchas direcciones IP (es un grupo de trabajo, varios equipos)

Host Múltiple(M): El nombre es único, aunque debido a múltiples interfaces de red en el mismo equipo, es necesaria esta configuración con varias IPs para permitir el registro. El número máximo de direcciones es 25.

NetBIOS permite compartir archivos e impresoras así como ver los recursos disponibles en Entorno de red.

NetBIOS **utiliza los puertos 137, 138 y 139**.

Podemos **averiguar si nuestro ordenador tiene NetBIOS activado** utilizando el comando **netstat -an**. Este comando nos informará si tenemos los tres puertos anteriores en modo LISTENING.

En realidad Netstat (*network statistics*) **muestra un listado de las conexiones activas de un ordenador, tanto entrantes como salientes.** La información que resulta del uso del comando incluye el **protocolo en uso, las direcciones IP tanto locales como remotas, los puertos locales y remotos utilizados y el estado de la conexión.**

Ejemplo:

```
C:\WINDOWS>netstat -an

Conexiones activas

  Proto  Dirección local     Dirección remota    Estado
  TCP    192.168.0.2:137     0.0.0.0:0           LISTENING
  TCP    192.168.0.2:138     0.0.0.0:0           LISTENING
  TCP    192.168.0.2:139     0.0.0.0:0           LISTENING
  UDP    192.168.0.2:137     *:*
  UDP    192.168.0.2:138     *:*
```

Si no necesitamos NetBIOS, es mejor deshabilitarlo (pues equivale a tener esos 3 puertos abiertos). Para ello se debe desinstalar: el Cliente para Redes Microsoft y Compartir Carpetas e Impresoras. De esta forma, no podremos compartir en la Red Windows, pero si a través de Internet (pues Internet funciona con TCP/IP).

Los equipos con sistema operativo Windows 9x pueden agruparse en los llamados **GRUPOS DE TRABAJO**. Estos grupos no tienen más propósito que proporcionar una forma de **organizar el entorno de red** en las redes locales. Pero **no tienen** aspectos de seguridad que impidan a un usuario no autorizado acceder a un grupo de trabajo.

Como los sistemas Windows 9x se apoyan exclusivamente en un protocolo **NETBIOS**, ***existirá un solo ordenador en la red*** que guarde todos los nombres NETBIOS. Ese ordenador recibe el nombre de ***Principal para examen o Servidor principal para examen.*** Cualquier ordenador de la red que ejecute NETBIOS puede convertirse en el Principal para examen; el proceso que usan los ordenadores de la red para saber quién es el principal se llama ***Elección de principal.*** Estas elecciones de principal ocurren siempre que cualquier ordenador no puede detectar un Principal para examen en la red.

Todos los ordenadores de la red anuncian su nombre NETBIOS cada 12 minutos para que en cualquier momento que alguno de los ordenadores no pueda obtener una respuesta de un Servidor principal para examen, tenga lugar una elección de principal. Estas elecciones **reducen la velocidad de la red mucho**, por lo que se debe intentar que esas elecciones se produzcan lo menos posible.

Hay 2 formas de acabar con ese problema:

1) Usar un **servidor WINS** (es un equipo que registra todos los nombres NETBIOS que se asignan a cada equipo de la red junto con su IP), pero WINS sólo funciona con NETBIOS sobre TCP/IP.

2) Modificar **las propiedades del servicio "Compartir impresoras y archivos para redes Microsoft".** Este servicio ***debe estar instalado*** en un sistema Windows 9x para que éste pueda compartir carpetas e impresoras. Hay 2 ajustes que se pueden hacer:

   a) *Examinar principal*: determina si esta máquina intentará convertirse en Servidor principal para examen durante una elección. La debemos deshabilitar en todos los ordenadores de la red, excepto en uno, que será siempre el Principal para examen. Pero esto tiene un riesgo, y es que este ordenador tiene que estar siempre conectado a la red, en caso contrario, el resto no navegará.

   b) *Anuncio LM:* no se usa, a no ser que tengamos máquinas DOS. Debe estar siempre en NO.

Familia Windows NT:

Windows NT

Hay 2 versiones:

- *Windows NT Workstation*: pensado para ordenadores de sobremesa o clientes.

  Usaba un modelo de seguridad basado en **servidor:** si un usuario quería acceder a cualquier recurso en un sistema Windows NT Workstation tenía que tener una cuenta de usuario y una contraseña en ese sistema.

  Por defecto había dos cuentas: Administrador y otra invitado.

Por defecto había 6 grupos: **Administradores** (todos los privilegios tiene)**, Usuarios avanzados** (casi como el administrador, pero no pueden instalar nuevos dispositivos o acceder a ficheros o carpetas de otros usuarios a menos que tengan permiso)**, Usuarios** (no pueden modificar el Registro, ni acceder a ficheros fundamentales del sistema)**, Operadores de copia de seguridad** (como los usuarios, pero además pueden ejecutar programas de copia de seguridad que acceden a cualquier fichero o carpeta)**, Replicador** (pueden duplicar carpetas y ficheros en un dominio)**, Invitado.**

Usaba un nuevo sistema de ficheros NTFS: con NTFS se podían definir **permisos.**

- *Windows NT Server*: pensado para servidores y con soporte para un modelo de seguridad basado en organización llamado un **dominio.**

  Windows NT Server tiene la capacidad de transformar un grupo de ordenadores Windows individuales, cada uno con sus propios usuario y grupos locales, en un modelo basado en organización llamado dominio.

  Un **dominio** funciona como un grupo de trabajo, pero tiene toda la seguridad centralizada en un solo servidor. El sistema (máquina) Windows NT Server que alojara ese punto central recibía el nombre de **controlador de dominio principal (PDC)**. Cualquier red Windows NT podía tener **sólo** un PDC, pero se podían añadir uno o más ordenadores **controladores de dominio de seguridad (BDC)** ejecutando también Windows NT Server para proporcionar cierta redundancia en caso de que fallara el PDC.

  Durante la instalación de Windows NT Server, se le pedía al usuario que definiera el **papel de la máquina.** Es decir, qué función iba a desempeñar en la red esa máquina. Así, un sistema Windows NT Server podía simplemente unirse a un **grupo de trabajo** y manejar sus propios usuario y grupos locales, podía **crear un nuevo dominio y ser el PDC del dominio**, podía **unirse a un dominio existente y actuar como un BDC** o podía **unirse a un dominio sin actuar como PDC ni BDC.** Una vez que se definió el papel del servidor, **ya no resultaba fácil cambiarlo.**

  Con Windows NT Server mantienen los **usuarios y grupos locales** (sólo válidos para esa máquina) pero aconseja no usarlos en una red con dominios y añaden los **usuarios y grupos globales** (válidos para todo el dominio).

Por defecto había 3 cuentas de dominio (o grupos) integradas: **Administradores de dominio** (Tienen todos los privilegios para todo el dominio), **Invitados de dominio** (igual que el invitado local, pero para todo el dominio), y **Usuarios de dominio** (usuarios que forman parte del dominio).

Windows 2000

Hay también 2 versiones:

- *Windows 2000 Profesional*: pensado para ordenadores de sobremesa o clientes.

  Un grupo de ordenadores Windows 2000 Profesional usará un **modelo de seguridad basado en servidor**.

  Todos los sistemas Windows 2000 Profesional todavía tienen **usuarios locales.** Así, si se inicia sesión en un sistema Windows 2000 Profesional y se quiere acceder desde allí a otro sistema Windows 2000 Profesional a través de Mis sitios de red, se necesitará una *cuenta local separada en ese sistema*

- *Windows 2000 Server*: pensado para servidores.

Añade soporte **Plug and Play** (NT no tenía).
Añade un grupo por defecto nuevo: **Todos (**pertenece aquí cualquier usuario que inicia una sesión en el sistema).

Cambia los **nombres de dominio** NETBIOS NT por nombres de dominio basados en **DNS.**

Introduce un nuevo superdominio llamado **Active Directory.**

Los servicios de directorio son áreas de almacenamiento centralizadas para información acerca de los recursos de la red, incluyendo usuarios, aplicaciones, ficheros e impresoras. Las aplicaciones que aparecen en los servicios de directorio permiten a los administradores gestionar y compartir centralmente información acerca de los usuarios y recursos de sus redes y centralizar la seguridad. Los servicios de directorio de Windows 2000 se llaman ACTIVE DIRECTORY.

