Tema 6°: IMPLANTACIÓN DE UNA RED DE ÁREA LOCAL

1. *Consideraciones previas*
2. *Otros protocolos de Red y de Transporte*
3. *Protocolos asociados a la arquitectura TCP/IP*
4. *Dispositivos Hardware utilizados en Redes*
5. *Instalación de una Red de Área Local (Windows 2000)*

6.1.- Consideraciones previas

Un **Sistema Operativo en Red** (NOS – Network Operating System) es el software que hace que un sistema informático pueda comunicarse con otros equipos en el ámbito de una red. Este software de red viene habitualmente integrado en el Sistema Operativo, pero a veces, en Sistemas Operativos antiguos, se necesita una instalación añadida a la del propio sistema en el equipo. Son ejemplos de software de red integrado en el S.O. Windows 98, NT, 2000, XP; Apple MacOS, Unix, Linux, etc.

Mientras que un ejemplo de software de red no integrado en el S.O. es el MS DOS. que en sus últimas versiones integraba programas de comunicaciones para que los usuarios pudieran hacer transferencias de ficheros a través de líneas serie sin necesidad de utilizar productos añadidos. Es el caso de utilidades como *Interlink – Interserver de DOS.*

Ejemplos de software añadido, es decir, productos que deben instalarse sobre DOS. para interactuar con otros nodos utilizando un adaptador de red, son Novell, Lantastic, etc.

Actualmente, los S.O. de red están perfectamente integrados, no sólo en funciones estrictas de red, sino que también se han constituido en plataformas, tanto de desarrollo de aplicaciones como de explotación de las mismas, en las que la red es una parte de los recursos del sistema. El desarrollo de la tecnología Internet ha estimulado especialmente esta integración; así, han aparecido tecnologías como *Intranet, Extranet, e-commerce, e-business,* etc.

La mayor parte de los Sistemas Operativos gestionan los recursos de la Red formando **Grupos de Trabajo**, de modo que se facilite su administración y gestión. Se define entonces el Grupo de Trabajo como una *agrupación simple de equipos, destinada únicamente a ayudar a los usuarios a buscar elementos como impresoras y carpetas compartidas en ese grupo.*

Los equipos de un grupo de trabajo se consideran del mismo nivel porque todos son iguales y comparten los recursos entre sí sin requerir un servidor. Cada usuario determina qué datos de su equipo se compartirán en la red. Compartir recursos comunes permite a los usuarios imprimir desde una sola impresora, tener acceso a información de carpetas compartidas y trabajar en un archivo único sin necesidad de transferirlo a un disco.

Por el contrario, un **Dominio** en una red *es un grupo de equipos que forman parte de una red y comparten una base de datos de directorio común. Un dominio se administra como una unidad con reglas y procedimientos comunes. Cada dominio tiene un nombre único.*

Un dominio puede estar constituido por un grupo de trabajo, al que se añaden otros aspectos como el de la centralización en la gestión de red, facilidades para la administración de los equipos, control de los usuarios y contraseñas, jerarquización de los recursos, etc.

Cuando en comunicaciones se utiliza el término ***dominio*** debe tenerse en cuenta que es un concepto ambiguo. Cada tecnología de red tiene un concepto distinto de dominio, aunque las características generales del concepto sean siempre las mismas. Así, en *Windows NT* o *2000* el concepto de dominio tiene mucha mas entidad que en el mundo Unix: Un ***dominio Windows*** lleva asociadas capacidades de gestión de recursos, de usuarios, políticas de administración de red, gestión de escritorios, etc.

Un ***dominio*** en ***Internet***, sin embargo, no es mas que un sinónimo cualificado y perfectamente estructurado para el nombre que recibe un nodo dentro de la propia Internet.

Un **servicio** es un programa, rutina o proceso que realiza una determinada función del sistema para ofrecer compatibilidad con otros programas, especialmente a bajo nivel (cerca del hardware).

Un **servicio de directorio** no es mas que *una base de datos jerárquica y organizada en forma de objetos que contienen información fácilmente accesible y útil para el sistema operativo, la red o los usuarios que solicitan recursos del sistema.*

Windows define el ***servicio de directorio*** como "tanto el origen de información del directorio como el servicio que hace que dicha información esté disponible para los usuarios. Un servicio de directorio permite a los usuarios encontrar un objeto con cualquiera de sus atributos". Cuando se ofrecen servicios a través de una red, se pueden publicar en Active Directory, facilitando así la administración y el uso centralizados de los mismos. Algunos ejemplos son el servicio Administrador de cuentas de seguridad, Replicación de archivos y el Servicio de enrutamiento y acceso remoto.

6.2.- Otros protocolos de red y de transporte

Entre los protocolos de red y de transporte mas utilizados se encuentran *IPX/SPX, NetBIOS/NetBEUI y TCP/IP* del que se ha hecho referencia en el capítulo anterior.

6.2.1.- IPX/SPX

Los protocolos de comunicación y transporte IPX/SPX fueron desarrollados por Novell a principio de los años ochenta, inspirándose en los protocolos del *Sistema de Red de SEROX (XNS).*

Sirven de interfaz entre el sistema operativo en red NetWare y las distintas arquitecturas de red (Ethernet, Token Ring, etc.). Consiste en una variedad de protocolos iguales tales como:

- IPX (Internetwork Packet Exchange)
- SPX (Sequential Packet Exchange)

- NCP (Network Core Protocol)
- RIP (Router Information Protocol)
- SAP (Service Advertising Protocol)

Novell ha implementado también el emulador **NetBIOS** para que las aplicaciones que utilicen NetBIOS puedan usar el protocolo IPX como protocolo de red.

Además se utilizan los protocolos *Echo y Error* para mantenimiento interno.

IPX (Internetwork Packet Exchange)

El protocolo de red IPX es un protocolo que transmite los datos en **datagramas** (paquetes autocontenidos que viajan de forma independiente desde el origen al destino en modo sin conexión pero no espera una confirmación de la estación receptora indicando si ha recibido correctamente o no el bloque de datos). De esta manera se mejora el rendimiento de la transmisión, pero no se pierde en fiabilidad de los datos por dos razones:

- Cada bloque de datos IPX contiene una *suma de comprobación* CRC que garantiza un 99 % de precisión
- En caso de no haber contestación en un intervalo determinado de tiempo, IPX reenvía el paquete de forma automática.

La estructura de un bloque de datos IPX es:

Campo	Tamaño
Suma de Comprobación	**2 Bytes**
Longitud	**2 Bytes**
Control de transporte	**1 Bytes**
Tipo de Paquete	**1 Bytes**
Red de destino	**4 Bytes**
Nodo de destino	**6 Bytes**
Conector de destino	**2 Bytes**
Red de origen	**4 Bytes**
Nodo de origen	**6 Bytes**
Conector de origen	**2 Bytes**
Datos	**N Bytes**

SPX (Sequential Packet Exchange)

El protocolo de transporte SPX es una extensión del protocolo de red IPX de superior nivel, orientado a conexión.

SPX utiliza IPX para enviar y recibir paquetes pero añade un interfaz para establecer una sesión entre la estación emisora y la receptora, de esta manera, se tiene una confirmación explícita de la recepción del paquete.

Además proporciona un mecanismo de secuenciación de paquetes. Como IPX envía los paquetes por el mejor camino disponible, es posible que los paquetes lleguen a la estación receptora en orden distinto al que fueron enviados, lo que provoca que lleguen fuera de secuencia. Así, SPX de la estación receptora puede organizar los paquetes en el orden adecuado o reclamar únicamente los paquetes perdidos.

Los paquetes SPX tienen la misma estructura de los IPX pero añadiendo a la cabecera un campo de 12 Bytes para el control de la conexión y el número de secuencia del paquete.

NCP (Network Core Protocol)

El protocolo NCP es un conjunto propietario de mensajes bien definidos que controlan el funcionamiento del servidor y son la clave del acceso a los servicios de NetWare

Define el procedimiento que sigue NetWare para aceptar y responder a las solicitudes de las estaciones. Existen protocolos de servicio NCP para cada servicio que una estación pueda solicitar a un servidor y, sin ellos, la estación no podría sacar ningún servicio del servidor.

Los NCP se pasan al servidor mediante paquetes IPX marcados de forma especial. No obstante, se pueden transmitir con cualquier otro protocolo de datagramas (por ejemplo, UDP en las redes basadas en TCP/IP).

RIP (Router Information Protocol)

Es un protocolo de información de encaminamiento que incorpora NetWare y se encarga de llevar los paquetes a su destino entre dos redes

Cada servidor realiza un seguimiento de los otros servidores a intervalos regulares y conserva su posición y distancia en una tabla de información sobre el encaminamiento.

Si un servidor detecta una inconsistencia, un encaminador existente lo notifica a los demás para que actualicen sus tablas. Si un encaminador falla, los demás encaminadotes lo descubren y buscan rutas alternativas que no tienen en cuenta al encaminador defectuoso.

El proceso de encaminamiento utiliza esa información para transmitir los paquetes por la ruta mas corta hasta su destino final.

SAP (Service Advertising Protocol)

El protocolo SAP es un mecanismo mediante el cual NetWare distribuye por toda la red información de los servicios disponibles.

Necesita un servidor que anuncie tres unidades de información a la red cada minuto: el nombre del servidor, el tipo de servidor y su dirección de red.

El resto de servidores recogen la información y la guardan en la tabla correspondiente.

Cuando un servidor descubre que se está desactivando, se lo indica a SAP y éste lo transmite a los demás servidores, que lo guardan en su tabla correspondiente.

Si un servidor deja de transmitir sin previo aviso, SAP supone que no está disponible y lo transmite a toda la red para que los demás servidores actualicen sus respectivas tablas.

