

APUNTES DE REDES DE COMPUTADORAS



COMPILACIÓN

ING. FELIPE DE JESÚS CANUL SCHWIETRS

ECATEPEC, EDO. DE MÉXICO, JULIO 2006

TEMARIO

Introducción	3
1.0 TECNOLOGIA DE REDES	4
1.1 Organizaciones de estándares para comunicación de datos.....	4
1.2 Circuitos de comunicación de datos.....	5
1.3 Códigos de comunicación de datos.....	5
1.4 Control de errores.....	5
1.5 Medios de transmisión.....	6
1.6 Numeración del conector RJ45.....	8
1.7 Métodos de acceso al medio.....	11
2.0 REDES DE COMPUTADORAS.....	13
2.1 Clasificación	13
2.2 LAN	13
2.3 MAN	13
2.4 WAN	13
2.5 Red local y aplicaciones	14
2.6 Nodo y estación de trabajo	14
2.7 Tipos de servidores	15
2.8 Configuración y topología	18

2.9 Modelo de referencia OSI	19
3.0 PROTOCOLOS DE COMUNICACIÓN DE DATOS.....	23
3.1 Tipos de redes	23
3.2 Topología de las redes de área local	23
3.3 Técnicas de transmisión.....	24
3.4 Topología.....	24
3.5 Componentes de una red	26
3.6 Protocolos TCP/IP	33
3.7 Arquitectura de protocolos TCP/IP	34
3.8 Direcciones IP y mascarar de red.....	37
3.9 Instalación de una red local	44
4.0 REDES DE AREA LOCAL	
4.1 LAN.....	52
4.2 TOKEN RING	53
4.3 Internet	55
4.4 Tipos de redes LAN	55
4.5 Administración de redes	62
4.5.1 Instalación y configuración del servidor DNS	62
4.5.2 Instalación y configuración del servidor DHCP	74
4.5.3 Configuración de los equipos clientes de la red LAN	81
4.5.4 Instalación del directorio activo	84
4.5.5 Creación de objetos en el directorio activo	93
4.5.6 Creación de cada unidad organizativa	96
4.5.7 Creación de una cuenta de usuario	97
4.5.8 Definición y tipos de grupo	100
4.5.9 Publicación de recursos en el directorio activo	105
4.6 Seguridad en el directorio activo	111
4.6.1 Permisos	112
4.6.2 Política de grupos	113
4.6.3 Plantillas administrativas	116

Introducción

Las redes de ordenadores nacen como evolución de los sistemas de acceso y transmisión a la información y cumplen fundamentalmente el objetivo de facilitar el acceso a información remota, comunicación entre personas y entretenimiento interactivo.

En un principio podemos clasificar las redes en dos tipos: redes de difusión y redes punto a punto. Con las primeras se puede dirigir un paquete o mensaje corto a todos las máquinas destinos quienes lo reciben y lo procesan. Sólo existe un canal de comunicación compartido por todas las máquinas de la red. Con las segundas para ir del origen al destino un mismo paquete tiene que visitar una o varias máquinas intermedias, las redes punto a punto consisten en muchas conexiones entre pares individuales de máquinas.

A veces son posibles múltiples rutas de diferente longitud. En general las redes geográficamente pequeñas suelen usar la difusión y las redes más grandes son de punto a punto.

Tecnología de Redes

Cuando queremos comunicar datos entre dos computadores ya sea en aplicaciones del hogar o industriales el conocer las redes de datos y de computadores nos es útil. El requisito fundamental para todas las aplicaciones que abarcan dos o más computadores es contar con un recurso de **comunicación de datos** adecuado. En la práctica es posible utilizar una amplia gama de recursos de comunicación distintos, cada uno orientado a un dominio de aplicación específico.

Sea cual sea el tipo de recurso que se use, en casi todas las aplicaciones los datos se transmiten entre computadores en modo de **bits en serie**. En consecuencia, como los datos se transfieren entre subsistemas dentro de un computador en modo de **palabras en paralelo**, es necesario efectuar una operación de conversión de paralelo a serie en la interfaz del computador antes de enviar los datos y la conversión de serie a paralelo inversa al recibirlos. Además el tipo de modo de transmisión y el hardware requerido varía y depende del lugar en el que estén los computadores y la velocidad de transmisión requerida.

Organizaciones de estándares

American National Standard Institute (ANSI: Instituto Nacional Estadounidense de Normas).

Una organización nacional de normas entre cuyos miembros están fabricantes y usuarios de computadores de Estados Unidos.

British Standards Institution (BSI: Institución Británica de Normas). Organización Nacional de Normas que se ocupa de producir normas para todo tipo de industrias de fabricación y consumo; es el miembro británico de la ISO.

European Computer Manufacturers Association (ECMA: Asociación de fabricantes Europeos de computadores): Los miembros de esta asociación son fabricantes de computadores de Europa. La ECMA produce sus propias normas y también contribuye con la ITU-T y la ISO.

Institute of Electrical and Electronics Engineers (IEEE: Instituto de Ingenieros eléctricos y electrónicos). Sociedad profesional estadounidense que también participa en la creación de normas para la industria de los computadores. En el contexto de la comunicación de computadores, el IEEE se ha encargado de la producción de normas relacionadas con las LAN y, en particular las que se ocupan de las subcapas de MAC Y LLC.

Internacional Organization for Standardization (ISO: Organización Internacional de Normas). Organización internacional formada por organismos de normas designados por los países participantes; se ocupa de una amplia gama de normas, cada una controlada por un comité técnico

independiente. El comité técnico que produce normas para la industria de la computación es TC97. Este comité se ha encargado de producir el modelo de referencia básico de la ISO para OSI.

OSI Network Management Forum (NMF: Foro de Gestión de Redes OSI): Organización a nivel mundial formada por compañías de telecomunicaciones y computadores, proveedores de servicios y usuarios de servicios.

Circuitos de comunicación de datos.

Cada conexión a través de una red de conmutación de circuitos se convierte en un canal de comunicación físico establecido a través de la red, desde el equipo del suscriptor que llama hasta el que es llamado. Mientras dura la llamada, esta conexión solo la utilizan los dos suscriptores.

En el contexto de la transmisión de datos, una conexión de circuitos conmutados tiene como característica que de hecho proporciona un canal de tasa de datos fija en el que ambos suscriptores deben operar. Además antes de poder transmitir datos por una conexión como esta, es preciso activar o establecer una conexión a través de la red.

Códigos de comunicación de datos.

Cuando introducimos datos en un computador a través de un teclado, los circuitos electrónicos de este último codifican cada elemento tecleado para obtener un patrón equivalente codificado en binario mediante uno de los esquemas de codificación estándar para intercambiar la información.

Los dos códigos de mayor aceptación para esta función son el código de intercambio ampliado decimal codificado en binario (EBCDIC) y el código del American Standard Comité for Información Interchange (ASCII).

Control de errores.

Durante las transmisiones de datos es común que las señales de bits transmitidos sufran cambios a causa de la interferencia electromagnética que los dispositivos eléctricos o electrónicos cercanos inducen en las líneas. Por lo que el equipo receptor debe contar con algún mecanismo que le permita deducir cuando la información recibida tiene errores e incluso se requerirá un mecanismo que permita crear una copia de la información.

Son dos las estrategias que se utilizan:

- 1) El control de errores hacia delante, en el que cada carácter o trama transmitido contiene información adicional que permite al receptor no solo detectar la presencia de errores, sino además determinar en que punto del flujo de bits recibidos está el error.

- 2) El control de errores por retroalimentación (retrospectivo). En el que cada carácter o trama incluye solo suficiente información adicional para que el receptor pueda saber si se presentan errores, pero no su ubicación exacta. Se emplea un esquema de control de retransmisión para solicitar el envío de otra copia de la información que, se espera será correcta.

Medios de transmisión. Tipos de Cable

El cable utilizado para formar una red se denomina a veces "*Medio*". Los tres factores que se deben tener en cuenta a la hora de elegir un cable para una red son:

@ Velocidad de transmisión que se quiere conseguir

@ Distancia máxima entre ordenadores que se van a conectar

@ Nivel de ruido e interferencias habituales en la zona que se va a instalar la red

Existen diferentes tipos de cables para la interconexión de computadoras, estos se caracterizan por el costo del cable, rango de transmisión, flexibilidad, facilidad para su instalación y por la transferencia que este ofrece.

En el siguiente cuadro se comparan 4 tipos de cables.

Características	Coaxial Thinnet (10-Base 2)	Coaxial Thicknet (10-Base 5)	Par Trenzado (10-Base T)	Fibra Óptica
Costo del Cable	Mas caro que el par trenzado	Mayor que el Thinnet	Menos Caro	Más Caro
Máxima Longitud	185 Metros	500 Metros	100 Metros	2 Kilómetros
Rango de Transmisión	10 Mbps	10 Mbps	10 Mbps - 100 Mbps	100 Mbps ó Mas
Flexibilidad	Bastante Flexible	Menos Flexible	El mas Flexible	No Flexible
Facilidad de Instalación	Fácil de Instalar	Fácil de Instalar	Muy Fácil de Instalar	Difícil de Instalar
Susceptibilidad de Interferencia	Buena Resistencia	Buena Resistencia	Susceptible a la Interferencia	No Susceptible a la Interferencia
Características Especiales	Componentes Eléctricos menos caros que el par trenzado	Componentes Eléctricos menos caros que el Par Trenzado	El mismo que el de Teléfono	Soporta Voz, Datos y Video

Medios magneto-ópticos.

Los disquetes, zips y en general los medios removibles, los podemos llevar de un sitio a otro.

Conexión y Cableado.

Conexión con cable coaxial fino.

El adaptador de red debe tener un puerto o entrada formado por un conector hembra de tipo BNC, que son idénticos a los empleados en antenas de televisión.

Es necesario cortar el cable coaxial a una medida determinada, instalar dos conectores BNC macho en los extremos y conectarlos a la tarjeta de red del ordenador mediante un derivador que como ya dijimos antes es un conector en forma de T.

Cable Par Trenzado.

Los conectores ahora son del tipo RJ45 que son iguales pero más anchos que los que se emplean en telefonía. Para montarlos hace falta una grimpadora que unirá los ocho cables de colores del cable a cada conector macho, podemos comprar los cables que deseemos ya con su conector de la medida que más nos interese.

Cable de fibra óptica.

Es igual que el anterior pero lleva un núcleo de ésta fibra y que va rodeado de un material de densidad diferente para impedir que los rayos de luz se esparzan.

Par trenzado.

Grosor de 1mm.

El ancho de banda depende del grosor y de la distancia.

Velocidad del orden de 10-100 Mbps.

Categorías de cable par trenzado:

- **STP** (apantallado): 2 pares de hilo, recubierto por malla.
- **UTP** (no apantallado): 4 pares de hilos.
 - **Categoría 3:** van de 4 en 4 (8 cables), alcanzando 30 Mbps.
 - **Categoría 5:** más retorcidos y mejor aislante (teflón), alcanzando 100 Mbps.

Cable coaxial

Los hay de 2 impedancias:

- **75 ohmios:** banda ancha, utilizado en TV, distintos canales, 300MHz.
- **50 ohmios:** banda base, utilizado en Ethernet, un canal.
- **10BASE5:** coaxial grueso, 500 metros, 10Mbps, conector "N".
- **10BASE2:** coaxial fino, 185 metros, 10 Mbps, conector "BNC".

Fibra óptica.

Se necesita una fuente de luz: láser o LED.

Se transmite por fibra y se capta por foto diodos.

La topología típica es el anillo

Alcanza un ancho de banda de 30000GHz.

Sólo necesita repetidores cada 30 Km.

No hay interferencias.

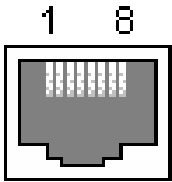
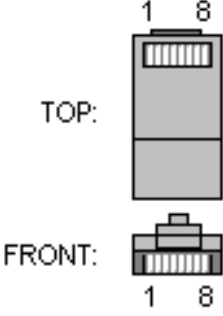
Pesa 8 veces menos que el cable par trenzado.

El cable y los conectores vistos bajo la norma Ethernet 802.3

El Cable

	Tipo de cable	Conexión	Longitud máxima	º max. de estaciones	Observaciones
10 base	Coaxial grueso, 50 ohmios, o cable amarillo,	Conectores tipo vampiro	500 m	100	Líneas acabadas en una impedancia del mismo valor que la Z característica, Líneas libres acabadas en tapones para evitar los rebotes
10 base 2	Coaxial fino, 50 ohmios RG58	BNC	185 m	30	conexión por "T" [Problema: hay que abrir la red] Líneas libres acabadas en tapones para evitar los rebotes
10 base T	Par trenzado	RJ-45 (ISO 8877).	100 m		Hub: Bus lógico en una caja y todas las estaciones colgando
100 base T	UTP categoría 5				

Numeración del conector RJ45

Hembra	Macho
Visto de frente	Conector visto de frente y desde arriba
	

Ethernet 10Base-T (T568A colores)

RJ45	Colores	Código	Utilidad	Pares
1	Blanco/Verde o el blanco del par verde	T3	RecvData +	PAR 3
2	Verde o Verde/blanco	R3	RecvData -	
3	Blanco/Naranja o el blanco del par naranja	T2	Txdata +	PAR 2
4	Azul o azul/blanco	R1		PAR 1
5	Blanco/Azul o el blanco del par azul	T1		
6	Naranja o naranja/blanco	R2	TxData -	
7	Blanco/marrón o el blanco del par marrón	T4		PAR 4
8	Marrón o marrón/blanco	R4		

Ethernet 10Base-T (T568B colores)

RJ45	Colores	Código	Utilidad	Pares
1	Blanco/Naranja o el blanco del par naranja	T2	Txdata +	PAR 2
2	Naranja o naranja/blanco	R2	TxData -	
3	Blanco/verde o el blanco del par verde	T3	RecvData +	PAR 3
4	Azul o azul/blanco	R1		PAR 1
5	Blanco/azul o el blanco del par azul	T1		
6	Verde o verde/blanco	R3	RecvData -	
7	Blanco/marrón o el blanco del par marrón	T4		PAR 4
8	Marrón o marrón/blanco	R4		

Cable cruzado para la comunicación de dos equipos con RJ45

1 (Txdata +) ----- 3 (RecvData +)
2 (Txdata -) ----- 6 (RecvData -)
3 (RecvData +)----- 1 (Txdata +)
6 (RecvData -) -----2 (Txdata -)

Pares usados según norma

ATM 155Mbps usa los pares 2 y 4 (pins 1-2, 7-8)

Ethernet 10Base - T4 usa los pares 2 y 3 (pins 1-2, 3-6)

Ethernet 100Base-T4 usa los pares 2 y 3 (4T+) (pins 1-2, 3-6)

Ethernet 100Base-T8 usa los pares 1,2,3 y 4 (pins 4-5, 1-2, 3-6, 7-8)

Cable usado según norma

Categoría	Velocidad	Donde se usa
1	No entra dentro de los criterios de la norma	
2	Hasta 1 MHz	Para telefonía
3	Hasta 16 MHz	Ethernet 10Base-T
4	Hasta 20 MHz	Token-Ring, 10Base-T
5	Hasta 100 MHz	100Base-T, 10Base-T

Método de acceso al medio

En las redes de difusión es necesario definir una estrategia para saber cuando una máquina puede empezar a transmitir para evitar que dos o más estaciones comiencen a transmitir a la vez (colisiones).

CSMA

Se basa en que cada estación monitoriza o "escucha" el medio para determinar si éste se encuentra disponible para que la estación puede enviar su mensaje, o por el contrario, hay algún otro nodo utilizándolo, en cuyo caso espera a que quede libre.

Token

El método del testigo(token) asegura que todos los nodos van a poder emplear el medio para transmitir en algún momento. Ese momento será cuando el nodo en cuestión reciba un paquete de datos especial denominado testigo. Aquel nodo que se encuentre en posesión del testigo podrá transmitir y recibir información, y una vez haya terminado, volverá a dejar libre el testigo y lo enviará a la próxima estación.

REDES DE COMPUTADORAS

Clasificación

Según la distancia entre computadoras se denominan a las redes de una forma u otra. Si los ordenadores se encuentran dentro de un mismo ámbito geográfico como una habitación, un edificio o un campus (como máximo del orden de 1 km) se llama **Red de Área Local** (Local Area Network). Si la distancia es del orden de la decena de kilómetro entonces se está ante una **Red de Área Metropolitana** (Metropolitan Area Network). Si la distancia es de varios cientos de kilómetros entonces se habla de una **Red de Área Extensa** (Wide Area Network) y si se trata de una red que cubre todo el planeta entonces se habla de **Internet**.

LAN

Hay tres parámetros característicos en una red de ordenadores: su tamaño, su tecnología de transmisión y su topología.

Las LAN están restringidas en cuanto a su tamaño y por ello se puede calcular su velocidad de transmisión. El medio de transmisión consiste en un cable al que están conectadas todas las máquinas. Su **topología**, es decir la forma en que enlazan los ordenadores puede ser en bus o en anillo, etc... como se verá más adelante.

MAN

Las redes de área metropolitana o MAN están basadas en una tecnología similar a las LAN y son capaces de transmitir datos, voz y señal de TV por cable local, tiene un mecanismo de arbitraje propio estándar llamado Distributed Queue Dual Bus **DQDB** o Bus Dual de Cola Distribuida. Consiste en dos cables unidireccionales.

WAN

Redes de área amplia o WAN. Está formada por un conjunto de máquinas destinadas a ejecutar programas de aplicación llamadas **Hosts** las cuales están a su vez conectadas por una subred. Esta subred tiene dos componentes distintos: las líneas de transmisión que mueven bits de una máquina a otra y los elementos de conmutación que conectan dos o más líneas de transmisión con el objeto de escoger una línea de salida para reenviarlos. Estos elementos se llaman **enrutadores** o nodos conmutadores de paquetes.

Gateways

Por último indicar la existencia de interredes formadas por redes LAN y WAN a veces diferentes entre sí conectadas mediante pasarelas o **gateways** que son máquinas que efectúan la labor de conexión y traducción. Éstas se diferencian significativamente de Internet que conecta gobiernos, universidades e individuos.

Red local y Aplicaciones.

Es un sistema de transmisión de información con el objetivo de compartir recursos con los que trabaja un ordenador normalmente, es decir, ficheros, directorios, impresoras, plotters, escáners, etc... entre ordenadores conectados entre sí o bien mediante redes conectadas entre sí.

La palabra local se refiere a que el conjunto de ordenadores se encuentra próximo geográficamente hablando es decir, que se encuentra en el espacio físico de un mismo centro.

En general una red local está caracterizada por una distancia corta entre ordenadores, un medio de comunicación entre éstos, una velocidad de conexión elevada, la utilización de cables de conexión simples (como los coaxiales o los telefónicos).

Cuentan con la facilidad de su instalación, de su administración y de su bajo precio.

En la mayoría de los casos una red se usa para compartir entre varios ordenadores una unidad de almacenamiento enorme o en general cualquier dispositivo periférico del que hagan uso varias personas de un mismo grupo de trabajo, de esta forma no es necesario comprar ese periférico para cada ordenador, por ejemplo una impresora láser.

Además constituye un valor añadido a la hora de compartir la información y distribuir tareas.

Nodo y Estación de trabajo.

Nodo.

Nodo es un término que se emplea en el ámbito de los grandes ordenadores (mainframes) y que en realidad a lo que se refiere es al principio, al final, o a la intersección de un enlace de comunicaciones, no a un dispositivo específico.

Estación de trabajo.

El término estación de trabajo describe cualquier microordenador, ordenador personal, terminal, y todos los periféricos conectados a éstos, o independientes (una impresora, un módem, un escáner, etc.) con una tarjeta interfaz de red instalada mediante la cual se puede acceder al servidor a través de los cables (o a través de ondas de radio, como es el caso de las redes inalámbricas). Para poder comunicarse con el servidor de la red, las estaciones de trabajo deben ejecutar un programa especial de comunicaciones.

Las estaciones de trabajo suelen ser microordenadores conectados a la red que por la general mantienen su capacidad de trabajar de forma autónoma utilizando su propio software, pero normalmente están conectadas al servidor de la red de modo que pueden acceder a la información contenida en éste. Para poder hacer esto, la estación de trabajo necesita un interfaz especial que se conecta a una de las ranuras de expansión de la estación, y al que se conecta un cable que lo enlaza con el servidor.

Tipos de Servidores

Hemos visto que una red local interconecta ordenadores, comparte dispositivos, pero para compartir eficientemente periféricos tales como discos duros o impresoras, es necesario configurar uno o más ordenadores como "gestores". Un gestor (también llamado servidor) es un ordenador que comparte sus periféricos con otros ordenadores. Un servidor de discos permite compartir zonas del disco. Un servidor de impresión es un ordenador que pueden utilizar todos los usuarios, y que se encarga de volcar el contenido de ficheros en una impresora.

Servidores de disco (Disk Server)

Al principio las redes utilizaban un servidor de disco donde se almacenaba la información que iban a compartir las distintas estaciones de trabajo de la red. Para ésta el servidor es simplemente otra unidad de disco duro donde almacenar ficheros. En el caso de un PC funcionando bajo MS-DOS la unidad asignada del servidor de ficheros es como un disco normal del que se mantiene una tabla de asignación de ficheros (FAT o file allocation table) propia para poder saber exactamente donde se encuentra un determinado fichero.

Lo de "propia" significa que el servidor de ficheros contiene varias particiones, cada una de ellas asignada a un usuario. Esto se hace para que cuando el PC necesite leer un fichero, lea la FAT de la partición que le ha sido asignada y busque en ella el fichero que necesita. Una vez modificado lo graba en el disco grabando la FAT en la partición asignada. De no ser así, podría darse el caso de que varios usuarios accediesen a grabar la FAT, que en cada caso sería distinta, produciéndose un complicado galimatías indescifrable y se perderían todos los datos.

Algunas particiones pueden definirse como públicas, pero normalmente suelen definirse como de sólo lectura de modo que no puedan modificarse. Todas las estaciones pueden acceder a esta información pero no pueden cambiarla. Un ejemplo de partición pública podría ser una base de datos de consulta.

Hay dos tipos de servidores de disco: dedicados y no dedicados. Normalmente los servidores dedicados no disponen de monitor, ni teclado; para lo único que sirven es para dar servicio a las solicitudes de otros ordenadores de la red. Los servidores no dedicados son ordenadores normales que tienen conectado un disco duro o impresora, y que al igual que los dedicados dan servicio a la red, con la diferencia de que se puede utilizar como un ordenador normal mientras actúa de servidor.

Servidores de ficheros (File Server)

Un servidor de ficheros es mucho más eficiente y sofisticado que un gestor de disco. Contiene software especial que procesa comandos antes de que el sistema operativo los reciba. El servidor de ficheros contiene su propia FAT. Cuando una estación de trabajo pide un determinado fichero, el servidor de ficheros ya sabe donde está el fichero y lo envía directamente a la memoria de la estación de trabajo. En este caso para la estación de trabajo el servidor de ficheros no es otra unidades discos más, como sucede con el servidor de disco. Es mucho más eficiente porque no necesita enviar una copia de la FAT a la estación que pide un fichero, y además no es necesario particionar la unidad de disco.

El servidor de ficheros se encarga de que en un momento dado, sólo hay un usuario utilizando un fichero determinad. Los usuarios pueden trabajar como si tuvieran un disco de gran capacidad conectado a su ordenador. Cualquiera puede tener acceso a los ficheros, a no ser que se establezcan claves de acceso.

Los servidores de ficheros pueden ser de cuatro tipos: centralizados, distribuidos, dedicados y no dedicados.

Servidores de ficheros centralizados y distribuidos.

Para la mayoría de las redes un único servidor de ficheros es más que suficiente. Este tipo de servidor se conoce con el nombre de servidor central. Funciona de manera muy similar como lo hace un miniordenador; una unidad se encarga de dar servicio a cada estación de trabajo.

Por razones de eficiencia en ocasiones es conveniente instalar más de un servidor para dar servicio a departamentos distintos. Estos servidores se conocen con el nombre de servidores distribuidos. Esta es una solución más eficiente porque se reducen los tiempos de acceso y además si uno de ellos queda fuera de servicio, la red puede seguir funcionando.

Servidores de ficheros dedicados y no dedicados.

Un servidor de ficheros dedicado es un microordenador con disco duro que se utiliza exclusivamente como servidor de ficheros. Dedicando toda su capacidad de memoria, procesamiento y recursos a dar servicio a las estaciones de trabajo se consigue un aumento de la velocidad y eficiencia de la red. Un servidor no dedicado es aquél que se usa, además de para funciones de servicio de ficheros, como estación de trabajo. Esto implica que la RAM debe estar dividida de forma que puedan ejecutarse programas en la máquina. Cuanto más rápido sea el microprocesador, más rápido puede el servidor realizar sus tareas lo que a su vez implica un costo más elevado.

Servidores de ficheros de una red punto a punto.

En una red punto a punto los usuarios deciden qué recursos de su ordenador desean compartir con el resto de los usuarios de la red.

Un usuario puede utilizar su unidad de disco duro como servidor de ficheros para otros usuarios de la red. Una red de este tipo puede constar de varias estaciones de trabajo que hacen funciones de servidor de ficheros no dedicado cuyos propietarios han decidido compartir con el resto de los usuarios de la red. Esta filosofía es aplicable así mismo a las impresoras y otros dispositivos.

Servidor de impresión.

Al igual que un servidor de ficheros permite compartir un disco duro, un servidor de impresión hace lo mismo, sólo que en esta ocasión lo que se comparten son las impresoras.

Cada uno de los ordenadores tiene conectada una impresora. Estas impresoras son suficientes para la mayoría de los trabajos, pero cuando es necesario hacer copias de mayor calidad, los usuarios utilizan la impresora láser conectada al servidor de impresión. El servidor de impresión puede tener varios tipos de impresoras, según las necesidades.

Para poder compartir impresoras, el servidor de impresión debe disponer del software adecuado y por lo general contiene lo que se conoce como un spooler de impresión, que es un buffer donde se almacenan los trabajos que cada estación manda a imprimir. Los trabajos se van poniendo en cola y se imprimen de forma secuencial en orden de llegada. Hay spoolers de impresión con funciones para cambiar el orden de impresión de los trabajos y para indicar la hora en la que se quiere imprimir un determinado trabajo. Por ejemplo, los trabajos que requieren muchísimo tiempo de impresión se ponen en el spooler de impresión para que se impriman fuera de las horas de trabajo.

Servidor de comunicaciones.

Los servidores de comunicaciones están diseñados para liberar a la red de las tareas relativas a la transmisión de información. El servidor de comunicaciones funciona igual que una centralita telefónica, haciendo las mismas funciones que un sistema PABX (centralita automática privada). Por medio del servidor de comunicaciones una estación puede llamar a una red externa o cualquier otro sistema, buscar cierta información y enviarla a la estación que la ha solicitado. El servidor de comunicaciones se puede utilizar también para conectar dispositivos incompatibles a una red.

A pesar de que un servidor de comunicaciones efectúa las funciones de un módem, en particular proporcionando acceso a redes telefónicas de larga distancia, hay bastantes diferencias entre ellos. La mayoría de los módems están conectados a una sola estación y sólo los puede utilizar esa estación. Los servidores de comunicaciones pueden responder a varias solicitudes a la vez. Además el servidor de comunicaciones ofrece más funciones, tales como multiplexación y conmutación, detección de errores, y además es mucho más fiable.

Es de destacar que para redes de unos 12 equipos y con las nuevas tecnologías se puede perfectamente compartir un módem como un periférico más, usando un software específico y diseñado para tal fin, algo muy común hoy día. De esta forma el servidor de comunicaciones no sería necesario, ya que el módem compartido haría todo el trabajo.

Configuración y Topología

El diseño de una red se debe planificar pensando en las necesidades de cada uno.

Existen tres tipos de configuraciones independientes del fabricante

Peer to Peer: en la que cada estación de trabajo puede compartir sus recursos con otras estaciones que están en la misma red.

Compartición de recursos: los recursos a compartir están centralizados en uno o más servidores y en éstos está toda la información. Las estaciones no pueden compartir sus recursos.

Cliente/Servidor: las aplicaciones o programas se dividen entre el servidor y las estaciones de trabajo. Hay por tanto una parte de la aplicación que está en el ordenador cliente y otra en el servidor.

Topología.

Nuestro objetivo es conseguir que todos los componentes de la red formen un todo y trabajen sin ningún problema de incompatibilidad, por ello si escogemos componentes hardware del mismo fabricante no tendremos ningún problema. Sin embargo, eso no siempre es posible y por ello existen

estándares de software o más conocidos como protocolos, ellos son los que permiten la comunicación entre las distintas redes.

La red local está formada por cables que conectan los ordenadores entre sí y a la forma en que se distribuyen el cableado y los componentes de la red se le llama topología. Existen tres topologías básicas: estrella, bus y árbol.

Topología en Bus: existe un solo enlace de comunicaciones que se llama bus al cual están conectados todos los equipos de la red.

Como el bus es un medio de acceso compartido, sólo un dispositivo de todos los que están conectados al bus puede transmitir en un mismo momento. La comunicación se efectúa troceando la información para evitar que una estación transmita constantemente y las demás no puedan hacerlo.

En los extremos del cable existen una piezas que se llaman terminadores, que indican el final o principio de la red.

Las conexiones entre la tarjeta de red y el bus se efectúan mediante un conector en forma de T, llamado derivador.

Topología en estrella.

Los enlaces en la red se disponen de forma radial partiendo de un dispositivo central. Este dispositivo radial se conoce como hub o concentrador. Cada rama de la estrella conecta al dispositivo central con otro periférico. El hub actúa como central de comunicaciones entre los dispositivos periféricos.

Topología en anillo

Los PC's se distribuyen alrededor de un anillo formado por el medio de transmisión . Este anillo está formado por un pequeño repartidor llamado MAU o unidad de acceso a múltiples estaciones.