Todas las funciones de dominio de Windows NT **siguen funcionando;** simplemente se han incorporado en Active Directory.

Un solo Active Directory consta de uno o más dominios.

Windows 2000 Server **se deshace de la idea de PDC y BDC**. En su lugar, todos los **controladores de dominio (DC) son iguales.** Si se crea un nuevo usuario en un DC, automáticamente replicará la información de nuevo usuario en todos los otros DC en Active Directory.

Durante la instalación de Windows 2000 Server, se pide al usuario que defina el **papel de la máquina.** Es decir, qué función va a desempeñar en la red esa máquina. Así, un sistema Windows 2000 Server puede ser **controlador de dominio,** o **servidor miembro** de un dominio pero sin ser su DC, o puede ser un **servidor independiente** sin unir a ningún dominio.

Windows XP

Hay también 2 versiones, pero ninguna es para SERVIDOR, ambas son para ordenadores de sobremesa:

- *Windows XP Home Edition:* pensado para usuarios domésticos y de pequeña oficina que no precisan las complejas funciones de seguridad de la versión XP Profesional. **No permite** unirse a dominios.

- *Windows XP Profesional:* pensado para funcionar en entornos de dominio (deriva de 2000 Profesional).

Windows VISTA

Hay también varias versiones pero ninguna orientada a SERVIDORES.

Ha sido un fracaso de sistema operativo, de hecho, ya están las beta del siguiente sistema operativo: WINDOWS 7.

Básicamente se intentó mejorar la interfaz del usuario, facilitándole las tareas multimedia (video, imagen y sonido), así como la seguridad de los datos.

Su prevención de intrusos es demasiado estricta hasta el punto de no dejar realizar tareas habituales sin dar permiso para ello.

Windows 7

Es el sustituo de Window Vista. Desde Enero de 2009 hay una beta disponible.

Intenta reparar los fallos del Vista y mejorar la interfaz del usuario.

Tampoco tiene versión para SERVIDOR.

Windows Server 2003

Prácticamente es igual que Windows 2000 Server. Con la excepción de algunos cambios en la interfaz y alguna utilidad más de red avanzada.

Usa los mismos **Active Directory,** denominación de **dominio, servicios e interfaces** que se usan en Windows 2000 Server.

Windows Server 2008

Es el sucesor de Windows Server 2003. Mejora sobre todo los aspectos relacionados con el control del hardware de forma remota y las políticas de seguridad.

Añade capacidad de reparar sistemas NTFS en segundo plano, creación de sesiones de usuario en paralelo, mejoras en la gestión concurrente de recursos, un nuevo sistema de archivos SMB2, protección contra malware en la carga de drivers en memoria, incluye una consola mejorada con soporte GUI para administración,...

3.3.3.2.-NOVELL NETWARE

- Existen 5 versiones destacadas: **NetWare 3.x, NetWare 4.x, NetWare 5.x, NetWare 6.x y Novell Open Enterprise Server (OES 1 y 2).**

- La cuenta de administrador se llama **superusuario o admin.**

- **NetWare 3.x**

Ofrece sólidas capacidades para compartir ficheros e impresoras usando la pila de protocolos IPX/SPX, pero carece de una BD de seguridad centralizada. Cada servidor NetWare 3.x mantiene su propia BD de seguridad llamada **Bindery.**

Un usuario que acceda a recursos en 3 servidores distintos tiene que tener 3 cuentas de usuario y contraseñas separadas.

NetWare 4.x

Añade **Novell Directory Services (NDS) y encapsulación TCP/IP** (permite poner paquetes IPX dentro de paquetes TCP/IP)**.**

NDS (es como el Active Directory de Windows, aunque éste fue posterior a NDS) organiza todos los usuarios y la información de recursos en una BD conocida como el **árbol NDS.** Este árbol NDS actúa como una BD de seguridad centralizada, permitiendo a los usuarios que inician una sesión en el directorio acceder a todos sus recursos desde cualquier lugar de la red.

NetWare 5.x y NetWare 6.x

NetWare 5.x y 6.x **ejecutan TCP/IP nativamente**, eliminando la necesidad de encapsular TCP/IP. Es decir, ya no necesita usar IPX/SPX aunque lo mantiene por compatibilidad.

Sigue usando la BD de seguridad NDS. Pero ahora se llama **eDirectory**.

Novell Open Enterprise Server 1 y 2 (OES 1 y 2)

Novell Open Enterprise Server es un sistema operativo de red basado en SUSE Linux Enterprise que cuenta con servicios de grupos de trabajo para empresas muy fácil de implantar y gestionar.

Se basa en la combinación de NetWare, líder en redes de seguridad y SUSE linux Enterprise Server, una de las principales plataformas de código abierto para la ejecución de aplicaciones empresariales. Así, pueden coexistir ambos sistemas en la empresa.

El **servicio de directorio** sigue siendo **eDirectory.**

3.3.3.3.-UNIX y LINUX

Actualmente existen muchas versiones incompatibles de Unix, también conocidas como **“Sabores de Unix”.** Las principales son: **Linux, Solaris de Sun, AIX UNIX de IBM, HP UNIX de Hewlett-Packard y BSD.**

Aunque todos los sabores (versiones) de UNIX comparten una apariencia y ambiente similares, un programa escrito para una versión a menudo requiere modificaciones significativas para poder funcionar en otro. Son **incompatibles.**

Unix sigue siendo el servidor elegido para dar **servicios basados en Internet** como navegación Web y correo electrónico.

El sistema de impresión usado es el **Sistema de impresión UNIX común (CUPS).** CUPS presta soporte a cualquier lenguaje de impresora, aunque suele estar asociado comúnmente con el PostScript. CUPS tiene **soporte integrado basado en Web** para las conexiones y gestión de impresoras.

En Unix/Linux también hay una **supercuenta** como en Windows y NetWare y se llama **root.**

3.3.3.4.-Mac OS (sistema operativo de Macintosh)

La versión actual es Mac OS X (basado en UNIX) de Apple. Usa una interfaz gráfica desarrollada por Apple llamada **Aqua.**

Las diferentes versiones de Mac OS X van apodadas con los nombres de grandes felinos en inglés. Así, la versión actual es la 10.5 llamada Leopard; la versión anterior fue la 10.4 llamada Tiger,...

Es compatible con Windows, incluso ejecuta el Office, y con otros sistemas.

4. PROTOCOLOS DE REDES LAN

4.1 PROTOCOLOS DE REDES UNIX

Unix se ha comunicado con el exterior a través de una serie de protocolos cuya utilización se ha extendido mundialmente. De hecho, esta familia de protocolos se ha convertido en un estándar *de facto*: es la familia de protocolos **TCP/IP.**

Los protocolos del modelo TCP/IP ya están vistos en el tema 3. Recordar cuáles son:

a) ***Protocolo IP (Internet Protocol):*** es el protocolo de nivel de red y es sin conexión. Este protocolo maneja ***paquetes de datos***. Cada paquete

puede seguir una ruta distinta para llegar a su destino. Cada paquete consta de una cabecera y un campo de datos. En la cabecera están los campos: **versión (IPv4 o IPv6), tiempo de vida (TTL), protocolo** de transporte que ha generado el paquete, por ej. TCP, UDP,...; **código de redundancia (CRC), IP origen, IP destino y** otros.

b) ***Protocolo ICMP (Protocolo de mensajes de control):*** es un protocolo de la capa de red, que encapsula en un único paquete IP algún evento que se produce en la red y muestra un mensaje informativo. Los mensajes más conocidos son: **Destino inalcanzable** (se usa cuando un paquete de una red no puede alcanzar otra red solicitada, o bien es alcanzada pero no en las condiciones deseadas), **Tiempo excedido** (se usa cuando el campo TTL del paquete se terminó),...

c) ***Protocolo ARP (Protocolo de resolución de direcciones):*** es un protocolo de la capa de red, que se encarga de convertir las direcciones IP en direcciones físicas de la red o MAC.

d) ***Protocolo RARP (Protocolo de resolución de direcciones inverso):*** es un protocolo de la capa de red, que se encarga de convertir direcciones físicas o MAC en direcciones IP. Básicamente se usa en estaciones de trabajo sin disco, que han conseguido su S.O. a través de la red.