6.2.2.- NETBIOS / NETBEUI

Cuando se empezaron a desarrollar las redes locales, IBM introdujo el protocolo NETBIOS (Network Basic Input/Output System), debido a la falta de normas estándar para los niveles superiores.

NETBIOS mantiene la sesión enviado periódicamente un bloque de dato sal nodo remoto, para informarle de que se encuentra disponible y que puede recibir datos, por lo que utiliza ciclos de memoria de manera continua aunque la aplicación del usuario no realice peticiones.

Novell hizo una implementación de NetBIOS para IPX de una forma análoga a SPX. Pero no genera bloques compatibles con el NetBios de IBM por lo que no puede comunicarse con otra red que utilice el entorno IBM.

El protocolo NetBEUI (NetBios Extended User Interface) es la extensión para NetBios utilizada por LAN manager y Microsoft Windows que corresponde a los niveles de red y transporte y que se utiliza en redes pequeñas, debido a la sencillez de configuración.

Entre sus inconvenientes se encuentra que no se puede utilizar para comunicarse con una red remota, ya que no permite el encaminamiento.

En estos protocolos, la identificación del equipo se hace con el *nombre de PC* (que se encuentra en *Identificación* del icono *Red* del *Panel de control*) y con 6 Bytes de la dirección de la tarjeta de red del ordenador.

6.3.-Protocolos asociados a la arquitectura TCP/IP

Utilizados por la arquitectura TCP/IP en sus distintos niveles se utilizan, o se pueden utilizar, los siguientes protocolos:

6.3.1.- Protocolos de nivel físico

Aunque TCP/IP no considera oficialmente el nivel físico como componente específico de su modelo y tiende a agrupar el nivel físico con el nivel de red, se describen en este apartado los protocolos ARP y RARP.

ARP (Address Resolution Protocol)

Es un protocolo que se utiliza para convertir las direcciones IP en direcciones físicas que puedan ser utilizadas por los manejadores.

Para poder realizar esta conversión, existe en cada ordenador un módulo ARP que utiliza una *tabla de direcciones ARP*, que, en la mayoría de los ordenadores se trata como si fuera una memoria intermedia (*caché*), de forma que la información que lleva mucho tiempo sin utilizarse se borra.

Si encuentra la correspondencia entre la dirección IP y la dirección física se procede a la transmisión.

Si no la encuentra en la tabla, se genera una petición ARP que se difunde por toda la red. Si alguno de los ordenadores reconoce su propia dirección IP en la petición ARP, envía un mensaje de respuesta indicando su dirección física y se graba en la tabla de direcciones ARP.

RARP (Reverse Address Resolution Protocol)

Este protocolo se utiliza cuando, al producirse el arranque inicial, los ordenadores todavía no conocen su propia dirección IP.

Requiere que exista en la red, al menos, un servidor RARP. Cuando un ordenador desea conocer su dirección IP envía un paquete que contiene su propia dirección física.

El servidor RARP, al recibir el paquete, busca en su tabla RARP la dirección IP correspondiente a la dirección física inicial indicada en el paquete y envía un paquete al ordenador origen con esta información.

A diferencia del protocolo ARP que se incorpora normalmente en todos los productos TCP/IP, el protocolo RARP sólo se incorpora con unos pocos productos.

6.3.2.- Protocolos de nivel de red

Aunque TCP/IP no especifica ningún protocolo para este nivel, se van a describir los protocolos SLIP, PPP y PPTP.

SLIP (Serial-Line Internet Protocol)

Es, históricamente, el primer protocolo que se desarrolló para satisfacer la necesidad de establecer una conexión TCP/IP empleando únicamente una línea serie.

La utilización actual más común de este protocolo es la conexión (a Internet, por ejemplo) a través de una línea telefónica, aunque también puede utilizarse para conectar dos ordenadores próximos mediante un cable serie.

Realiza un mecanismo muy sencillo de transmisión de paquetes. De hecho, su único cometido es el envío de datagramas en formato IP a través de una línea serie.

Sus inconvenientes más significativos son:

- Carece de métodos de corrección de errores, delegando estas funciones en las capas superiores del software.
- Es incapaz de realizar tareas de gestión del enlace.

- Carece de métodos de autentificación

- Es incapaz de negociar parámetros fundamentales de la comunicación (direcciones de red, tamaño de los paquetes o el empleo de algoritmos de compresión de datos). Todas estas características deben establecerse antes de efectuar la conexión, y deben coincidir en ambos extremos del enlace.

Existe una versión de SLIP denominada *CSLIP* que es capaz de comprimir las cabeceras TCP, con el aumento de eficiencia que esto supone por la menor cantidad de datos que se precisa transmitir.

PPP (Point-to-Point Protocol)

Es un protocolo SLIP mejorado con control y recuperación de errores. Funcionalmente es mucho más completo y robusto que SLIP y, además de asumir todas sus funciones, incorpora múltiples mejoras:

- Es posible negociar el tamaño máximo de los paquetes entre los dos extremos o la utilización de técnicas de compresión.

- Existe posibilidad de autentificación

- Puede monitorizarse la calidad del enlace

Una característica que hace a PPP aún mas interesante es la posibilidad de conexión a través de RDSI.

Existe una gran cantidad de software comercial y de dominio público disponible para PPP.

PPTP (Point to Point Tunnelling Protocol)

Aunque no es protocolo propio de TCP/IP, se describe en esta sección ya que es un nuevo protocolo de red, incorporado en Windows, que utiliza redes privadas multiprotocolo para permitir a los usuarios remotos tener acceso de forma segura, a través de Internet, a redes de Empresas (Extranet)

Ofrece las siguientes ventajas:

- **Costes de transmisión mas bajos**. Ya que usa Internet para la conexión, en lugar de una llamada normal a través de la línea telefónica

- **Menores costes de hardware.** Ya que permite separar los módems y las tarjetas RDSI , así como colocarse en un servidor de comunicaciones

- **Mayor nivel de seguridad.** Funciona con cifrado de datos y actúa con cualquier protocolo.

Los datos enviados con PPTP se encapsulan en paquetes PPP cifrados, que se envían a través de Internet, aunque también puede ser usado para transportar el tráfico de acceso remoto IPX y NetBEUI.

6.3.3.- Protocolos de nivel de Internet

En este nivel se encuentran los protocolos ICMP e IP

ICMP (Internet Control Message Protocol)

Es un protocolo de mantenimiento/gestión de red que ayuda a supervisar la red.

Se utiliza para poder encontrar una ruta a través de la cual los datagramas viajen por la red y alcancen su destino.

El objetivo principal de ICMP es proporcionar la información de error o control entre los nodos. La implementación de ICMP es obligatoria como un subconjunto lógico del protocolo IP. Los mensajes de error de este protocolo normalmente los genera y los procesa TCP/IP y no el usuario.

Existen cuatro tipos de mensajes ICMP:

- Mensajes de destino no alcanzable.
- Mensajes de control de congestión
- Mensajes de direccionamiento
- Mensajes de tiempo excedido

Una de las utilidades de diagnóstico que utiliza este protocolo es la utilidad PING (que comprueba que un equipo está conectado a la red)

IP (Internet Protocol)

Este protocolo se encarga de seleccionar la trayectoria a seguir por los datagramas, es decir, por donde se deben encaminar los datagramas salientes, pudiendo llevar a cabo tareas de fragmentación y reensamblado.

Este protocolo, que no es fiable ni está orientado a la conexión, no garantiza el control del flujo, la recuperación de errores, ni que los datos lleguen a su destino.

IP no se encarga de controlar que sus datagramas, que envía a través de la red, puedan perderse, llegar desordenados o duplicados. Otros protocolos de nivel de transporte serán los que contemplen estos controles.

Los datagramas IP contienen una cabecera con información para el nivel IP y datos. Estos datagramas se encapsulan en tramas que, dependiendo de la red física utilizada, tienen una longitud determinada.

Cuando los datagramas viajan de unos equipos a otros, pueden atravesar diferentes tipos de redes. El tamaño máximo de estos paquetes puede variar de una red a otra dependiendo del medio físico que se emplee para su transmisión. A este tamaño máximo se le denomina *MTU (Unidad Máxima de Transmisión)* y ninguna red puede transmitir ningún paquete cuya longitud exceda del MTU de dicha red.

Debido a este problema, es necesario reconvertir los datagramas IP en el formato requerido por cada una de las redes que va atravesando. Esto es lo que se denomina *fragmentación y reensamblado*.

La *fragmentación* divide los paquetes en fragmentos de menor longitud (se realiza en el nivel mas inferior posible y de forma transparente al resto de los niveles) y el *reensamblado* realiza la operación contraria.

6.3.4.- Protocolos de nivel de transporte

En este nivel se encuentran los protocolos TCP y UDP.

TCP (Transmisión Control Protocol)

Es un protocolo orientado a conexión que utiliza los servicios del nivel *Internet*.

Al igual que cualquier protocolo orientado a conexión, consta de tres fases:

- **Establecimiento de la conexión.** Se inicia con el intercambio de tres mensajes, garantiza que los dos extremos de la transmisión estén preparados para la transferencia de datos y permite que ambos acuerden los números iniciales de secuencia (cada extremo elige un número de forma aleatoria)
- **Transferencia de datos.** La unidad de datos que utiliza es el *segmento* y su longitud se mide en octetos. La transmisión es fiable ya que permite la recuperación de datos perdidos, erróneos o duplicados, así como garantiza la secuencia de entrega, para lo que se añade a la cabecera del segmento los datos del número de secuencia y un código de control. La fiabilidad de la recepción se consigue mediante la confirmación de la recepción, los temporizadores de espera de confirmación y la retransmisión de segmentos.
- **Liberación de la conexión.** Cuando una aplicación comunica que no tiene mas datos que transmitir, TCP finaliza la conexión en una dirección. Desde ese momento, TCP no vuelve a enviar datos en ese sentido, permitiendo que los datos circulen en el sentido contrario hasta que el emisor cierra también la conexión.