A diferencia de la topología en bus, en la que la información que un dispositivo dejada en el medio era recibida por todos los integrantes de la red, ahora viaja a su equipo adyacente y si no es para él se lo pasa al siguiente.

Ventajas e inconvenientes.

La de árbol y la de estrella son muy flexibles y económicas pero la señal puede sufrir una atenuación si la red es extensa.

La de anillo sin embargo no presenta este inconveniente pero si falla un solo dispositivo puede acabar con toda la red.

El modelo OSI

Una de las necesidades más acuciantes de un sistema de comunicaciones es el establecimiento de estándares, sin ellos sólo podrían comunicarse entre si equipos del mismo fabricante y que usaran la misma tecnología.

La conexión entre equipos electrónicos se ha ido estandarizando paulatinamente siendo las redes telefónicas las pioneras en este campo. Por ejemplo la histórica CCITT definió los estándares de telefonía: PSTN, PSDN e ISDN.

Otros organismos internacionales que generan normas relativas a las telecomunicaciones son: ITU-TSS (antes CCITT), ANSI, IEEE e ISO

La ISO (Internacional Organization for Standardisation) ha generado una gran variedad de estándares, siendo uno de ellos la norma ISO-7494 que define el modelo OSI, este modelo nos ayudará a comprender mejor el funcionamiento de las redes de ordenadores.

El modelo OSI no garantiza la comunicación entre equipos pero pone las bases para una mejor estructuración de los protocolos de comunicación. Tampoco existe ningún sistema de comunicaciones que los siga estrictamente, siendo la familia de protocolos TCP/IP la que más se acerca.

El modelo OSI describe siete niveles para facilitar los interfaces de conexión entre sistemas abiertos, en la página siguiente puedes verlo con más detalle.

Nivel	Nombre	Función	Dispositivos y protocolo
1	Físico	Se ocupa de la transmisión del flujo de bits a través del medio.	Cables, tarjetas y repetidores (hub). RS-232, X.21.
2	Enlace	Divide el flujo de bits en unidades con formato (tramas) intercambiando estas unidades mediante el empleo de protocolos.	Puentes (bridges). HDLC y LLC.
3	Red	Establece las comunicaciones y determina el camino que tomarán los datos en la red.	Encaminador(router). IP, IPX.
4	Transporte	La función de este nivel es asegurar que el	Pasarela (gateway).

		receptor reciba exactamente la misma información que ha querido enviar el emisor, y a veces asegura al emisor que el receptor ha recibido la información que le ha sido enviada. Envía de nuevo lo que no haya llegado correctamente.	UDP, TCP, SPX.
5	Sesión	Establece la comunicación entre las aplicaciones, la mantiene y la finaliza en el momento adecuado. Proporciona los pasos necesarios para entrar en un sistema utilizando otro. Permite a un mismo usuario, realizar y mantener diferentes conexiones a la vez (sesiones).	Pasarela.
6	Presentación	Conversión entre distintas representaciones de datos y entre terminales y organizaciones de sistemas de ficheros con características diferentes.	Pasarela. Compresión, encriptado, VT100.
7	Aplicación	Este nivel proporciona unos servicios estandarizados para poder realizar unas funciones específicas en la red. Las personas que utilizan las aplicaciones hacen una petición de un servicio (por ejemplo un envío de un fichero). Esta aplicación utiliza un servicio que le ofrece el nivel de aplicación para poder realizar el trabajo que se le ha encomendado (enviar el fichero).	X.400

La comunicación según el modelo OSI siempre se realizará entre dos sistemas. Supongamos que la información se genera en el nivel 7 de uno de ellos, y desciende por el resto de los niveles hasta llegar al nivel 1, que es el correspondiente al medio de transmisión (por ejemplo el cable de red) y llega hasta el nivel 1 del otro sistema, donde va ascendiendo hasta alcanzar el nivel 7. En este proceso, cada uno de los niveles va añadiendo a los datos a transmitir la información de control relativa a su nivel, de forma que los datos originales van siendo recubiertos por capas de control.

De forma análoga, al ser recibido dicho paquete en el otro sistema, según va ascendiendo del nivel 1 al 7, va dejando en cada nivel los datos añadidos por el nivel equivalente del otro sistema, hasta quedar únicamente los datos a transmitir. La forma, pues de enviar información en el modelo OSI

tiene una cierta similitud con enviar un paquete de regalo a una persona, donde se ponen una serie de papeles de envoltorio, una o más cajas, hasta llegar al regalo en sí.

Emisor	Paquete	Receptor
Aplicación	C7 Datos	Aplicación
Presentación	C6 C7 Datos	Presentación
Sesión	C5 C6 C7 Datos	Sesión
Transporte	C4 C5 C6 C7 Datos	Transporte
Red	C3 C4 C5 C6 C7 Datos	Red
Enlace	C2 C3 C4 C5 C6 C7 Datos	Enlace
Físico	C2 C3 C4 C5 C6 C7 Datos	Físico

C7-C2 : Datos de control específicos de cada nivel.

Los niveles OSI se entienden entre ellos, es decir, el nivel 5 enviará información al nivel 5 del otro sistema (lógicamente, para alcanzar el nivel 5 del otro sistema debe recorrer los niveles 4 al 1 de su propio sistema y el 1 al 4 del otro), de manera que la comunicación siempre se establece entre niveles iguales, a las normas de comunicación entre niveles iguales es a lo que llamaremos protocolos. Este mecanismo asegura la modularidad del conjunto, ya que cada nivel es independiente de las funciones del resto, lo cual garantiza que a la hora de modificar las funciones de un determinado nivel no sea necesario reescribir todo el conjunto.

En las familias de protocolos más utilizadas en redes de ordenadores (TCP/IP, IPX/SPX, etc.) nos encontraremos a menudo funciones de diferentes niveles en un solo nivel, debido a que la mayoría de ellos fueron desarrollados antes que el modelo OSI.

PROTOCOLOS DE COMUNICACIÓN DE DATOS

Protocolos de red

Conjuntos de normas que definen todos los aspectos que intervienen en una comunicación, por tanto definen el formato que van a tener los paquetes de información y las órdenes que un dispositivo va a aceptar

NetBios: fabricado por Microsoft e IBM y se usa para redes de área local o de área metropolitana.

TCP/IP: siglas de Protocolo de Control de Transmisión/Protocolo Internet, fue desarrollado por el departamento de Defensa para su red de comunicaciones ARPANET. Es muy empleado en máquinas UNIX y en redes de área extensa por sus facilidades de enrutamiento.

Tiene la ventaja de tener compatibilidad con todos los sistemas operativos, tecnología capaz de conectar sistemas con protocolos distintos entre sí, por ejemplo FTP o Telnet, es el protocolo que se usa en Internet.

IPX/SPX: siglas de Intercambio de Paquetes entre Redes/Intercambio de Paquetes Secuencial. Fue definido por la compañía Novell como soporte de sus redes de área local, es plenamente enrutable.

Apple Talk: es la contribución de la compañía Apple a los protocolos, sólo se emplea en este tipo de ordenadores.

Todos los protocolos anteriormente mencionados los soporta Windows NT, Novell soporta su protocolo IPX/SPX.

Tipos de redes.

Ethernet: topología de Bus con cable coaxial grueso o delgado o bien con par trenzado. Velocidad: 10 Mbps

Token ring: combina la topología en estrella y en anillo y opera en un ancho de banda de 4 o 16 Mbps.

ArcNet: usa una topología en bus o en estrella y generalmente opera a 2,5 Mbps, ArcNet Plus opera a 20 Mbps.

Tipología de las redes de área local.

Hay muchos parámetros que conforman la arquitectura de una red de área local, aquí veremos algunos de ellos.

- **Según la técnica de transmisión:** redes de difusión y redes punto a punto.
- **Según método de acceso al medio:** CSMA y Token.
- **Por su topología o disposición en el espacio:** estrella, bus, anillo y mixtas.

Técnicas de transmisión

Redes de difusión

Tienen un solo canal de comunicación compartido por todas las máquinas, en principio todas las máquinas podrían "ver" toda la información, pero hay un "código" que especifica a quien va dirigida.

Redes punto a punto

Muchas conexiones entre pares individuales de máquinas.

La información puede pasar por varias máquinas intermedias antes de llegar a su destino.

Se puede llegar por varios caminos, con lo que se hacen muy importantes las rutinas de enrutamiento o ruteo. Es más frecuente en redes MAN y WAN.

Topología

Se entiende por topología de una red local la distribución física en la que se encuentran dispuestos los ordenadores que la componen. De este modo, existen tres tipos, que podíamos llamar "puros". Son los siguientes:

- Estrella.
- Bus.
- Anillo

Topología en Estrella.

Esta topología se caracteriza por existir en ella un punto central, o más propiamente nodo central, al cual se conectan todos los equipos, de un modo muy similar a los rayos de una rueda.

De esta disposición se deduce el inconveniente de esta topología, y es que la máxima vulnerabilidad se encuentra precisamente en el nodo central, ya que si este falla, toda la red fallaría. Este posible fallo en el nodo central, aunque posible, es bastante improbable, debido a la gran seguridad que suele poseer dicho nodo. Sin embargo presenta como principal ventaja una gran modularidad, lo que permite aislar una estación defectuosa con bastante sencillez y sin perjudicar al resto de la red.

Para aumentar el número de estaciones, o nodos, de la red en estrella no es necesario interrumpir, ni siquiera parcialmente la actividad de la red, realizándose la operación casi inmediatamente.

La topología en estrella es empleada en redes Ethernet y ArcNet.

Topología en Bus

En la topología en bus, al contrario que en la topología de Estrella, no existe un nodo central, si no que todos los nodos que componen la red quedan unidos entre sí linealmente, uno a continuación del otro.

El cableado en bus presenta menos problemas logísticos, puesto que no se acumulan montones de cables en torno al nodo central, como ocurriría en un disposición en estrella. Pero, por contra, tiene la desventaja de que un fallo en una parte del cableado detendría el sistema, total o parcialmente, en función del lugar en que se produzca. Es además muy difícil encontrar y diagnosticar las averías que se producen en esta topología.

Debido a que en el bus la información recorre todo el bus bidireccionalmente hasta hallar su destino, la posibilidad de interceptar la información por usuarios no autorizados es superior a la existente en una Red en estrella debido a la modularidad que ésta posee. La red en bus posee un retardo en la propagación de la información mínimo, debido a que los nodos de la red no deben amplificar la señal, siendo su función pasiva respecto al tráfico de la red. Esta pasividad de los nodos es debida más bien al método de acceso empleado que a la propia disposición geográfica de los puestos de red.

La Red en Bus necesita incluir en ambos extremos del bus, unos dispositivos llamados terminadores, los cuales evitan los posibles rebotes de la señal, introduciendo una impedancia característica (50 Ohm.)

Añadir nuevos puesto a una red en bus, supone detener al menos por tramos, la actividad de la red. Sin embargo es un proceso rápido y sencillo.

Es la topología tradicionalmente usada en redes Ethernet.

Topología en Anillo

El anillo, como su propio nombre indica, consiste en conectar linealmente entre sí todos los ordenadores, en un bucle cerrado. La información se transfiere en un solo sentido a través del anillo, mediante un paquete especial de datos, llamado **testigo**, que se transmite de un nodo a otro, hasta alcanzar el nodo destino.

El cableado de la red en anillo es el más complejo de los tres enumerados, debido por una parte al mayor coste del cable, así como a la necesidad de emplear unos dispositivos denominados Unidades de Acceso Multiestación (MAU) para implementar físicamente el anillo.

A la hora de tratar con fallos y averías, la red en anillo presenta la ventaja de poder derivar partes de la red mediante los MAU's, aislando dichas partes defectuosas del resto de la red mientras se determina el problema. Un fallo, pues, en una parte del cableado de una red en anillo, no debe detener toda la red. La adición de nuevas estaciones no supone una complicación excesiva, puesto que una vez más los MAU's aíslan las partes a añadir hasta que se hallan listas, no siendo necesario detener toda la red para añadir nuevas estaciones.

Dos buenos ejemplos de red en anillo serían Token-Ring y FDDI (fibra óptica)

Topologías híbridas.

Son las más frecuentes y se derivan de la unión de topologías "puras": estrella-estrella, bus-estrella, etc.

Componentes de una red.

Dentro de lo que son componentes de una red vamos a distinguir entre equipos de red, cableados y conectores a la misma; y, dentro de los equipos de red, también vamos a hacer una subdivisión en equipos que interconectan redes y equipos conectados a un segmento de las mismas.

Equipos que interconectan redes.

HUB (CONCENTRADORES)

Dispositivo que interconecta host dentro de una red. Es el dispositivo de interconexión más simple que existe. Sus principales características son:

- @ Se trata de un armario de conexiones donde se centralizan todas las conexiones de una red, es decir un dispositivo con muchos puertos de entrada y salida.

- @ No tiene ninguna función aparte de centralizar conexiones.

- @ Se suelen utilizar para implementar topologías en estrella física, pero funcionando como un anillo o como un bus lógico.

Hubs activos: permiten conectar nodos a distancias de hasta 609 metros, suelen tener entre 8 y 12 puertos y realizan funciones de amplificación y repetición de la señal. Los más complejos además realizan estadísticas.

Hubs pasivos: son simples armarios de conexiones. Permiten conectar nodos a distancias de hasta 30 metros. Generalmente suelen tener entre 8 y 12 puertos.

Repetidores.

Los repetidores son equipos que trabajan a nivel 1 de la pila OSI, es decir, repiten todas las señales de un segmento a otro a nivel eléctrico.

Se utilizan para resolver los problemas de longitudes máximas de los segmentos de red (su función es extender una red Ethernet más allá de un segmento). No obstante, hay que tener en cuenta que, al retransmitir todas las señales de un segmento a otro, también retransmitirán las colisiones. Estos equipos sólo aíslan entre los segmentos los problemas eléctricos que pudieran existir en algunos de ellos.

El número máximo de repetidores en cascada es de cuatro, pero con la condición de que los segmentos 2 y 4 sean IRL, es decir, que no tengan ningún equipo conectado que no sean los repetidores. En caso contrario, el número máximo es de 2, interconectando 3 segmentos de red.

El repetidor tiene dos puertas que conectan dos segmentos Ethernet por medio de transceivers (instalando diferentes transceivers es posible interconectar dos segmentos de diferentes medios físicos) y cables drop.

El repetidor tiene como mínimo una salida Ethernet para el cable amarillo y otra para teléfono.

Con un repetidor modular se puede centralizar y estructurar todo el cableado de un edificio, con diferentes medios, adecuados según el entorno, y las conexiones al exterior.

Un Concentrador es un equipo igual a un multiport repeater pero con salida RJ-45.

Los repetidores con buffers es la unión de dos redes por una línea serie mediante una pareja de repetidores.

Sus principales características son:

@ Conectan a nivel físico dos intranets, o dos segmentos de intranet. Hay que tener en cuenta que cuando la distancia entre dos host es grande , la señal que viaja por la línea se atenúa y hay que regenerarla.

@ Permiten resolver problemas de limitación de distancias en un segmento de intranet.

@ Se trata de un dispositivo que únicamente repite la señal transmitida evitando su atenuación; de esta forma se puede ampliar la longitud del cable que soporta la red.

@ Al trabajar al nivel más bajo de la pila de protocolos obliga a que:

@ Los dos segmentos que interconecta tenga el mismo acceso al medio y trabajen con los mismos protocolos.

@ Los dos segmentos tengan la misma dirección de red.

Puentes o Bridges.

Estos equipos se utilizan asimismo para interconectar segmentos de red, (amplía una red que ha llegado a su máximo, ya sea por distancia o por el número de equipos) y se utilizan cuando el tráfico no es excesivamente alto en las redes pero interesa aislar las colisiones que se produzcan en los segmentos interconectados entre sí.

Los bridges trabajan en el nivel 2 de OSI, con direcciones físicas, por lo que filtra tráfico de un segmento a otro.

Esto lo hace de la siguiente forma: Escucha los paquetes que pasan por la red y va configurando una tabla de direcciones físicas de equipos que tiene a un lado y otro (generalmente tienen una tabla dinámica), de tal forma que cuando escucha en un segmento un paquete de información que va dirigido a ese mismo segmento no lo pasa al otro, y viceversa.

No filtra los broadcasts, que son paquetes genéricos que lanzan los equipos a la red para que algún otro les responda, aunque puede impedir el paso de determinados tipos de broadcast. Esto es típico para solicitar las cargas de software, por ejemplo. Por tanto, al interconectar segmentos de red con bridges, podemos tener problemas de tormentas de broadcasts, de saturación del puente por sobrecarga de tráfico, etc.

El número máximo de puentes en cascada es de siete; no pueden existir bucles o lazos activos, es decir, si hay caminos redundantes para ir de un equipo a otro, sólo uno de ellos debe estar activo, mientras que el redundante debe ser de backup. Para esto, cuando se está haciendo bridging en las redes, se usa el algoritmo de spanning-tree, mediante el cual se deshacen los bucles de los caminos redundantes.

Las posibles colisiones no se transmiten de un lado a otro de la red. El bridge sólo deja pasar los datos que van a un equipo que él conoce.

El bridge generalmente tiene una tabla dinámica, aíslan las colisiones, **pero no filtran protocolos**.

El bridge trabaja en el nivel 2 de OSI y aísla las colisiones

La primera vez que llega un paquete al bridge lo transmitirá, pero aprende (ya que, si el paquete no lo coge nadie, significa que no está).

El peligro de los bridges es cuando hay exceso de broadcast y se colapsa la red. A esto se le llama tormenta de broadcast, y se produce porque un equipo está pidiendo ayuda (falla).

Sus principales características son:

- @ Son dispositivos que ayudan a resolver el problema de limitación de distancias, junto con el problema de limitación del número de nodos de una red.

- @ Trabajan al nivel de enlace del modelo OSI, por lo que pueden interconectar redes que cumplan las normas del modelo 802 (3, 4 y 5). Si los protocolos por encima de estos niveles son diferentes en ambas redes, el puente no es consciente, y por tanto no puede resolver los problemas que puedan presentársele.

- @ Se utilizan para:

- @ Ampliar la extensión de la red, o el número de nodos que la constituyen.

- @ Reducir la carga en una red con mucho tráfico, uniendo segmentos diferentes de una misma red.

- @ Unir redes con la misma topología y método de acceso al medio, o diferentes.

- @ Cuando un puente une redes exactamente iguales, su función se reduce exclusivamente a direccionar el paquete hacia la subred destino.

- @ Cuando un puente une redes diferentes, debe realizar funciones de traducción entre las tramas de una topología a otra.

Cada segmento de red, o red interconectada con un puente, tiene una dirección de red diferente.

Los puentes no entienden de direcciones IP, ya que trabajan en otro nivel.

Los puentes realizan las siguientes funciones:

- @ Reenvío de tramas: constituye una forma de filtrado. Un puente solo reenvía a un segmento a aquellos paquetes cuya dirección de red lo requiera, no traspasando el puente los paquetes que vayan dirigidos a nodos locales a un segmento. Por tanto, cuando un paquete llega a un puente, éste examina la dirección física destino contenida en él, determinado así si el paquete debe atravesar el puente o no.

- @ Técnicas de aprendizaje: los puentes construyen tablas de dirección que describen las rutas, bien sea mediante el examen del flujo de los paquetes (puenteado transparente) o bien con la obtención

de la información de los "paquetes exploradores" (encaminamiento fuente) que han aprendido durante sus viajes la topología de la red.

Los primeros puentes requerían que los gestores de la red introdujeran a mano las tablas de dirección.

Los puentes trabajan con direcciones físicas.

Routers.

Estos equipos trabajan a nivel 3 de la pila OSI, es decir pueden filtrar protocolos y direcciones a la vez. Los equipos de la red saben que existe un router y le envían los paquetes directamente a él cuando se trate de equipos en otro segmento.

Además los routers pueden interconectar redes distintas entre sí; eligen el mejor camino para enviar la información, balancean tráfico entre líneas, etc.

El router trabaja con tablas de encaminamiento o enrutado con la información que generan los protocolos, deciden si hay que enviar un paquete o no, deciden cual es la mejor ruta para enviar un paquete o no, deciden cual es la mejor ruta para enviar la información de un equipo a otro, pueden contener filtros a distintos niveles, etc.

Poseen una entrada con múltiples conexiones a segmentos remotos, garantizan la fiabilidad de los datos y permiten un mayor control del tráfico de la red. Su método de funcionamiento es el encapsulado de paquetes.

Para interconectar un nuevo segmento a nuestra red, sólo hace falta instalar un router que proporcionará los enlaces con todos los elementos conectados.

Sus principales características son:

- @ Es como un puente incorporando características avanzadas.

- @ Trabajan a nivel de red del modelo OSI, por tanto trabajan con direcciones IP.

- @ Un router es dependiente del protocolo.

- @ Permite conectar redes de área local y de área extensa.

- @ Habitualmente se utilizan para conectar una red de área local a una red de área extensa.

- @ Son capaces de elegir la ruta más eficiente que debe seguir un paquete en el momento de recibirlo.

@ La forma que tienen de funcionar es la siguiente.

@ Cuando llega un paquete al router, éste examina la dirección destino y lo envía hacia allí a través de una ruta predeterminada.

@ Si la dirección destino pertenece a una de las redes que el router interconecta, entonces envía el paquete directamente a ella; en otro caso enviará el paquete a otro router más próximo a la dirección destino.

@ Para saber el camino por el que el router debe enviar un paquete recibido, examina sus propias tablas de encaminamiento.

Existen routers multiprotocolo que son capaces de interconectar redes que funcionan con distintos protocolos; para ello incorporan un software que pasa un paquete de un protocolo a otro, aunque no son soportados todos los protocolos.

Cada segmento de red conectado a través de un router tiene una dirección de red diferente.

Gateways.

También llamados traductores de protocolos, son equipos que se encargan, como su nombre indica, a servir de intermediario entre los distintos protocolos de comunicaciones para facilitar la interconexión de equipos distintos entre sí.

Su forma de funcionar es que tienen duplicada la pila OSI, es decir, la correspondiente a un protocolo y, paralelamente, la del otro protocolo. Reciben los datos encapsulados de un protocolo, los van desencapsulando hasta el nivel más alto, para posteriormente ir encapsulando los datos en el otro protocolo desde el nivel más alto al nivel más bajo, y vuelven a dejar la información en la red, pero ya traducida.

Los gateways también pueden interconectar redes entre sí.

Sus características principales son:

@ Se trata de un ordenador u otro dispositivo que interconecta redes radicalmente distintas.

@ Trabaja al nivel de aplicación del modelo OSI.

@ Cuando se habla de pasarelas a nivel de redes de área local, en realidad se está hablando de routers.

@ Son capaces de traducir información de una aplicación a otra como por ejemplo las pasarelas de correo electrónico.

Equipos de red conectados a un segmento.

Transceivers.

Son equipos que son una combinación de transmisor/receptor de información. El transceiver transmite paquetes de datos desde el controlador al bus y viceversa.

En una ethernet, los transceivers se desconectan cuando el equipo al que están conectados no está funcionando, sin afectar para nada al comportamiento de la red.

Multitransceivers.

Son transceivers que permiten la conexión de más de un equipo a la red en el mismo sitio, es decir, tienen varias salidas para equipos.

Multiport-transceivers

Son equipos que van conectados a un transceiver y que tienen varias puertas de salida para equipos. La única limitación que tienen es que mediante estos equipos no se pueden interconectar equipos que conecten redes entre sí.

Fan-out.

Estos equipos van conectados a un transceiver, y permiten dividir la señal del mismo a varios equipos. Su limitación estriba en que la longitud de los cables que vayan a los equipos es menor, porque no regeneran la señal, a diferencia de los multiport-transceivers.

El fan-out permite conectar hasta ocho DTE's utilizando un sólo transceiver. Poniendo un fan-out en cascada de dos niveles, se podría conseguir hasta 64 DTE's con un transceiver conectado a la red.

El fan-out puede configurar una red de hasta ocho estaciones sin usar cable ethernet ni transceivers, por medio de un fan-out, funcionando así de modo aislado.

La longitud del cable AUI, desde el segmento al DTE se reduce a 40m. si hay un fan-out en medio.

Multiport-repeaters.

Son equipos que van conectados a red, dando en cada una de sus múltiples salidas señal de red regenerada. Entre sí mismos se comportan como un segmento de red.

El multiport cuenta como un repetidor. Tiene salida AUI o BNC y es parecido al fan-out, pero en cada una de sus salidas regenera señal. Es un repetidor.

Servidores de Terminales.

Son equipos que van conectados a la red, y en sus salidas generan una señal para un terminal, tanto síncrono como asíncrono, desde el cual se podrá establecer una sesión con un equipo o host.

El servidor de terminales es un dispositivo configurado para integrar terminales "tontas" o PCs por interfase serie con un emulador de terminales. Puede utilizar los protocolos TCP/IP y LAT para una red ethernet, y se puede acceder a cualquier ordenador que soporte TCP/IP o LAT (DECnet).

Protocolos TCP/IP

Protocolos de comunicaciones.

Los protocolos que se utilizan en las comunicaciones son una serie de normas que deben aportar las siguientes funcionalidades:

- Permitir localizar un ordenador de forma inequívoca.
- Permitir realizar una conexión con otro ordenador.
- Permitir intercambiar información entre ordenadores de forma segura, independiente del tipo de máquinas que estén conectadas (PC, Mac, AS-400...).
- Abstracta a los usuarios de los enlaces utilizados (red telefónica, radio enlaces, satélite...) para el intercambio de información.
- Permitir liberar la conexión de forma ordenada.

Debido a la gran complejidad que conlleva la interconexión de ordenadores, se ha tenido que dividir todos los procesos necesarios para realizar las conexiones en diferentes niveles. Cada nivel se ha creado para dar una solución a un tipo de problema particular dentro de la conexión. Cada nivel tendrá asociado un protocolo, el cual entenderán todas las partes que formen parte de la conexión.

Diferentes empresas han dado diferentes soluciones a la conexión entre ordenadores, implementando diferentes familias de protocolos, y dándole diferentes nombres (DECnet, TCP/IP, IPX/SPX, NETBEUI, etc.).

¿Qué es TCP/IP?

Cuando se habla de TCP/IP , se relaciona automáticamente como el protocolo sobre el que funciona la red Internet . Esto , en cierta forma es cierto , ya que se le llama TCP/IP , a la familia de protocolos que nos permite estar conectados a la red Internet . Este nombre viene dado por los dos protocolos estrella de esta familia :

- El protocolo TCP, funciona en el nivel de transporte del modelo de referencia OSI, proporcionando un transporte fiable de datos.
- El protocolo IP, funciona en el nivel de red del modelo OSI, que nos permite encaminar nuestros datos hacia otras maquinas.

Pero un protocolo de comunicaciones debe solucionar una serie de problemas relacionados con la comunicación entre ordenadores , además de los que proporciona los protocolos TCP e IP .

Arquitectura de protocolos TCP/IP

Para poder solucionar los problemas que van ligados a la comunicación de ordenadores dentro de la red Internet , se tienen que tener en cuenta una serie de particularidades sobre las que ha sido diseñada TCP/IP:

- Los programas de aplicación no tienen conocimiento del hardware que se utilizara para realizar la comunicación (módem, tarjeta de red...)
- La comunicación no esta orientada a la conexión de dos maquinas, eso quiere decir que cada paquete de información es independiente, y puede viajar por caminos diferentes entre dos maquinas.
- La interfaz de usuario debe ser independiente del sistema, así los programas no necesitan saber sobre que tipo de red trabajan.
- El uso de la red no impone ninguna topología en especial (distribución de los distintos ordenadores).

De esta forma, podremos decir, que dos redes están interconectadas, si hay una maquina común que pase información de una red a otra. Además, también podremos decir que una red Internet virtual realizara conexiones entre redes, que ha cambio de pertenecer a la gran red, colaboraran en el trafico de información procedente de una red cualquiera, que necesite de ella para acceder a una red remota. Todo esto independiente de las maquinas que implementen estas funciones, y de los sistemas operativos que estas utilicen .

Descomposición en niveles de TCP/IP.

Toda arquitectura de protocolos se descompone en una serie de niveles , usando como referencia el modelo OSI . Esto se hace para poder dividir el problema global en subproblemas de más fácil solución .

Al diferencia de OSI , formado por una torre de siete niveles , TCP/IP se descompone en cinco niveles , cuatro niveles software y un nivel hardware . A continuación pasaremos a describir los niveles software , los cuales tienen cierto paralelismo con el modelo OSI.

Nivel de aplicación

Constituye el nivel mas alto de la torre TCP/IP . A diferencia del modelo OSI , se trata de un nivel simple en el que se encuentran las aplicaciones que acceden a servicios disponibles a través de Internet . Estos servicios están sustentados por una serie de protocolos que los proporcionan . Por ejemplo , tenemos el protocolo FTP (File Transfer Protocol), que proporciona los servicios necesarios para la transferencia de ficheros entre dos ordenadores.

Otro servicio, sin el cual no se concibe Internet , es el de correo electrónico, sustentado por el protocolo SMTP (Simple Mail Transfer Protocol) .

Nivel de transporte

Este nivel proporciona una comunicación extremo a extremo entre programas de aplicación. La maquina remota recibe exactamente lo mismo que le envió la maquina origen. En este nivel el emisor divide la información que recibe del nivel de aplicación en paquetes, le añade los datos necesarios para el control de flujo y control de errores , y se los pasa al nivel de red junto con la dirección de destino.

En el receptor este nivel se encarga de ordenar y unir las tramas para generar de nuevo la información original.