e) ***Protocolo TCP (Protocolo de control de transmisión):*** es un protocolo de la capa de transporte y que usa conexión. Fue especialmente diseñado para realizar conexiones en redes inseguras. TCP maneja unos paquetes de datos llamados ***segmentos.*** TCP es el responsable de ensamblar los datagramas IP (paquetes) recibidos por el receptor, ya que la red IP puede desordenarlos al usar caminos diferentes para alcanzar su destino. Los puntos de acceso al servicio (SAP de OSI) en la capa de transporte se llaman **sockets** o conectores TCP/IP y son muy útiles en la programación de aplicaciones de red.

f) ***Protocolo UDP (Protocolo de datagrama de usuario):*** es un protocolo de transporte sin conexión y, por tanto, sin garantía de entrega. Se usa en transmisiones rápidas que no necesitan seguridad en la transmisión.

g) ***Protocolo NFS (Network File System):*** es un protocolo de la capa de aplicación del modelo OSI. Permite que distintos sistemas conectados a una misma red accedan a ficheros remotos como si fuesen locales. Originalmente fue desarrollado por SUN Microsystem con el objetivo de que fuese independiente de la máquina, su sistema operativo y el protocolo de transporte; esto fue posible gracias a que está implementado sobre otros 2 protocolos XDR (de presentación) y RPC (de sesión). Este protocolo NFS **está incluido por defecto en los sistemas operativos UNIX y las distribuciones GNU/Linux. Se puede usar en cualquier S.O.: Windows, Linux,...**

h) *Existen muchos más protocolos de aplicación:* ***HTTP, PPP, SMTP, POP3,...***

4.2 PROTOCOLOS DE REDES NOVELL NETWARE

Las redes NetWare utilizan una arquitectura cliente/servidor. Estas redes utilizan **cualquiera de los protocolos de nivel físico y enlace** que existen, ya sean 802.3/Ethernet, Token Ring, FDDI,... Hasta el lanzamiento de la versión 5.x de NetWare todas las redes usaban el protocolo **IPX como único protocolo de la capa de red**, sin embargo, en la actualidad, también soportan **TCP/IP.**

En las redes Netware en vez del concepto de paquete de datos se habla de MENSAJE. Así los mensajes tienen una estructura con varios campos: dirección origen, dirección destino,...

NetWare de Novell es un conjunto propietario de protocolos que incluyen los siguientes:

a) ***Protocolo IPX (Internet Packet Exchange) :*** es un protocolo de la capa de red (capa 3) no orientado a conexión y define la red y las direcciones de nodo.

En las redes NetWare **cada red física se identifica con un nº de 32 bits**. Este nº lo usa IPX para diferenciar redes separadas.

A parte, **cada servidor Netware también tiene un identificador de 8 caracteres hexadecimales** (por ej. 87A53F15) con el fin de que los enrutamientos sean según el camino lo más corto posible.

En cuanto al direccionamiento IPX se usa una **dirección que consta de 2 partes:**

- **el nº de red física (de 32 bits)**
- **el nº de nodo de 48 bits que es la MAC del nodo**

Así, un ejemplo de dirección IPX será: 12345678.00-01-02-02-04-05 y el ordenador 12345678.66-1A-33-4F-21-C5 estarán en la misma red.

b) ***Protocolo SPX (Sequenced Packet Exchange):*** es un protocolo de nivel de transporte (capa 4) según el modelo OSI y que se comunica con el protocolo IPX de nivel inferior. Es un protocolo orientado a la conexión. Las tareas que realiza son: **recuperación de datos duplicados y de errores (por ello, cada mensaje tiene un nº de secuencia).** También realiza el **control del flujo:** el dispositivo destino no tiene por qué reconocer cada mensaje (como los paquetes TCP/IP) que le llega de forma inmediata, sino que se establece una ventana, cuyo nº representa cada cuántos mensajes recibidos tiene que enviar un mensaje de reconocimiento.

c) ***Protocolo NCP (Netware Control Protocol):*** es un protocolo y es una interfaz de usuario que sirve para solicitar servicios de la red a sus proveedores de servicios. Sus funciones corresponden a los niveles de transporte (capa 4), sesión (capa 5) y presentación (capa 6) según el modelo de referencia OSI. Cada servicio tiene una **identificación dada por el servidor**, el cual se lo envía al cliente dentro de un mensaje del protocolo NCP. También se incluye un nº de conexión por cada sesión establecida con el servidor.

d) ***Protocolo SAP (Service Advertising Protocol):*** es un protocolo que se usa para advertir a los dispositivos proveedores de servicios de la red (**servidores)** de los servicios disponibles en la red y sus direcciones (dónde están disponibles).

Sus funciones corresponden a las capas de transporte(4), sesión (5), presentación (6) y aplicación (7) según el modelo OSI.

El servidor envía un mensaje SAP de broadcast cada 60 segundos, conteniendo la información del servicio. Todos los nodos SAP emplean ese intervalo de tiempo. De esta forma, todos los nodos SAP pueden actualizar sus tablas y tener todos la misma información.

Sin embargo, eso puede provocar congestión en grandes redes.

Un agente SAP debe existir en cada servidor. Estos agentes recogen la información de este servicio y su dirección y lo guardan en una tabla llamada **Server Information.** Todos los agentes SAP se intercambian su información, con lo cual estas tablas contendrán la información de todos los servidores. Estas tablas se guardan en los servidores y enrutadores y nunca en las estaciones cliente.

Los clientes, en cambio, pueden contactar con los agentes SAP para obtener información de los servidores disponibles y sus servicios.

e) ***Protocolo RIP:*** es diferente del RIP de IP. Facilita el intercambio de información de enrutamiento.

4.3 PROTOCOLOS DE REDES APPLE

Las redes Apple usan los protocolos **AppleTalk** (es también el nombre comercial usado para identificar las redes LAN con ordenadores Apple). Sin embargo, a nivel **físico** emplean el mismo protocolo especificado por la IEEE y el modelo de referencia OSI.

Existen muchos protocolos, veremos sólo los más importantes, puesto que Apple ahora usa ya los protocolos TCP/IP y no estos.

Protocolos a nivel de capa de acceso al medio (enlace OSI):

- **Ethertalk:** cumple las especificaciones del IEEE 802.3 y habilita a los protocolos de AppleTalk para operar sobre el estándar físico IEEE 802.3
- **TokenTalk:** cumple las especificaciones del IEEE 802.5 y habilita a los protocolos de AppleTalk para operar sobre el estándar físico IEEE 802.5
- **FDDI Talk:** cumple las especificaciones del FDDI y habilita a los protocolos de AppleTalk para operar sobre el estándar físico FDDI.
- **LocalTalk:** Lo inventó Apple, funciona en topología bus y con método de acceso CSMA/CA (el usado por Wi-Fi).

Protocolos a nivel de capa de control del enlace (enlace OSI):

Manejan la interacción entre los protocolos de AppleTalk y sus correspondientes estándares de la capa de acceso al medio. Las capas superiores no reconocen las direcciones de hardware de estos estándares, así que los protocolos **ELAP (***Ethernet Link Access Protocol),* **TLAP** *(Token Link Access Protocol),* **FLAP** *(FDDI Link Access Protocol) y* **LLAP** *(LocalTalk Link Access Protocol)* usan las tablas de mapeo de direcciones mantenidas por el Protocolo de Resolución de Direcciones (**AARP-**AppleTalk Address-Resolution Protocol) para direccionar las transmisiones adecuadamente.

Protocolos a nivel de red:

El principal es el **DDP (Datagram Delivery Protocol)** que se encarga de encaminar los datagramas de forma parecida a como lo hace IP en las redes TCP/IP y, al igual que IP no está orientado a la conexión. Existen otros protocolos a parte de este.

Protocolos a nivel de transporte:

NBP (Name Binding Protocol) se encarga de asociar nombres de servicios con direcciones, de modo que los usuarios puedan usar nombres para solicitar servicios de la red.

ATP (AppleTalk Translation Protocol) es orientado a conexión y equivale al TCP de las redes TCP/IP.

En las capas superiores habría también protocolos como **AFP** (para el intercambio de ficheros),...

4.4 PROTOCOLOS DE REDES MICROSOFT

Las redes Microsoft suelen usar protocolos propuestos por otros fabricantes. Los principales son:

4.4.1.- NetBIOS/NetBEUI (*Network Basic Input/Output System/NetBIOS Extended User Interface):*

Es un conjunto de protocolos de red rápidos y simples apropiados para redes pequeñas que **no usen enrutadores**, ya que NetBEUI no admite enrutamiento.

Hasta Windows 2000 inclusive se incluyó. En Windows XP se debía instalar si se quería usando el CD. Y en Windows Vista no está claro si se implementa o no.