TCP permite *multiplexación*, es decir, una conexión TCP puede ser utilizada simultáneamente por varios usuarios.

Como normalmente existe mas de un proceso de usuario o aplicación utilizando TCP de forma simultánea, es necesario identificar los datos asociados a cada proceso. Para ello se utilizan los ***puertos***. Un ***puerto*** es una palabra de 16 bits que identifica hacia qué aplicación o proceso han de dirigirse los datos.

Hay aplicaciones que tiene asignado el mismo número de puerto, ya que realizan funciones de servidores normalizados que utilizan los servicios TCP/IP. Estos puertos reservados se encuentran en el archivo ***SERVICES*** que, a su vez, se encuentra en el subdirectorio ***ETC*** y corresponden a números superiores a 1, indicando también si corresponden al protocolo TCP o UDP.

Algunos ejemplos de puertos son:

Nº de puerto	Servicio
21	FTP
23	Telnet
25	SMTP

69	TFTP
111	RFC
161	SNMP

Un ***socket*** está compuesto por un par de números que identifican de manera única cada aplicación. Cada socket se compone de dos campos:

1º.- La dirección IP del ordenador en el que se está ejecutando la aplicación.

2º.- El puerto a través del cual la aplicación se comunica con TCP/IP

UDP (User Datagram Protocol)

Es un protocolo que se basa en el intercambio de datagramas. UDP permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

El inconveniente de esta forma de actuación es que no hay confirmación de recepción ni de haber recibido los datagramas en el orden adecuado, debiendo se la aplicación la que se encargue de controlarlo.

Al igual que el protocolo TCP, utiliza puertos y sockets y, también, permite la multiplexación.

6.3.5.- Protocolos de nivel de Aplicación

Todas las aplicaciones TCP/IP utilizan el modelo cliente / servidor.

En este nivel se encuentran un buen número de protocolos de los cuales se van a describir los siguientes: FTP, HTTP, NFS, NTP, RPC, SMTP, SNMP, TELNET y TFTP

FTP (File Transfer Protocol)

Es el mas utilizado de los protocolos da aplicación y uno de los mas antiguos. Se utiliza para transferencia de archivos proporcionando un acceso interactivo, especificaciones de formato y control de autentificación (aunque es posible conectarse como el usuario *anonymous* que no necesita contraseña.

HTTP (HyperText Transfer Protocol)

Es uno de los protocolos mas recientes. Se utiliza para manejar la consulta de hipertexto y el accedo a datos de *World Wide Web* (WWW). El tráfico de este protocolo ha pasado, debido a la influencia de *Internet*, a ser muy grande.

NFS (Network File System)

Ha sido desarrollado por *Sun Microsystems Incorporated*y autoriza a los usuarios el acceso en línea a archivos que se encuentran en sistemas remotos (esto es, accede a un

archivo remoto como si se tratara de un archivo local). La mayoría del tráfico NFS es ahora un caso especial del protocolo RPC.

NTP (Network Time Protocol)

Permite que todos los sistemas sincronicen la hora con un sistema designado como servidor horario

RPC (Remote Procedure Call)

Es una llamada a un procedimiento que se ejecuta en un sistema diferente del que realiza la llamada.

El proceso cliente envía un mensaje al proceso servidor y espera una respuesta. Éste, al recibir la llamada, estudia los procedimientos del proceso llamado, obtiene los resultados y los envía de vuelta al proceso cliente mediante un mensaje de respuesta.

Existen dos tipos de servidores

1º.- El **servidor iterativo** que recibe una llamada, proporciona el servicio y vuelve al estado de espera

2º.- El **servidor concurrente** que recibe la llamada, contesta al mensaje enviando al cliente un número de puerto, arranca un proceso paralelo para prestar el servicio requerido por el cliente y vuelve al estado de espera. Cuando el proceso paralelo haya finalizado el servicio requerido, acaba su ejecución.

SMTP (Simple Mail Transfer Protocol)

Es un protocolo de correo electrónico. Especifica el formato exacto de los mensajes que un cliente debe enviar desde un ordenador al servidor de otro, pero no especifica cómo debe almacenarse el correo ni con qué frecuencia se debe intentar el envío de los mensajes.

SNMP (Simple Network Management Protocol)

Este protocolo sirve para administrar los sistemas de forma remota. También se puede utilizar para supervisar el tráfico de red desde una o varias estaciones de trabajo, llamadas administradores SNMP

Los elementos de una red que puede administrar y monitorizar son dispositivos como ordenadores, puertas de enlace (*gateways*), encaminadotes (*routers*), mainframes, mini ordenadores, hubs, etc.

SNMP minimiza el número y la complejidad de las funciones realizadas por el administrador y cuenta con las siguientes ventajas:

- Reduce el coste de desarrollo del software del agente de administración necesario para soportar este protocolo.
- Aumenta el grado de las funciones de administración utilizadas de forma remota, permitiendo un uso completo de los recursos de *Internet* en dichas tareas

- Permite que las funciones de administración sean de fácil comprensión y uso por parte de los desarrolladores de herramientas de administración de la red.

Utiliza una arquitectura distribuida que consiste en agentes y sistemas de administración

❖ Un **Agente** es un ordenador que ejecuta el software de agente SNMP o un encaminador.

La obligación principal de un agente es ejecutar las tareas iniciadas por los comandos SNMP que han sido requeridas por un sistema de administración.

Los comandos SNMP que se utilizan pertenecen a los tipos siguientes:

- **GetRequest**: Es el comando que usa el sistema de administración para solicitar información a un agente.
- **GetNextRequest**: También es empleado por el sistema de administración para solicitar información al agente y se utiliza si la información deseada se encuentra en forma de tabla o matriz (se usa de forma repetitiva hasta que se hayan conseguido todos los datos de la matriz).
- **GetResponse**: El agente consultado utiliza este comando para contestar una solicitud hecha por el sistema de administración.
- **SetRequest**: El sistema de administración lo utiliza para cambiar el valor de un parámetro del MIB (*Management Information Base*).
- **Trap**: Este comando lo utiliza un agente para informar al sistema de administración de un suceso determinado que se ha producido.

❖ Un **Sistema de administración** es un ordenador que ejecuta un software de administración SNMP. Puede iniciar las operaciones de los comandos *GetRequest GetNextRequest* y *SetRequest.*

Un agente únicamente puede iniciar el comando *Trap* para informar al sistema de administración de un suceso extraordinario y contestar al sistema con el comando *GetResponse*.

La forma que actúa el protocolo SNMP es la siguiente:

1º.- El sistema de administración envía primero una solicitud al agente para obtener el valor de una variable de MIB.

2º.- El agente contesta a la solicitud en función del nombre de la comunidad que acompaña a la solicitud.

Una **comunidad** comprende un grupo de ordenadores que ejecutan el servicio SNMP. El uso de un nombre de comunidad proporciona una seguridad mínima para los agentes que reciben solicitudes e inician capturas (*Traps*) así como para las tareas iniciadas por los sistemas de administración.

Un agente no responderá a una solicitud de un sistema de administración distinto a aquellos que tenga configurados (un agente puede pertenecer a varias comunidades a la vez).

MIB describe los objetos que están incluidos en la base de datos de un agente SNMP. Los objetos que haya en MIB deben estar definidos para que los desarrolladores de software para la administración de las estaciones de trabajo los conozcan, así como sus valores respectivos.

MIB registra y almacena información sobre el ordenador en el que se está ejecutando. Un administrador SNMP puede solicitar y recoger información de un agente MIB así como revisar o alterar los objetos que contiene.

TELNET

TELNET permite que un usuario, desde un terminal, acceda a los recursos y aplicaciones de otros ordenadores. Una vez que la conexión queda establecida, actúa de intermediario entre ambos ordenadores.

Se fundamenta en tres principios:

- El **concepto de terminal virtual de red** *(NVT)*. Corresponde a la definición de cómo han de ser los datos, caracteres de control y las secuencias de los mandatos que han de circular por la red para permitir una heterogeneidad de los sistemas.

- La **simetría entre terminales y procesos.** La comunicación puede ocurrir entre dos terminales, dos procesos o entre un terminal y un proceso.

- **Permite que el cliente y el servidor negocien sus opciones.** La conexión comienza con una fase de negociación de opciones en las que se utilizan cuatro mandatos: WILL, WONT, DO y DONT.

WILL se envía para mostrar el deseo de comenzar una opción (que se ha de indicar) y se contesta con DO (respuesta positiva) o DONT (respuesta negativa).

WONT se envía para mostrar el deseo de no comenzar una opción (que se ha de indicar) y se contesta con DONT (mostrando el acuerdo de no utilización)

DO se envía para indicar que comience a utilizar una opción (que se ha de indicar) y se contesta con WILL (respuesta positiva) o WONT (respuesta negativa)

DONT se envía para indicar que no comience a utilizar una opción (que se ha de indicar) y se contesta con WONT (mostrando el acuerdo de no utilización)

TFTP

Es un protocolo destinado a la transferencia de archivos aunque sin permitir una interacción entre cliente y servidor como la que existe en FTP.

Además existe otra diferencia. En lugar de utilizar el protocolo TCP utiliza el protocolo UDP.

Sus reglas son muy sencillas. En el envío del primer paquete se establece una interacción entre el cliente y el servidor. Se empieza una numeración de los bloques (empezando desde 1). Cada paquete de datos contiene una cabecera que especifica el bloque que contiene. Un bloque de menos de 512 octetos indica que es el último y corresponde al final del archivo.

6.4.- Dispositivos Hardware utilizados en Redes

6.4.1.- Tarjetas de red

La tarjeta de red actúa como interfaz física de conexión entre el ordenador y el cable de red. Se coloca en una ranura de expansión de cada ordenador de la red. Después de que la tarjeta ha sido instalada, se conecta el cable de red a la puerta de la misma para hacer la conexión física actual entre los ordenadores y el resto de la red.