Para implementar el nivel de transporte se utilizan dos protocolos :

- **UDP:** proporciona un nivel de transporte no fiable de datagramas, ya que apenas añade información al paquete que envía al nivel inferior, solo la necesaria para la comunicación extremo a extremo. Lo utilizan aplicaciones como NFS y RPC, pero sobre todo se emplea en tareas de control.
- **TCP (Transport Control Protocol):** es el protocolo que proporciona un transporte fiable de flujo de bits entre aplicaciones. Esta pensado para poder enviar grandes cantidades de información de forma fiable, liberando al programador de aplicaciones de la dificultad de

gestionar la fiabilidad de la conexión (retransmisiones, pérdidas de paquete, orden en que llegan los paquetes ,duplicados de paquetes, ...) que gestiona el propio protocolo. Pero la complejidad de la gestión de la fiabilidad tiene un coste en eficiencia, ya que para llevar a cabo las gestiones anteriores se tiene que añadir bastante información a los paquetes a enviar. Debido a que los paquetes a enviar tienen un tamaño máximo, como mas información añade el protocolo para su gestión , menos información que proviene de la aplicación podrá contener ese paquete. Por eso, cuando es mas importante la velocidad que la fiabilidad, se utiliza UDP, en cambio TCP asegura la recepción en destino de la información a transmitir.

Nivel de red

También recibe el nombre de **nivel Internet**. Coloca la información que le pasa el nivel de transporte en datagramas IP, le añade cabeceras necesaria para su nivel y lo envía al nivel inferior. Es en este nivel donde se emplea el algoritmo de encaminamiento, al recibir un datagrama del nivel inferior decide, en función de su dirección, si debe procesarlo y pasarlo al nivel superior, o bien encaminarlo hacia otra maquina. Para implementar este nivel se utilizan los siguientes protocolos:

- **IP (Internet Protocol):** es un protocolo no orientado a la conexión, con mensajes de un tamaño máximo . Cada datagrama se gestiona de forma independiente, por lo que dos datagramas pueden utilizar diferentes caminos para llegar al mismo destino, provocando que lleguen en diferente orden o bien duplicados. Es un protocolo no fiable , eso quiere decir que no corrige los anteriores problemas, ni tampoco informa de ellos. Este protocolo recibe información del nivel superior y le añade la información necesaria para su gestión (direcciones IP , checksum)
- **ICMP (Internet Control Message Protocol):** proporciona un mecanismo de comunicación de información de control y de errores entre maquinas intermedias por las que viajaran los paquetes de datos . Esto datagramas los suelen emplear las maquinas (gateways, host, ...) para informarse de condiciones especiales en la red, como la existencia de una congestión , la existencia de errores y las posibles peticiones de cambios de ruta. Los mensajes de ICMP están encapsulados en datagramas IP.
- **IGMP (Internet Group Management Protocol):** este protocolo esta íntimamente ligado a IP . Se emplea en maquinas que emplean IP multicast . El IP multicast es una variante de IP que permite emplear datagramas con múltiples destinatarios .

También en este nivel tenemos una serie de protocolos que se encargan de la resolución de direcciones:

- **ARP (Address Resolution Protocol):** cuando una maquina desea ponerse en contacto con otra conoce su dirección IP , entonces necesita un mecanismo dinámico que permite conocer su dirección física . Entonces envía una petición ARP por broadcast (o sea a todas las maquinas). El protocolo establece que solo contestara a la petición , si esta lleva su dirección IP . Por lo tanto solo contestara la maquina que corresponde a la dirección IP buscada , con un mensaje que incluya la dirección física . El software de comunicaciones debe mantener una cache con los pares IP-dirección física . De este modo la siguiente vez que hay que hacer una transmisión a es dirección IP , ya conoceremos la dirección física.
- **RARP (Reverse Address Resolution Protocol):** a veces el problema es al revés, o sea, una máquina solo conoce su dirección física, y desea conocer su dirección lógica. Esto ocurre, por ejemplo, cuando se accede a Internet con una dirección diferente, en el caso de PC que acceden por módem a Internet, y se le asigna una dirección diferente de las que tiene el proveedor sin utilizar. Para solucionar esto se envía por broadcast una petición RARP con su dirección física , para que un servidor pueda darle su correspondencia IP.
- **BOOTP (Bootstrap Protocol):** el protocolo RARP resuelve el problema de la resolución inversa de direcciones, pero para que pueda ser mas eficiente, enviando más información que meramente la dirección IP, se ha creado el protocolo BOOTP. Este además de la dirección IP del solicitante , proporciona información adicional, facilitando la movilidad y el mantenimiento de las maquinas.

Nivel de enlace

Este nivel se limita a recibir datagramas del nivel superior (nivel de red) y transmitirlo al hardware de la red. Pueden usarse diversos protocolos: DLC(IEEE 802.2), Frame Relay, X.25, etc.

La interconexión de diferentes redes genera una red virtual en la que las maquinas se identifican mediante una dirección de red lógica. Sin embargo a la hora de transmitir información por un medio físico se envía y se recibe información de direcciones físicas. Un diseño eficiente implica que una dirección lógica sea independiente de una dirección física, por lo tanto es necesario un mecanismo que relacione las direcciones lógicas con las direcciones físicas. De esta forma podremos cambiar nuestra dirección lógica IP conservando el mismo hardware, del mismo modo podremos cambiar una tarjeta de red, la cual contiene una dirección física, sin tener que cambiar nuestra dirección lógica IP.

Direcciones IP y máscaras de red

En una red TCP/IP los ordenadores se identifican mediante un número que se denomina **dirección IP**. Esta dirección ha de estar dentro del rango de direcciones asignadas al organismo o empresa a la que pertenece, estos rangos son concedidos por un organismo central de Internet, el **NIC** (Network Information Center).

Una dirección IP está formada por 32 bits, que se agrupan en octetos:

01000001 00001010 00000010 00000011

Para entendernos mejor utilizamos las direcciones IP en formato decimal, representando el valor decimal de cada octeto y separando con puntos:

129.10.2.3

Las dirección de una máquina se compone de dos partes cuya longitud puede variar:

- **Bits de red:** son los bits que definen la red a la que pertenece el equipo.
- **Bits de host:** son los bits que distinguen a un equipo de otro dentro de una red.

Los bits de red siempre están a la izquierda y los de host a la derecha, veamos un ejemplo sencillo:

Bits de Red	Bits de Host
10010110 11010110 10001101	11000101
150.214.141.	197

Para ir entrando en calor diremos también que esta máquina pertenece a la red 150.214.141.0 y que su máscara de red es 255.255.255.0. Si queréis ir reflexionando sobre algo os mostramos de nuevo en formato binario la máscara de red llevando a caballitos a la dirección de la máquina:

10010110	11010110	10001101	11000101
11111111	11111111	11111111	00000000

La máscara de red es un número con el formato de una dirección IP que nos sirve para distinguir cuando una máquina determinada pertenece a una subred dada, con lo que podemos averiguar si dos máquinas están o no en la misma subred IP. En formato binario todas las máscaras de red tienen los "1" agrupados a la izquierda y los "0" a la derecha.

Para llegar a comprender como funciona todo esto podríamos hacer un ejercicio práctico.

Ejercicio 1

Sea la dirección de una subred 150.214.141.0, con una máscara de red 255.255.255.0

Comprobar cuales de estas direcciones pertenecen a dicha red:

150.214.141.32

150.214.141.138

150.214.142.23

Paso 1: para ver si son o no direcciones validas de dicha subred clase C tenemos que descomponerlas a nivel binario:

150.214.141.32	10010110.1101010.10001101.10000000
150.214.141.138	10010110.1101010.10001101.10001010
150.214.142.23	10010110.1101010.10001110.00010111
255.255.255.0	11111111.11111111.11111111.00000000
150.214.141.0	10010110.1101010.10001101.00000000

Paso 2: una vez tenemos todos los datos a binario pasamos a recordar el operador lógico AND o multiplicación:

Valor A	Valor B	Resultado
0	0	0
0	1	0
1	0	0
1	1	1

Vamos a explicar como hace la comprobación el equipo conectado a una red local.

Primero comprueba la dirección IP con su máscara de red, para ello hace un AND bit a bit de todos los dígitos:

150.214.141.32	10010110.1101010.10001101.10000000
255.255.255.0	11111111.11111111.11111111.00000000
<hr/>	
150.214.141.0	10010110.1101010.10001101.00000000

Luego hace la misma operación con la dirección IP destino.

```
150.214.141.138  10010110.1101010.10001101.10001010
255.255.255.0    11111111.11111111.11111111.00000000
```

```
150.214.141.0    10010110.1101010.10001101.00000000
```

El resultado que obtenemos ambas veces es la dirección de red, esto no indica que los dos equipos están dentro de la misma red.

Paso3: vamos a hacerlo con la otra dirección IP

```
150.214.142.23  10010110.1101010.10001110.00010111
255.255.255.0    11111111.11111111.11111111.00000000
```

```
150.214.142.0    10010110.1101010.10001110.00000000
```

Como vemos este resultado nos indica que dicho equipo no pertenece a la red sino que es de otra red en este caso la red sería 150.214.142.0.

Ejercicio 2

Pasamos ahora a complicar un poco más la cosa. Como hemos leído antes la dirección IP se compone de dos partes la dirección de red y la dirección de host(máquina o PC). Imaginemos que en nuestra red solo hace falta 128 equipos y no 254 la solución sería dividir la red en dos partes iguales de 128 equipos cada una.

Primero cogemos la máscara de red.

Dirección de red Dirección de host.

```
_____._____._____._____
255.255.255.0 11111111.11111111.11111111.00000000
```

Si lo que queremos es crear dos subredes de 128 en este caso tenemos que coger un bit de la parte de identificativa del host.

Por lo que la máscara de red quedaría de esta manera.

Dirección de red Dirección de host.

_____._____._____.X._____

255.255.255.128 11111111.11111111.11111111.10000000

Donde X es el bit que hemos cogido para dicha construcción. Por lo que el último octeto tendría el valor 10000000 que es 128 en decimal.

Si la dirección de red que hemos utilizado es la 150.214.141.0 al poner esta máscara de red tendríamos dos subredes.

La 150.214.141.0 y la 150.214.141.128 que tendrían los siguientes rangos IP:

La 150.214.141.0 cogería desde la 150.214.141.1 hasta la 150.214.141.127

La 150.214.141.128 sería pues desde la 150.214.141.128 hasta la 150.214.141.254.

La máscara de red para las dos subredes sería la 255.255.255.128.

Comprobar.

Sea la máscara de red 255.255.255.128

La dirección de red 150.214.141.128

Comprobar si las siguientes direcciones pertenecen a dicha subred.

150.214.141.134

150.214.141.192

150.214.141.38

150.214.141.94

Si hemos realizado el ejercicio se tiene que comprobar que:

150.214.141.134 150.214.141.192 pertenecen a la subred 150.214.141.128

150.214.141.38 150.214.141.94 pertenecen a la subred 150.214.141.0

Clases de red

Para una mejor organización en el reparto de rangos las redes se han agrupado en cuatro clases, de manera que según el tamaño de la red se optará por un tipo u otro.

Las direcciones de clase A

Corresponden a redes que pueden direccionar hasta 16.777.214 máquinas cada una.

Las direcciones de red de clase A tienen siempre el primer bit a 0.

0 + Red (7 bits) + Máquina (24 bits)

Solo existen 124 direcciones de red de clase A.

Ejemplo:

	Red	Máquina		
Binario	0 0001010	00001111	00010000	00001011
Decimal	10	15	16	11

Rangos(notación decimal):

1.xxx.xxx.xxx - 126.xxx.xxx.xxx

Las direcciones de clase B

Las direcciones de red de clase B permiten direccionar 65.534 máquinas cada una.

Los dos primeros bits de una dirección de red de clase B son siempre 01.

01 + Red (14 bits) + Máquina (16 bits)

Existen 16.382 direcciones de red de clase B.

Ejemplo:

	Red		Máquina	
Binario	10 000001	00001010	00000010	00000011
Decimal	129	10	2	3

Rangos(notación decimal):

128.001.xxx.xxx - 191.254.xxx.xxx

Las direcciones de clase C

Las direcciones de clase C permiten direccionar 254 máquinas.

Las direcciones de clase C empiezan con los bits 110

110 + Red (21 bits) + Máquina (8 bits)

Existen 2.097.152 direcciones de red de clase C.

Ejemplo:

	Red			Máquina
Binario	110 01010	00001111	00010111	00001011
Decimal	202	15	23	11

Rangos(notación decimal):

192.000.001.xxx - 223.255.254..xxx

Las direcciones de clase D

Las direcciones de clase D son un grupo especial que se utiliza para dirigirse a grupos de máquinas. Estas direcciones son muy poco utilizadas. Los cuatro primeros bits de una dirección de clase D son 1110.

Direcciones de red reservadas

Existen una serie de direcciones IP con significados especiales.

- Direcciones de subredes reservadas:

000.xxx.xxx.xxx (1)

127.xxx.xxx.xxx (reservada como la propia máquina)

128.000.xxx.xxx (1)

191.255.xxx.xxx (2)

192.168.xxx.xxx (reservada para intranets)

223.255.255.xxx (2)

- Direcciones de máquinas reservadas:

xxx.000.000.000 (1)

xxx.255.255.255 (2)

xxx.xxx.000.000 (1)

xxx.xxx.255.255 (2)

xxx.xxx.xxx.000 (1)

xxx.xxx.xxx.255 (2)

1. Se utilizan para identificar a la red.
2. Se usa para enmascarar.

Instalación de una Red Local

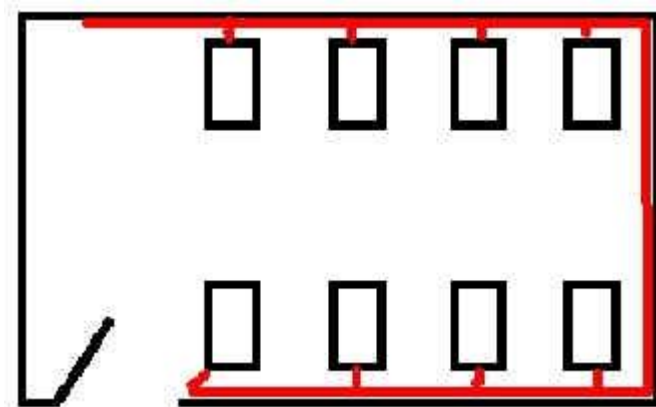
¿QUE ES PRIMERO?

Lo primero que se tiene que tomar en cuenta para la instalación de una red local es saber el lugar en donde se va a instalar y si cuenta con las características necesarias como son: Espacio, Instalaciones eléctricas y sobre todo el espacio.

Ya que este ultimo es muy importante ya que si no existe un espacio suficiente será muy difícil trabajar en la instalacion de la red.

No olvidemos que tenemos que tener en cuenta el numero total de las maquinas a instalar en la red, axial como las impresoras, entre otras cosas.

El este caso, la red contara con 8 maquinas y 4 impresoras. Cuando se tiene esto en cuenta se recomienda que se realice un plano de la habitación donde se va a instalar la red pero con una vista desde arriba como se muestra en el grafico.



La imagen anterior presenta la colocación de los ordenadores y como podemos ver, la mejor colocación para el cableado(color rojo) es en forma de U , de esta forma podemos evitar realizar complicadas instalaciones de cables y que no molesten a los usuarios.

¿EL MATERIAL?

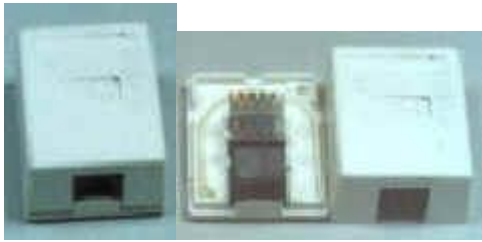
Una vez determinado el numero de Maquinas o nodos a instalar se procede a determinar el material que se va a utilizar para la instalacion de red. En el caso de esta red se va a necesitar el siguiente material.

- @ 1 Hub o concentrador de 16 puestos (8 puestos ordenador + 4 puestos impresora).
- @ 24 conectores hembra de base RJ45(estos son el tipo de clavija) para pared.
- @ Cable UTP(Sin Apantallar) o STP(Apantallado).
- @ 24 conectores aéreos macho RJ45.
- @ Material diverso para la instalación (canaletas, herramientas, grapas de pared, etc...)

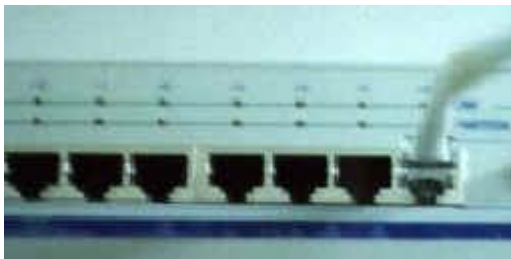
INICIAR CON LA INSTALACION DE LA RED

Cuando ya se cuente con todo el material se pasara a la instalacion de las canaletas, que es donde se encontrara el cable de nuestra red.

Después de haber instalado las canaletas se continuara a instalar los conectores base RJ45, estos se tienen que encontrar lo mas cerca posible de los nodos, ya que es donde se conectara el cable UTP, que después ira a el HUB



Una vez instalados todos los conectores base RJ45, se pasara el cable por las canaletas para después conectar el cable UTP a las maquinas, una vez conectado todo el cable y pasado por las canaletas lo único que resta es conectar nuestros cables al HUB. como se muestra en la siguiente imagen.



Cómo instalar una red de computadoras

Luego de elegir un nuevo computador, generalmente quedan en el hogar o en la oficina computadores antiguos, con discos duros de baja capacidad, escasa memoria RAM y de relativa baja velocidad (ejemplo: Pentium 100, 64 RAM y 4GB de disco duro) que prácticamente ya no soportan nuevos programas. La solución para mantenerlos activos es conectarlos en red, aprovechando la mayor velocidad y capacidad de los computadores más nuevos. Se puede conectar dos o más computadoras con el fin de compartir recursos como impresoras, escáner o conexión a Internet. Mediante este sistema, se pueden compartir los archivos, incluso dejándolos guardados en el de mayor capacidad. Se puede utilizar en forma compartida la conexión a Internet, cualquiera sea la velocidad de conexión (MODEM de 56 kbs hasta líneas ADSL), de manera simultánea.

Existen incluso sistemas más avanzados en que es posible transformar el computador más lento en un terminal, permitiendo que el computador del ejemplo anterior posea la velocidad, memoria, sistema operativo y conexión a Internet del computador más avanzado. Dicho sistema requiere poseer el nuevo sistema operativo de Windows XP o Windows 2000 e instalar el sistema Linux en el computador que actuará de terminal. Ciertos programas (Winconnect) son capaces de realizar dicho proceso. El sistema operativo Linux se encuentra disponible en forma gratuita en la Internet (son 2 discos de 650 megabytes cada uno, se requiere poseer un grabador de CD para traspasarlos y dejarlos activos para su instalación; se requiere como mínimo 64 MB de RAM).

¿CÓMO SE INSTALA UNA RED CASERA?

Hay varias formas, pero las más comunes son interconectarlas mediante un cable de red tipo Ethernet, igual que en cualquier oficina, o hacer una red inalámbrica, permitiendo usar las computadoras desde cualquier punto de la casa sin necesidad de instalaciones que afecten la decoración.

Para instalar la red se necesita:

a) **Red alámbrica:** Tarjetas de red Ethernet (valor aproximado: \$15 000), Cable de red (\$700 x metro), terminales de cable (\$1 000 c/u).

b) **Red inalámbrica:** Tarjetas de red tipo Airport (Precios variables).

Para compartir una conexión a Internet, es necesario que una de las PC sirva como puerta de entrada y distribuya la señal a las otras máquinas. Esto se logra con aplicaciones como Wingate o Winroute, o bien instalando un LAN Módem que realice la función.

La mayoría de los nuevos computadores vienen con la tarjeta de red incluida, sin embargo, los antiguos no la traen y se les debe instalar. Para ello, hay que confirmar que exista un hueco o "slot" del tipo PCI libre, lo que generalmente es así.

Una vez instalada la tarjeta, se debe configurar la red. Partiremos en el computador nuevo, asignando el protocolo la dirección IP, que es el equivalente a un número telefónico y es individual para cada computador. En el menú de inicio, seleccionar las conexiones y pedir que se muestren todas, seleccionar el dispositivo de red con el botón derecho del mouse y seleccionar las propiedades. Seleccionar el protocolo de Internet (TCP/IP) e indicar que se quiere seleccionar una dirección IP específica, (asume que se cuenta con Windows XP, para instalación a Windows 98, ir a panel de control y seleccionar redes) (figura 1).

Se debe seleccionar una dirección IP (el "número telefónico"). Hay muchas alternativas, sugiero 192.168.0.xxx (este número va desde el 1 al 999 y permite conectar muchos computadores) y la "subset mask", que es otro número necesario que se calcula a partir de la dirección IP, pero que en el ejemplo es 255.255.255.0.

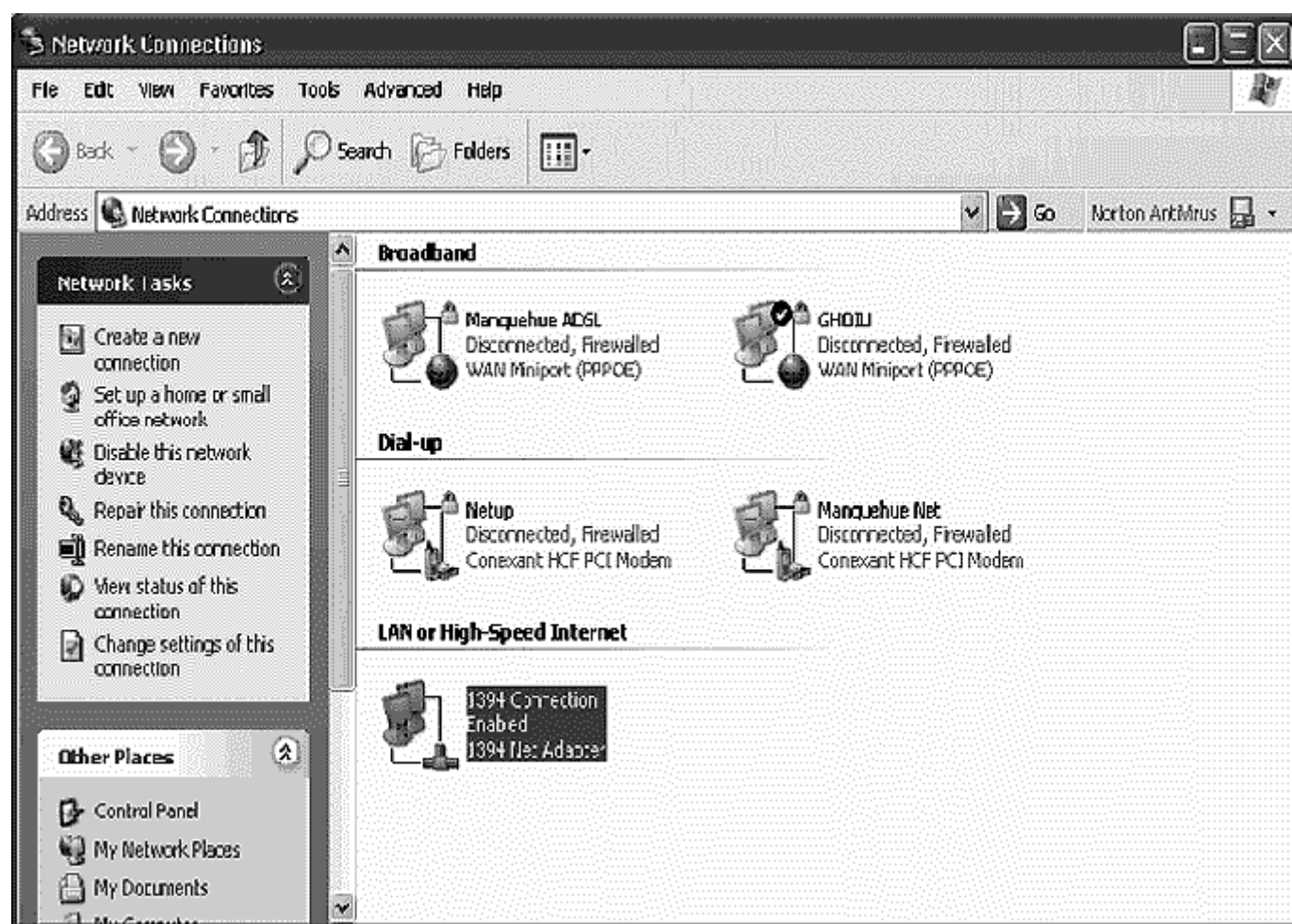


Figura 1.

En Windows 98 y versiones anteriores de Windows, es necesario reiniciar el computador, no así en Windows 2000, para que surtan efecto los cambios.

Luego, se debe configurar el computador secundario. Se debe realizar el mismo procedimiento (redes en Windows 95 ó 98) y seleccionar las propiedades del protocolo de Internet (TCP/IP). El número IP tiene un segmento compartido, en el ejemplo 192.168. 0.xxx (en que xxx debe ser un número diferente del otro computador). La "subnet mask" debe ser 255.255.255.0 (existen innumerables otras alternativas, pero deben ser obtenidas de tablas especiales para que funcione). Finalmente, se debe indicar el servidor DNS preferido, que debe ser el número indicado en el computador nuevo (192.168.0.2 en el caso del ejemplo) (figura 2).

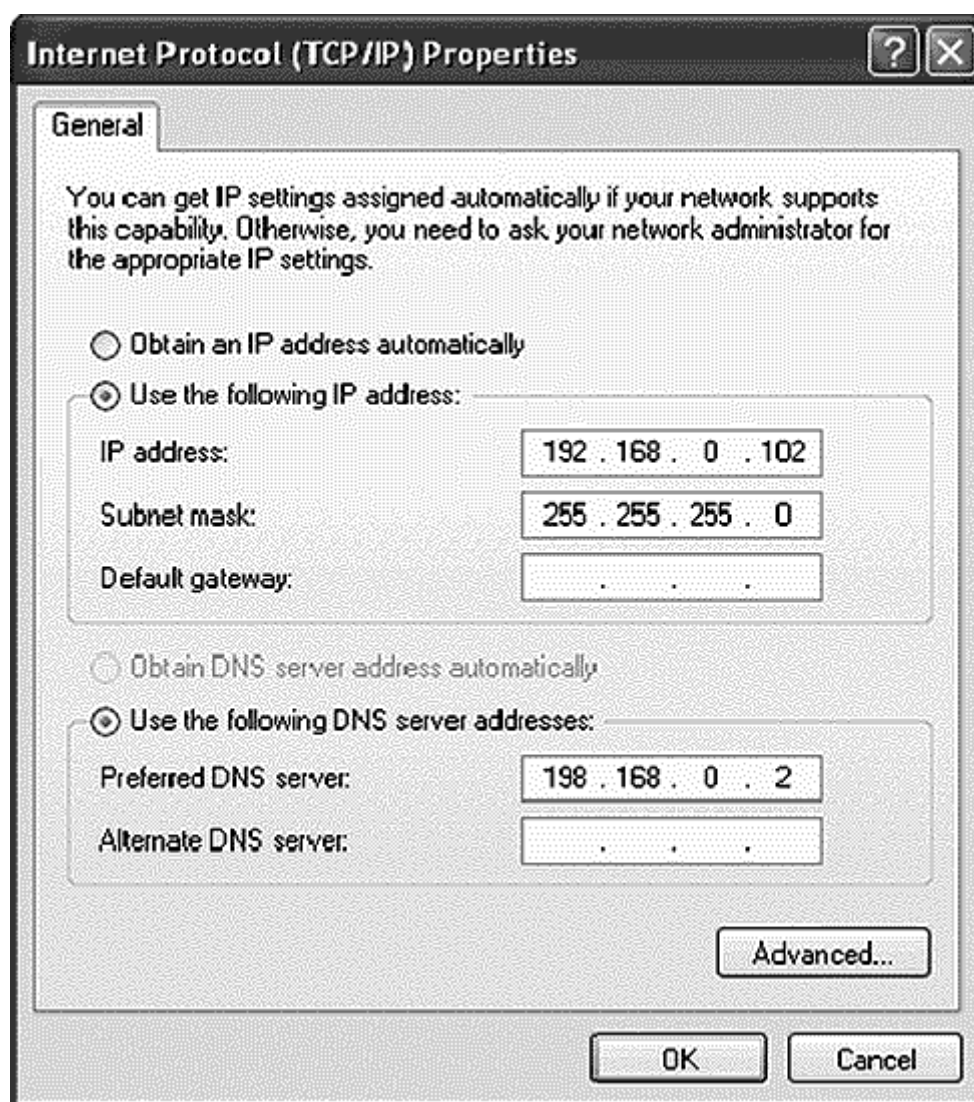


Figura 2.

La segunda fase consiste en compartir los archivos de ambos computadores para que puedan ser accesibles. Ello se debe realizar en cada una de las carpetas de cada uno de los computadores, eligiendo las que quedaran disponibles para ser compartidas (figura 3).