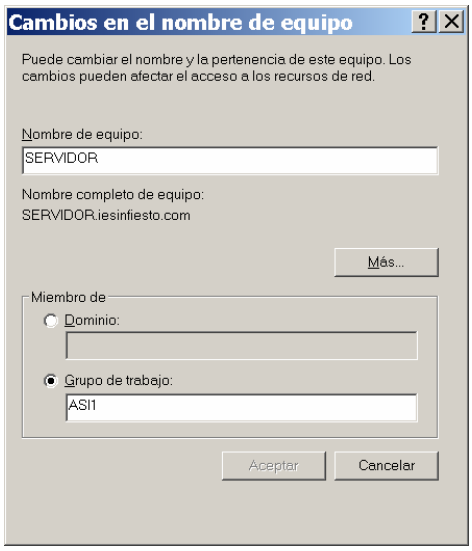
Hoy en día ha sido sustituido por TCP/IP.

Cuando Windows se desarrolló, Microsoft decidió integrar NetBIOS en el núcleo del SO Windows. Cuando instalamos Windows, se nos pide que demos al ordenador un nombre. **Ese nombre es el nombre NetBIOS.** El problema era que nadie (excepto los expertos) notaba que estaba pasando esto, ya que no aparecía la palabra NetBIOS por ningún sitio (sólo nos pedía el nombre del PC). A lo largo de los años se ha separado NetBIOS de NetBEUI para ejecutarlo con TCP/IP (por ejemplo).

NETBIOS provee los servicios de sesión (capa 5) descritos en OSI. Es decir, se encarga de establecer la sesión y mantener las conexiones. NetBIOS gestiona las sesiones basándose en los nombres de los ordenadores implicados. Pero este protocolo debe transportarse entre máquinas a través de otros protocolos; debido a que por sí mismo no es capaz para transportar los datos tanto en redes LAN como en WAN, para lo cual debe usarse otro mecanismo de transporte (por ej. en redes LAN el protocolo NETBEUI, en redes WAN el protocolo TCP/IP). Los protocolos que pueden prestar transporte a NETBIOS son: **NETBEUI, IPX/SPX y TCP/IP.**

Un **nombre NetBIOS** está formado por 2 componentes:

- El ***nombre de red de un sistema (nombre de la máquina)***, que se puede establecer usando el subprograma Sistema del Panel de control o en Botón Dcho sobre MI PC-Propiedades. Puede contener hasta 15 caracteres ASCII.



- Un ***sufijo*** *específico de la función que desempeña ese equipo dentro de la red.* Este sufijo constituye el 16º byte del nombre NetBIOS y define el papel que jugará la máquina en la red, en esa sesión concreta. Los sufijos más usados son los vistos anteriormente en este mismo tema.

Veamos un ejemplo de cómo Windows gestiona los nombres NetBIOS:

Instalamos en nuestra red 3 equipos Windows, llamados JUAN, MARIA y ANA. Estos nombres de equipo, sin que nosotros digamos nada serán los nombres NetBIOS de esos equipos, puesto que Windows lo configura él solo. Por defecto, todos los ordenadores Windows actúan como clientes. Configuramos los equipos JUAN y MARIA para que sean servidores de ficheros e impresoras, dejando a ANA sólo como cliente. Sólo por hacer esto, ahora, **JUAN tendrá ahora al menos 2 nombres NetBIOS: JUAN<00>, que identifica a JUAN como cliente y JUAN<20>, que identifica a JUAN como servidor de ficheros e impresoras. MARÍA también tendrá 2 nombres: MARIA<00> y MARIA<20>. ANA, por el contrario, sólo registrará un nombre: ANA<00>, que identifica a ANA como cliente.**

Si me siento en el PC MARIA y accedo a un fichero en JUAN, tanto MARIA como JUAN deben administrar esa conexión. Para abrir la conexión, MARIA el cliente, alias MARIA<00>, abre una conexión con JUAN el servidor, alias JUAN<20>. Según empieza JUAN a enviar el fichero solicitado a MARIA, otro usuario, por ejemplo Daniel, se sienta en el PC ANA y abre otro fichero en JUAN. Cada uno de los PC mantiene el seguimiento de estas conversaciones simultáneas usuando sus nombres NetBIOS.

Al usar un nombre NetBIOS diferente para cada función, los sistemas en red pueden seguir múltiples conexiones entre ellos simultáneamente.

NetBEUI funciona en la capa de transporte (capa 4). Este protocolo no requiere configuración después de su instalación.

Este protocolo se salta la capa de red y habla directamente con la capa 2 (de enlace de datos). Cuando un router recibe un paquete NetBEUI no encuentra la información de enrutamiento que necesita, de modo que simplemente descarta el paquete. Por eso se dice que **no admite enrutamiento y por eso, no es adecuado para redes con routers.**

5. INSTALACIÓN DE UNA RED DE ÁREA LOCAL

Veremos los pasos que hay que seguir para instalar una red a partir de unas especificaciones de diseño surgidas como consecuencia de un análisis de las necesidades.

5.1 ANÁLISIS DE NECESIDADES

Si en cualquier organización se ha decidido instalar una red LAN, será porque hay una serie de necesidades que lo hacen conveniente. Por tanto, habrá que investigar cuáles son esas necesidades y qué tipo de problemas se intentan solucionar implantando la red LAN.

Para ello, deberemos fijarnos, al menos, en los siguientes aspectos:

- ¿Cómo se realiza actualmente el trabajo?
- ¿Con qué volumen de datos se trabaja habitualmente?
- ¿Cuáles son los procedimientos de operación más comunes?
- ¿Qué esperan conseguir con la implantación de la red?
- ¿Qué volumen de usuarios trabajarán con la red?
- ¿Existe ya alguna red instalada?
- ¿Qué servicios de red se necesitarían?

A veces, en la implantación de una red LAN no se parte de cero, sino que se trata de la ampliación de una red ya existente. Es **de vital importancia, por tanto, averiguar el tipo de instalación que tienen en uso, qué problemas solucionan con esa red y cuáles son las principales dificultades con que se encuentran.**

Además, en el nuevo diseño, habrá que tener en **en cuenta el hardware y software que existe para que sea integrado, si es conveniente, con los nuevos elementos de diseño.** En ocasiones es

imprescindible perder alguna funcionalidad en la nueva red para permitir la integración de elementos tecnológicamente más antiguos, pero que hagan menos traumática la transición.

5.2 DISEÑO DE LA RED Y DE LOS SERVICIOS

Una vez determinadas las necesidades, hay que dar una respuesta que intente solventar los problemas de modo asequible. Esta respuesta es lo que se conoce como **diseño de la red.**

En el diseño intervendrán diferentes elementos: hardware, software, servicios, interconexión con el exterior, tiempo de instalación,...

5.2.1.Hardware

- Debe hacerse un análisis del hardware necesario para dar respuesta a las necesidades de los usuarios. Esto implica la **elección de una plataforma de hardware o una combinación de plataformas** (PC, Macintosh, estaciones UNIX,...)
- Cabe distinguir varios análisis de hardware diferentes, en función de si estamos estudiando los servidores, las estaciones o la red misma.
- Se deben analizar diferentes aspectos a tener en cuenta según sean las necesidades de esa LAN: **CPU** necesaria para el servidor y las estaciones, **memoria** para el servidor y estaciones, **discos** para el servidor y las estaciones, **adaptadores de red** según el flujo de datos que se prevea, el interface de conexión,...; **topología de la red** y **cableado de la red** (al diseñar el cableado de red, habrá que decidir si se pone o no cableado estructurado (lo veremos en el próximo apartado) y el tipo de cableado o inalámbrico si se desea).
- También se debe analizar el **hardware existente** ya en la organización. Debemos ver si es aprovechable o no y si compensa mantenerlo o es mejor renovarlo por otro más sofisticado.

5.2.2. Software

- Se debe decidir **qué S.O. usar (tanto para servidores como para estaciones cliente).** Éste estará condicionado por el hardware que hayamos elegido. O viceversa, si elegimos primero el S.O. estaremos condicionando el hardware necesario.
- Además decidiremos si la red será cliente-servidor o entre iguales. También si los servidores serán dedicados o no.

- Se debe analizar el volumen ocupado por el S.O. y los protocolos de red que incorpora.
- Si en la red no se parte de cero, habrá que elegir software compatible con el existente.
- Se deben decidir qué aplicaciones de usuario son necesarias. Además deberemos garantizar que las aplicaciones existentes correrán sin problemas en los nuevos sistemas o bien aconsejar las actualizaciones pertinentes de las mismas.