Una tarjeta realiza las siguientes acciones:

- **Prepara los datos del ordenador para su envío a la red**. Los datos se mueven en el ordenador, a través del *bus de datos*, en forma de bits en paralelo (los viejos buses, como los usados en el original IBM-PC se conocían como buses de 8 bits, ya que sólo podían mover 8 bits simultáneamente. El IBM-PC-AT usaba un bus de 16 bits. Actualmente se utilizan buses de 32 y 64 bits) y, cuando llegan a la tarjeta, los transmite en forma de bits en serie.

- **Envía dichos datos a la red**. Indicando su dirección para distinguirlos de otras tarjetas de red (la dirección de red son 12 dígitos hexadecimales y son determinadas por la IEEE). El Comité asigna bloques de direcciones a cada fabricante de tarjetas. Los fabricantes introducen esas direcciones en *chips* en las tarjetas mediante un proceso conocido por *burning*. Mediante este proceso, cada tarjeta, y por lo tanto cada ordenador, tiene una dirección física única en la red.

- **Controla el flujo de datos** entre el ordenador y el sistema de cableado

- **Recibe los datos entrantes en serie** del cable y los traduce en octetos en paralelo que el ordenador pueda comprender.

Antes de que la tarjeta emisora envíe datos a la red, se establece un diálogo electrónico con la tarjeta receptora para que ambas se pongan de acuerdo en lo siguiente:

- El tamaño máximo de los paquetes de datos que se quieren enviar
- El total de datos a ser enviados antes de la confirmación
- El intervalo de tiempo entre cada envío de paquetes de datos
- El tiempo a esperar antes de que sea enviada la confirmación.
- Cuántos datos se pueden almacenar en la memoria de cada tarjeta
- La velocidad de transmisión de los datos

Cada tarjeta indica a la otra sus parámetros y acepta (o se adapta) a los parámetros de la otra. Cuando todos los detalles de la comunicación han sido determinados, las dos tarjetas empiezan a enviar o recibir datos.

Opciones de configuración

Las tarjetas de red tienen opciones configurables que deben ser establecidas para que funcionen correctamente:

- **Interrupción**
- **Dirección de entrada / salida**
- **Dirección de memoria base**
- **Conector**

Algunas veces es posible especificar las configuraciones de las tarjetas por software, pero, otras veces, ha de ser mediante ***puentes*** (*jumpers*) y/o ***conmutadores*** (*switchs*).

Interrupción

Las líneas de petición de **Interrupción** (IRQ) son señales electrónicas por las que los dispositivos como puertos de entrada o salida, teclado, unidades de disco y tarjetas de red pueden enviar peticiones de servicio al procesador del ordenador.

Las líneas de petición de interrupción están construidas en el hardware interno del ordenador y tienen asignados diferentes niveles de prioridad para que el procesador pueda determinar la importancia relativa de las peticiones de servicio entrantes.

Cuando la tarjeta de red envía una petición al ordenador, utiliza una interrupción. Cada dispositivo del ordenador debe utilizar una diferente **IRQ** y debe ser especificada cuando se configura cada dispositivo.

Dirección de entrada / salida

La dirección de entrada / salida (**Base I/O port**) es el canal de comunicación entre la tarjeta de red y el procesador.

Cada dispositivo hardware en el sistema debe tener un número diferente (en formato hexadecimal) de dirección de entrada / salida y debe ser especificado cuando se configura cada dispositivo.

Dirección de memoria base

La dirección de memoria base (**Base Memory Address**) identifica un lugar en la memoria del ordenador. Esta localización es usada por la tarjeta de red como un *buffer* para almacenar las tramas de datos entrantes y salientes. Esto se llama, a veces, la dirección de comienzo o arranque de RAM.

A menudo, la dirección de memoria base para una tarjeta de red es D8000. Es necesario seleccionar una dirección que no esté siendo usada por otro dispositivo.

Algunas tarjetas contienen un ajuste que permite especificar el total de memoria para almacenar tramas de datos. Especificando mas memoria se proporcionan mejores prestaciones, pero deja menos memoria disponible para otros usos.

Conector

Cada tarjeta de red puede tener varios conectores integrados (BNC, RJ45, o AUI) y, si no se realiza automáticamente, será necesario determinar el que se desea utilizar.

Arquitectura del bus de datos

En el entorno del ordenador personal hay cuatro tipos de arquitecturas de bus: ISA, EISA, Micro Channel y PCI. Cada tipo de bus es físicamente diferente de los otros.

ISA

ISA (**Industry Standard Architecture**) es la arquitectura utilizada en los IBM PC, XT, AT y en todos sus clónicos. Permite añadir varios adaptadores al sistema mediante la inserción de tarjetas en ranuras de expansión. Comenzó siendo de 8 bits y, en 1984, fue expandida a 16 bits en el IBM PC/AT. Las ranuras de 8 bits son mas cortas que las de 16 que, actualmente, constan de dos ranuras, una detrás de la otra (una tarjeta de 8 bits puede entrar en una ranura de 16 bits, pero no al contrario). Posee una velocidad de transferencia de 3 a 5 Mbps y su frecuencia de operación es 8MHz.

EISA

EISA (**Extended Industry Standard Architecture**) es el bus estándar introducido en 1988 por un consorcio de 9 fabricantes de ordenadores. Ofrece un camino de datos de 32 bits y mantiene compatibilidad con ISA a la vez que proporciona prestaciones introducidas por IBM en su arquitectura Micro Channel

Realiza transferencias de datos a 33 Mbps y su frecuencia de operación es de 8 MHz.

Micro Channel

Micro Channel o **Arquitectura Micro Canal** fue introducida por IBM en 1988 como parte de su desarrollo PS/2. Es eléctrica y físicamente incompatible con el bus ISA. Funciona como un bus de 32 bits y puede ser conducido independientemente por hasta ocho procesadores en simultáneo.

Realiza transferencias de datos a 40 Mbps y su frecuencia de operación es 10 MHz.

PCI

PCI(**Peripheal Component Interconnect**) es un bus de 32 bits utilizado en la mayoría de los ordenadores *Pentium y Apple Macintosh*. Es una tecnología desarrollada en 1993 por Intel. Es compatible con ISA y EISA. Opera con un bus de datos de 32 bits a 33 MHz. Puede utilizar vías de acceso de 32 o 64 bits de datos para el procesador, el cual puede simultanearlos con múltiples periféricos con dominio del bus.

Realiza transferencias de datos a 132 Mbps.

La arquitectura de bus PCI actual cumple la mayoría de los requerimientos para proporcionar funcionalidad **Plug and Play** que permite cambiar la configuración de un ordenador sin intervención del usuario.

6.4.2.- Multiplexores y Concentradores (Hubs)

Los **multiplexores** son equipos que permiten mantener mas de una comunicación simultánea por una sola línea. Cada una de las comunicaciones opera como si tuviera la línea

de forma exclusiva, pudiendo utilizar diferentes velocidades y protocolos en cada una de ellas.

Los **concentradores** son equipos que permiten compartir el uso de una línea entre varios ordenadores. Todos los ordenadores conectados a los concentradores pueden usar la línea, aunque no de forma simultánea, ni utilizando distintos protocolos ni distintas velocidades de transmisión.

6.4.3.-Dispositivos para conexión de una red local con el exterior

Cuando se está trabajando en una red local, puede ser necesario enviar o recibir determinada información del exterior de la red.

Estos datos pueden proceder de otro ordenador, de otra red o de un *mainframe/*mini ordenador y, por tanto, antes de proceder a establecer conexión con ellos, se han de resolver los problemas que existen en las comunicaciones (direccionamiento, control de errores, método de transmisión, formato, etc.).

Dentro de los equipos necesarios para realizar la transmisión de datos con el exterior de la red se encuentran:

- Una tarjeta RDSI, si se va a acceder al exterior desde un ordenador utilizando RDSI
- Un módem, si se va a acceder a un microordenador independiente o a otro sistema que está lejos y no se accede a él de forma periódica
- Un puente (*bridge*) para conectar dos redes
- Un conmutador (*switches*) para conexión selectiva entre redes
- Un encaminador (*router*) que dirige el paquete de datos determinando la ruta hacia su destino
- Una pasarela (*gateway*) para establecer un enlace con un mini ordenador o un mainframe

Tarjeta RDSI

La tarjeta **RDSI** es una tarjeta interna que permite conectar un único ordenador al exterior utilizando el sistema de comunicaciones RDSI. Tiene la ventaja, respecto al módem, de enviar los datos con mayor rapidez.

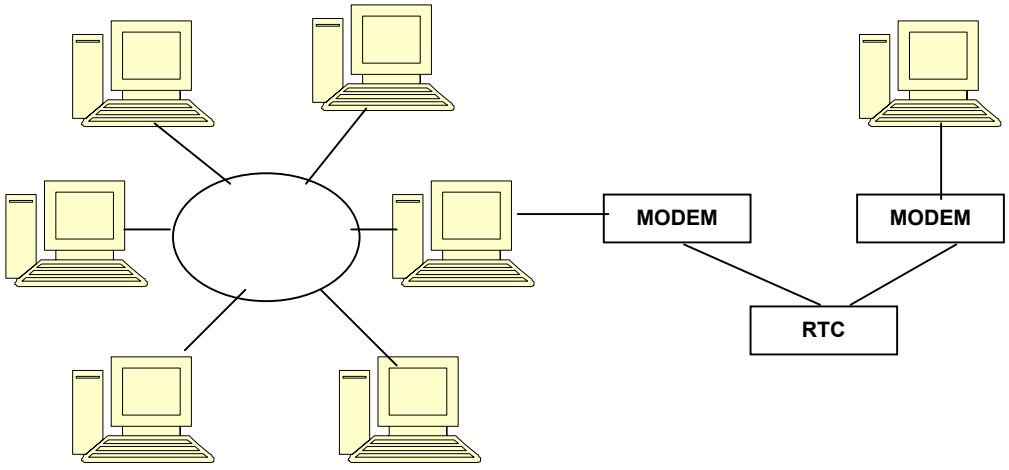
Módem

La función básica que desarrolla un **módem** es aceptar datos de un ordenador y convertir las señales digitales en analógicas para que se transmitan a través de la línea telefónica.