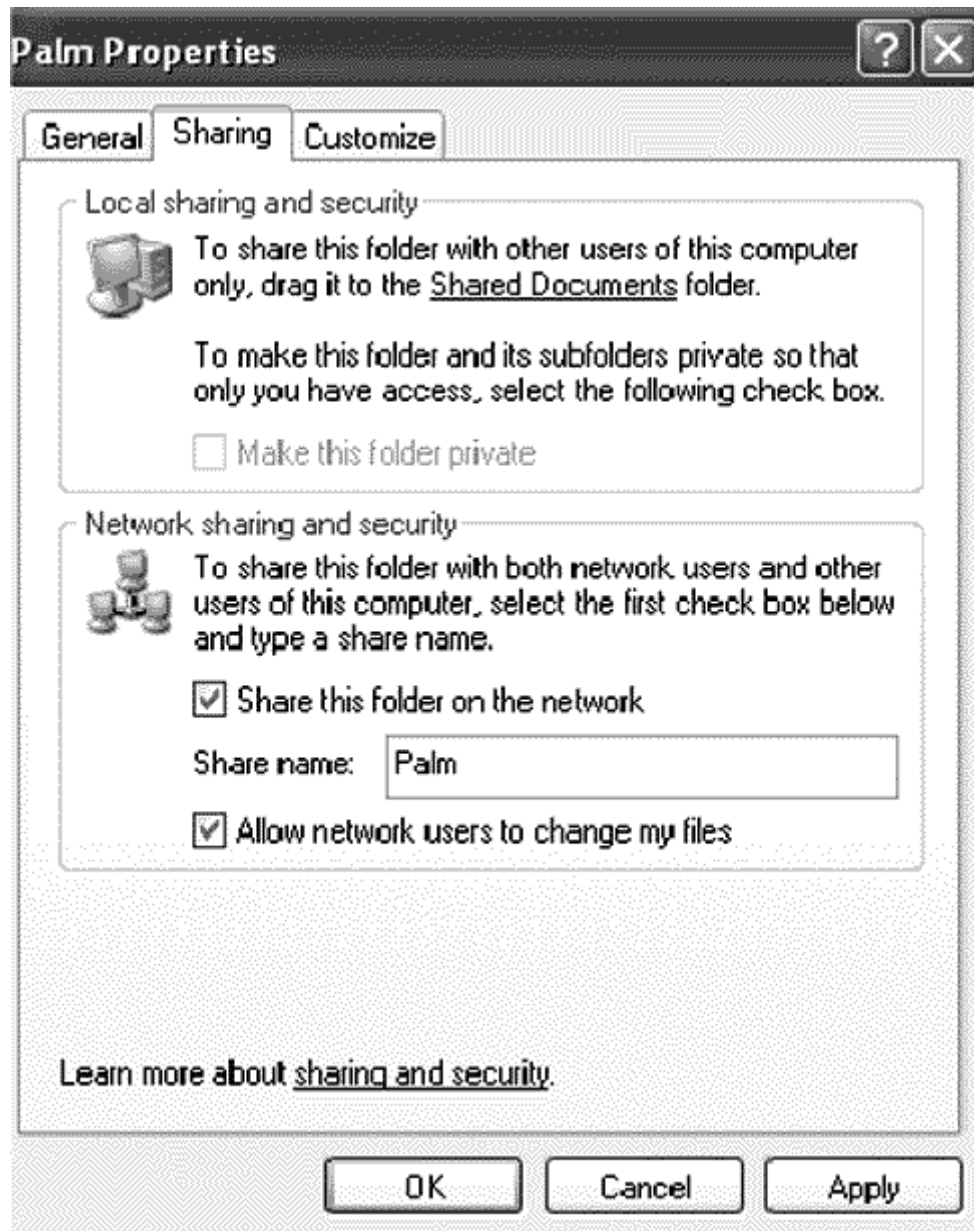


Figura 3.

Con el botón derecho del mouse se marca la carpeta y se eligen sus propiedades. Luego, se accede a "sharing" o compartir y se elige dicha alternativa.

En Windows 2000, además se debe permitir que distintos usuarios accedan al computador. Para ello, en el panel de control, se debe elegir usuarios e incorporar al otro computador con una clave de acceso. En Windows 95 y 98, se debe crear una cuenta de usuario independiente (en el panel de control). Se debe elegir un nombre de usuario y una clave. De no realizar este proceso, no se podrá establecer conexión entre las computadoras.

Finalmente, en Windows 95, 98 y 2000, se debe acceder a través de la red que generalmente se encuentra en el menú de inicio o en la pantalla de comienzo. Cada computador tiene su propio nombre, el cual aparecerá automáticamente al solicitar la búsqueda en el "grupo de trabajo" o "workgroup".

REDES DE AREA LOCAL

LANs: Iniciales de red de área local (Local Area Network), grupo de computadoras y otros dispositivos en un área limitada, como un edificio, conectadas por un enlace de comunicaciones que permite interactuar a los dispositivos de la red.

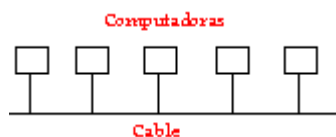
Características preponderantes:

- ☐ Los canales son propios de los usuarios o empresas.
- ☐ Los enlaces son líneas de alta velocidad.
- ☐ Las estaciones están cercas entre sí.
- ☐ Incrementan la eficiencia y productividad de los trabajos de oficinas al poder compartir información.
- ☐ Las tasas de error son menores que en las redes WAN.
- ☐ La arquitectura permite compartir recursos.

LANs mucha veces usa una tecnología de transmisión, dada por un simple cable, donde todas las computadoras están conectadas.

Existen varias topologías posibles en la comunicación sobre LANs.

- **Bus:** esta topología permite que todas las estaciones reciban la información que se transmite, una estación trasmite y todas las restantes escuchan.



Desventajas: al existir un solo canal de comunicación entre las estaciones de la red, si falla el canal o una estación, las restantes quedan incomunicadas. Algunos fabricantes resuelven este problema poniendo un bus paralelo alternativo, para casos de fallos o usando algoritmos para aislar las componentes defectuosas.

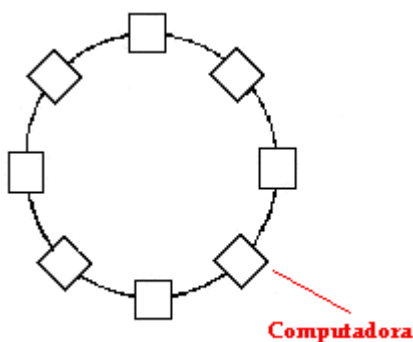
Existen dos mecanismos para la resolución de conflictos en la transmisión de datos:

1. **CSMA/CD:** son redes con escucha de colisiones. Todas las estaciones son consideradas igual, por ello compiten por el uso del canal, cada vez que una de ellas desea transmitir debe escuchar el canal, si alguien está transmitiendo espera a que termine, caso contrario

transmite y se queda escuchando posibles colisiones, en este último espera un intervalo de tiempo y reintenta nuevamente.

2. **Token Bus:** Se usa un token (una trama de datos) que pasa de estación en estación en forma cíclica, es decir forma un anillo lógico. Cuando una estación tiene el token, tiene el derecho exclusivo del bus para transmitir o recibir datos por un tiempo determinado y luego pasa el token a otra estación, previamente designada. Las otras estaciones no pueden transmitir sin el token, sólo pueden escuchar y esperar su turno. Esto soluciona el problema de colisiones que tiene el mecanismo anterior.

- **Anillo:** Recibe este nombre por su aspecto circular. El flujo de datos circula en una sola dirección, cada estación recibe el dato y lo envía a la estación siguiente del anillo.



Ventajas: los cuellos de botellas son muy pocos frecuentes

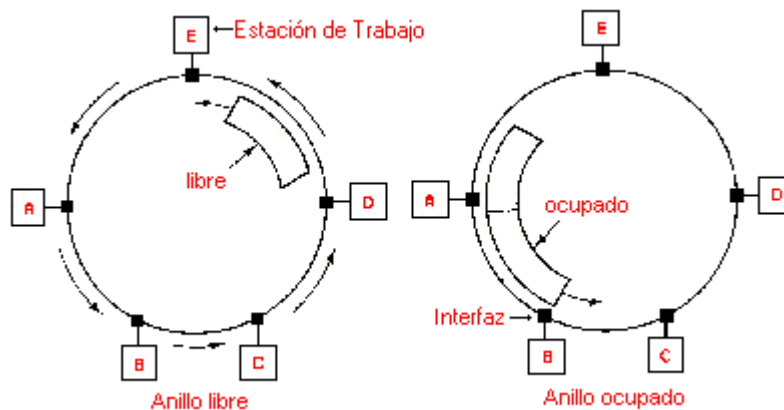
Desventajas: al existir un solo canal de comunicación entre las estaciones de la red, si falla el canal o una estación, las restantes quedan incomunicadas. Algunos fabricantes resuelven este problema poniendo un canal alternativo para casos de fallos, si uno de los canales es viable la red está activa, o usando algoritmos para aislar las componentes defectuosas.

Es muy compleja su administración, ya que hay que definir una estación para que controle el token.

Existe un mecanismo para la resolución de conflictos en la transmisión de datos:

- **Token Ring:** La estación se conecta al anillo por una unidad de interfaz (RIU), cada RIU es responsable de controlar el paso de los datos por ella, así como de regenerar la transmisión y pasarla a la estación siguiente.
- Si la dirección de cabecera de una determinada transmisión indica que los datos son para una estación en concreto, la unidad de interfaz los copia y pasa la información a la estación de trabajo conectada a la misma.
- Se usa en redes de área local con o sin prioridad, el token pasa de estación en estación en forma cíclica, inicialmente en estado desocupado. Cada estación cuando tiene el token (en este momento la estación controla el anillo), si quiere transmitir cambia su estado a ocupado,

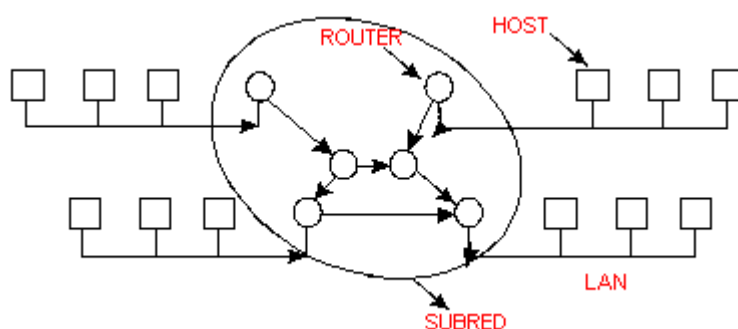
agregando los datos atrás y lo pone en la red, caso contrario pasa el token a la estación siguiente. Cuando el token pasa de nuevo por la estación que transmitió, saca los datos, lo pone en desocupado y lo regresa a la red.



MAN: Redes de área metropolitana (Metropolitan Area Network) con dos buses unidireccionales, cada uno de ellos es independiente del otro en cuanto a la transferencia de datos. Es básicamente una gran versión de LAN y usa una tecnología similar. Puede cubrir un grupo de oficinas de una misma corporación o ciudad, esta puede ser pública o privada. El mecanismo para la resolución de conflictos en la transmisión de datos que usan las MANs, es DQDB.

DQDB consiste en dos buses unidireccionales, en los cuales todas las estaciones están conectadas, cada bus tiene una cabecera y un fin. Cuando una computadora quiere transmitir a otra, si esta está ubicada a la izquierda usa el bus de arriba, caso contrario el de abajo.

1. oras especializadas usadas por dos o más líneas de transmisión. Para que un paquete llegue de un router a otro, generalmente debe pasar por routers intermedios, cada uno de estos lo recibe por una línea de entrada, lo almacena y cuando una línea de salida está libre, lo retransmite.



INTERNET WORKS: Es una colección de redes interconectadas, cada una de ellas puede estar desallorada sobre diferentes software y hardware. Una forma típica de Internet Works es un grupo de redes LANs conectadas con WANs. Si una subred le sumamos los host obtenemos una red.

El conjunto de redes mundiales es lo que conocemos como Internet.

TIPOS DE REDES LAN

La topología de una red define únicamente la distribución del cable que interconecta los diferentes ordenadores, es decir, es el mapa de distribución del cable que forma la intranet. Define cómo se organiza el cable de las estaciones de trabajo. A la hora de instalar una red, es importante seleccionar la topología más adecuada a las necesidades existentes. Hay una serie de factores a tener en cuenta a la hora de decidirse por una topología de red concreta y son :

- @ La distribución de los equipos a interconectar.
- @ El tipo de aplicaciones que se van a ejecutar.
- @ La inversión que se quiere hacer.
- @ El coste que se quiere dedicar al mantenimiento y actualización de la red local.
- @ El tráfico que va a soportar la red local.
- @ La capacidad de expansión. Se debe diseñar una intranet teniendo en cuenta la escalabilidad.

No se debe confundir el término topología con el de arquitectura. La arquitectura de una red engloba:

- @ La topología.
- @ El método de acceso al cable.
- @ Protocolos de comunicaciones.

Actualmente la topología está directamente relacionada con el método de acceso al cable, puesto que éste depende casi directamente de la tarjeta de red y ésta depende de la topología elegida

TOPOLOGIAS FISICAS

Es lo que hasta ahora se ha venido definiendo; la forma en la que el cableado se realiza en una ed. Existen tres topología físicas puras :

Topología en anillo.

Topología en bus.

Topología en estrella.

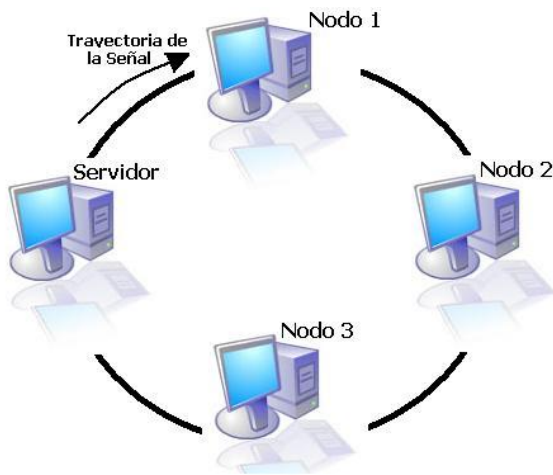
Existen mezclas de topologías físicas, dando lugar a redes que están compuestas por mas de una topología física.

TOPOLOGIA EN ANILLO

Red de área local en la que los dispositivos, nodos, están conectados en un bucle cerrado o anillo. Los mensajes en una red de anillo pasan de un nodo a otro en una dirección concreta. A medida que un mensaje viaja a través del anillo, cada nodo examina la dirección de destino adjunta al mensaje. Si la dirección coincide con la del nodo, éste acepta el mensaje. En caso contrario regenerará la señal y pasará el mensaje al siguiente nodo dentro del bucle.

Esta regeneración permite a una red en anillo cubrir distancias superiores a las redes en estrella o redes en bus. Puede incluirse en su diseño una forma de puentear cualquier nodo defectuoso o vacante. Sin embargo, dado que es un bucle cerrado, es difícil agregar nuevos nodos.

El tipo de tarjeta utilizada para este tipo de red es la de Token Ring.



TOPOLOGIA EN BUS

En una red en bus, cada nodo supervisa la actividad de la línea. Los mensajes son detectados por todos los nodos, aunque aceptados sólo por el nodo o los nodos hacia los que van dirigidos. Como una red en bus se basa en una "autopista" de datos común, un nodo averiado sencillamente deja de comunicarse; esto no interrumpe la operación, como podría ocurrir en una red en anillo, en la que los mensajes pasan de un nodo al siguiente.

Para evitar las colisiones que se producen al intentar dos o más nodos utilizar la línea al mismo tiempo, las redes en bus suelen utilizar detección de colisiones, o paso de señales, para regular el tráfico.

El tipo de tarjeta que se utiliza para este tipo de red es la Ethernet.

Sus principales ventajas son :

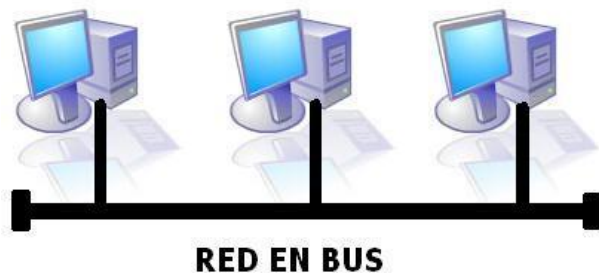
@ Fácil de instalar y mantener.

@ No existen elementos centrales del que dependa toda la red, cuyo fallo dejaría inoperativas a todas las estaciones.

Sus principales inconvenientes son :

@ Si se rompe el cable en algún punto, la red queda inoperativa por completo.

Cuando se decide instalar una red de este tipo en un edificio con varias plantas, lo que se hace es instalar una red por planta y después unir las todas a través de un bus troncal.



TOPOLOGIA EN ESTRELLA

Sus principales características son:

@Todas la estaciones de trabajo están conectadas a un punto central (concentrador), formando una estrella física.

@Habitualmente sobre este tipo de topología se utiliza como método de acceso el medio Pooling, siendo el nodo central el que se encarga de implementarlo.

@Cada vez que se quiere establecer comunicación entre dos ordenadores, la información transferida de un hacia el otro debe pasar por el punto central.

@Existen algunas redes con esta topología que utiliza como punto central una estación de trabajo que gobierna la red.

@La velocidad suele ser alta para comunicaciones entre el nodo central y los nodos extremos, pero es baja cuando se establece entre nodos extremos.

@Este tipo de topología se utiliza cuando el trasiego de información se va a realizar preferentemente entre el nodo central y el resto de los nodos, y no cuando la comunicación se hace entre nodos extremos.

@Si se rompe un cable sólo se pierde la conexión del nodo que interconectaba.

@Es fácil detectar y de localizar un problema en la red.

ADMINISTRACION DE REDES

Instalación y configuración del servidor DNS.

El Directorio Activo está integrado con DNS y para poder instalar y configurar el Directorio Activo primero debe de instalarse y configurarse un servidor DNS. Por lo tanto debe de abrirse el asistente “Asistente para configurar su servidor” con la ruta **Inicio\Herramientas administrativas\Asistente para configurar su Servidor** tal y como se muestra en la Figura 1.

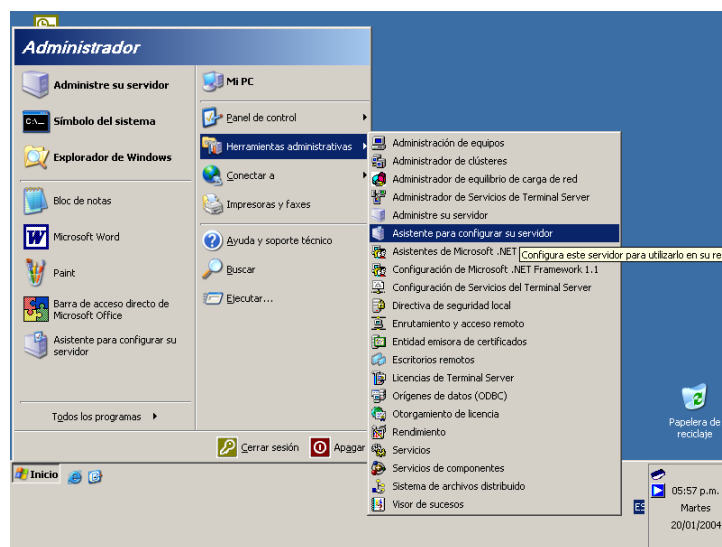


Figura 1.

El Asistente muestra un aviso informativo indicando el propósito de este Asistente, solo se debe dar un clic sobre la opción **Siguiente**; esto se muestra en la Figura 2.

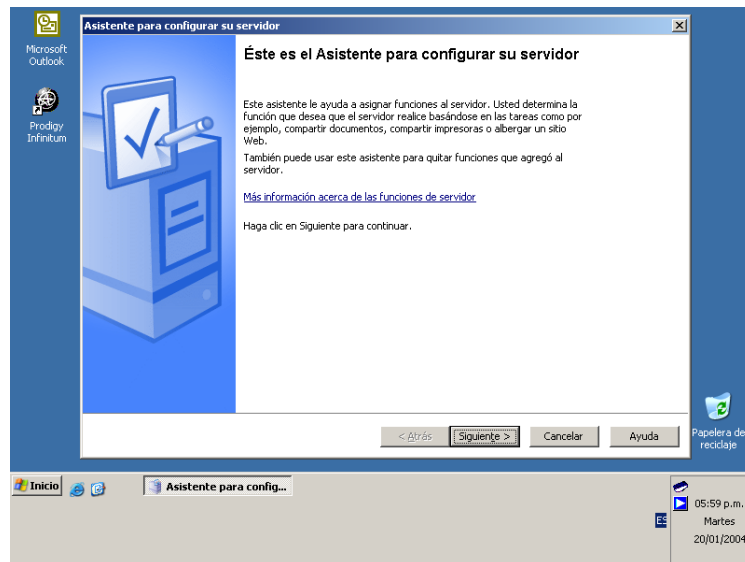


Figura 2.

El Asistente hace un recordatorio sobre los pasos preliminares que deben realizarse para poder continuar con el Asistente, una vez que se ha verificado el cumplimiento de estos pasos se debe dar un clic sobre **Siguiente**, mostrándose esto en la Figura 3.

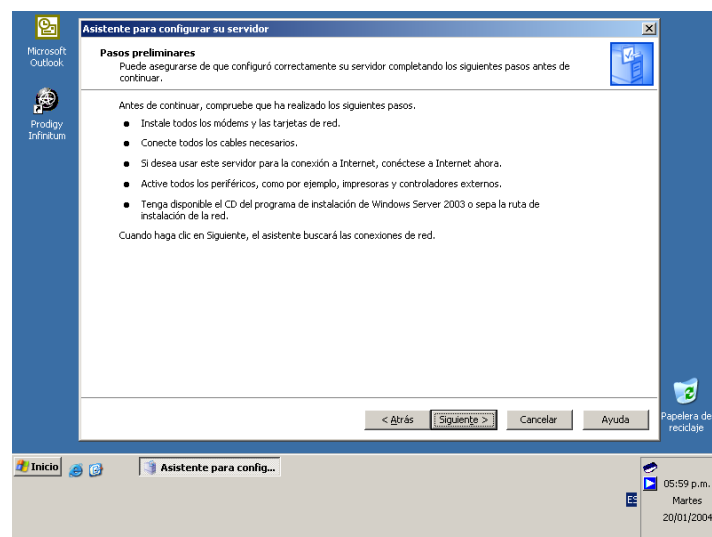


Figura 3.

Ahora el Asistente comienza a detectar las conexiones de red existentes así como su configuración de cada una de ellas, eso se ilustra en la Figura 4.

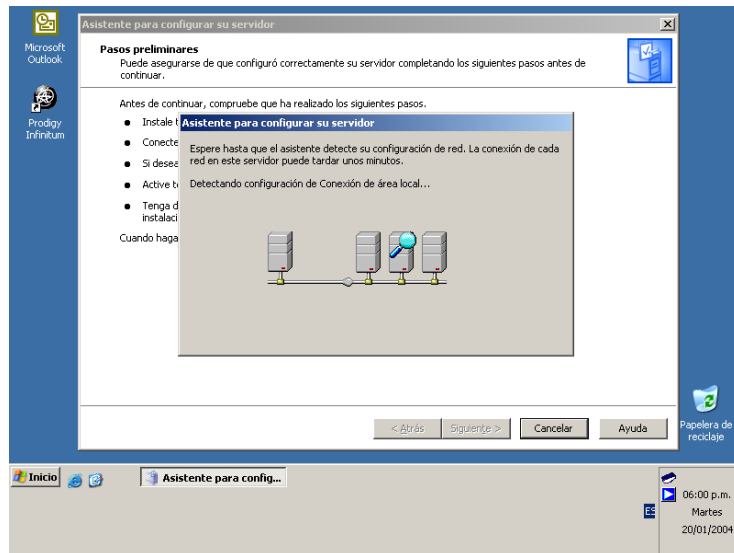


Figura 4.

Al iniciar por primera vez este Asistente, se presenta una pantalla donde se debe indicar el tipo de configuración que se escogerá, es recomendable escoger la opción **configuración personalizada**; una vez seleccionada la opción mas adecuada se debe dar un clic sobre **Siguiente**, esto se muestra en la Figura 5.

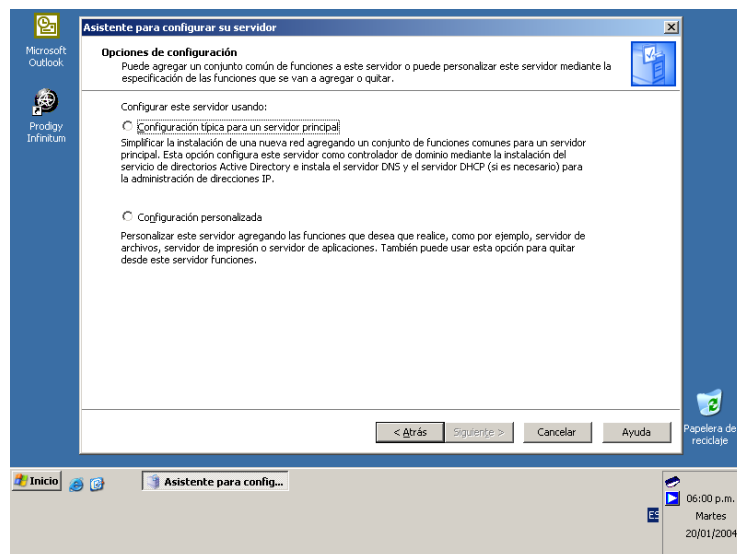


Figura 5.

La siguiente pantalla mostrada por el Asistente indica las posibles funciones que pueden configurarse en un Servidor, en este momento se escoge la opción **Servidor DNS** y se da un clic sobre **Siguiente**, esto se ilustra en la Figura 6.

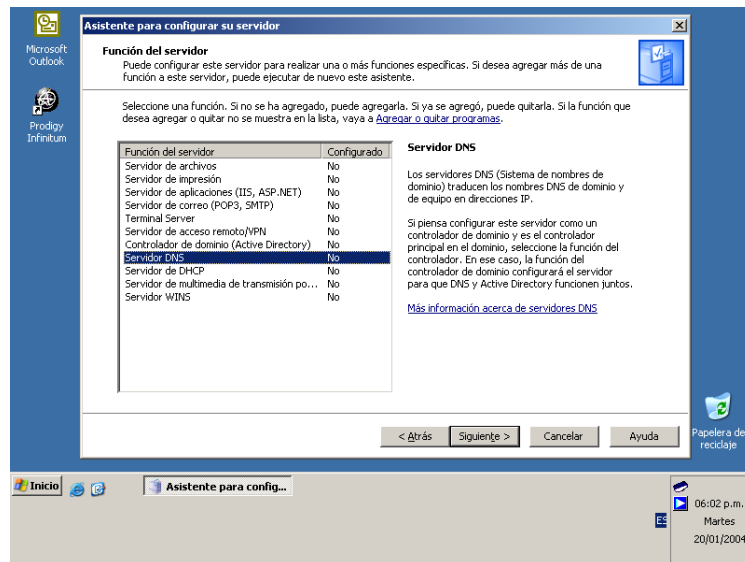


Figura 6.

Ahora el asistente muestra un resumen de las funciones seleccionadas para instalar en el Servidor, se da un clic sobre **Siguiente**, tal como se muestra en la Figura 7.

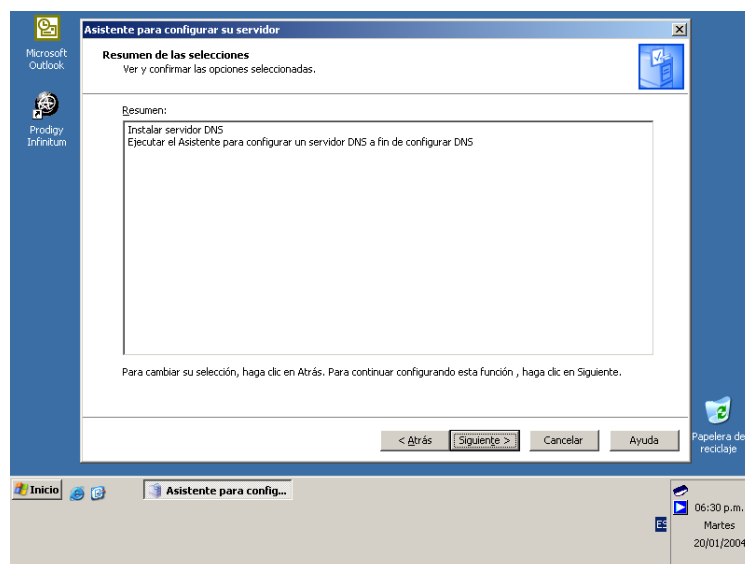


Figura 7.

Ahora se inicia el “Asistente para configurar un servidor DNS”, se da un clic sobre **Siguiente**, esto se muestra en la Figura 8.

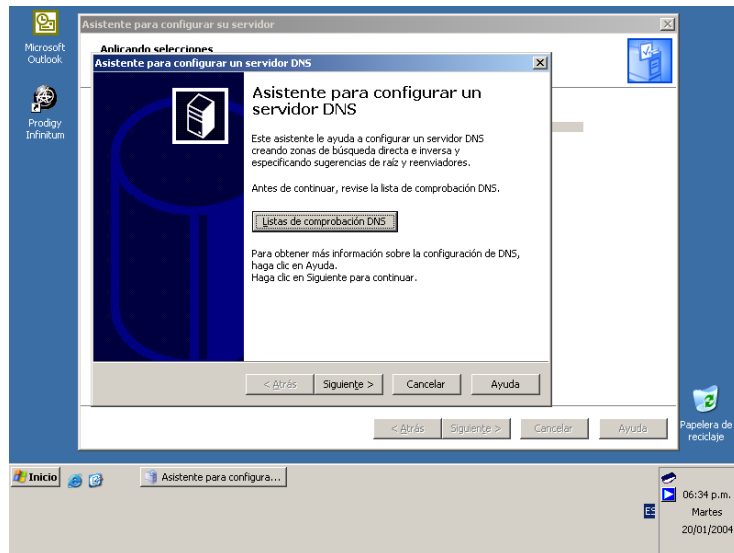


Figura 8.

Ahora el asistente muestra los posibles tipos de zona de búsqueda a crear, se escoge la opción “Crear zonas de búsqueda directa e inversa” y se da un clic sobre **Siguiente**, esto se muestra en la Figura 9.

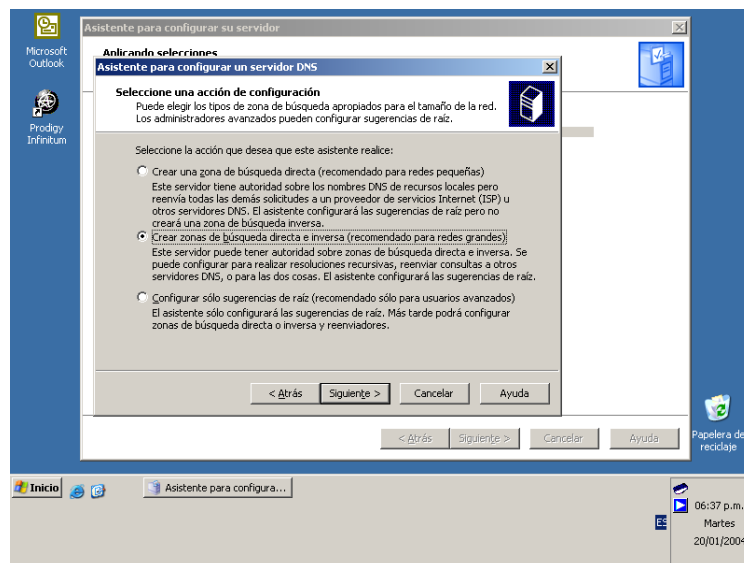


Figura 9.