5.2.3. Servicios

- Se debe decidir **qué servicios** son necesarios en la red:
  - ***De disco:*** implantar sistemas de backup, de redundancia,...
  - ***De impresoras:*** gestores de impresión, servicios de compartir impresoras de red o locales,...
  - ***De correo electrónico:*** Hay que establecer el tipo de correo electrónico que usarán los usuarios: si necesitan agentes externos (internet), si habrá aplicaciones que lo usen,...si se necesita un servidor interno de correo electrónico,...
  - ***De páginas web:*** ver si se necesita un servidor de páginas web o se debe acceder a alguno.
  - ***De transferencia de ficheros:*** ver si se necesita un servidor FTP de ficheros o acceder a alguno.
  - ***Etc.***

5.2.4. Conexiones con el exterior

- Si la red debe estar conectada con otras hay que preveer cómo se realizará esta interconexión: líneas punto a punto o multipunto, conexión RDSI, ADSL, así como la velocidad de conexión, volumen de datos a transferir,...

5.3 EJECUCIÓN DEL DISEÑO

Ahora se trata de poner en marcha lo que se diseñó en la fase anterior. Para ello, hay que asegurarse de que la instalación de fluido eléctrico es correcta. En general, es conveniente la asistencia de un electricista que

supervise la instalación, asegurándose de que las tensiones son correctas, y de que la instalación aguantará el flujo de corriente eléctrica.

Posteriormente se **tiende el cableado** de datos según el plan decidido en la fase de diseño. Esto exige la instalación de algún rack, del cableado estructurado, de los conectores apropiados,... **Debe probarse cada uno de los cables antes de la puesta en funcionamiento final**.

Después se instalan los equipos, tanto el hardware como el software. Se dan de alta los distintos servicios, se configuran los protocolos, se crean las cuentas y directorios de usuario, se instalan aplicaciones,...

En ocasiones, cuando se trata de una ampliación de red o de la sustitución de un servidor por otro, es necesario **salvar los datos de los usuarios para hacer el cambio**. Una vez realizado, hay que restituir los datos a la nueva configuración.

5.4 SEGURIDAD

Se debe confeccionar la seguridad de la red: dar los permisos apropiados a los usuarios sobre cada recurso de red, determinar los derechos de acceso a las aplicaciones y, en general, evitar intrusiones (accidentales o no) a lugares de los sistemas de ficheros no autorizados.

5.5 PRUEBAS

Una vez completada la instalación, se pasa a la fase de pruebas. Es necesario diseñar un sistema de pruebas para garantizar que los servicios de la red están disponibles y funcionan correctamente para todos los usuarios que deben servirse de ellos.

Una vez realizadas las pruebas es posible que haya que revisar el diseño original de la red, ajustándose mejor a las necesidades.

5.6 EXPLOTACIÓN

Una vez probada la red, se puede proceder a su explotación. A lo largo de la vida de la red, el administrador deberá usar herramientas que le ayuden a tomar decisiones sobre posibles mejoras en el rendimiento de la red: mejoras en el rendimiento de la CPU, accesos a disco, ... Es decir, la red requiere un **mantenimiento**.

6 CABLEADO ESTRUCTURADO

6.1. ¿Qué es el cableado estructurado?

El concepto de **cableado estructurado** es tender cables en un edificio de manera tal que cualquier servicio de voz, datos, vídeo, audio, tráfico de Internet, seguridad, control y monitoreo este disponible desde y hacia cualquier roseta de conexión del edificio. Y se pueda cambiar, identificar y mover periféricos o equipos de una red con flexibilidad y sencillez.

A pesar de los constantes cambios que los negocios deben afrontar día a día, el sistema de cableado estructurado puede aliviar las interrupciones en el trabajo y las caídas de la red debidas a la reestructuración de las oficinas.
Ningún otro componente de la red tiene un ciclo de vida tan largo, por ello merece una atención tan especial.

Un buen sistema de cableado debe cumplir: **seguridad y flexibilidad**

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

6.2. Organismos y normas que regulan el cableado estructurado

ORGANISMOS

- **ANSI: American National Standards Institute (Instituto Nacional Americano de Normalización).**
  Organización Privada sin fines de lucro fundada en 1918, la cual administra y coordina el sistema de estandarización voluntaria del sector privado de los Estados Unidos.

- **EIA: Electronics Industry Association (Asociación de Industrias electrónicas).**
  Fundada en 1924. Desarrolla normas y publicaciones sobre las principales áreas técnicas: los componentes electrónicos, electrónica del consumidor, información electrónica, y telecomunicaciones.

- **TIA: Telecommunications Industry Association (Asociación de la Industria de las Telecomunicaciones).**

  Fundada en 1985 después del rompimiento del monopolio de AT&T. Desarrolla normas de cableado industrial voluntario para muchos productos de las telecomunicaciones y tiene más de 70 normas preestablecidas.

- **ISO: International Standards Organization (Organización de Estándares Internacional).**

  Organización no gubernamental creada en 1947 a nivel Mundial, de cuerpos de normas nacionales, con más de 140 países.

- **IEEE: Instituto de Ingenieros Eléctricos y de Electrónica.**

  Principalmente responsable por las especificaciones de redes de área local como 802.3 Ethernet, 802.5 TokenRing, ATM y las normas de GigabitEthernet, entre otros.

NORMAS

- **ANSI/TIA/EIA-568-A**

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

  El propósito de esta norma es permitir la planeación e instalación del cableado de edificios con muy poco conocimiento de los productos de telecomunicaciones que serán instalados con posterioridad.
  Actualmente esta norma ha sido sustituida por la ANSI/TIA/EIA-568-B que surgió en 2.001.

- **ANSI/TIA/EIA-568-B**

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

  Actualmente sustituye a la 568-A.
  Define tipos de cable, distancias, conectores, arquitecturas, terminaciones de cables y características de rendimiento, requisitos de instalación de cable y métodos de pruebas de cables instalados.

  – **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 emiten una serie de normas que complementan la 568-B, que es la norma general de cableado, como son: la ANSI/TIA/EIA-569-A, EIA/TIA 570, EIA/TIA 606, EIA/TIA 607 y EIA/TIA 758.

- **ANSI/TIA/EIA-569-A**

  Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales (**Cómo enrutar el cableado).**

  Define cómo deben ser los elementos de diseño para trayectos (tuberías, bajo suelo, canaletas, registros,...) y para

cuartos dedicados a equipos de telecomunicaciones. La norma especifica dimensiones de las tuberías, tamaño de las puertas, iluminación, polvo, temperatura, y humedad entre otras, dimensiones de los armarios de telecomunicaciones, cantidad de armarios, espacios entre las paredes y los equipos en la sala de equipos, separación con relación a fuentes de energía,...

- **ANSI/TIA/EIA-570-A**

  Normas de Infraestructura Residencial de Telecomunicaciones. Establece el cableado de uso residencial y de pequeños negocios.

- **ANSI/TIA/EIA-606-A**

  Normas de Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales.

  Proporciona normas para la codificación de colores, etiquetado, y documentación de un sistema de cableado instalado.

- **ANSI/TIA/EIA-607**

  Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales. Define el sistema de tierra física y el de alimentación bajo los cuales se deberán de operar y de proteger los elementos del sistema estructurado.

- **ANSI/TIA/EIA-758**

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

Existe una entidad BiCSi (Building Industry Consulting Service International) (www.bicsi.org) que compila y armoniza diversos estándares de telecomunicaciones .

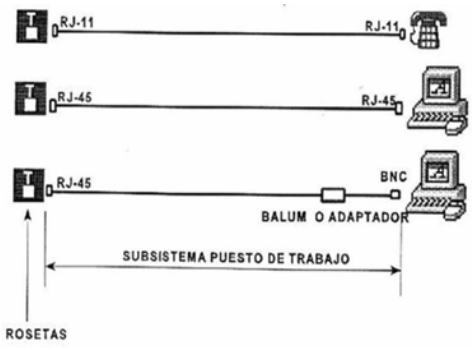
6.3. Componentes de un sistema estructurado

En conjunto, a todo el cableado de un edificio se le llama **SISTEMA,** y a cada parte en la que se subdivide se llama **SUBSISTEMA**.