Cuando los datos llegan al punto de destino el módem receptor realiza la función inversa, es decir, vuelve a transformar las señales analógicas en digitales para que el ordenador receptor las pueda entender.

La comunicación se puede establecer en ambos sentidos pero no simultáneamente (*semidúplex*), o en ambos sentidos (*dúplex*). Es independiente el número de hilos de que consta el cableado de la forma de establecer la comunicación.

La velocidad a la que puede transmitir un módem se denomina **caudal del canal** (*throughput*) y se mide en bits por segundo. Las velocidades inferiores a 1200 bps pueden también denominarse como *baudios* aunque no significan lo mismo. Un baudio se refiere al cambio de estado de la señal analógica, y que normalmente se corresponde con un bps en velocidades inferiores a 1200 bps. Pero en velocidades superiores puede conseguirse mas de un bps por cada cambio de estado (por ejemplo, un módem de 1200 bps puede corresponder con 600 baudios).



Es necesario destacar que es importante para la velocidad del proceso que el módem cuente con una velocidad alta, ya que cuanto mayor sea la velocidad menor será el tiempo que invertirá en el proceso (por ejemplo, un módem a 2400 bps tarda en transmitir los datos 8 veces menos tiempo que uno de 300 bps).

De todas formas, si se transmite por la *Red Telefónica Conmutada* (RTB), la velocidad máxima que se puede conseguir actualmente es de, aproximadamente, 33000 bps, por tanto, si se desean conseguir velocidades mayores será preciso utilizar líneas dedicadas.

Otra posibilidad que incorporan los módems es la compresión de los datos que se van a transmitir. Dichos datos están formados por texto y gráfico, que, normalmente, contienen secuencias de información idéntica. La compresión de los datos reemplaza alguno de los caracteres de la información repetida con unos pocos caracteres y transmite sólo una copia de la secuencia repetida.

Entre los métodos de compresión mas utilizados por los módems se encuentran

MNP3	Elimina los bits de inicio y parada .Consigue hasta un 108 % de eficiencia
MNP4	Elimina los bits de inicio y parada y optimiza los protocolos. Consigue un 120 % de eficiencia
MNP5	Consigue un 200 % de eficiencia

V.42bis	Consigue un 400 % de eficiencia

De esta manera se aumenta la velocidad efectiva de la transmisión (por ejemplo, un módem que transmita a una velocidad de 28800 bps con una compresión V.42bis puede llegar a conseguir una velocidad efectiva de 115200 bps.

Entre las características mas importantes que incorporan los módem está la de poseer un *listín telefónico* donde almacena los números de teléfono y puede marcarlos automáticamente en el momento, o bien hacerlo en una fecha y una hora programada. En el caso de estar la línea ocupada, vuelven a intentar la llamada al cabo de un tiempo preestablecido.

También cuentan con respuesta automática a una llamada y la posibilidad de que se devuelva una llamada una vez comprobado que el emisor está autorizado para solicitarlo.

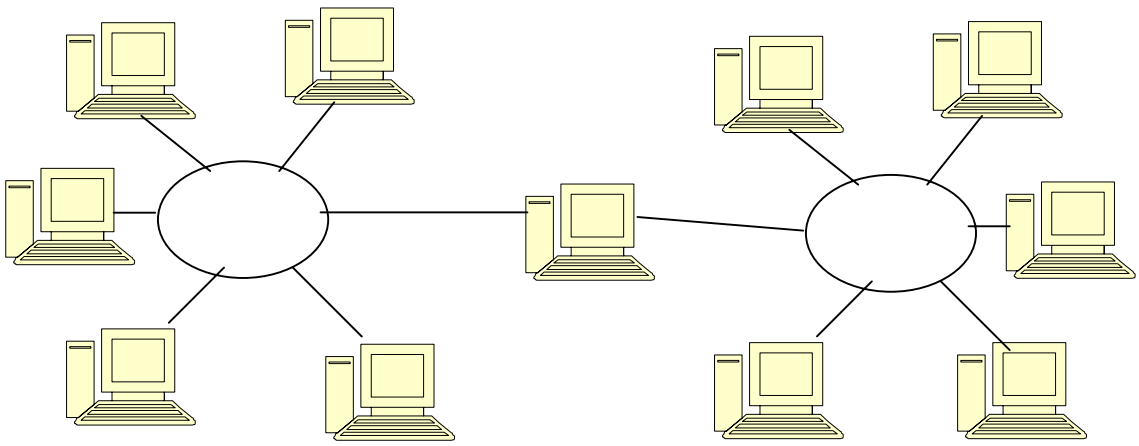
Su mayor utilidad para la expansión de una red es para el acceso remoto de una estación de trabajo móvil.

Puente (Bridge)

Es un sistema formado por hardware y software que permite conectar dos redes locales entre sí. Se pueden colocar en el servidor de archivos o, mejor, en el servidor de comunicaciones.

Cuando dos redes locales necesitan comunicarse entre sí , necesitan contar con un puente en cada una de ellas, para poder conectarse.

Ambas redes deben usar el mismo protocolo de comunicaciones.



A diferencia de un repetidor, un puente actúa sobre los paquetes de datos o tramas que se transfieren en los niveles de enlace de datos, particularmente sobre el *Nivel de Control de Acceso al Medio* (MAC).

Sus funciones básicas son las de autoaprendizaje, filtrado y reenvío. Es decir, si necesita reenviar un paquete de datos a una dirección de red que no está incluida en su

tabla de destinos, examina los campos de dirección del paquete (filtrado) y la dirige a la dirección que ha localizado (reenvío). A continuación, añade la dirección a la tabla de destinos (autoaprendizaje).

La utilización de puentes para unir dos redes es una idea mejor que la configuración de una red grande que englobe a ambas. La razón está en que las redes van perdiendo rendimiento al aumentar el tráfico y se va perdiendo tiempo de respuesta; utilizando puentes, al estar dividida la red, se reduce el tráfico y el tiempo de respuesta.

Otra razón es el límite de expansión de la red grande. Todas las redes cuentan con un número máximo de estaciones que pueden soportar. Si se desea sobrepasar ese número, la única alternativa es crear otra red conectada por un puente.

Conmutadores (Switches)

Los **conmutadores** se caracterizan por no enviar los paquetes a todos los puertos sino únicamente al puerto correspondiente al destinatario. La diferencia entre un conmutador y un puente (*bridge*) es que el puente debe recibir todo el paquete antes de dirigirlo al puerto correspondiente y un conmutador dirige el paquete a su destino una vez recibido el encabezado del paquete (en donde se encuentra la dirección IP del destinatario). Gracias a ello, los conmutadores producen un retraso mínimo en la conmutación (del orden de 40 μs, mientras que un puente supera los 1000 μs)

Encaminador (Router)

Un encaminador no sólo incorpora la función de filtrado, característica de los puentes, sino que, además, determina la ruta hacia su destino. Se utiliza tanto en redes de área local como en redes de área extensa.

Los encaminadores se diferencian de los puentes en dos aspectos:

- Actúa sobre los paquetes transferidos entre los niveles de red de las estaciones, a diferencia de los puentes, que lo hacen sobre el nivel de enlace de datos.
- Ambos equipos son, teóricamente transparentes a las estaciones finales que comunican. Sin embargo, normalmente las estaciones tienen definido el encaminador el que deben dirigirse.

Se basan en la utilización de un esquema de direccionamiento jerárquico (*Tablas de rutas*) que distinguen entre la posición del dispositivo dentro de la red y la dirección de la red. Para ello incorporan protocolos del nivel de red.

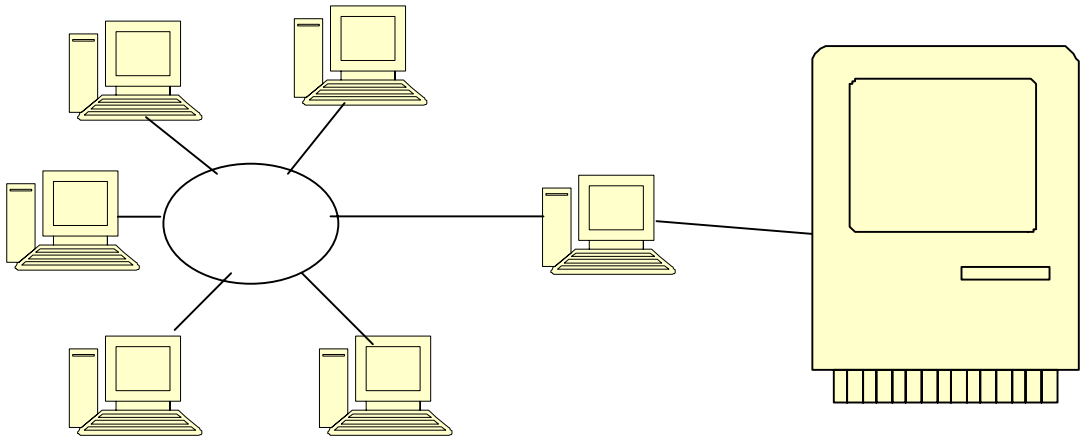
Para realizar su función incorporan algún tipo de algoritmo, siendo uno de los más básicos el *Protocolo de Información de Encaminamiento* (RIP) que calcula la distancia entre el encaminador y la estación receptora de un paquete como el número de saltos requeridos, ignorando otros tipos de atributos como el tiempo de transferencia entre dos saltos, etc.