Como siguiente paso se escogerá la opción que permita crear una zona de búsqueda directa en este momento, tal y como se muestra en la Figura 10.

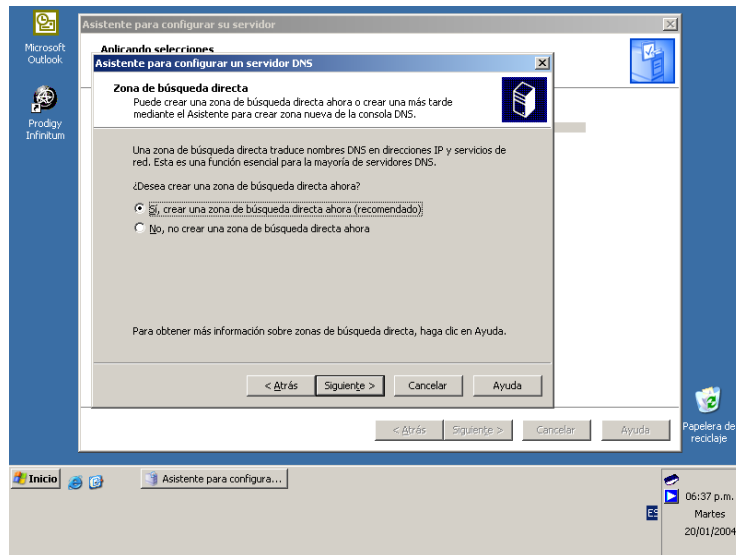


Figura 10.

Ahora se debe indicar al Asistente el tipo de zona a crear y se deberá escoger la opción **zona principal**, como se muestra en la Figura 11.

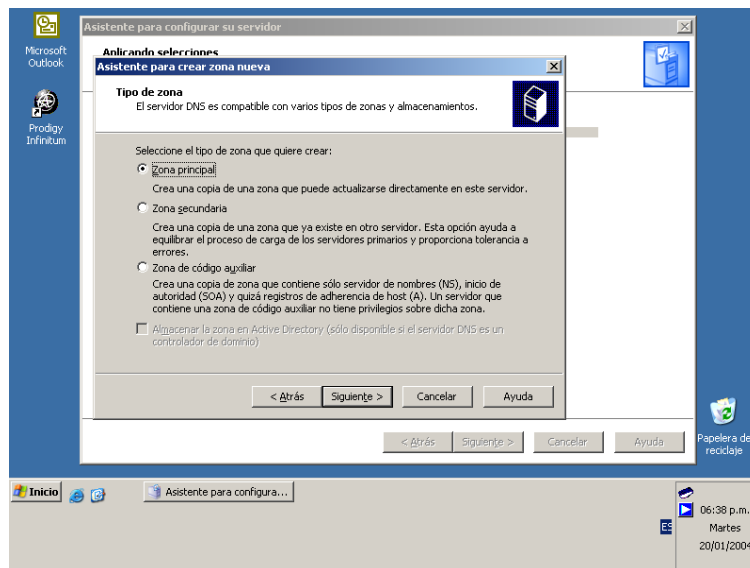


Figura 11.

Ahora se debe de nombrar a esta zona de búsqueda con un nombre DNS, para ilustrar este proceso de instalación se nombra a la zona de búsqueda directa **electrónica.edu**, esto se ilustra en la Figura 12.

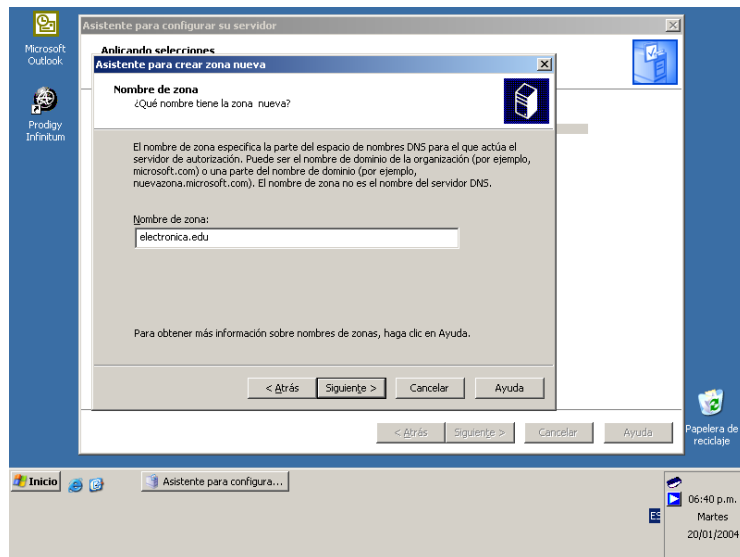


Figura 12.

En este momento se debe crear un archivo de zona y el Asistente por sí mismo sugiere un nombre para este archivo, dependiendo de las necesidades de la red se puede renombrar o simplemente aceptar la sugerencia del Asistente, esto se ilustra en la Figura 13.

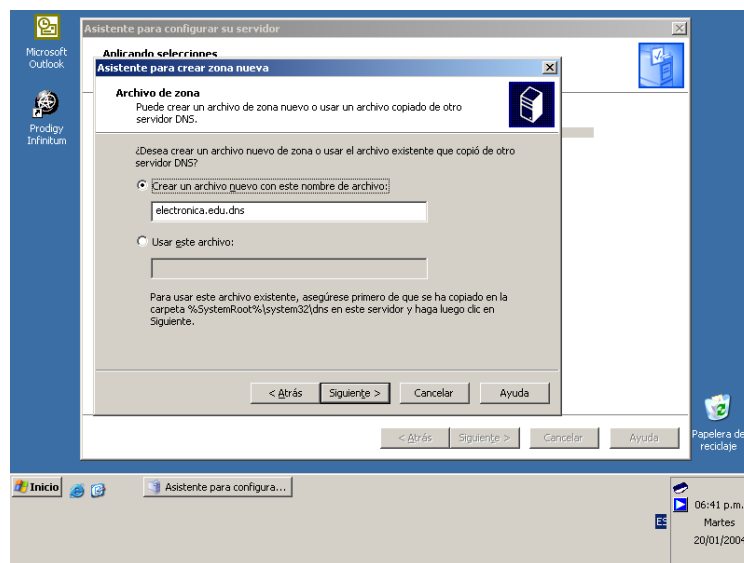


Figura 13.

Como siguiente paso se debe de especificar el tipo de actualización que se empleara en la zona DNS, se escoge la opción que mejor satisfaga las necesidades de la red LAN, tal como se muestra en la Figura 14.

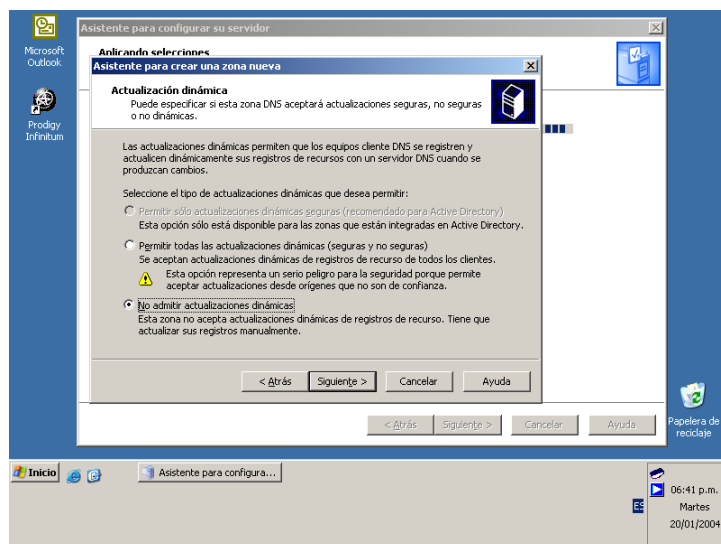


Figura 14.

Ahora el Asistente pregunta si se instalará en este momento una zona de búsqueda inversa o si se prefiere crearla posteriormente, se escoge la opción para crear esta zona en este momento, esto se muestra en la Figura 15.

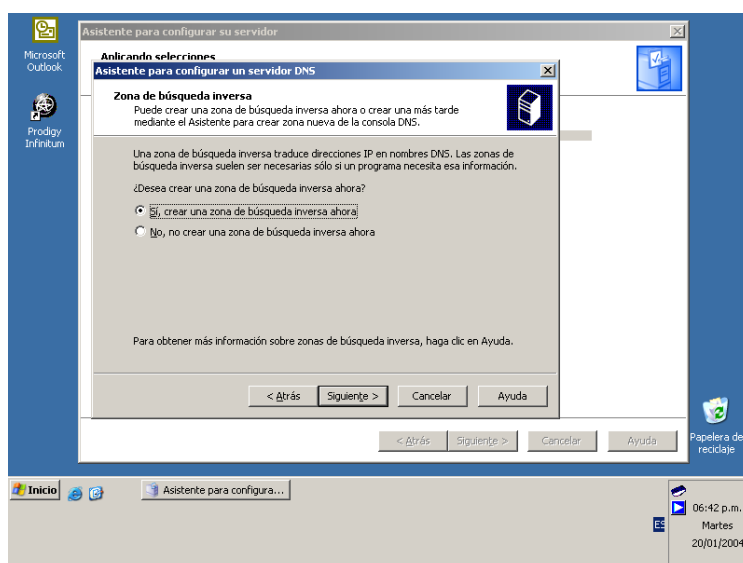


Figura 15.

Ahora se debe indicar al Asistente que tipo de zona será creada, por lo tanto se escoge crear una zona principal; ilustrando esto la Figura 16.

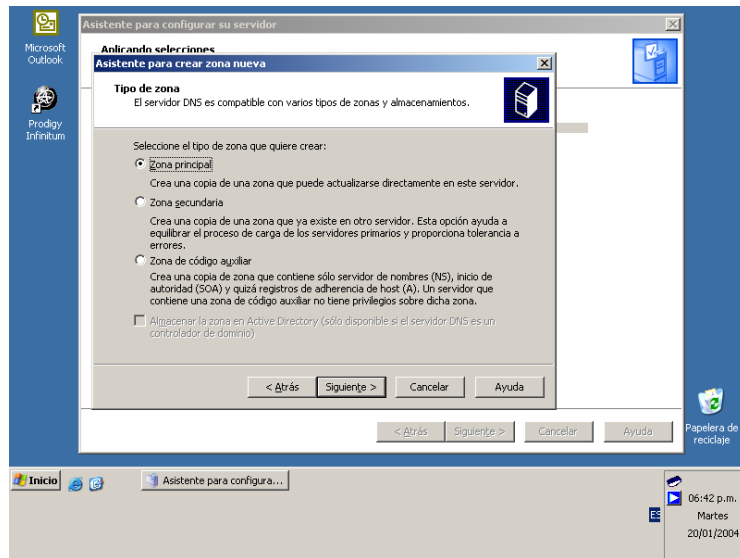


Figura 16.

Ahora se nombrará a la zona de búsqueda inversa. La zona de búsqueda directa resuelve nombres en direcciones IP, por lo tanto una zona de búsqueda inversa resolverá direcciones IP en nombres DNS. Por lo tanto al tratarse de una zona de búsqueda inversa su nombre de ésta zona es una dirección IP y debe de corresponder al ID de la red LAN, tal como se muestra en la Figura 17.

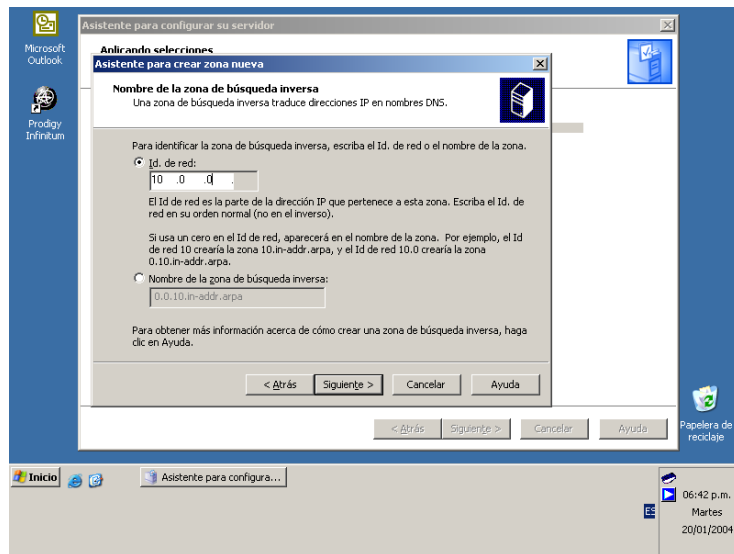


Figura 17.

Al igual que en una zona de búsqueda directa se debe crear un archivo de zona para la zona de búsqueda inversa y nuevamente el Asistente sugiere un nombre para éste archivo de zona, esto se muestra en la Figura 18.

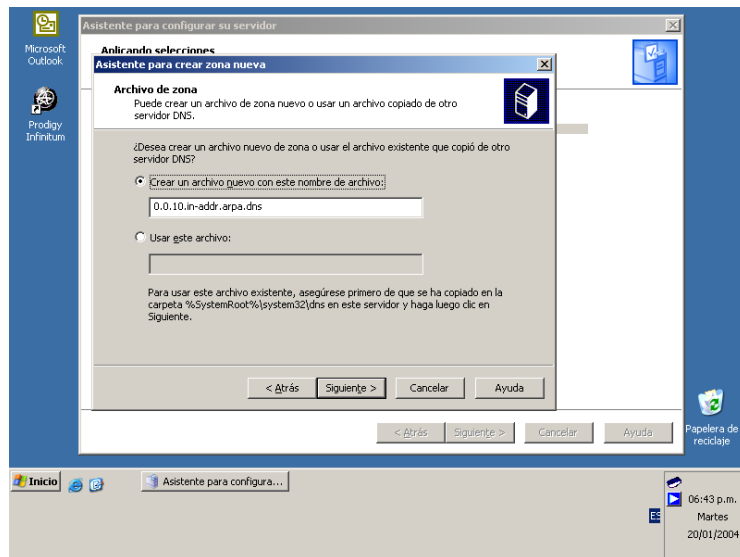


Figura 18.

Ahora es necesario definir el tipo de actualización que se utilizará en esta zona se escoge la mejor opción tal como se muestra en la Figura 19.

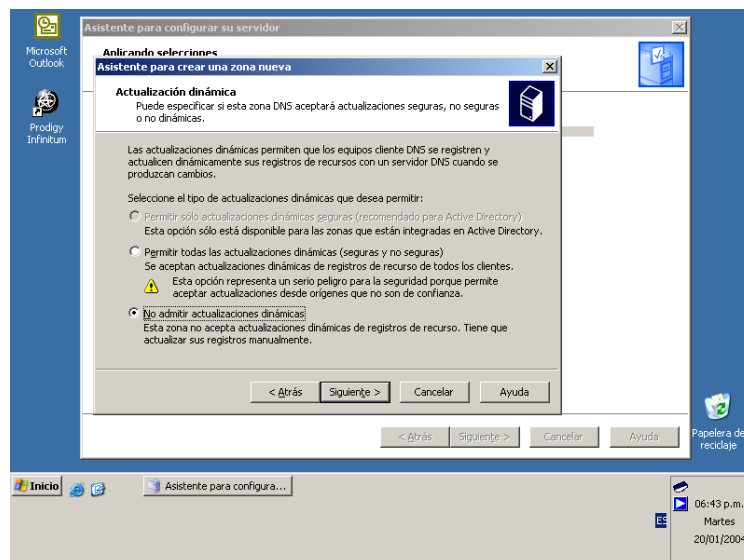


Figura 19.

El objetivo de un servidor DNS es resolver nombres en direcciones IP y viceversa; pero cuando el servidor DNS no puede resolver la petición de un usuario, el servidor DNS puede reenviar esta petición a otro servidor DNS configurado para resolver esta petición. Por lo tanto se puede configurar al servidor DNS para que utilice el servicio de reenviadores. En este caso no se utilizará este servicio. Ver Figura 20.

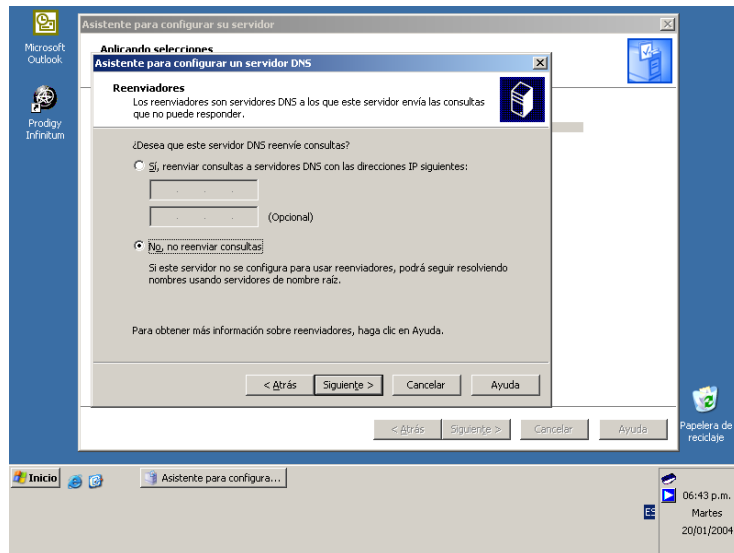


Figura 20.

El Asistente muestra a continuación una pantalla donde se resume la configuración escogida para el servidor DNS. Ver Figura 21.

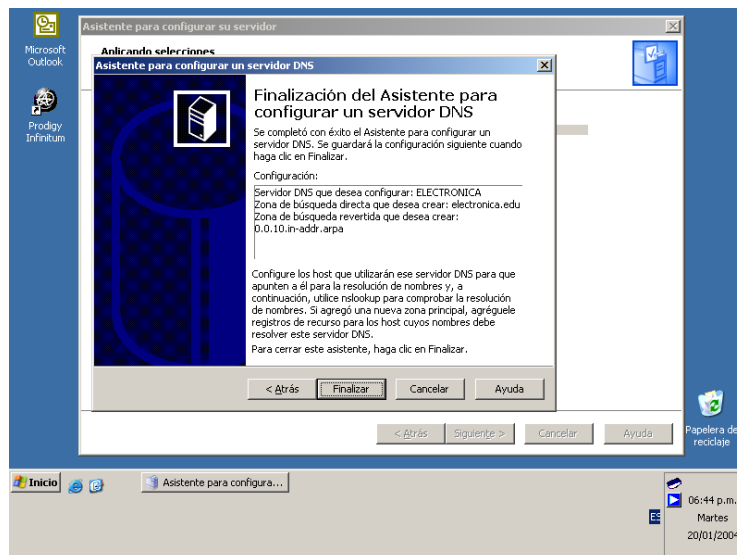


Figura 21.

El Asistente muestra a continuación un aviso informativo indicando que se ha configurado el servidor como un servidor DNS, tal como se muestra en la Figura 22.

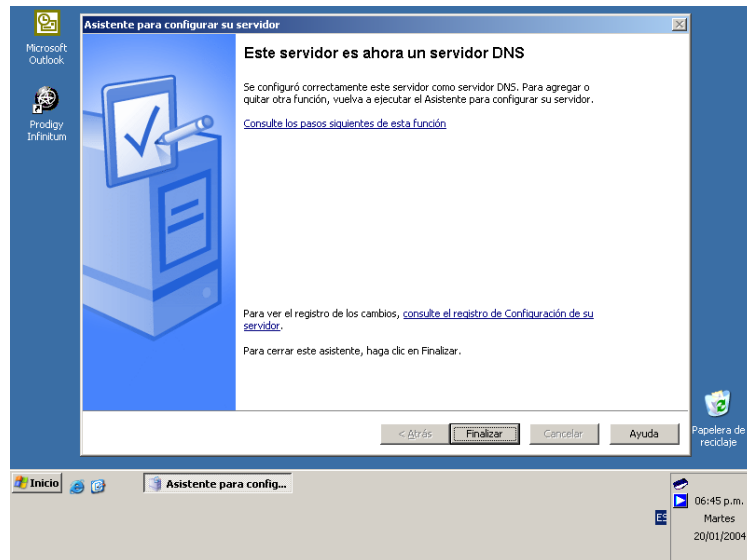


Figura 22.

Una vez finalizada la instalación del Servidor DNS se abre la consola del servidor DNS con la siguiente ruta **Inicio\Herramientas administrativas\DNS**, entonces aparecerá la consola mostrada en la Figura 23.

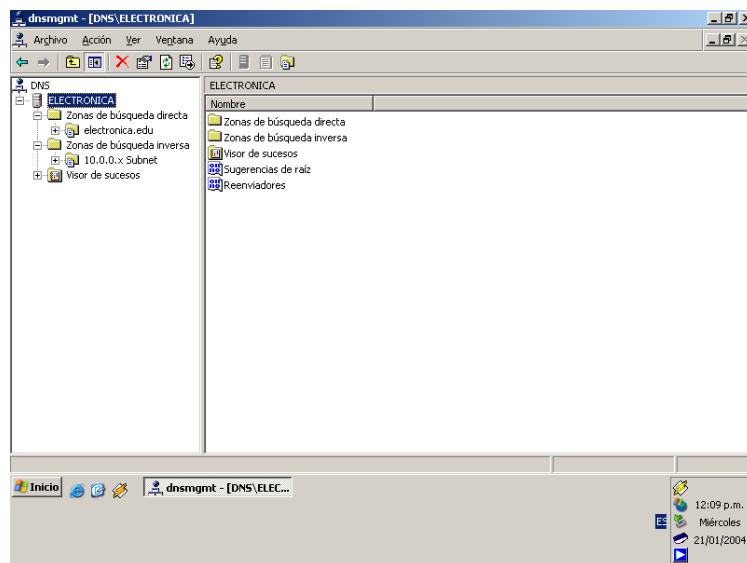


Figura 23.

Una vez iniciada la consola del servidor DNS se verifica que las zonas de búsqueda directa e inversa estén activas; esto se muestra en las Figuras 24 y 25.

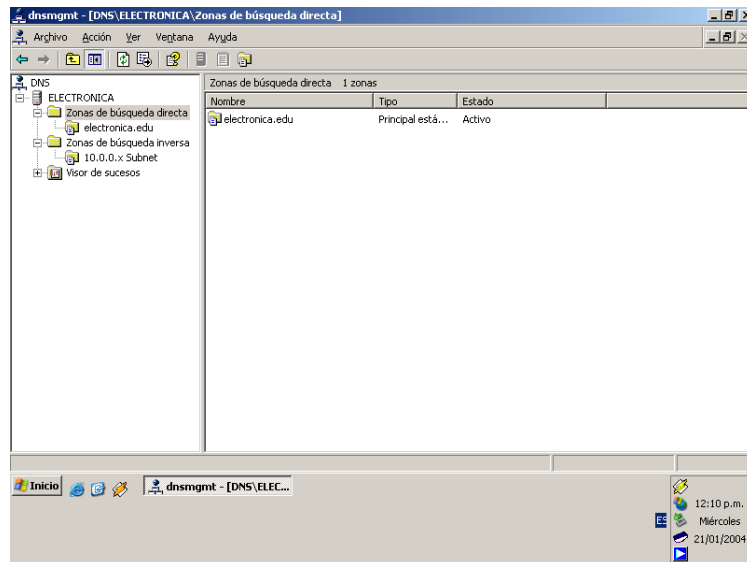


Figura 24.

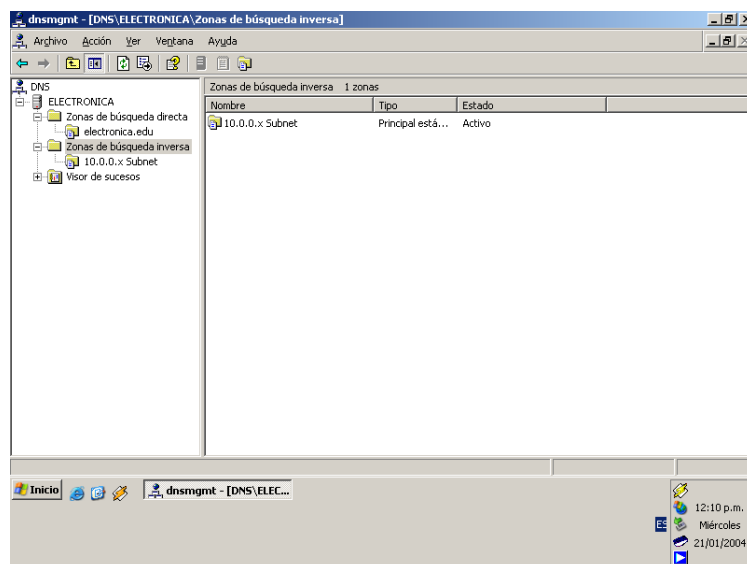


Figura 25.

Por último se procede a verificar que este servidor DNS está autorizado para utilizar el nombre DNS de dominio que se utilizará para nombrar al primer dominio del Directorio Activo. Para verificar esto se debe abrir una ventana de símbolo del sistema y se debe escribir el siguiente comando sobre el *prompt* del directorio raíz, **nslookup**. Esto se ilustra en la Figura 26.

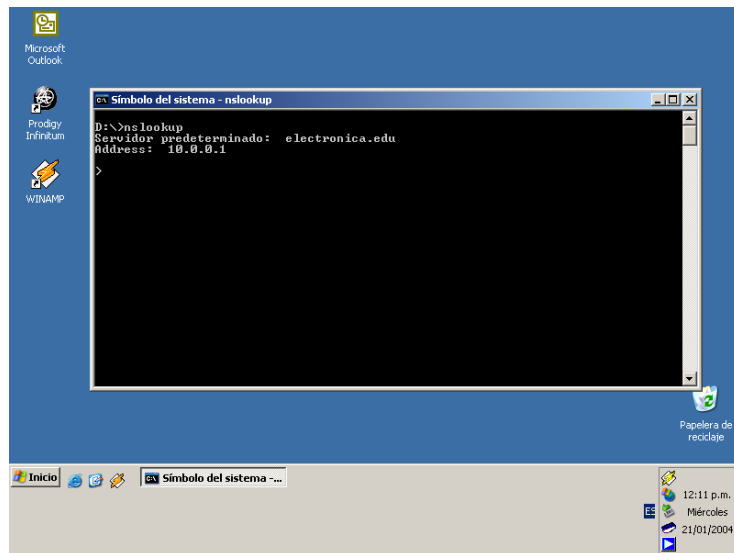


Figura 26.

Instalación y configuración del servidor DHCP.

Un servidor DHCP es un servidor que asigna direcciones IP a las computadoras clientes cada vez que éstas lo solicitan. Una computadora que forma parte de una red LAN pregunta por su dirección IP al momento de iniciar con la carga de su sistema operativo. Por lo que resulta evidente la importancia de instalar y configurar un servidor DHCP. Como primer paso se debe iniciar de nuevo el “Asistente para configurar su servidor”, y de esta forma asignar la función de servidor DHCP; como se muestra en la Figura 27.

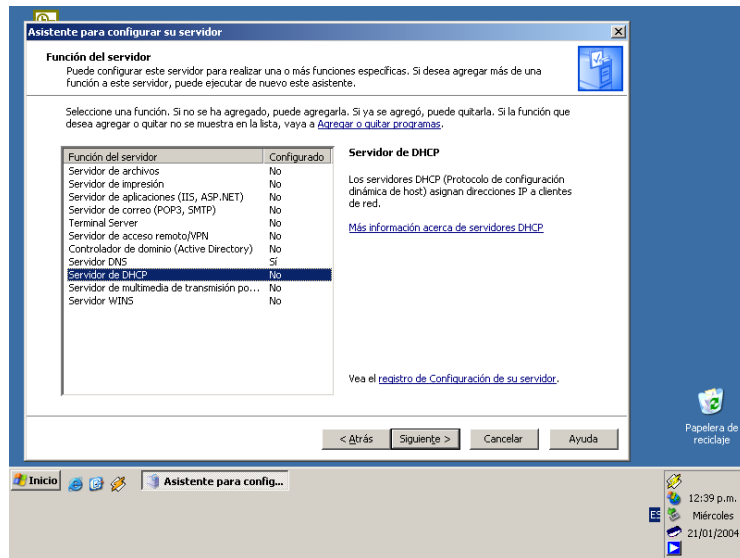


Figura 27.

Posteriormente se inicia el Asistente para ámbito nuevo, como se muestra en la Figura 28.

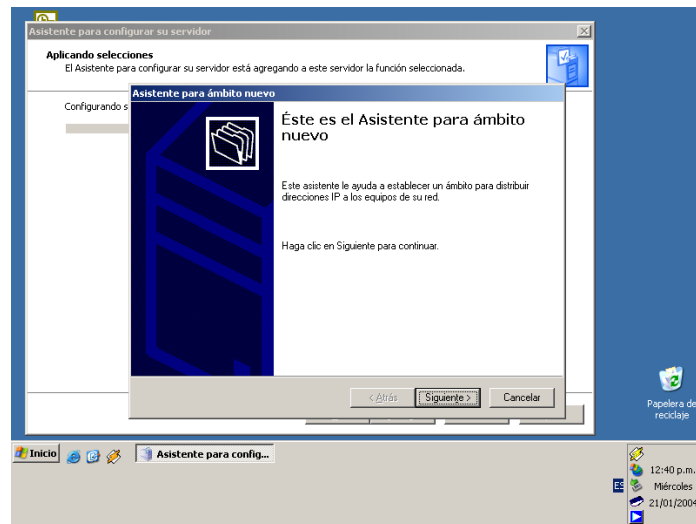


Figura 28.