Los componentes de un sistema estructurado son:

6.3.1.-**SUBSISTEMA DE PUESTO DE TRABAJO**

- Compone los elementos que van desde la toma de usuario (la roseta) hasta el terminal de datos o de voz (el equipo del usuario).
- A cada puesto de trabajo deben poder llegar todos los posibles medios de transmisión que se requieran: fibra, UTP, voz, RDSI,...
- Puede ser un simple cable con los conectores adecuados o un cable con los conectores o adaptadores adecuados.
- El cable que va de la roseta al puesto de trabajo se llama **latiguillo** y no puede superar (en cable trenzado) los **3 metros** de distancia (según la **TIA/EIA 568-B)**
- El **nº de puntos de conexión (rosetas)** en una instalación se determina en función de las superficies útiles (m^2) del recinto o en función de los metros lineales de la fachada, mediante la aplicación de la siguiente normal: **1 punto de acceso (roseta: simple o doble o...) por cada 8 a 10 m^2 o por cada 1,35 metros de fachada.** Este nº se debe ajustar en función de las características específicas del emplazamiento, por ejemplo, los locales del tipo de salas de informática, salas de reuniones, y laboratorios.
- En el caso de que coexistan telefonía e informática, un dimensionado de 3 tomas por punto de conexión es un buen criterio.
- Ver gráfico:



6.3.2.-**SUBSISTEMA HORIZONTAL**

- Es el cableado que une los puntos de distribución de planta con el conector o conectores del puesto de trabajo. Incluye las rosetas de conexión del area de trabajo.

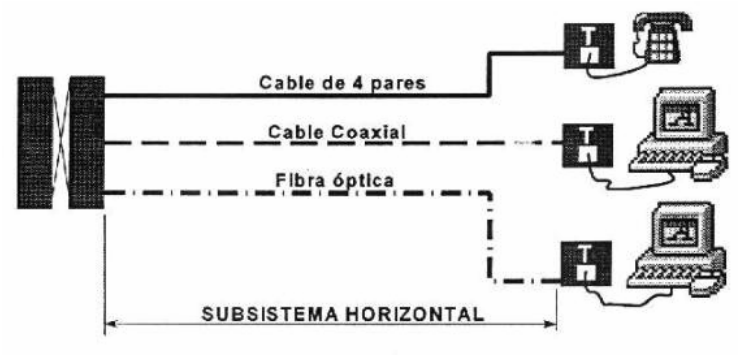
- Este subsistema se compone de:

a) El ***cable Horizontal y Hardware de Conexión:*** También llamado "cableado horizontal". Proporciona los medios para transportar señales de telecomunicaciones entre el área de trabajo y el punto de distribución de planta. Estos componentes son los "*contenidos*" de las rutas y espacios horizontales.

b) Las ***rutas y espacios horizontales:*** También llamado "sistemas de distribución horizontal". Las rutas y espacios horizontales son utilizados para distribuir y soportar cable horizontal y conectar hardware entre la salida del área de trabajo y el punto de distribución de planta. Estas rutas y espacios son los "*contenedores*" del cableado horizontal.

.

- Gráficamente:



- Es uno de los subsistemas más importantes a la hora del diseño.
- En el diseño se debe tener en cuenta los servicios y sistemas que se tienen en común:
  - Sistemas de voz y centrales telefónicas
  - Sistemas de datos
  - Redes LAN
  - Sistemas de video
  - Sistemas de seguridad
  - Sistemas de control
  - Otros servicios

- No se permiten puentes, derivaciones y empalmes a lo largo de todo el trayecto del cableado.

- Se debe considerar su proximidad con el cableado eléctrico que genera altos niveles de interferencia electromagnética (motores, elevadores, transformadores, etc.) y cuyas limitaciones se encuentran en el estándar **ANSI/EIA/TIA 569**.

- **TOPOLOGÍA:** Se utiliza **topología en estrella**. Es decir, todos los nodos o estaciones de trabajo se conectan con cable UTP,STP, o fibra óptica hacia un concentrador que será un PATCH PANEL ubicado en un armario de telecomunicaciones de cada piso.

  Un cable para cada salida en los puestos de trabajo.

  Todos los cables del cableado horizontal deben estar terminados en cajas y paneles.

  El **estándar ANSI/TIA/EIA 569** especifica que cada piso deberá contener por lo menos un armario para el cableado y que por cada 1000 m^2 se deberá agregar un armario para el cableado adicional. Asimismo, si el cableado horizontal supera los 90m también se deberá añadir un nuevo armario.

- **DISTANCIA MÁXIMA DEL CABLE:** La **máxima longitud** permitida independientemente del tipo de medio de transmisión utilizado es **90m** (en total el cable UTP admite 100m que serán= 90 m cable horizontal+ 3 m área trabajo + 7 m cables patch pannel). Los cables “patch pannel” se llaman **cables de conexión cruzada y de puenteo** e interconectan el cableado horizontal con el vertical en el armario de telecomunicaciones.

- **TIPOS DE CABLE:** Los **cables permitidos** para este subsistema según la ANSI/TIA/EIA 568 son:

  - ***Par trenzado de 4 pares***:

    - ***UTP (UnshleldedTwistedPair)***: Par trenzado sin blindaje) -100 ohms, 22/24 AWG, cat 5e y 6.

      - ***STP (ShieldedTwistedPair)*** :Par trenzado con blindaje -150 ohms, 22/24 AWG, cat 5e y 6.

  - ***Fibra Optica multimodo 62.5/125 y 50/125 µm de 2 fibras o más fibras.***.

- El cable a usar debe ser con protección antiincendios. Este tipo de cables son cables **plenum o riser. Los plenum** proporcionan más protección antiincendios que los **riser.**

- Las **categorías de cable permitidas son:**

  - ***Cableado de categoría 1 :***
    Descrito en el estándar EIA/TIA 568B. El cableado de Categoría 1 se utiliza para comunicaciones telefónicas y no es adecuado para la transmisión de datos.
  - ***Cableado de categoría 2 :***
    El cableado de Categoría 2 puede transmitir datos a velocidades de hasta 4 Mbps.
  - ***Cableado de categoría 3 :***
    El cableado de Categoría 3 se utiliza en redes 10BaseTy puede transmitir datos a velocidades de hasta 10 Mbps.
  - ***Cableado de categoría 4 :***
    El cableado de Categoría 4 se utiliza en redes TokenRingy puede transmitir datos a velocidades de hasta 16 Mbps.
  - ***Cableado de categoría 5 :***
    El cableado de Categoría 5 puede transmitir datos a velocidades de hasta 100 Mbps. O 100 BaseT
  - ***Cableado de categoría 6:***
    Redes de alta velocidad hasta 1Gbps (Equip

- **MANEJO DEL CABLE:** El destrenzado de pares individuales en los conectores y páneles de empate (patch panels) debe ser menor a 1.25 cm. para cables UTP categoría 5.

  El radio de doblado del cable no debe ser menor a cuatro veces el diámetro del cable.

  Para par trenzado de cuatro pares categoría 5 el radio mínimo de doblado es de 2.5 cm.

- **EVITADO DE INTERFERENCIA ELECTROMAGNÉTICA:** Se debe evitar el paso del cable por los siguientes dispositivos:

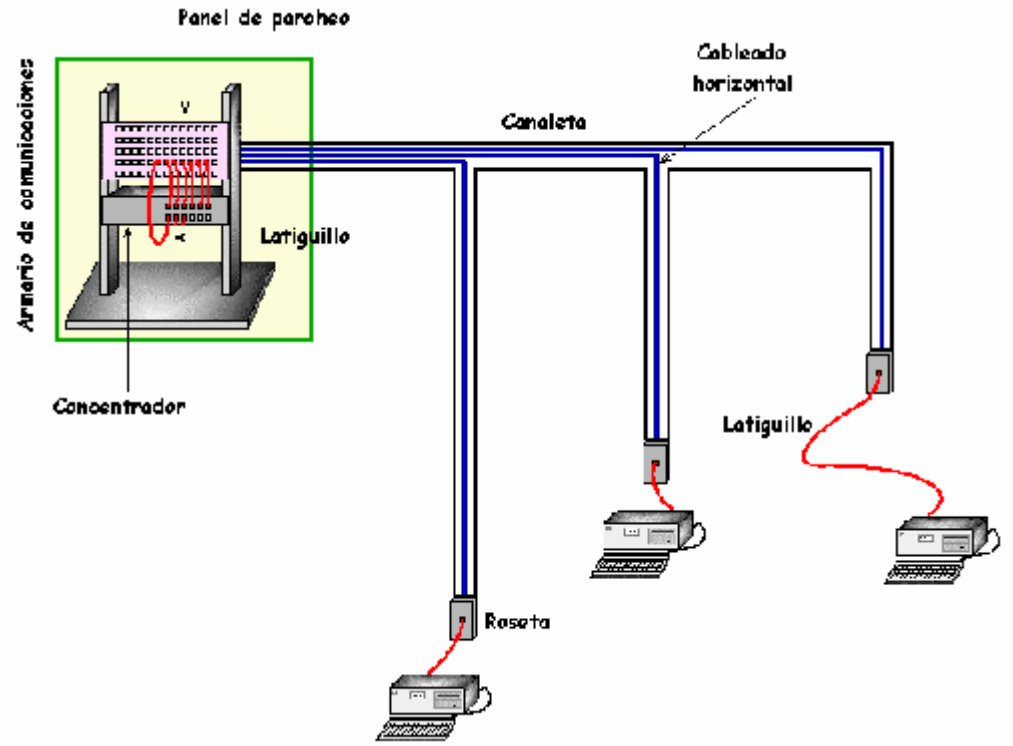
  - Motores eléctricos grandes o transformadores (mínimo 1.2 metros).
  - Cables de corriente alterna
  - Luces fluorescentes (mínimo 12 centímetros). El ducto debe ir perpendicular a las luces fluorescentes y cables o ductos eléctricos.

- Intercomunicadores (mínimo 12 cms.)
- Equipo de soldadura

.

- Aires acondicionados, ventiladores, calentadores (mínimo 1.2 metros).
- Otras fuentes de interferencia electromagnética y de radio frecuencia.

- Las canaletas van desde el panel de parcheo hasta las rosetas de cada uno de los puestos de la red.



- ***Es muy conveniente que el panel de parcheo junto con los dispositivos de interconexión centralizada (concentradores, latiguillos, router, fuentes de alimentación, etc.) estén encerrados un armario de comunicaciones***. De esta forma se aíslan del exterior y por lo tanto de su manipulación "accidental". También facilita el mantenimiento al tenerlo todo en un mismo lugar.

6.3.3.-**SUBSISTEMA VERTICAL**

- También conocido como cableado **troncal**, permite la interconexión entre los distribuidores de cableado de las distintas plantas en un edificio, o entre distintos edificios en un campus. Es decir, hace la interconexión entre armarios de comunicaciones, salas de equipamientos y entradas y salidas de los edificios.

- Obsérvese que este cableado, agrega el ancho de banda de todas las plantas. Por eso, suele utilizarse otra tecnología de cableado con mayor ancho de banda. Por ejemplo, FDDI o Gigabit Ethernet.

- **TOPOLOGÍA:** En estrella y si se necesita un anillo, éste debe ser lógico y no físico.

- **CABLES RECONOCIDOS:**

  - Cable UTP de 100 Ohmnios. Multipar (**800 mts para voz y 90 mts para datos**)
  - Cable STP de 150 Ohmnios . Multipar (**90 mts para datos**)
  - Cable de múltiples Fibras Opticas 62.5/125 µm (**3 km para datos)**.
  - Cable de múltiples Fibras Opticas Monomodo (9/125 µm) (**2 km para datos).**

6.3.4.-**SUBSISTEMA DE ADMINISTRACIÓN O REPARTIDORES**

- Este subsistema se divide en dos:

  - **Administración principal:** es el repartidor principal del edificio en cuestión, normalmente ubicado en el sótano o planta baja y a donde suele llegar el cable de la red pública y 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.

- Los **repartidores** son armarios de comunicaciones se usan para centralizar los paneles de parcheo y equipamientos activos, generalmente de la distribución horizontal, pero también de la intermedia. Están constituidos por unos armarios metálicos de varios tamaños normalizados, a veces con alimentación eléctrica,

en los que se instalan los elementos activos, los paneles de parcheo, etc.

- Existen una serie de normas que regulan el tamaño, ubicación, condiciones de temperatura y humedad,… de los armarios de cableado que dicen:

  - **TAMAÑO:**

    - El armario para el cableado debe ser lo suficientemente espacioso como para alojar todo el equipo y el cableado necesario, así como incluir espacio adicional para un futuro crecimiento.

    - El **estándar ANSI/TIA/EIA 569** especifica que cada piso deberá contener por lo menos un armario para el cableado y que por cada 1000 m^2 se deberá agregar un armario para el cableado adicional. Asimismo, si el cableado horizontal supera los 90m también se deberá añadir un nuevo armario.

    - Los armarios los hay de diferentes anchuras y alturas normalizadas (es muy típico de 19").

  - **UBICACIÓN DEL ARMARIO:**

    - Para buscar la ubicación del armario: 1º se debe hacer un plano del piso o consultar los planos del edificio.

    - El armario principal **debe estar lo más cerca posible** de la entrada al edificio de los servicios de telecomunicaciones proporcionados por la compañía telefónica.

    - Cualquier ubicación que se elija para instalar el armario, debe satisfacer ciertos requisitos ambientales, que incluyen suministro eléctrico y aspectos relacionados con el sistema de calefacción/ventilación/aire acondicionado. Además el armario debe protegerse contra el acceso no autorizado y debe cumplir con todos los códigos de construcción y de seguridad aplicables.

    - Cualquier habitación o armario que se elija para servir de armario para el cableado debe cumplir con las pautas que rigen aspectos como:

      a) Materiales para paredes, pisos y techos

b) Temperatura y humedad

c) Ubicaciones y tipo de iluminación

d) Tomacorrientes

e) Acceso a la habitación y al equipamiento

f) Acceso a los cables y facilidad de mantenimiento.

- **PAREDES, PISOS Y T ECHOS:**

  - Siempre que sea posible, la habitación deberá tener el piso elevado a fin de poder instalar los cables horizontales entrantes que provienen de las áreas de trabajo. Si esto no fuera posible, deberá instalarse un bastidor de escalera de 30,5 cm. en una configuración diseñada para soportar todo el equipamiento y el cableado propuesto.

  - El piso deberá estar revestido de cerámica o cualquier otro tipo de superficie acabada. Esto ayuda a controlar el polvo y protege al equipo de la electricidad estática.

  - Además se deben usar materiales de prevención de incendios que cumplan con todos los códigos aplicables en la construcción del armario para el cableado.

  - Los techos de las habitaciones no deben ser techos falsos. Para evitar el acceso no autorizado.

- **TEMPERATURA Y HUMEDAD:**

  - El armario para el cableado deberá incluir suficiente calefacción/ventilación/aire acondicionado como para mantener una temperatura ambiente de aproximadamente 21 º C cuando el equipo completo de la LAN esté funcionando a pleno.

  - No deberá haber cañerías de agua ni de vapor que atraviesen o pasen por encima de la habitación, salvo un sistema de rociadores, en caso de que los códigos locales de seguridad contra incendios así lo elijan.

- **ACCESO A LA HABITACIÓN Y AL EQUIPAMIENTO:**

  - La puerta de un armario para el cableado deberá tener por lo menos 0,91 m. de ancho, y deberá abrirse hacia fuera de la habitación, permitiendo de esta manera que los trabajadores puedan salir con facilidad.

  - La cerradura deberá ubicarse en la parte externa de la puerta, pero se debe permitir que cualquier persona que se encuentre dentro de la habitación pueda salir en cualquier momento.

6.3.5.-**SUBSISTEMA SALA DE EQUIPOS**

- **La sala de equipos** se define como el espacio donde residen los equipos de telecomunicaciones comunes de un edificio. Estos equipos pueden ser: centrales telefónicas (PBX), centrales de video, Servidores, etc. Se ubicarán aquí todos los elementos necesarios **distribuidos sobre una pared, o preferiblemente en un armario o armarios de 19" o de otra medida**. Se podrán añadir elementos que mejoren el servicio como SAI's, etc.

- Solo se admiten equipos directamente relacionados con los sistemas de telecomunicaciones.

- En su diseño se debe prever tanto para equipos actuales como para equipos a implementar en el futuro.

- El tamaño mínimo recomendado es 13.5 m^2.

- Si un edificio es compartido por varias empresas la Sala de Equipos puede ser compartido.

- Es recomendable que esté ubicada **cerca** de las canalizaciones backbone del edificio.