Los protocolos de encaminamiento varían en función de las diferentes arquitecturas de comunicaciones de red existentes, por lo que se diseñan para una arquitectura específica.

Existen algunos dispositivos que poseen características tanto de los puentes (transparencia a los protocolos con aprendizaje) como a los encaminadores (selección del camino óptimo) que se denominan ***brouters*** (unión de bridges y routers). Este dispositivo funciona normalmente como un encaminador siempre que los protocolos de nivel superior permitan el encaminamiento. En caso contrario funcionan como puentes.

Pasarelas (Gateways)

Es un sistema formado por hardware y software que permite las comunicaciones entre una red local y un gran ordenador (*mainframe*) o un mini ordenador (por que utilizan protocolos de nivel de transporte, sesión, presentación y aplicación distintos). Se suelen colocar en el servidor de comunicaciones.



Mainframe

De este modo, podrá obtener datos del mini o del mainframe o bien enviarles datos para su almacenamiento.

La pasarela realiza la traducción completa entre las familias de protocolos, proporcionando una conectividad completa entre redes de distinta naturaleza.

El enlace entre ambos protocolos necesitará algún tipo de emulación que haga que la estación de trabajo imite el funcionamiento de un terminal y ceda el control al mini o al mainframe. Esta emulación se puede conseguir por medio de software. Esta emulación se puede conseguir por medio de software (con un programa), de hardware (con una tarjeta), o con ambos.

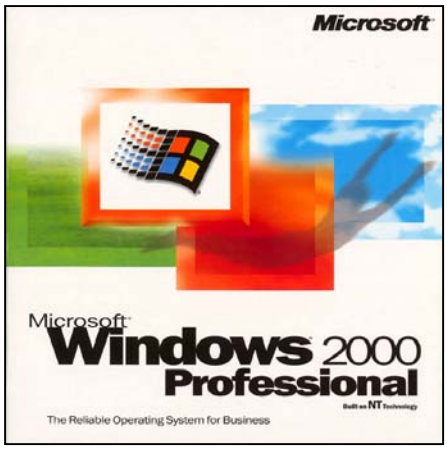
Al igual que los encaminadotes, están definidos para un determinado escenario de comunicaciones.

Pero, a cambio de sus ventajas, el retraso de propagación de un paquete que atraviesa una pasarela es mucho mayor que el experimentado en los otros dispositivos.

6.5.- Instalación de una red de Área Local (Windows 2000)

6.5.1.- Instalación del cliente (Windows 2000 Professional)

La instalación de Windows 2000 Professional puede iniciarse de varias maneras:



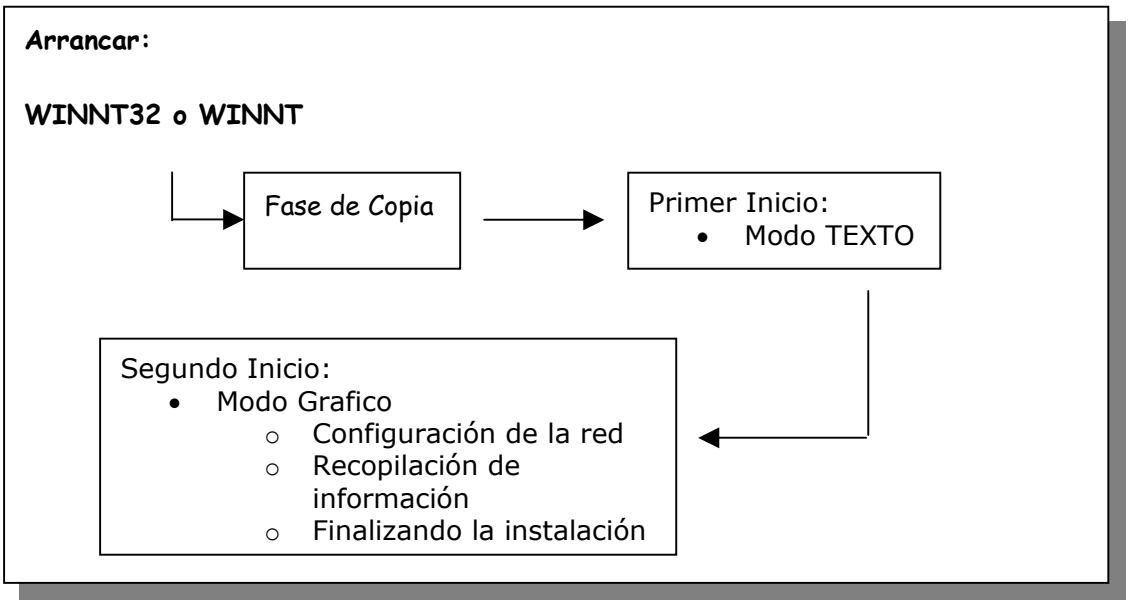
- Desde Discos de Inicio
- Desde el CD-ROM
- Desde la Red

Desde el CD-ROM, el primer paso será configurar la BIOS para que arranque desde el CD-ROM (First Boot = CR-ROM), una vez dado este paso solo hará falta reiniciar el ordenador y la instalación comenzará.

Si nuestro ordenador ya tuviese un sistema operativo como por ejemplo Windows 98 e insertamos el CD de Windows 2000 y además tenemos activado el '*autoplay*' se arrancará un proceso de instalación el cual nos mostrará al asistente de instalación de Windows 2000.

Si nos encontramos en la situación descrita anteriormente, el asistente nos permitirá, bien actualizar nuestro sistema operativo a Windows 2000, o bien seleccionando las opciones "avanzadas" de instalación, seleccionar una nueva instalación y permitirnos el seleccionar durante la instalación la partición o disco en el cual queremos instalar Windows 2000.

Procedimiento de la instalación



Fase de Copia.

Cuando usamos WINNT o WINNT32 para iniciar una instalación, todos los ficheros necesarios para completar la instalación son copiados a una carpeta temporal llamada *WIN_NT.~LS*. A dicha carpeta se copian o bien todos los ficheros necesarios para la instalación.

Primara Fase de la Instalación: Modo Texto

Esta primera fase de instalación está limitada al núcleo de Windows 2000, el cual, ejecuta una versión de Instalación en modo texto que sirve para acondicionar la máquina antes de empezar con la verdadera instalación de Windows 2000.

Paso 1: Aceptar el Acuerdo de Licencia de usuario Final. (Solo si se utiliza WINNT.EXE, con WINNT32.EXE el acuerdo –EULA- es mostrado y debe ser aceptado antes de reiniciar en modo texto pulsando la tecla F8).

Paso 2: Seleccionar / Crear la partición de Instalación.

Paso 3: Formatear o convertir (por ejemplo de FAT a NTFS) la partición seleccionada.

Paso 4: Escoger un directorio de instalación. Si se selecciona un nombre de directorio y este ya existiese se le preguntará si desea rescribir su contenido o bien le permitirá seleccionar un nuevo nombre. Generalmente Windows 2000 es instalado en el directorio WINNT de la unidad seleccionada (en caso de que existan varias).

Inmediatamente nada mas arrancar en modo texto, tenemos la posibilidad durante 2 segundos de pulsar F6 (cuando nos lo está solicitando en la línea inferior de la pantalla). Esta opción nos permite incorporar nuevos controladores SCSI o RAIS de terceros que sean necesarios para poder reconocer ciertas tarjetas SCSI no soportadas en la distribución de Windows 2000).

En la instalación en modo texto, todos los ficheros requeridos para la instalación son copiados desde el directorio temporal al directorio de instalación del disco duro. Después de que el modo texto finalice, comenzará el modo gráfico.

Segunda Fase de la Instalación: Modo Gráfico

En modo gráfico, se arrancará el asistente de instalación de Windows 2000 que solicitará la intervención del usuario. Durante el modo gráfico, la información especifica del ordenador, como por ejemplo el 'nombre' del ordenador y el nombre del usuario, debe ser suministrada. El modo gráfico consta de tres fases distintas:

Fase 1: Obtener información sobre el ordenador.

Durante esta fase el usuario deberá responder a varias pantallas que le solicitarán: Registro del Usuario, Opciones Locales y de Teclado, Modo de la Licencia (solo en el Servidor), y Nombre del Ordenador.

Fase 2: Instalar la red de Windows 2000.

Durante la instalación se puede instalar la red de Windows 2000. Es necesario instalar la red para compartir recursos del ordenador con otros ordenadores de la red, o bien para acceder a Internet.

Por defecto, el Instalador permite instalar tres componentes de red durante la instalación:

Cliente: Cliente para redes Microsoft

Servicios: Compartir Archivos e Impresoras para redes Microsoft, '*Packet Scheduler Microsoft Driver*'y Agente SAP.

Protocolos: Varios protocolos incluyendo TCP/IP, NWLink (IPX/SPX), NetBEUI, DLC, etc.

Fase 3: Finalizar la Instalación y completar datos y opciones.

El Instalador copia los ficheros, configura el ordenador, guarda la configuración y elimina todos los ficheros y carpetas temporales. El sistema se re-inicia por fin y la instalación ha finalizado.

6.5.2.- Instalación de un servidor (Windows 2000 Server)

Al igual que la instalación de la versión Professional, la de Windows 2000 Server puede iniciarse también de tres formas:

- Desde Discos de Inicio
- Desde el CD-ROM
- Desde la Red

Es importante reseñar que la instalación de Windows 2000 Professional puede realizarse sobre W98, aunque las versiones Server y Advanced Server requieren NT o una instalación limpia (es decir con el disco formateado ó en una partición en la que no haya otro sistema operativo a no ser que este sea Windows NT).