Ahora se debe de nombrar el nuevo ámbito, así como una descripción del mismo. Ver Figura 29.

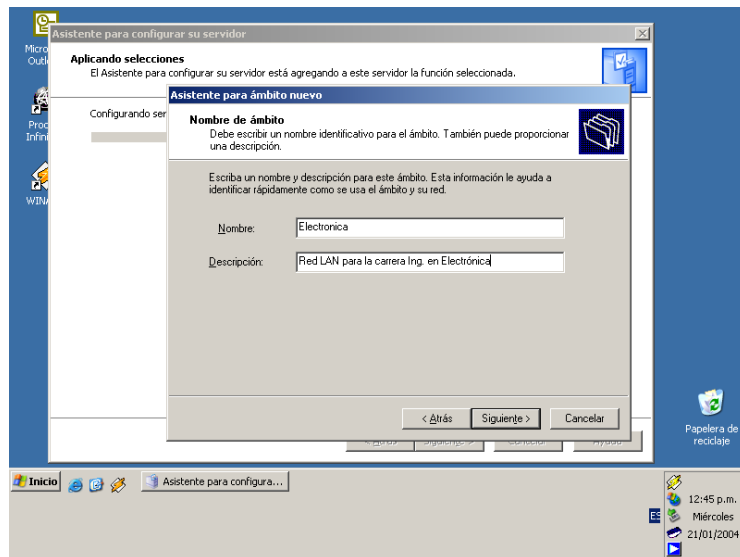


Figura 29.

Posteriormente se define el intervalo de dirección IP a utilizar en el ámbito DHCP, esto es se define un grupo de direcciones IP que serán válidas y podrán ser asignadas a cualquier cliente que lo solicite. Ver Figura 30.

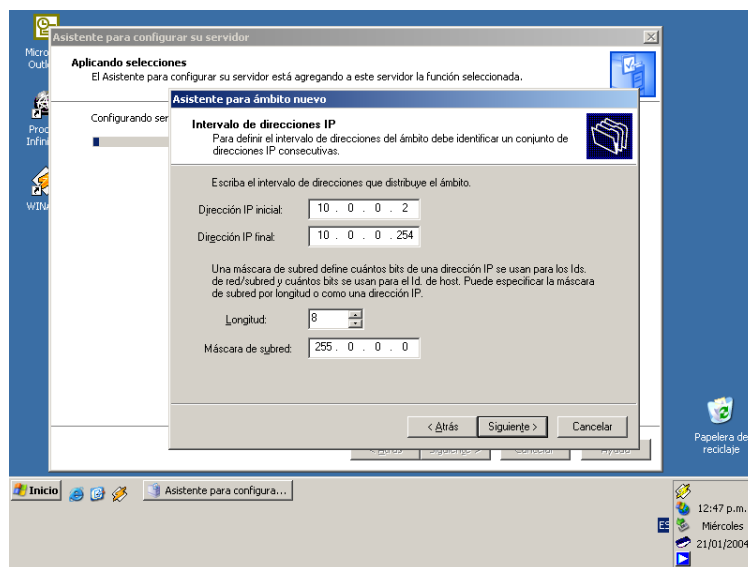


Figura 30.

El servidor DHCP ofrece una opción que permite excluir direcciones IP del ámbito DHCP, esto es, las direcciones IP que estén restringidas no podrán ser asignadas a ningún cliente. Ver Figura 31.

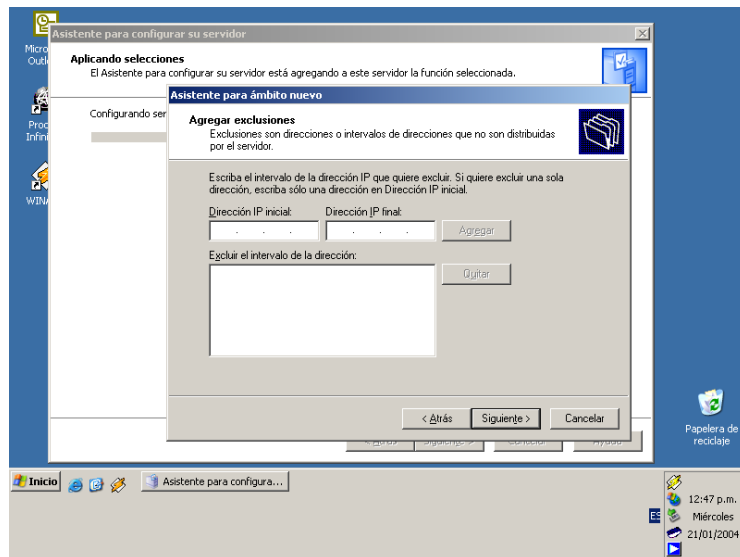


Figura 31.

Otra opción que ofrece el servidor DHCP es poder definir el tiempo que un cliente puede utilizar una dirección IP del ámbito, como se muestra en la figura 32.

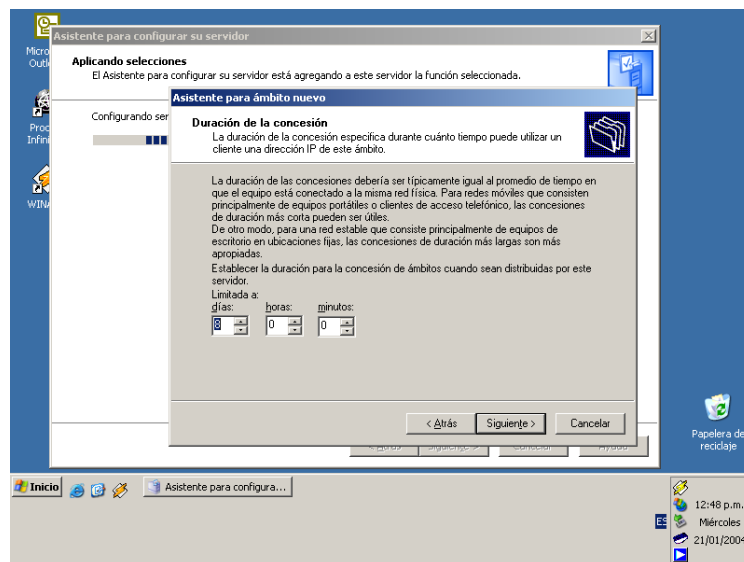


Figura 32.

El Asistente indica la posibilidad de configurar en este momento o más tarde las opciones adicionales del servidor DHCP, por lo tanto se escoge la opción para configurar las opciones en este momento, como se puede ver en la Figura 33.

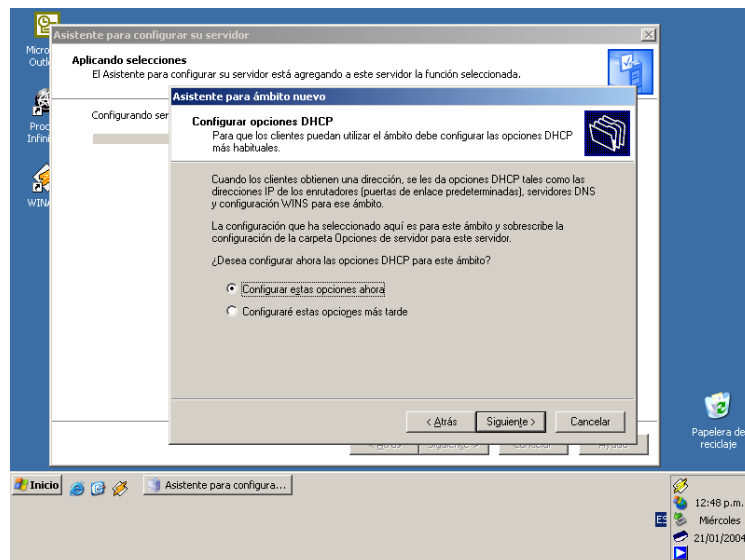


Figura 33.

Una opción adicional que presenta el servidor DHCP es la de configurar un *router* o *gateway* por lo que si se cuenta con uno de estos dispositivos se debe de definir su dirección IP en este campo del Asistente. Ver Figura 34.

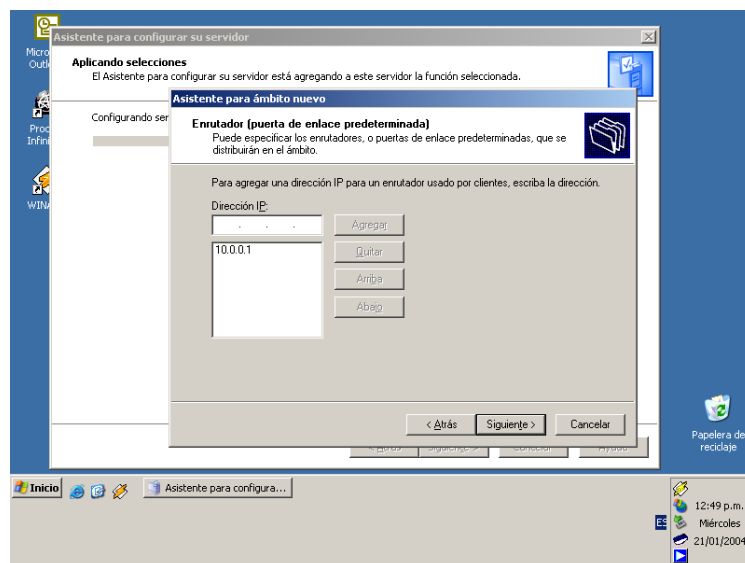


Figura 34.

Como siguiente paso se debe indicar al Asistente el nombre del dominio principal al cual se desee que los clientes envíen sus peticiones de resolución de nombres DNS así como la dirección IP del servidor, esto se muestra en la Figura 35.

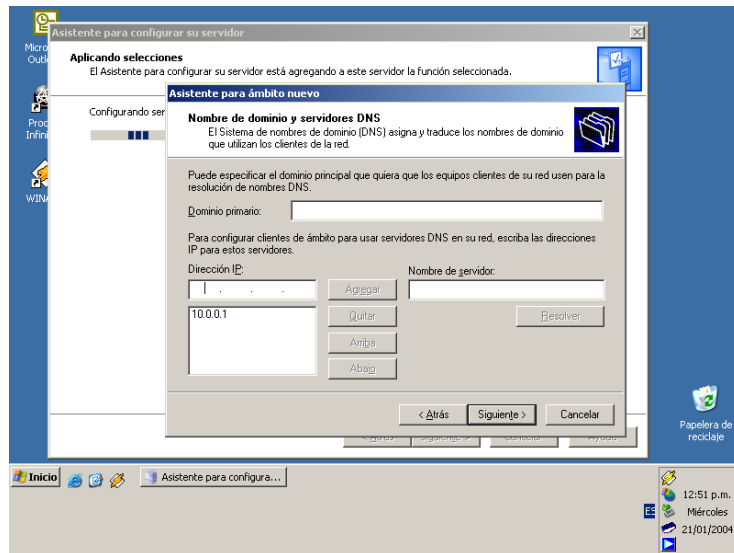


Figura 35.

Como siguiente paso se debe indicar el nombre y dirección IP del servidor WINS, el cual resolverá direcciones IP en nombres NetBIOS. Ver Figura 36.

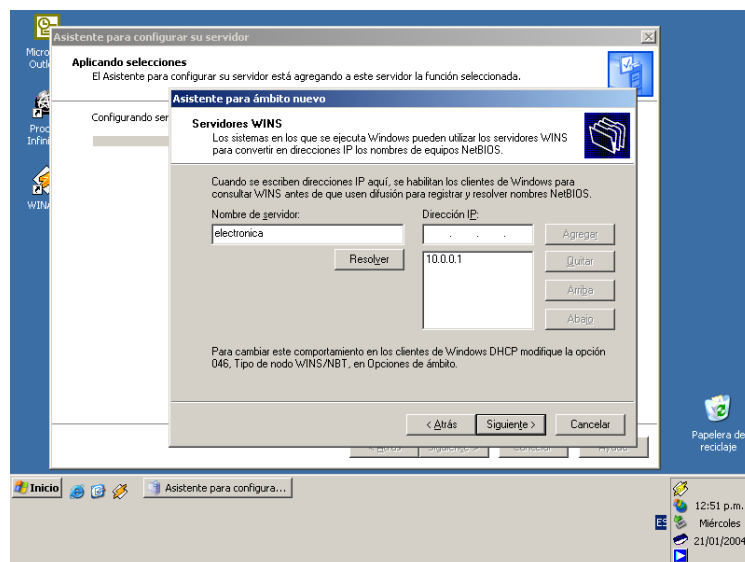


Figura 36.

Posteriormente el Asistente indica si se desea activar en este momento el ámbito o si se desea activar después. Ver Figura 37.

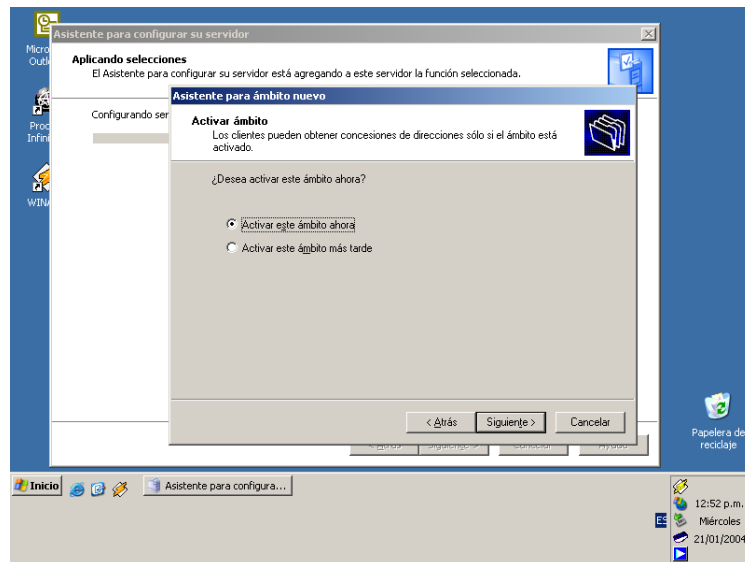


Figura 37.

El Asistente indica que se ha completado el proceso de instalación del servidor DHCP como se ve en la Figura 38.

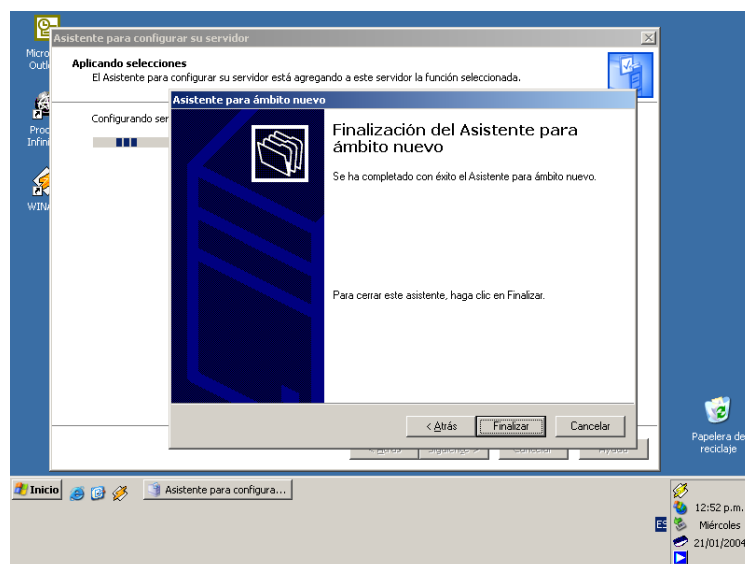


Figura 38.

La siguiente pantalla en aparecer es meramente informativa e indica que el servidor ahora tiene la función de servidor DHCP, como se muestra en la Figura 39.

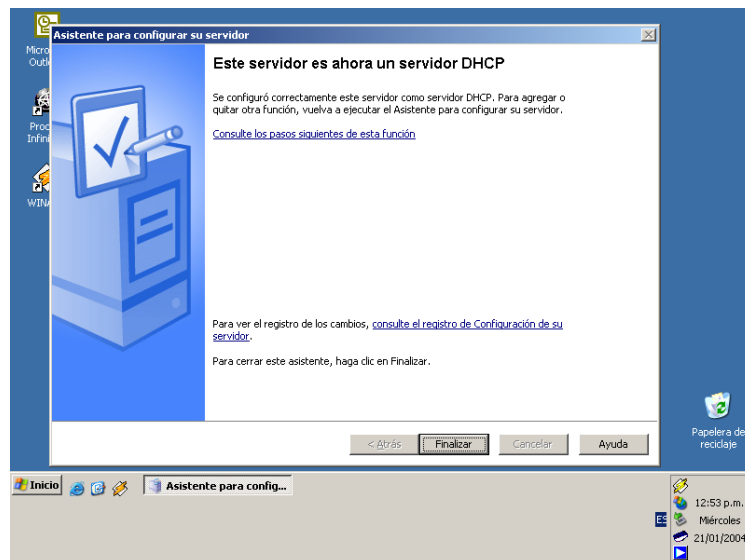


Figura 39.

Por último se inicia la consola del servidor DHCP para verificar que el ámbito está activo, se debe seguir la siguiente ruta para iniciar ésta consola **Inicio\Herramientas administrativas\DHCP**. La consola DHCP se muestra en la Figura 40.

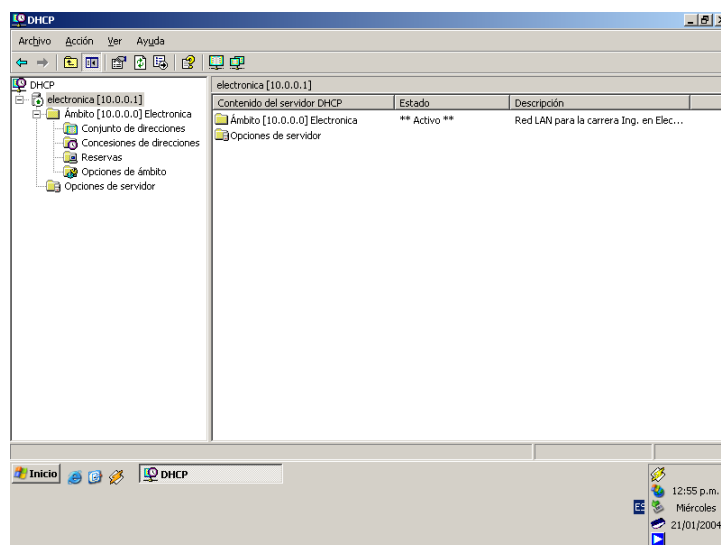


Figura 40.

Configuración de los equipos clientes de la red LAN.

En este momento se ilustrará el proceso para la configuración de los equipos clientes, con la finalidad de que se pueda establecer comunicación entre el servidor y el cliente. Los elementos necesarios para poder configurar al equipo cliente son los dos siguientes:

- 1.-Cliente para redes Microsoft.
- 2.-Protocolo Internet (TCP/IP).

Estos elementos se pueden acceder tal como se muestra a continuación en la Figura 41. En caso de no existir alguno de estos elementos solo bastará dar un clic en **Instalar**, después aparecerá una lista de los elementos posibles a instalar; por lo tanto se escoge el elemento que pueda faltar y se instalara.

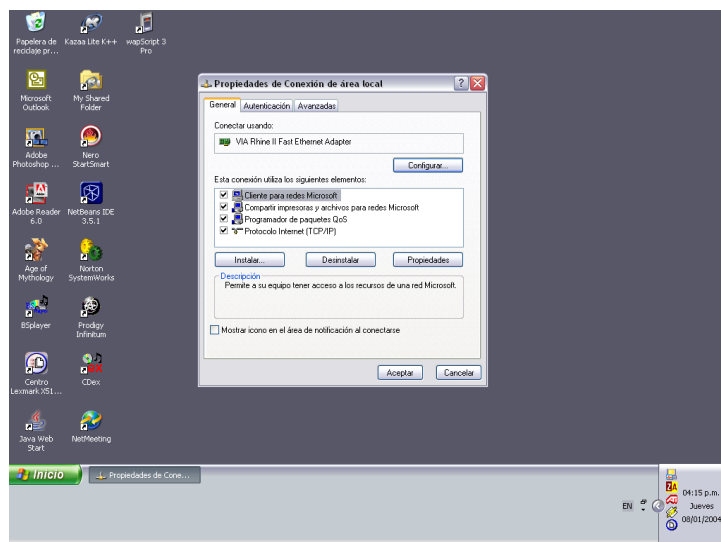


Figura 41.

Después de haber instalado y verificado que se encuentran los elementos anteriormente descritos; se procede a seleccionar el elemento **Protocolo Internet (TCP/IP)** y se dará un clic sobre **Propiedades** y a continuación aparecerá la pantalla mostrada en la Figura 42.

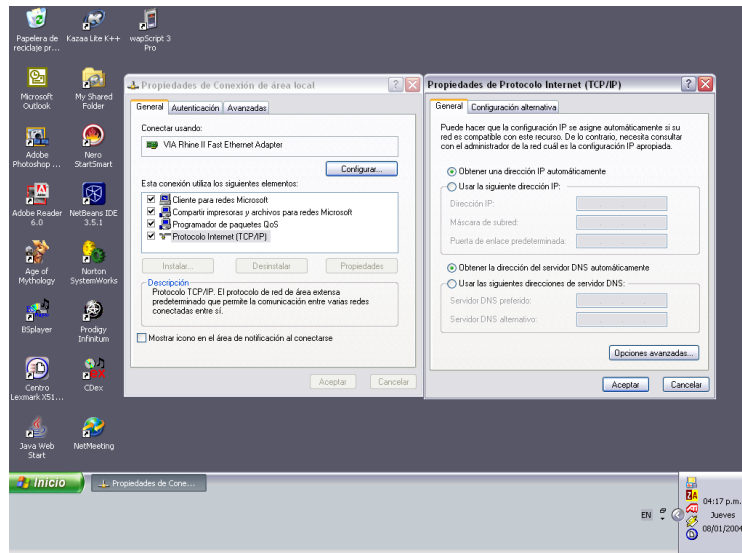


Figura 42.

Como se puede observar en la pestaña **General** aparece un campo que dice **Obtener una dirección IP automáticamente**, éste valor no se debe alterar debido a que el servidor DHCP se encargará de asignar y configurar una dirección IP en el cliente. El siguiente campo es el referente al servidor DNS, en este campo se debe de escoger la opción **Usar las siguientes direcciones de servidor DNS**, posteriormente en el campo **Servidor DNS preferido** se debe de escribir la dirección IP del servidor DNS primario; el siguiente campo, **Servidor DNS alternativo** se modifica sólo cuando existe más de un servidor DNS en la red LAN. Ver Figura 43.

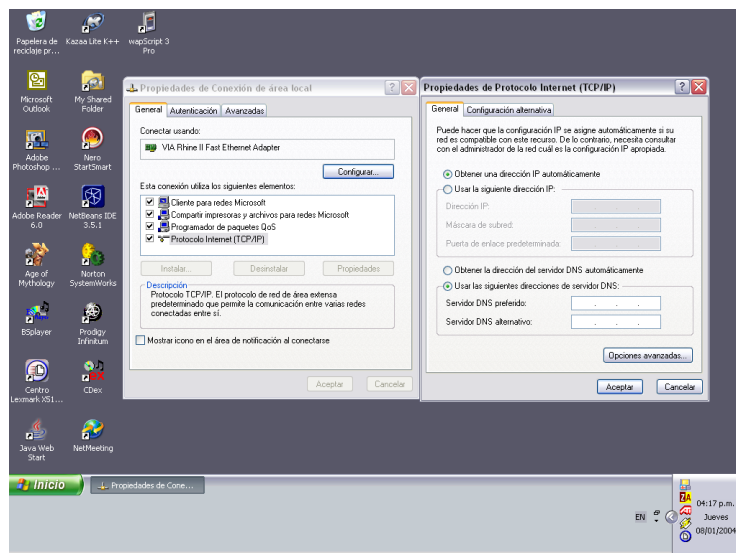


Figura 43.

Instalación del Directorio Activo.

A continuación se describe el proceso de instalación del Directorio Activo en un servidor que corre el sistema operativo Microsoft Windows 2003 Server. Como primer paso se debe iniciar nuevamente el Asistente para configurar su servidor y se escoge la función **Controlador de dominio (Active Directory)**, como se observa en la Figura 44.

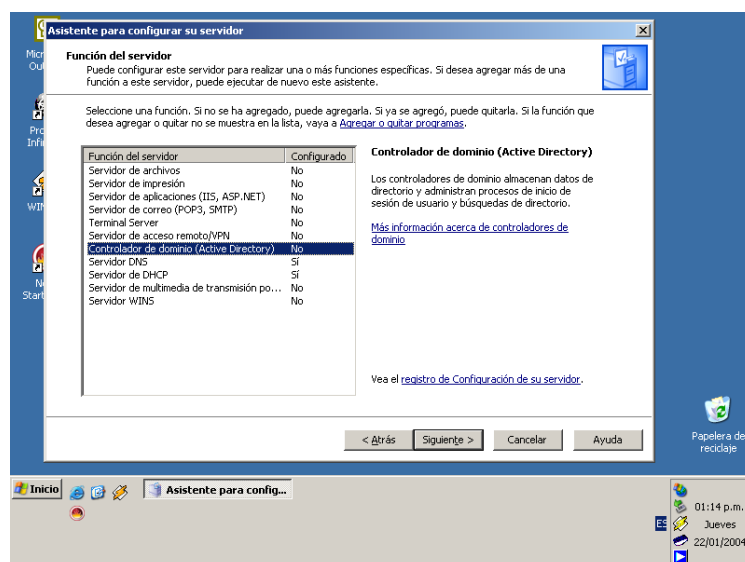


Figura 44.

El asistente muestra un resumen de la función seleccionada. Ver Figura 45.

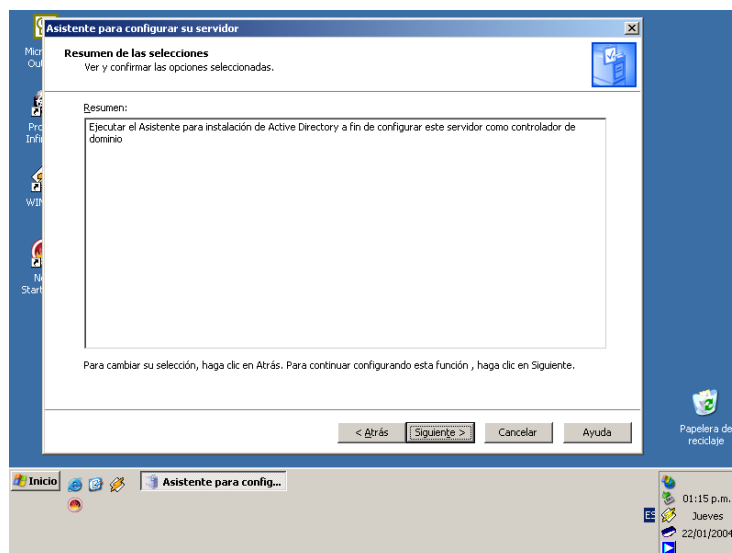


Figura 45.

La siguiente pantalla en aparecer es la correspondiente al **Asistente para instalación de Active Directory**, como se puede observar en la Figura 46.

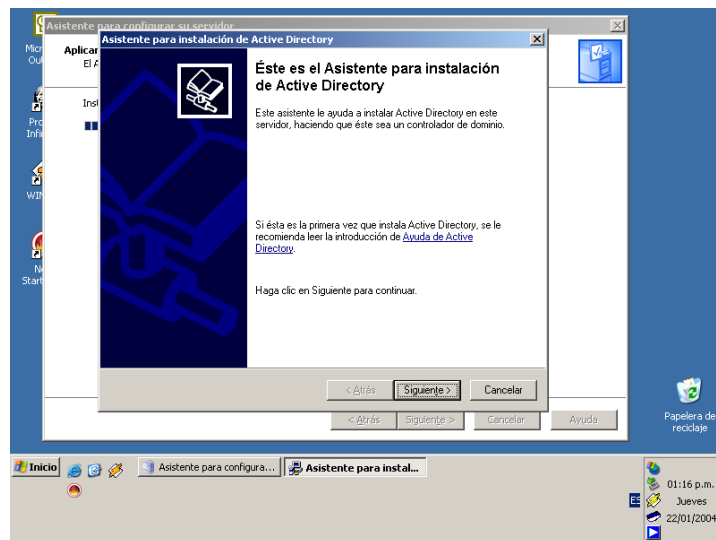


Figura 46.

La siguiente pantalla es informativa e indica que las versiones anteriores del sistema operativo Microsoft Windows, tales como Windows 95 y Windows NT 4.0 SP3 o anteriores, no cumplen con los nuevos requisitos de seguridad y por lo tanto no pueden acceder a los recursos de red ni tampoco pueden iniciar sesión en el controlador de dominio; sin embargo, es recomendado que los clientes con Windows 95, Windows 98 y Windows Millennium Edition ejecuten el Editor de directivas del sistema (Poedit.exe) en el equipo local. Esto garantiza que el archivo Config.pol creado sea compatible con dichos sistemas operativos. A continuación copie el archivo Config.pol resultante en la carpeta SysVol del controlador de dominio. Aunque la directiva de grupo reemplaza en gran parte al Editor de directivas del sistema (Poedit.exe), éste resulta útil en determinadas circunstancias. Ver Figura 47.