- Los componentes que debe incluir cualquier sala de equipos son:

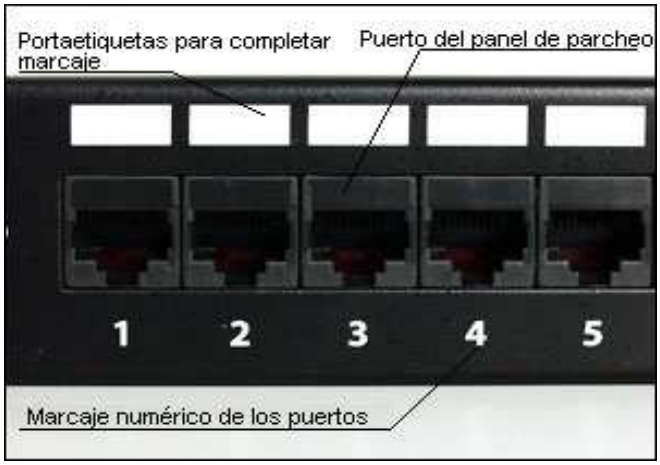
a) ***Estantes de equipos también llamados BASTIDORES (cuando van desde el suelo):*** proporcionan una plataforma segura y estable para todos los componentes hardware. Suelen tener 19" de ancho, pero varían en altura. Así, los hay de atornillar a la pared o incluso que van del suelo al techo.

b) ***Paneles de conexiones y cables o "paneles de parcheo" o patch panels:*** Un panel de conexiones es una caja con una fila de conectores hembra (puertos) delante y conexiones permanentes detrás, a las que se conectan los cables horizontales del cableado estructurado.

Ejemplo:

En la parte frontal del panel de conexión, los puertos están numerados y tienen unos portaetiquetas (espacio para poner etiquetas) para poder etiquetar y nombrar así, cada uno de los puertos. Es **muy importante etiquetar** para sabér a dónde va cada cable y así tenerlo identificado en caso de fallo. El estándar TIA/EIA 606 pone las normas de etiquetado, aunque cada empresa puede usar unos códigos internos de etiquetado.

En la parte posterior se conectan los cables provenientes del cableado horizontal.



Los paneles de parcheo *se diferencian por la cantidad de puertos, por la categoría y por el método de sujeción*:

- Según *la cantidad de puertos*: los paneles más conocidos son de 12, 24 y 48 puertos. Pero también los hay de 16, 32 e incluso más puertos.

- Según la *categoría:* habitualmente se usan los de las categorías 5e y 6.

Panel de parcheo de la categoría 5e con patch cords

- Según el *método de sujeción:* los hay para instalar en pared y los hay para instalar en armarios o racks de 19" principalmente.

- También los hay para diferentes tipos de puertos: UTP, STP, fibra óptica,…

c) ***Cables de conexión o "patch cord":*** son cables UTP cortos (hasta 6 m aproximadamente) que nos permiten unir los patch panels a los distintos equipos activos que tengamos en el armario o rack (routers, switcho, hub,…). Normalmente los patch cord son **directos.** Pero existen **crossover cord** que son cruzados.

Los hay de diferentes colores.

d) ***Organizadores de cables***

6.3.6.-**SUBSISTEMA CAMPUS**

- Este subsistema es el que se encarga de conectar dos o más edificios que tengan cableado estructurado y los pone en comunicación.
- Comprende el conjunto de dispositivos (cable, protecciones, interfaces, adaptadores) que permiten la conexión y la comunicación entre los sistemas de cableado estructurado que tienen instalado los edificios.
- Se puede usar cable UTP, multipares o fibra ópticas para exteriores con características especiales según el terreno y método utilizado para su distribución.
- Dentro de los sistemas de distribución más utilizados encontramos el tendido aéreo mediante postes metálicos o, tuberías o ductos enterrados y finalmente cable enterrado directamente.

6.4. Etiquetado del cable

Aunque no se use el etiquetado oficial EIA/TIA 606, **sí que se debe etiquetar de todas formas las líneas.**

Se debe diseñar un sistema de etiquetado para toda la empresa: por ejemplo, se puede hacer que todas las conexiones del lado norte del edificio empiecen con la letra N, seguida de un nº de 3 dígitos empezando en 001. Una vez diseñado el sistema de etiquetado, se usará.

La parte más importante del etiquetado es que los dos extremos de un cable deben decir lo mismo. Por ejemplo, un cable que va al patch panel en un extremo con la etiqueta N001, y en el otro extremo termina en una roseta. Esa roseta debe etiquetarse como N001.

6.5. Probar las líneas de cable

Una vez instalado el sistema de cableado, se deben probar todas las líeas de cable. Esta prueba no consiste sólo en verificar que cada conector está enchufado correctamente, sino que se deben comprobar varios parámetros como son: verificar que la línea es capaz de manejar la velocidad de la red, ratio atenuación-cruce,...
Normalmente un administrador o técnico de red típico no puede probar de forma apropiada una nueva línea de cable. El EIA/TIA proporciona una serie de importantes estándares muy complejos para probar cables. Por eso se suele contratar a un profesional instalador de cable para realizar las pruebas. Además, el **equipo necesario** para realizar las pruebas sobrepasa el coste de la mayoría de las instalaciones de red pequeñas. Estas herramientas pueden costar más de 10.000€.

Algunas preguntas que se pueden hacer los administradores pueden ser:

- ¿Cuán largo es el cable?
- ¿Alguno de los cables está roto?
- Si hay uno roto, ¿dónde está?
- ¿Hay algún cable formando cortocircuito?
- ¿Hay algún cable que no esté en el orden apropiado (hay pares divididos o cruzados)?
- ¿Hay interferencias eléctricas o de radio?

Veremos algunas herramientas de gama baja que responden a alguna de esas preguntas:

a) **Comprobador de cable:**

a.1) ***Comprobadores de continuidad:*** sólo comprueban si hay cables rotos o no. Un cable que puede conducir electricidad se dice que

tiene continuidad; por tanto, un cable roto carece de continuidad. Suelen costar menos de 100€

a.2) ***Tester de cable (cable Tester)***: Son comprobadores de cable que además de la continuidad o no, también buscan pares divididos o cruzados y cortocircuitos. En estos se requiere normalmente que se inserten los 2 extremos del cable en el comprobador. Esto es un problema si el cable ya está instalado en la pared.

Multi Modular Cable Tester LAN/USB

a.3) ***Comprobadores TDR (reflectómetro del dominio del tiempo)***: Es un comprobador de precio medio y tiene la capacidad de determinar la longitud de un cable e incluso puede decir dónde se encuentra la rotura.

Network Cable Tester SC8108

b) **Certificadores de cable:**

Comprueban características eléctricas del cable y generan un informe que el instalador puede imprimir y presentar como certificado de que las líneas de cable están conforme a los estándares de la EIA/TIA.

Algunos de estos aparatos tiene potentes funciones añadidas como la capacidad de conectar con la red y, literalmente, dibujar un esquema de toda la red, incluyendo información como las MAC de los sistemas, las IP o incluso los sistemas operativos de los ordenadores.

Certificador Cat 6 / 5E - Microtest Omniscanner (3.400€)

c) **Generador de tonos:**

Es un dispositivo que permite **rastrear un cable**, es deci, seguir la pista de por dónde va el cable en una instalación de cableado.

En realidad los técnicos usan un dispositivo llamado **tóner o rastreador** que es un nombre genérico que usan para 2 dispositivos distintos que se usan juntos: **un generador de tonos y una sonda de tonos.**

El generador de tonos se conecta al cable usando clips, pequeños ganchos o un enchufe de red, y envía una señal eléctrica a lo largo del cable a determinada frecuencia.

La sonda de tonos emite un sonido cuando se pone cerca de un cable conectado al generador de tonos.

Estos 2 dispositivos a menudo reciben el nombre de marca **Fox (zorro) y Hound (sabueso),** un popular modelo de rastreador fabricado por Triplett Corporation.

Para rastrear un cable, conecte el generador de tonos en el extremo conocido del cable en cuestión y después ponga la sonda de tonos cerca del otro extremo del grupo de cables entre los que puede estar el correcto. La sonda de tonos emitirá un sonido cuando esté cerca del cable correcto.

Otros rastreadores más avanzados incluyen clavijas de teléfono, permitiendo a la persona que manipula el generador de tonos comunicarse con la persona que manipula la sonda de tonos: “¡Luis, pon el generador de tonos en el siguiente puerto!”.

Cada generador emite una frecuencia distinta.

Los rastreadores son baratos (menos de 50€).