La instalación de Windows 2000 Server conlleva los mismos pasos que la instalación de la versión Professional que son los siguientes:

La elección de cómo instalar Windows 2000 Server depende de lo que ya hay en el servidor, de dónde se encuentran los archivos de instalación y de cuántas instalaciones haya que hacer. Si se dispone de Windows 95/98 o Windows NT en la máquina, hay que ejecutar la instalación de Windows 2000 de 32 bits desde Windows 95/98 o Windows NT. También se puede iniciar desde el CD-ROM de Windows 2000 o desde el disco de inicio de instalación (o un disco de inicio de MS-DOS con controladores de CD-ROM o de red) y ejecutar el programa de instalación de Windows 2000 de 16 bits. Ambas versiones de la instalación se pueden ejecutar desde la red o se pueden automatizar.

Instalación desde Windows 95/98 ó Windows NT

Si tenemos instalado Windows 95/98 ó Windows NT, la instalación recopila información y copia los archivos que necesita el equipo para iniciar en el modo de texto de Windows 2000 y después reinicia en modo texto. Se puede entonces (opcionalmente) seleccionar la partición apropiada, después de lo cual se instala Windows 2000 en el disco duro y se pasa al Asistente para instalación de Windows 2000 en modo gráfico, que recopila más información, configura los dispositivos y termina de copiar los archivos. Después de esto, la instalación está completa y el equipo se reinicia en Windows 2000.

- Insertar el CD-ROM de Windows 2000 y pulsar en Instalar Windows 2000, si está activa la Reproducción automática del CD-ROM (Notificación automática de inserción). Si no es así, hay que ejecutar winnt32.exe desde la carpeta \i386 del CD-ROM de Windows 2000.

- Para instalar Windows 2000 Server desde la red, hay que ejecutar el programa winnt32.exe desde la unidad de disco de red que contenga los archivos de instalación de \w2ks y después, proceder con la instalación normalmente.

- Dependiendo del Sistema Operativo que tengamos y de la Licencia que hayamos adquirido (Actualización o OEM), el sistema activará o desactivará las siguientes opciones, ofreciendo todas las posibilidades de instalación posibles:

  - Actualizar a Windows 2000.

  - Instalar una nueva copia de Windows 2000.

Después de elegir la opción deseada pulsamos **Siguiente**.

Contrato de Licencia: Se debe leer el contrato de licencia, seguidamente hay que elegir el botón de opción Acepto este contrato y pulsar con el ratón en Siguiente. La instalación muestra la ventana Seleccionar opciones especiales, y que se utiliza para personalizar las opciones de idioma, cambiar cómo copiará la instalación los archivos y activar el uso de utilidades de accesibilidad durante la instalación para usuarios con problemas de visión.

Seleccionar opciones especiales: En esta pantalla se pueden configurar las siguientes pociones:

- **Opciones de Idioma:** Si se desea configurar el sistema operativo Windows 2000 para que utilice conjuntos de caracteres de varios idiomas, hay que pulsar en el botón Opciones de idioma, elegir el idioma principal de la lista desplegable, seleccionar cualquier grupo de idiomas adicionales para los cuales se desea instalar soporte y después pulsar Aceptar

- **Opciones avanzadas:** Para especificar la carpeta y partición de instalación de Windows 2000, o para decirle a la instalación de Windows 2000 la ubicación de los archivos de instalación, hay que pulsar con el ratón en el botón Opciones avanzadas en la ventana Seleccionar opciones especiales para abrir la ventana Opciones avanzadas.

- **Opciones de accesibilidad:** Para configurar las opciones de pantalla con configuraciones especiales para disminuidos físicos.

Se debe pulsar en **Siguiente** para copiar los archivos de instalación al equipo. Después de que la instalación termine de copiar archivos, se reinicia el equipo y se pasa al modo de texto de Windows 2000 para la parte de la instalación basada en texto.

Asistente para la instalación de Windows 2000

Cuando la fase basada en texto de la instalación concluya, el equipo reiniciará y Windows 2000 se iniciará por primera vez, cargando el Asistente para la instalación de Windows 2000. Para utilizar el Asistente para la instalación hay que seguir los pasos que se indican a continuación. Al final de cada paso hay que pulsar con el ratón el botón Siguiente o el botón Aceptar para continuar.

1. **Pantalla Instalando Dispositivos:** el Asistente para la instalación detecta y configura los dispositivos instalados en el equipo. Si la instalación no puede detectar de forma apropiada un dispositivo, mostrará un cuadro de diálogo de configuración de dispositivo para la configuración manual del dispositivo.

2. **Configuración regional:** Después de detectar el hardware, se solicitan los parámetros regionales. Estos parámetros afectan a factores tales como la disposición del teclado y cómo se muestran las fechas y la moneda. Para escoger la localización que se quiere utilizar, para establecer la posibilidad de leer y escribir documentos en otros idiomas o para especificar el formato de números, fechas y monedas, hay que pulsar el primer botón Personalizar.

- En el cuadro de lista desplegable **Su idioma (ubicación)**, hay que elegir la localización que se desea utilizar para la configuración de números, monedas y fecha y hora. Para configurar el sistema de forma que se puedan leer o escribir documentos en otros idiomas, hay que seleccionar la casilla de verificación situada junto a los idiomas que se quieren activar para lectura y escritura. Las otras pestañas se utilizan para modificar el formato de los números, monedas, fechas y horas.

- Para modificar la disposición del teclado, hay que pulsar el segundo botón Personalizar en la ventana Configuración regional, y utilizar entonces las opciones de Idiomas instalados para configurar el teclado para el idioma que se quiere utilizar. Hay que pulsar Siguiente.

3. **Personalización del Software:** Se debe introducir el nombre de la persona bajo la que se registrará el equipo además de la empresa.

4. **Clave del Producto:** Introducir el CD-KEY del producto que se está instalando.

5. **Modos de licencia:** Hay que escoger el modo de licencia en la siguiente ventana, como Por servidor o Por puesto. Por defecto aparecerán las licencias para las que tiene el producto. Si se escoge Por servidor, hay que especificar cuántas Licencias de acceso de cliente se han adquirido.

6. **Nombre del equipo y contraseña del administrador:** Hay que introducir el nombre del equipo en el cuadro de texto Nombre de equipo. El nombre del equipo puede contener los números del cero al nueve, letras en mayúscula y minúscula y el carácter guión, pero no espacios o puntos. El nombre debería ser compatible con DNS y puede tener un máximo de 63 caracteres de longitud, pero en interés de la compatibilidad con clientes anteriores a Windows 2000, debería ser menor de 15 caracteres.

7. Tras introducir el **nombre del equipo**, hay que introducir la contraseña de la cuenta del administrador de hasta 14 caracteres de longitud en el cuadro de texto Contraseña de administrador, y escribirla de nuevo en el cuadro de texto Confirmar contraseña. Hay que pulsar Siguiente.

8. Para hacer que el sistema sea lo más seguro posible, hay que asignar siempre una **contraseña a la cuenta de administrador**, preferiblemente una contraseña de al menos siete caracteres de longitud y que consista en letras y caracteres mezclados, mayúsculas y minúsculas. También se debería limpiar el historial de accesos después de instalar Windows 2000 para que los aspirantes a hackers tengan que adivinar tanto la contraseña como el nombre de usuario. Otra buena precaución después de la instalación es utilizar la cuenta de administrador incorporada para crear una segunda cuenta con todos los privilegios administrativos. Esta cuenta puede tener el nombre del administrador o llamarse de alguna forma descriptiva. Conviene usarla para el trabajo administrativo de cada día. Hay que asignar una contraseña especial segura para la cuenta de administrador incorporada y cambiarle el nombre predeterminado. Hay que esconder la contraseña y el nombre en algún lugar seguro y relegar esa cuenta a una semi-jubilación. Como es posible desactivar cualquier cuenta de administrador, incluyendo la cuenta de administrador incorporada, resulta prudente tener una cuenta de reserva. De esta

forma, siempre se tendrá una cuenta de administrador no contaminada; y que se sabe que es buena, a la que recurrir sólo si se da el caso.

9. **Componentes de Windows 2000:** La siguiente ventana sirve para seleccionar los componentes a instalar en este momento. Para instalar una opción, hay que seleccionar la casilla de verificación situada a la izquierda de la opción, o seleccionar la opción y pulsar con el ratón en el botón Detalles para modificar los subcomponentes que se deseen instalar.

10. En la ventana de ubicación de marcado que se muestra si la instalación detecta un módem, hay que seleccionar el país, introducir el código de zona o la línea telefónica (si la hay), introducir los códigos necesarios para obtener línea al exterior y pulsar Siguiente. (Se pueden escoger localizaciones adicionales o modificar la localización actual por medio de la herramienta Opciones de teléfono y módem del Panel de control cuando haya concluido la instalación.)

11. **Valores de fecha y hora:** Hay que revisar la fecha, hora e información de la zona horaria, realizar cualquier corrección necesaria y pulsar **Siguiente** para configurar los parámetros de red.

12. Si se seleccionó Servicios de Terminal Server, hay que escoger el modo de operación, que puede ser Modo de administración remoto o Modo de servidor de aplicaciones. Pulsar Siguiente.

13. **Configuración de Red:** Nos da dos posibilidades de configuración, una personalizada o típica.

    - **Configuración típica:** se instalan los siguientes protocolos y servicios de red usados comúnmente: Cliente para redes Microsoft, Compartir impresoras y archivos para redes Microsoft y TCP/IP configurado para utilizar DHCP (o Direcciones IP privadas automáticas (APIPA, Automatic Prívate IP Adressing) si no hay ningún servidor DHCP disponible.)