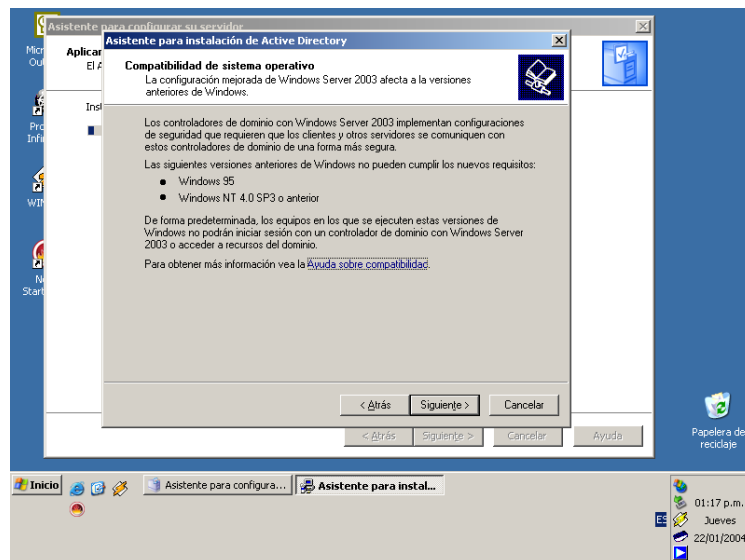


Figura 47.

Cuando se instala por primera vez el Directorio Activo en un servidor, se promueve a este servidor para que cumpla la función de controlador de dominio de forma implícita. Debido a que se está creando un nuevo dominio se debe escoger la opción **Controlador de dominio para un dominio nuevo**, tal como se observa en la figura 48.

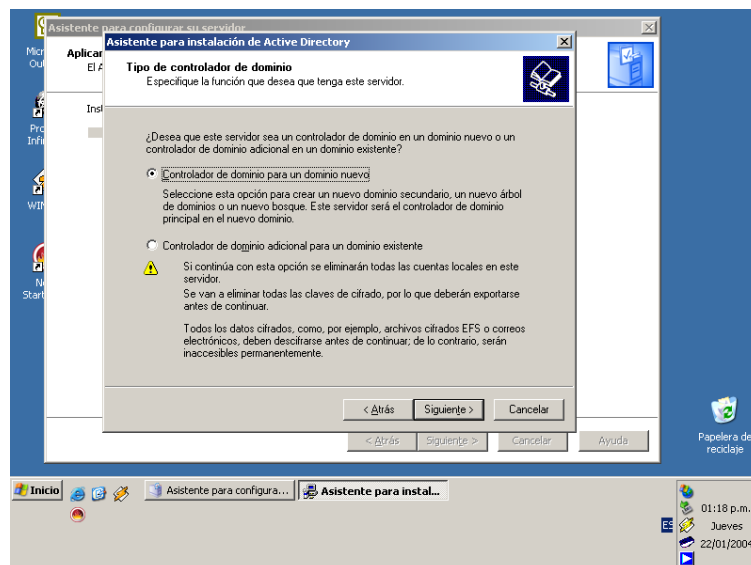


Figura 48.

En este caso también debe crearse un nuevo bosque debido a que en la red LAN no existe un dominio ni un bosque; por lo tanto se debe escoger la opción **Dominio en un nuevo bosque**, tal como se puede observar en la Figura 49.

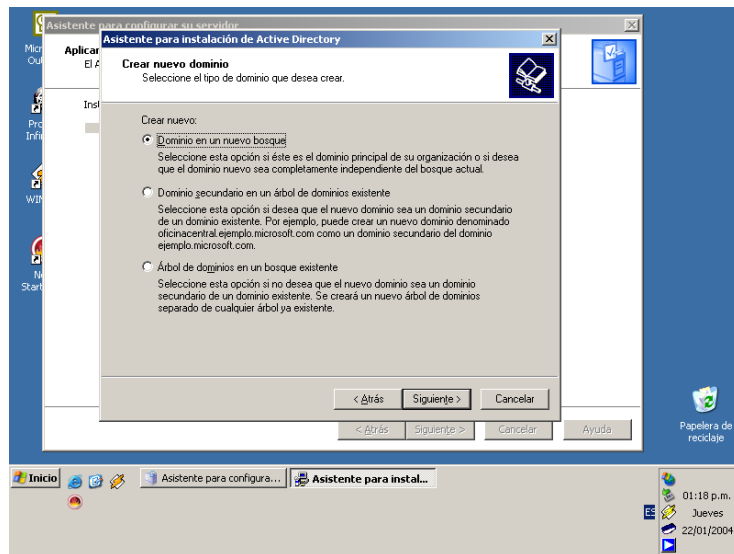


Figura 49.

Ahora se debe nombrar al dominio, con un nombre DNS completo, como se muestra en la Figura 50.

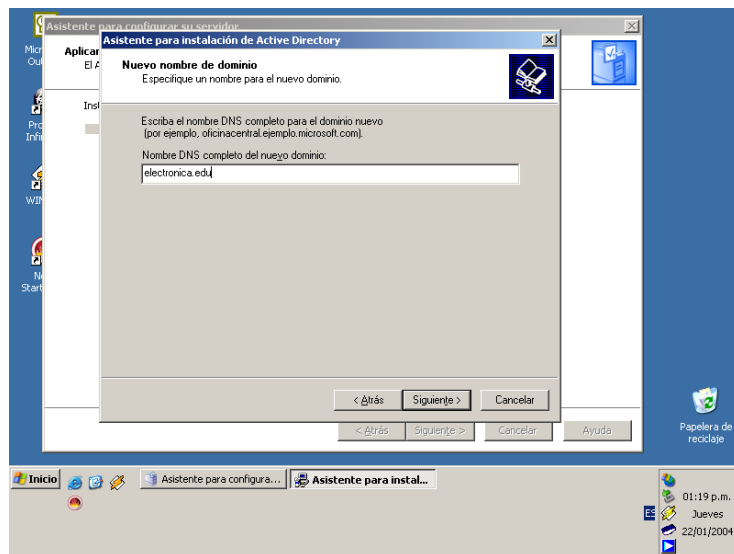


Figura 50.

Una vez que se ha nombrado al dominio con un nombre DNS; también debe nombrarse con un nombre NetBIOS y el Asistente sugiere un nombre. Ver Figura 51.

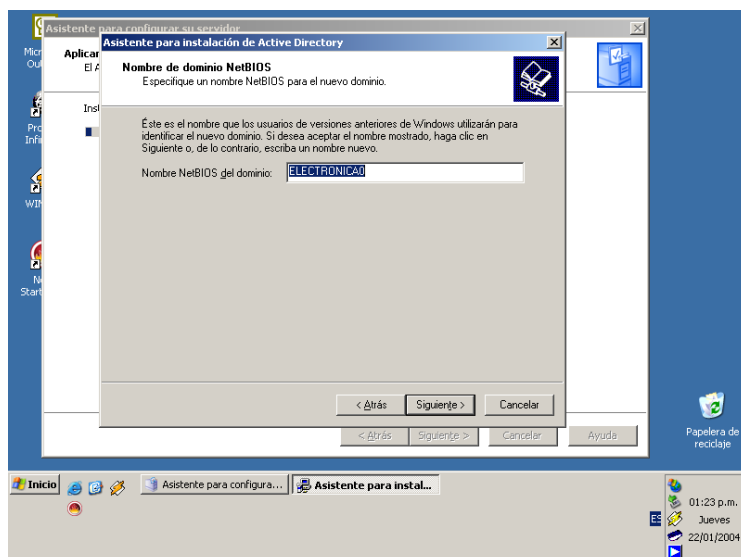


Figura 51.

El siguiente paso es crear carpetas especiales que contienen la base de datos y el registro del Directorio Activo. Para aumentar el rendimiento y la capacidad de recuperación se recomienda almacenar estas dos carpetas en discos duros separados. Ver Figura 52.

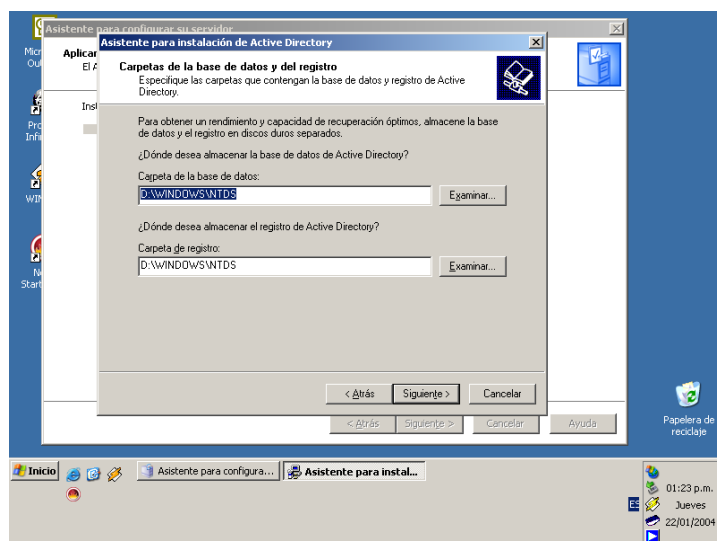


Figura 52.

La siguiente pantalla del Asistente muestra la ubicación en donde se alojará la carpeta **Sysvol**, tal como se observa en la Figura 53.

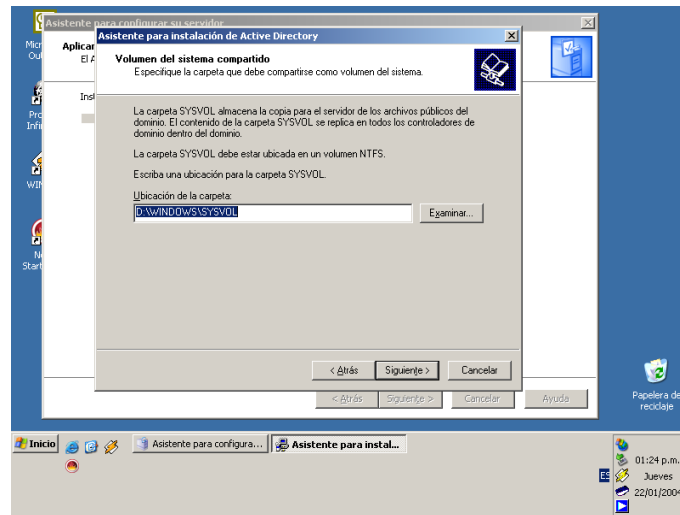


Figura 53.

El Asistente ejecuta automáticamente un diagnóstico del servidor DNS y su compatibilidad con el Directorio Activo. Ver Figura 54.

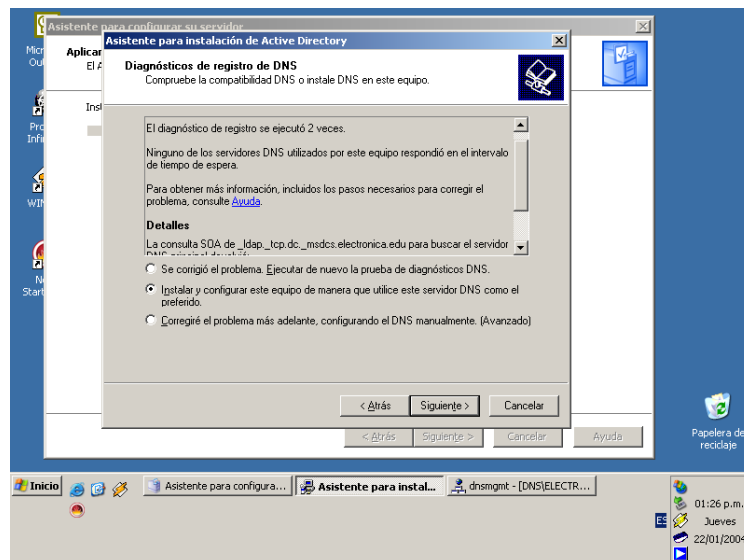


Figura 54.

Si en la red LAN existen otros servidores que corren sistemas operativos anteriores a Windows 2000 o Windows NT, se les debe de permitir leer información almacenada en los controladores de dominio para poder ejecutar ciertos programas de servidor; de no ser así solo

se permitirá la compatibilidad con servidores basados en Windows 2000 y Windows 2003. Esto se puede observar en la Figura 55.

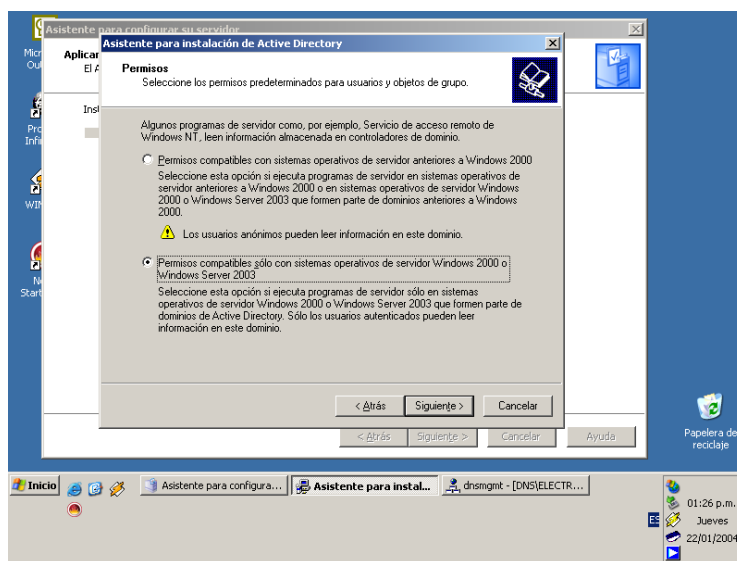


Figura 55.

A continuación se debe definir una contraseña de administrador del modo de restauración de directorio; no olvidar que se deben cumplir con los requerimientos mínimos establecidos por Windows Server 2003 para una contraseña. Figura 56.

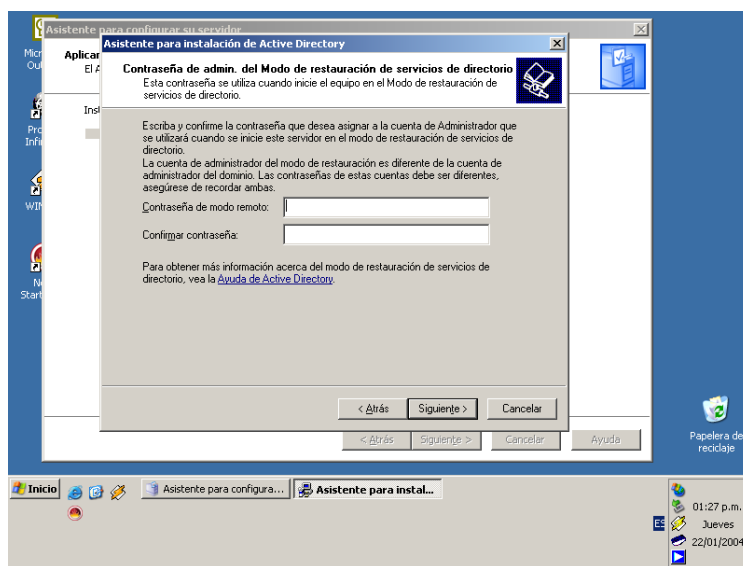


Figura 56.

El Asistente presenta un resumen de las opciones seleccionadas. Ver Figura 57.

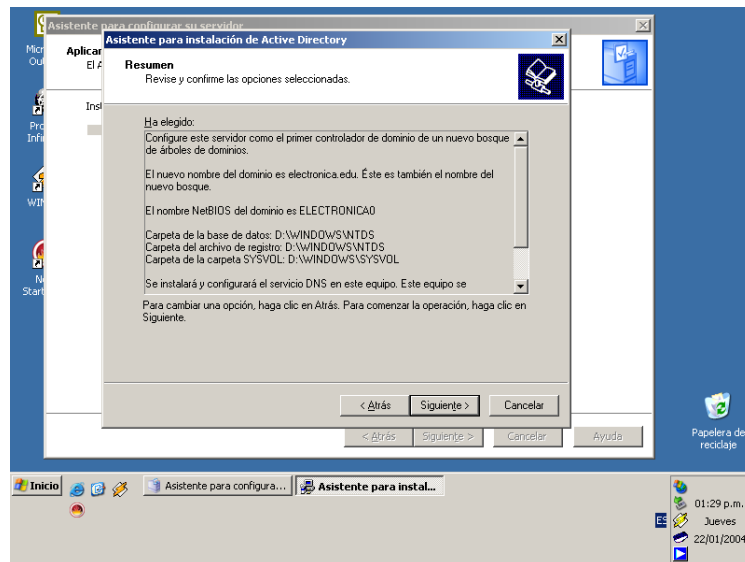


Figura 57.

Una vez que se han verificado las opciones seleccionadas en el resumen presentado por el Asistente; éste comienza a configurar el Directorio Activo en el servidor. Ver Figura 58.

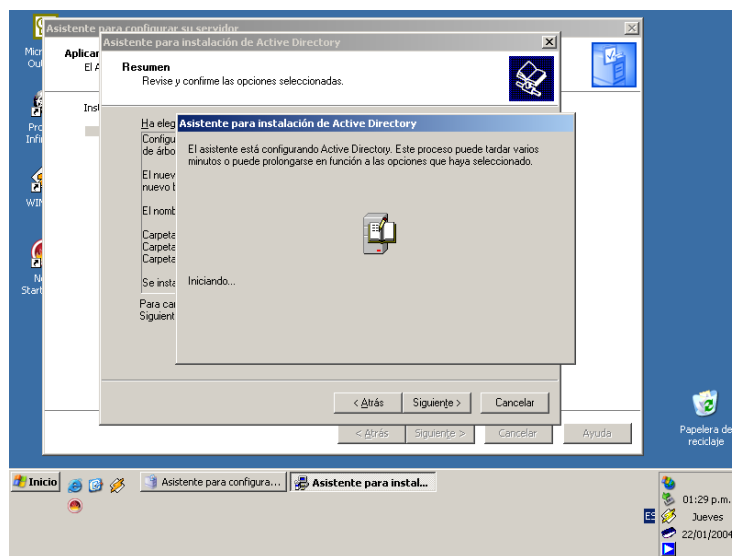


Figura 58.

El Asistente muestra un aviso donde indica se ha instalado el Directorio Activo en el servidor. Ver Figura 59.

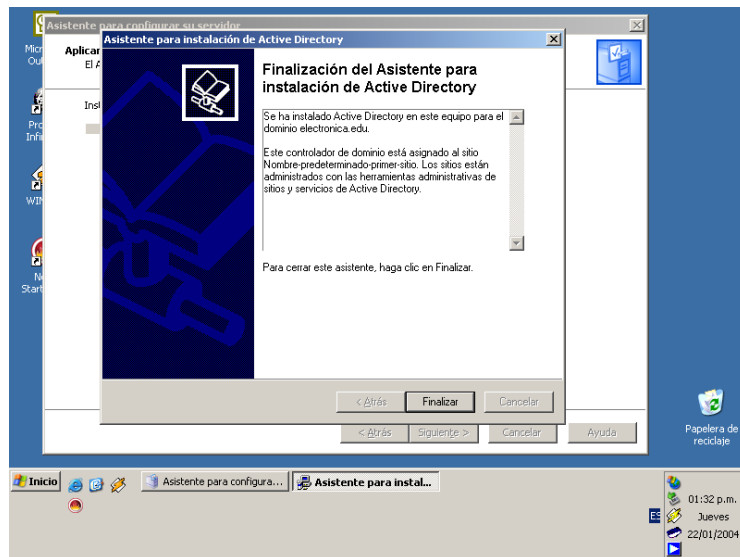


Figura 59.

Una vez finalizado el Asistente para la instalación del Directorio Activo, aparece un mensaje donde indica que los cambios realizados por el Asistente para instalación del Directorio Activo debe reiniciarse el equipo como se observa en la Figura 60.

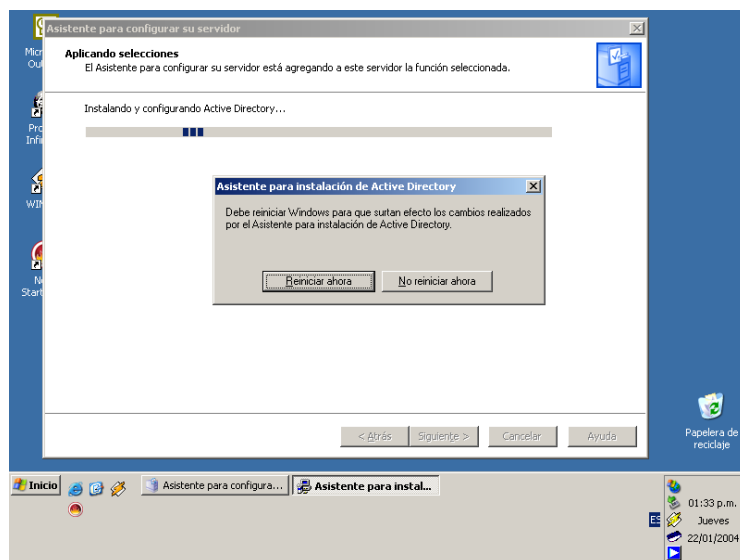


Figura 60.

Después de haber reiniciado el servidor el **Asistente para configurar su servidor** presenta un mensaje informativo en donde indica que el servidor ya es un controlador de dominio. Ver Figura 61.

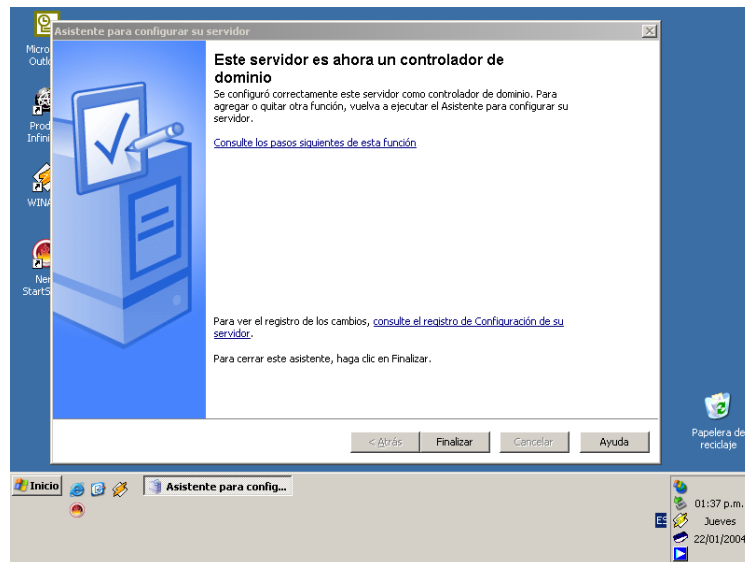


Figura 61.

Creación de objetos en el Directorio Activo.

Como primer paso se debe iniciar la consola **Usuarios y equipos de Active Directory**. Que tiene la siguiente ruta **Inicio\herramientas administrativas\Usuarios y equipos de Active Directory**; tal como se muestra en la Figura 62.

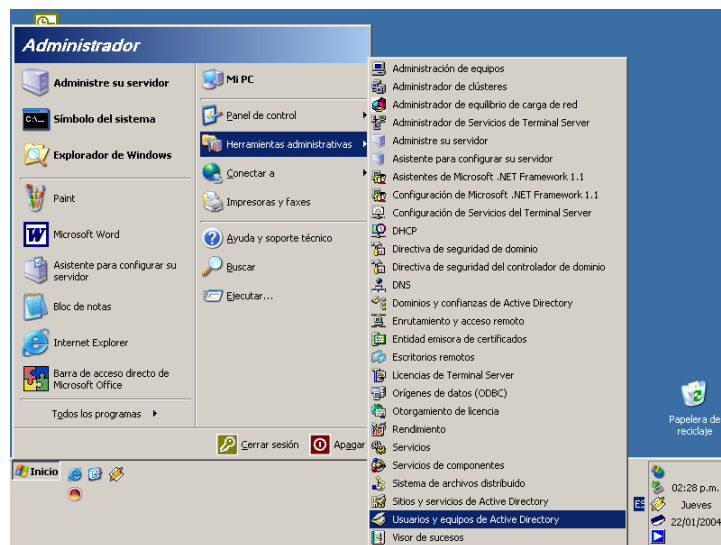


Figura 62.

La consola tiene el aspecto mostrado en la Figura 63.

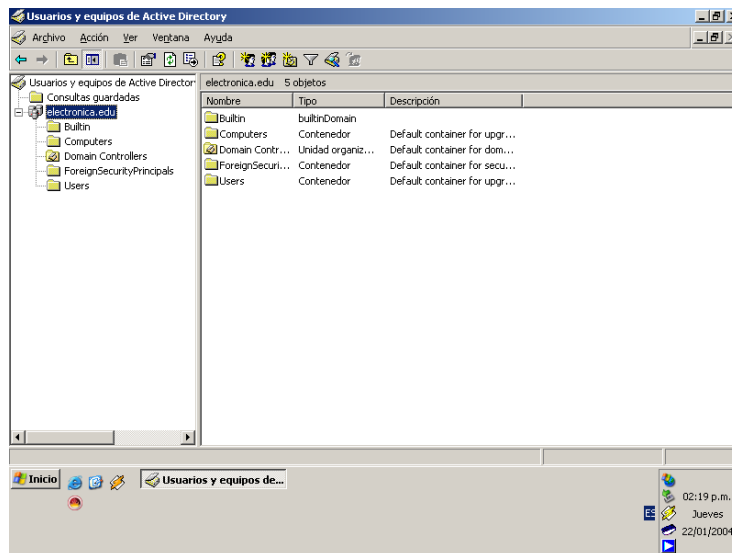


Figura 63.

Como puede observarse aparecen 5 carpetas que pertenecen dominio raíz. Éstas carpetas son creadas por *default* durante la instalación del Directorio Activo. Estas son las carpetas creadas por el Asistente:

- 1.-Builtin: Es un objeto contenedor. Es utilizado para almacenar los grupos de seguridad integrados creados por *default*.
- 2.-Computadoras: Es un objeto contenedor. Este objeto es la locación por *default* para las cuentas de computadoras.
- 3.-Controladores de dominio: Es una unidad organizativa. Este objeto es la locación por *default* para la cuentas de computadoras que son controladores de dominio.
- 4.-Principales de Seguridad Externa: Es un objeto contenedor. Este objeto es utilizado para almacenar identificadores de seguridad (SIDs, *Security Identifier*) desde dominios de confianza del exterior.
- 5.-Usuarios: Es un objeto contenedor. Este objeto es la locación por *default* para las cuentas de usuarios y grupos.

A continuación se presentan los elementos contenidos en los objetos creados por el Asistente para instalación del Directorio Activo. Ver Figuras 64, 65 y 66.

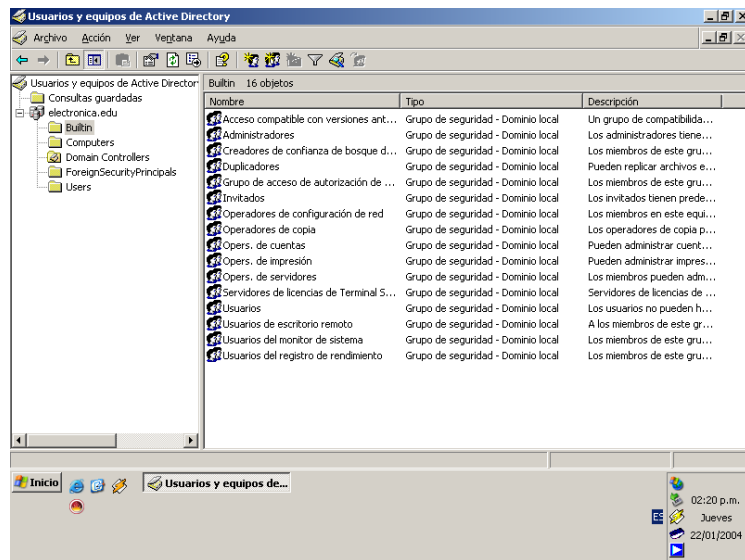


Figura 64.

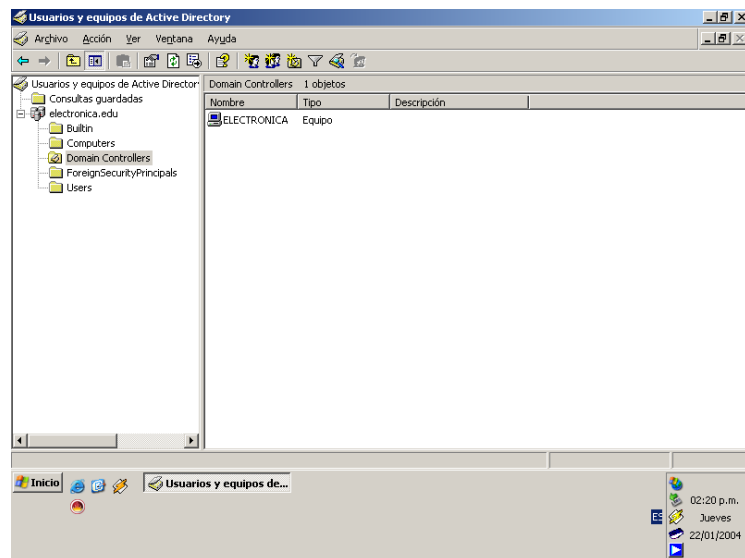


Figura 65.

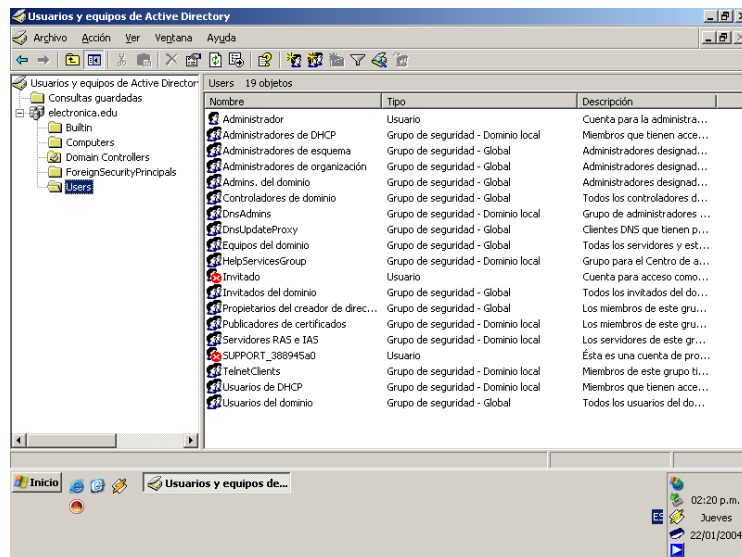


Figura 66.