    - **Configuración personalizada:** muestra la lista predeterminada de componentes de red y que se puede modificar según las necesidades. Para instalar componentes adicionales hay que pulsar el botón **Instalar**, seleccionar Cliente, Servicio o Protocolo, pulsar Agregar, seleccionar el componente deseado y pulsar **Aceptar**. Para desactivar un componente instalado hay que desmarcar la casilla de verificación situada al lado del componente y pulsar Desinstalar para eliminarla del sistema.

14. **Grupo de Trabajo y Dominio:** Para unirse a un grupo de trabajo, hay que elegir la primera opción de la ventana Grupo de trabajo o dominio del equipo y escribir el nombre del grupo de trabajo en el cuadro de texto Dominio o grupo de trabajo del equipo.

15. Si se está configurando un nuevo dominio, hay que escoger la primera opción y teclear en el cuadro de texto Dominio o grupo de trabajo del equipo el nombre del dominio futuro (la instalación hace que se cree un grupo de trabajo con ese mismo nombre). Para unirse a un dominio existente, hay que pulsar la segunda opción e introducir el nombre del dominio al que se desea unirse en el cuadro de texto Dominio o grupo de trabajo del equipo.

16. Hay que pulsar Siguiente cuando se haya terminado de configurar los parámetros del dominio o grupo de trabajo. Si se escoge unirse a un dominio, aparece un cuadro de diálogo pidiendo la introducción de un nombre de usuario y una contraseña para un usuario con permisos suficientes para crear una nueva cuenta de equipo para el servidor. Hay que introducir el nombre de usuario y la contraseña y pulsar después Aceptar. La instalación inicia sesión en el dominio y configura una cuenta de equipo para el servidor.

17. **Instalando componentes:** El programa instala después los componentes especificados y configura Windows 2000. Cuando finaliza ese proceso, se borran todos los archivos de instalación temporales y se solicita la extracción de cualquier CD-ROM o disquete que haya en las unidades. Hay que pulsar Finalizar para reiniciar el equipo.

18. Si se produce algún error durante el proceso de instalación, el programa de instalación muestra un mensaje de error y pregunta si se desea ver el archivo de registro setuplog.txt creado. Para hacer esto, hay que pulsar Aceptar. Conviene revisar el archivo y pulsar después Cerrar para reiniciar el sistema.

19. Cuando la instalación reinicie el equipo, se verá la ventana de inicio de sesión estándar de Windows 2000. Cuando se inicie sesión aparecerá el asistente para Configurar el servidor que servirá de guía durante la configuración de los parámetros adicionales del servidor.

Cuando el asistente finaliza la instalación de Windows 2000, se reinicia el equipo. El programa de instalación ya ha realizado la instalación básica. El programa Configurar el servidor, que aparecerá en la pantalla si inició la sesión como administrador del equipo, simplifica las tareas adicionales de configuración. En este momento puede registrar su copia de Windows 2000 Server y configurar el servidor.

La siguiente tabla proporciona información detallada acerca de las opciones disponibles al elegir los iconos de Configurar el servidor:

Icono	Nombre	Elementos que puede configurar
	Active Directory	Cuentas y directivas de usuarios y grupos, funciones del servidor (en dominios), permisos y otros elementos que le ayudarán a mantener la seguridad y hacer un seguimiento de la información de usuario.
	Servidor de archivos	Carpetas compartidas y otros recursos de red compartidos.
	Servidor de impresión	Impresoras, colas de impresora y otros elementos relacionados con la impresión.
	Servidor Web/multimedia	Sitios Web, multimedia y FTP, y otros elementos relativos al uso compartido de información en una Intranet o en Internet. Para poder utilizar estos servicios, debe instalar los componentes apropiados en Windows 2000 Server.
	Funciones de red	Protocolos de red, acceso remoto y enrutamiento. Incluye DHCP y DNS (servicios de resolución de nombres y direcciones utilizados con TCP/IP). También incluye un vínculo a temas acerca de WINS (otro servicio de resolución de nombres).

	Servidor de aplicaciones	Servicios de componentes y compatibilidad relacionada para aplicaciones distribuidas en la red; también incluye Servicios de Terminal Server.
	Avanzadas	Herramientas de soporte del Kit de recursos y todos los componentes opcionales (como los Servicios de instalación remota) que no se no instalan durante la instalación de Windows 2000.

Para iniciar Configurar el servidor en cualquier momento, haga clic en Inicio, seleccione Programas, Herramientas de administración y haga clic en Configurar el servidor. También hay disponibles otras herramientas de configuración en Herramientas de administración.

Mediante el Asistente **Configurar su servidor** de **Windows 2000**.

1. Presionar CTRL-ALT-SUPR e iniciar la sesión en el servidor como administrador

2. Cuando aparezca la página Configurar su servidor de Windows 2000, seleccionar Éste es el único servidor de mi red y hacer clic en Siguiente.

3. Hacer clic en Siguiente para configurar el servidor como controlador de dominio e instalar Active Directory, DHCP y DNS.

4. En la página ¿Desea poner un nombre a su dominio?, escribir el nombre del dominio(AULA09)

5. Hacer clic en Siguiente para ejecutar el asistente. Cuando se pida, insertar el CD-ROM de Windows 2000 Professional. Cuando finalice el asistente se reiniciará el ordenador.

6. El Asistente Configurar su servidor instalará DNS y DHCP, y configurará DNS, DHCP y Active Directory.

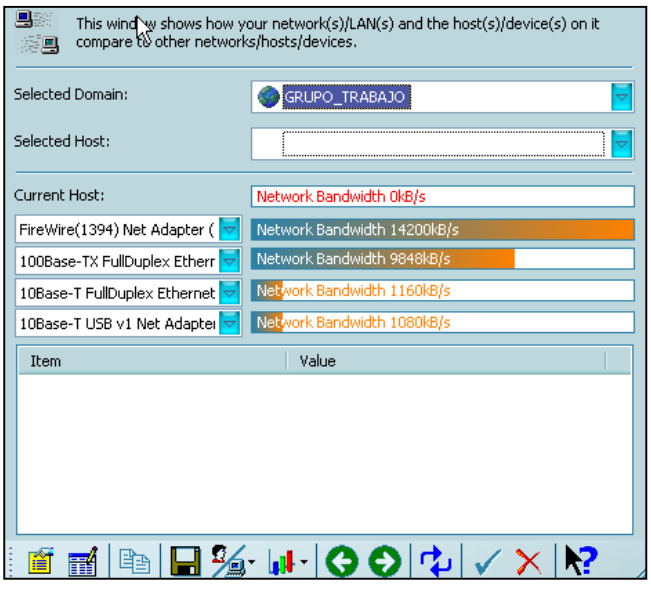
6.5.3.- Implementación de subredes en la red local

Si queremos incluir una serie de subredes dentro de una red local, tendremos que realizar la siguiente operación:

$$2^n-2>= N$$

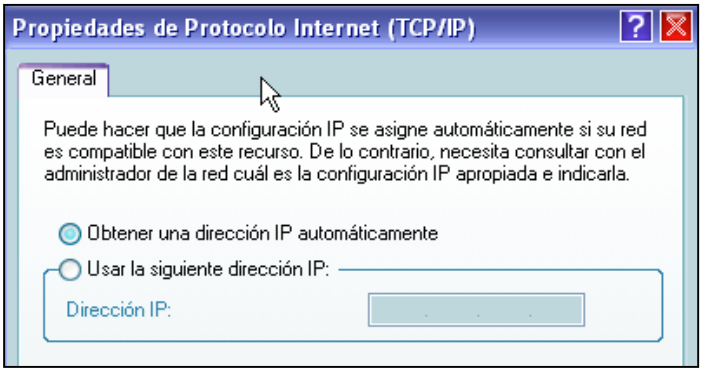
siendo N el número de subredes necesarias y n será el número de bits a uno que tendrá la máscara de subred que usaremos.

El número de ordenadores que pueden pertenecer a cada subred, lo obtendremos mediante la resta de 32bits-n, donde le valor de n será el obtenido en la operación indicada anteriormente. Sabiendo el número de ordenadores que



puedo meter en cada subred, ya podemos obtener la dirección de cada una de las subredes.

Ahora pincharemos con el botón derecho en Mi PC, y en la etiqueta "Identificación de red", entrar en propiedades, y definir el grupo de trabajo, y la estación de trabajo y pulsar aceptar una vez echo esto. No hay que reiniciar todavía el equipo, ya que hay que definir la dirección IP. Pulsar con el botón derecho en "Mis sitios de red", con el botón derecho también en conexión de área local. Hemos de elegir la opción "Propiedades del protocolo TCP/IP, y es ahí donde introducimos las nuevas direcciones de subred, e IP. A continuación es necesario reiniciar el ordenador para que los cambios surjan efecto.



Después de haber reiniciado, se observa que en "Mis sitios de red", en "Toda la red", "Contenido completo", "Red de Microsoft Windows", aparece la nueva subred creada.

NOTA: Cuando tenemos más de una subred en una misma red física, hay que tener cuidado respecto a las direcciones de broadcasting. De acuerdo con los últimos estándares, hay dos formas distintas para que un host de la subred 128.6.20 pueda enviar un broadcast en la red local. Una es usar la dirección 128.6.20.255. La otra es usar la dirección 255.255.255.255. La dirección 128.6.20.255 dice, explícitamente, *"todos los hosts de la subred 128.6.20"*; la 255.255.255.255 expresa *"todos los hosts de mi red local"*. Normalmente, ambas tienen el mismo efecto. Pero no lo tienen cuando hay varias subredes en una red física. Si la red 128.6.19 está en la misma red, también recibirá el mensaje enviado a 255.255.255.255. Sin embargo, los hosts con números 128.6.19.x no escucharán los mensajes enviados a 128.6.20.255. El resultado es que ahí tenemos dos tipos distintos de direcciones de broadcast con dos significados distintos. Esto conlleva que debemos tener cuidado configurando el software de red, para asegurarnos de que nuestros broadcasting llegan a donde queremos que lo hagan.