Creación de una unidad organizativa.

Estos objetos creados durante la instalación del Directorio Activo, satisfacen las necesidades de una pequeña red LAN, pero si es necesario pueden crearse nuevos objetos. El Directorio Activo está basado en la administración de unidades organizativas (OU, *Organizational Unit*), que son objetos contenedores, esto significa que pueden almacenar otros objetos. Por lo tanto se ilustrará el proceso para crear una nueva unidad organizativa, OU. Primero se debe dar un clic con el botón derecho del *mouse* sobre el dominio; posteriormente se debe posicionar el puntero en **Nuevo**, después se seleccionará unidad organizativa. Ver Figura 67.

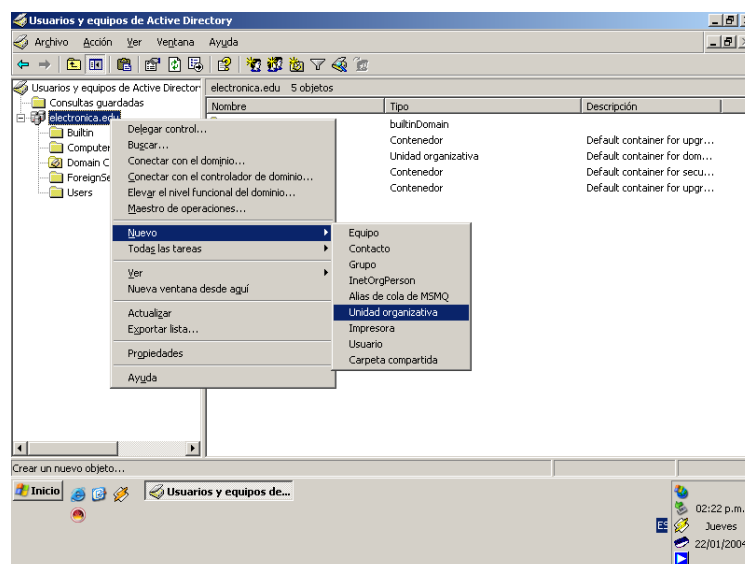


Figura 67.

Ahora aparece una ventana indica en donde se va a crear la nueva unidad organizativa y solo resta nombrar a esta nueva unidad organizativa. Ver Figura 68.

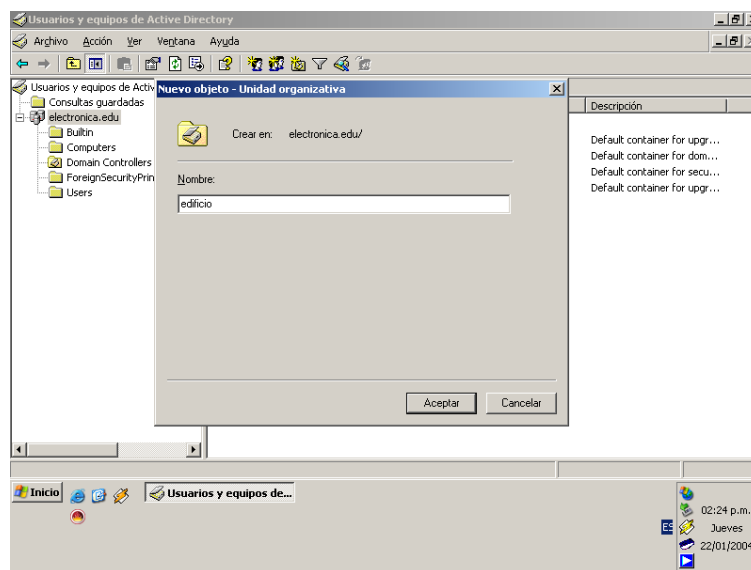


Figura 68.

Creación de una cuenta de usuario.

Para crear una nueva cuenta de usuario se debe definir dentro de cual unidad organizativa se creará ésta nueva cuenta de usuario; en este ejemplo se creará la nueva cuenta de usuario dentro de la unidad organizativa creada anteriormente. Se da un clic con el botón derecho del *mouse* sobre la unidad organizativa, a continuación se posiciona el puntero sobre **Nuevo** y se selecciona **Usuario**. Como se muestra en la Figura 69.

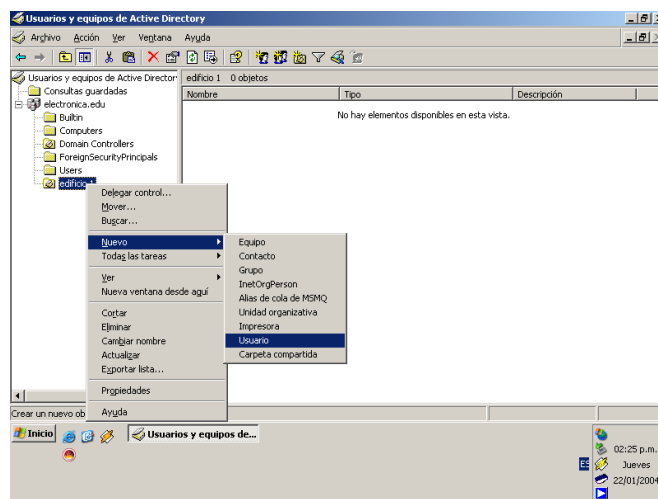


Figura 69.

La siguiente pantalla en aparecer lleva por título **Nuevo objeto-Usuario**, también indica en que unidad organizativa se va a crear este nuevo usuario, en este ejemplo

electrónica.edu/edificio 1; los siguientes 4 campos se deben modificar con los datos del usuario, tal como su nombre, iniciales y apellidos. Una vez definidos los datos personales del nuevo usuario, se debe crear un nuevo **Nombre de inicio de sesión de usuario**, en este ejemplo es **carloshernandez**; como se puede observar el campo correspondiente al dominio al cual va a pertenecer esta cuenta de usuario se caracteriza por tener el carácter @ y a continuación el nombre DNS del dominio, **electrónica.edu**. Por último se puede observar que existe la opción de dar un nombre de usuario para equipos anteriores a Windows 2000, esto permite que el usuario se pueda autenticar en una cualquier computadora sin importar el sistema operativo que tenga instalado. Ver Figura 70.

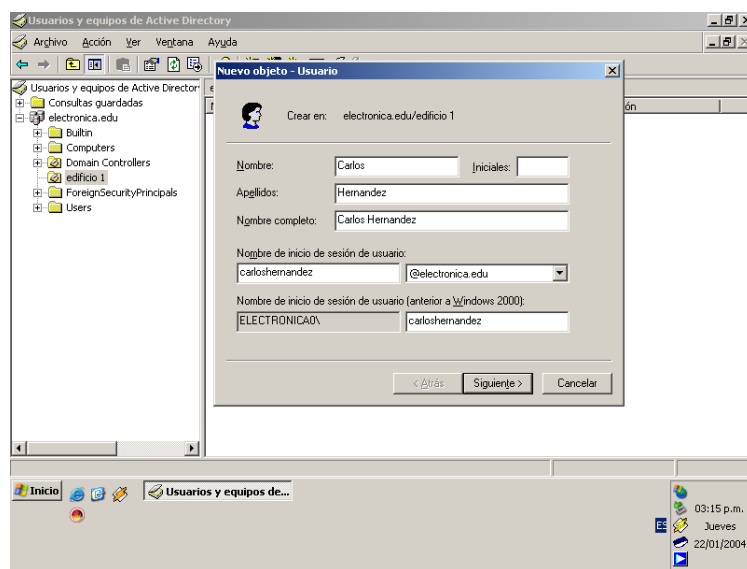


Figura 70.

Una vez definidos los datos personales del usuario y el nombre de sesión que utilizará para autenticarse en el dominio, se debe de asignar una contraseña a ésta cuenta de usuario. Los requerimientos mínimos que exige el sistema de seguridad de Windows 2003 Server para crear una contraseña válida son que ésta contraseña debe contener al menos un carácter con mayúscula, contener letras en minúsculas y contener números, además la longitud mínima de la contraseña debe ser de 8 caracteres. Después de tomar estas restricciones en cuenta, se crea una contraseña para la cuenta de usuario. Como puede observarse en la Figura 71 existen cuatro opciones más que afectan a ésta cuenta de usuario.

Los campos mencionados son los siguientes:

1.-El usuario debe cambiar la contraseña al iniciar una sesión de nuevo. Esto significa que el usuario al autenticarse por primera vez en el dominio deberá introducir la contraseña que le

indique el Administrador; pero la segunda vez que se autentique en el dominio el usuario podrá cambiar su contraseña sin que el Administrador sepa cual es la nueva contraseña.

2.-El usuario no puede cambiar la contraseña. Esto quiere decir que la contraseña que asigne el Administrador para ésta cuenta de usuario no podrá ser modificada por el usuario.

3.-La contraseña nunca caduca. Ésta opción es para definir el tiempo de vida de la contraseña, es decir, si es habilitada ésta opción, la contraseña asignada por el Administrador a ésta cuenta de usuario nunca terminará su tiempo de vida, siempre será vigente. Por el contrario, si se deshabilita entonces la contraseña ya no será vigente y entonces el usuario podrá modificar su contraseña sin previo aviso al Administrador.

4.-La cuenta está deshabilitada. Esta opción sirve para minimizar la carga de trabajo del Administrador ya que si ya no es necesario que una cuenta de usuario esté vigente solamente se habilita ésta opción; cuando de nuevo se requiera de una nueva cuenta de usuario simplemente se deshabilita ésta opción y se introducen los datos correspondientes a la nueva cuenta de usuario.

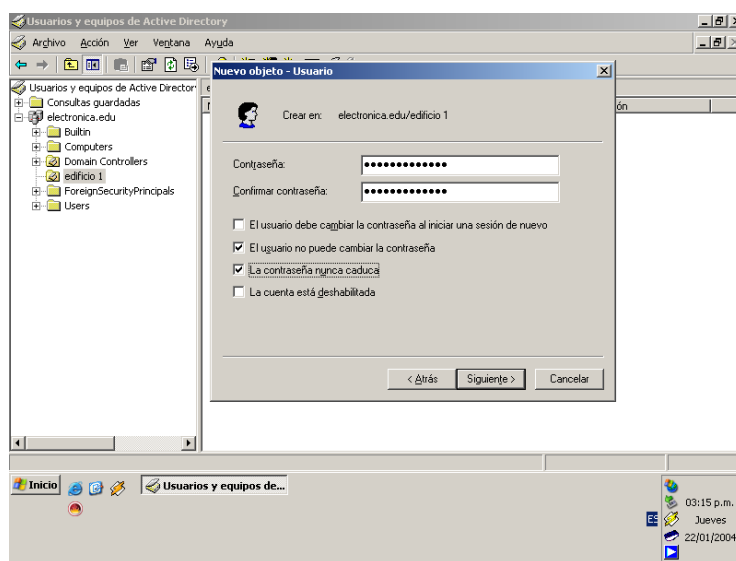


Figura 71.

Ahora se presenta una pantalla donde resume las opciones de la nueva cuenta de usuario que será creada. Ver Figura 72.

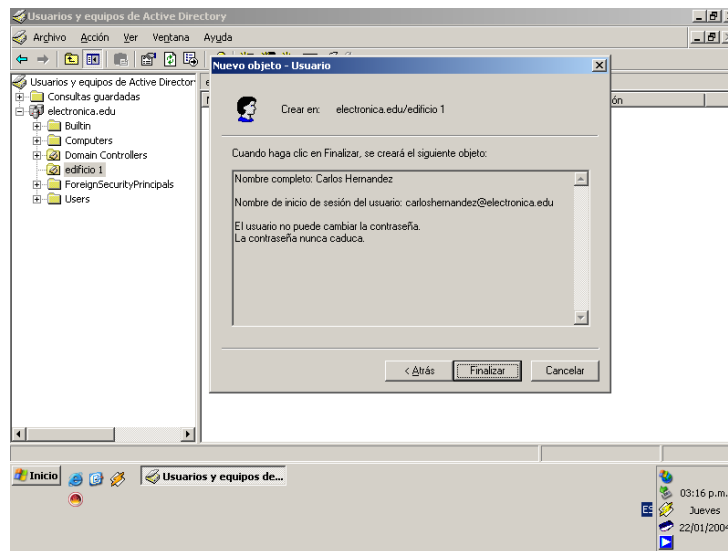


Figura 72,

En este ejemplo se incluyen dos cuentas de usuario como se puede observar en la Figura 73.

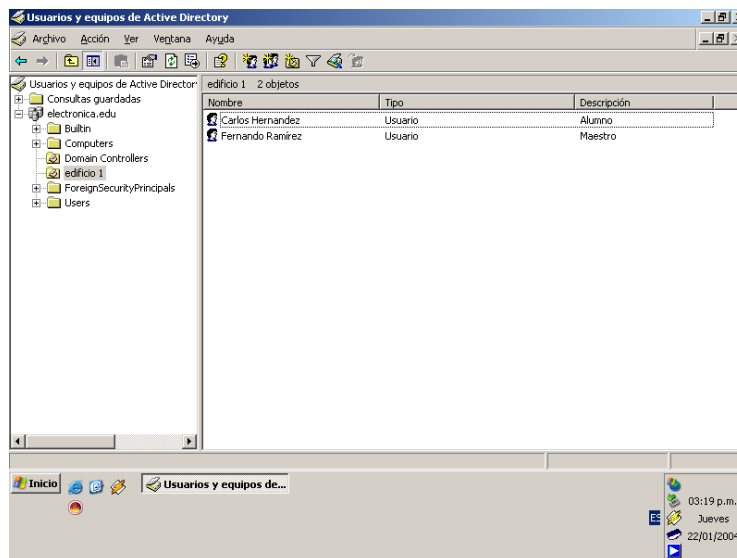


Figura 73.

Definición y tipos de Grupo.

La creación de **Grupos** dentro del Directorio Activo permite administrar los accesos de los usuarios de dominio a los recursos del dominio, a través de la asignación de permisos una sola vez a un **Grupo** en vez de hacerlo usuario por usuario. Los usuarios pueden ser miembros de

varios **Grupos**. Se utilizan los **Grupos** de seguridad para asignar permisos a grupos de usuarios y de computadoras. Los grupos de Distribución pueden ser utilizados para propósitos de seguridad. Los grupos de Seguridad y Distribución tienen el atributo ámbito. El ámbito de un grupo determina quien puede ser miembro del grupo, y cuando puede ser utilizado éste grupo dentro de la red LAN.

Uso de un Grupo Global.

Se utiliza un grupo Global para organizar usuarios que comparten las mismas tareas de trabajo y necesitan accesos de red similares.

A continuación se resumen las directivas de membresía para un Grupo Global:

- 1.-Membresía: En modo mixto puede contener cuentas de usuarios desde el mismo dominio. En modo nativo puede contener cuentas de usuarios y grupos globales del mismo dominio.
- 2.-Puede ser miembro de: En modo mixto, el grupo global solamente puede ser miembro de grupos locales dentro del dominio. En modo nativo, el grupo global puede ser miembro de grupos universales y de grupos locales en cualquier dominio, además de grupos globales dentro del mismo dominio.
- 3.-Ámbito: Un grupo global es visible dentro de su dominio y de todos los dominios en los cuales existe una relación de confianza, lo cual incluye todos los dominios en el bosque.
- 4.-Pueden ser asignados permisos para: Todos los dominios dentro del bosque.

Debido a que los grupos globales tienen una visibilidad a lo largo de todo el bosque, no pueden ser creados específicamente para acceder a recursos de un dominio específico. Los grupos globales son una buena elección para organizar usuarios y grupos de usuarios. Un tipo diferente de grupo es más apropiado para controlar los accesos a recursos dentro de un dominio.

Uso de un Grupo Dominio Local.

Se utiliza un grupo dominio local para asignar permisos de accesos a recursos que están localizados dentro del mismo dominio en el cual se crea el grupo dominio local.

A continuación se resumen las directivas de membresía para un grupo dominio local:

- 1.-Membresía: En un modo mixto puede contener cuentas de usuarios y grupos globales desde cualquier dominio. En modo nativo puede contener cuentas de usuarios, grupos globales, y

grupos universales desde cualquier dominio dentro del bosque, y grupos dominio local del mismo dominio.

2.-Puede ser miembro de: En modo mixto, el grupo dominio local no puede ser miembro de ningún grupo. En modo nativo, el grupo dominio local puede ser miembro de grupos dominio local dentro del mismo dominio.

3.-Ámbito: El grupo dominio local es visible solamente en su propio dominio.

4.-Pueden ser asignados permisos para: El dominio dentro del cual el grupo dominio local existe.

Se pueden crear tantos grupos dominio local como se necesiten para compartir los mismos recursos dentro de un grupo dominio local apropiado.

Uso de un Grupo Universal.

Se utilizan grupos universales para sobreponer grupos globales y así poder asignar permisos a recursos relacionados dentro de diferentes dominios. **Para poder utilizar grupos universales el dominio debe estar modo nativo.**

A continuación se resumen las directivas de membresía para un grupo universal:

1.-Membresía: No se pueden crear grupos universales en modo mixto. En modo nativo puede contener cuentas de usuarios, grupos globales, y otros grupos universales de cualquier dominio en el bosque.

2.-Puede ser miembro de: El grupo universal no puede ser creado en modo mixto. En modo nativo, el grupo universal puede ser miembro de grupos dominio local y grupos universales en cualquier dominio.

3.-Ámbito: Los grupos universales son visibles en todos los dominios en el bosque.

4.-Pueden ser asignados permisos para: Todos los dominios en el bosque.

Creación de un nuevo Grupo.

Una vez definido lo que es un grupo y los tipos de grupos que existen, se ilustrará el proceso para crear un nuevo grupo. Debido a que este ejemplo se desarrolla en un bosque con un solo dominio solo pueden crearse grupos dominio local y globales. Se crearán dos grupos uno llamado **Profesores** y uno más, llamado **Alumnos**; además que estos grupos serán creados en la unidad organizativa **edificio 1**. Ver Figura 74.

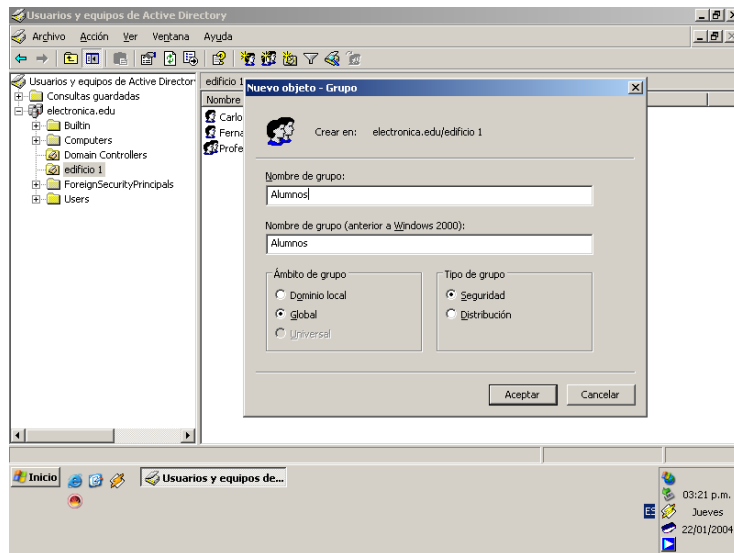


Figura 74.

Una vez creados los dos grupos, se mostrará como unir una cuenta de usuario a un grupo. Primero se debe dar doble clic sobre el usuario y entonces aparecerán las propiedades de éste usuario, se da un clic sobre la pestaña **Miembro de** y se da un clic sobre **Agregar**. Ver Figura 75.

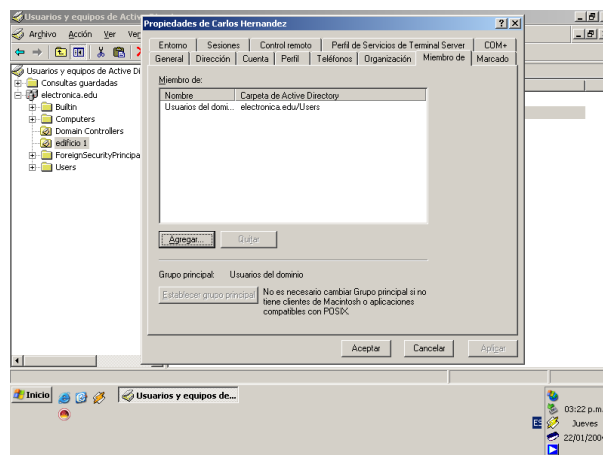


Figura 75.

Ahora aparecerá una pantalla en donde se seleccionará el grupo al cual se desea unir éste usuario. Ver Figura 76.

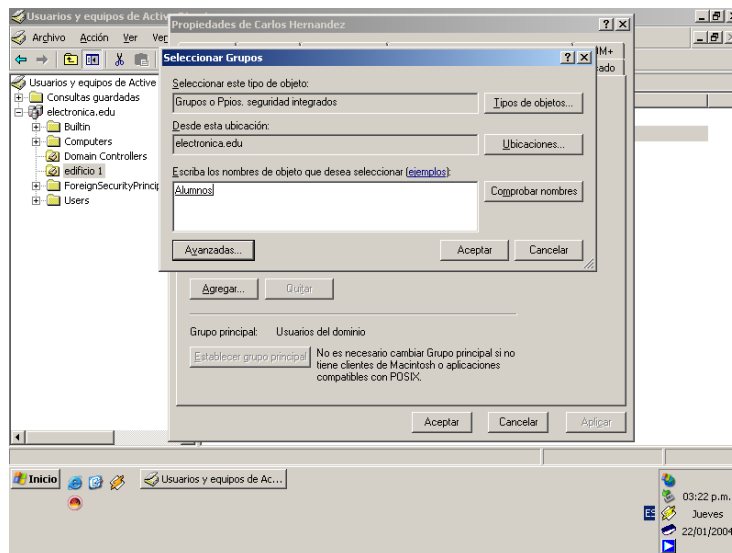


Figura 76.

Una vez indicado el grupo al cual se unirá el usuario, se muestra el nuevo grupo en la pantalla de propiedades del usuario. Ver Figura 77.

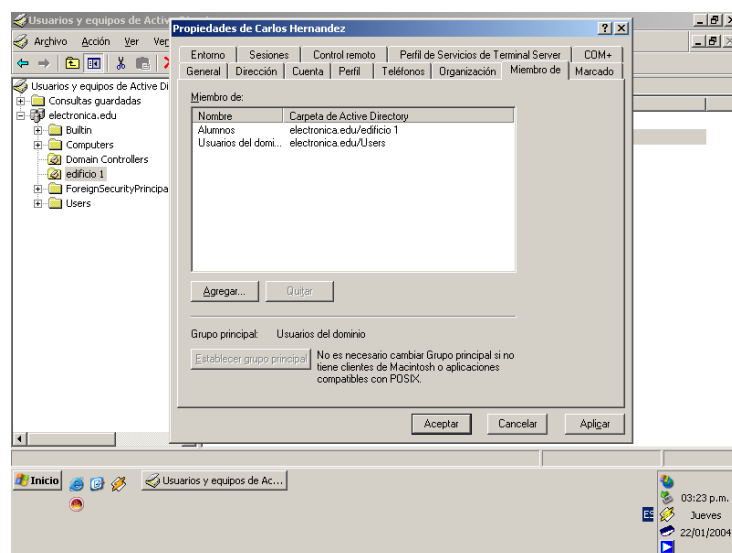


Figura 77.

Las cuentas de usuarios creadas en este ejemplo se unieron a los grupos de la siguiente forma. La cuenta de usuario **Carlos Hernández** es miembro del grupo **Alumnos** y la cuenta de usuario **Fernando Ramírez** pertenece al grupo **Profesores**. Ver Figura 78.

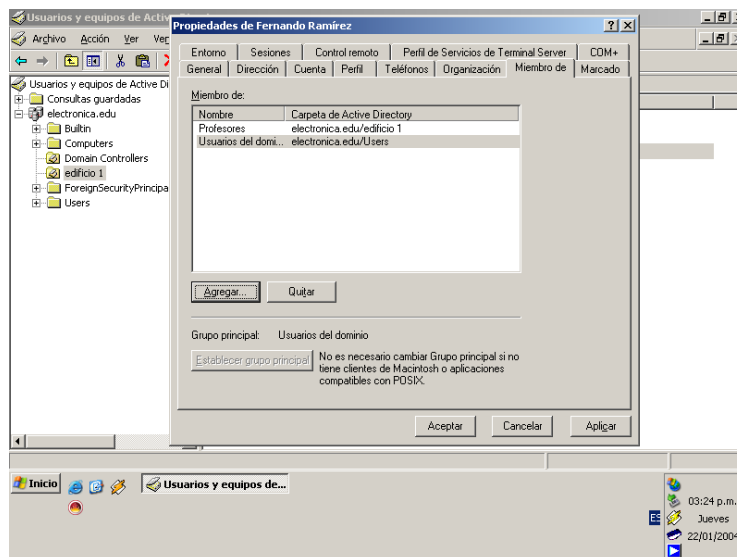


Figura 78.

Publicación de recursos en el Directorio Activo.

Como siguiente paso se ilustrará el proceso para publicar un recurso en el Directorio Activo. **Publicar** significa crear objetos en el Directorio Activo que contienen directamente la información que se desea hacer disponible, o proveer una referencia a esa información.

No es necesario publicar recursos que ya existen en el Directorio Activo, tales como cuentas de usuarios. Sin embargo es necesario publicar recursos que no existen en el Directorio Activo. Dos ejemplos de recursos que no existen en el Directorio Activo son las impresoras conectadas a una computadora que está corriendo un sistema operativo anterior de Microsoft Windows 2000 y las carpetas compartidas.

Publicar una impresora en el Directorio Activo.

Para configurar un servidor de impresión, se inicia el Asistente para configurar su servidor mediante una de las acciones siguientes:

En Administre su servidor, se debe hacer clic en **Agregar o quitar función**. De forma predeterminada, Administre su servidor se inicia automáticamente al iniciar la sesión. Para abrir Administre su servidor, hacer clic en **Inicio**, **Panel de control**, hacer doble clic en **Herramientas administrativas** y, a continuación, hacer doble clic en **Administre su Servidor**. Ver Figura 79.

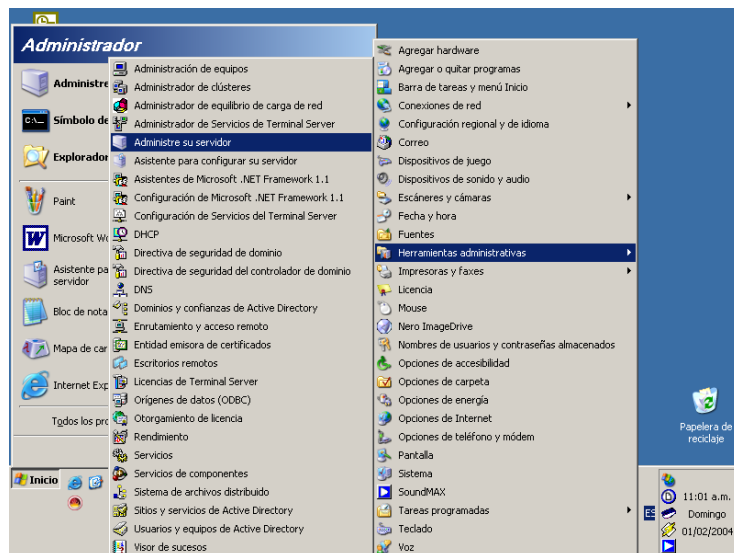


Figura 79.

La segunda opción es la siguiente, primero hacer clic en **Inicio**, después hacer clic en **Panel de control**, hacer doble clic en **Herramientas administrativas** y, a continuación, hacer doble clic en **Asistente para configurar su servidor**. Ver Figura 80.

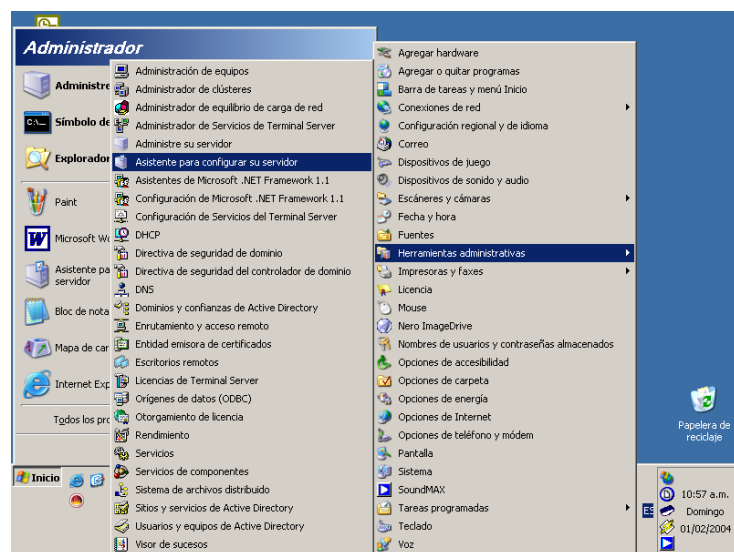


Figura 80.

En la página **Función del servidor**, hacer clic en **Servidor de impresión** y, a continuación, en **Siguiente**.

Impresoras y controladores de impresora

En la página **Impresoras y controladores de impresora**, realizar una de las acciones siguientes:

Si todos los clientes de la red ejecutan Windows XP Home Edition, Windows XP Professional o Windows 2000, hacer clic en **Sólo clientes Windows 2000 y Windows XP**.

Si alguno de los clientes ejecuta Windows XP 64-Bit Edition, Windows NT 4.0, Windows Millennium Edition, Windows 98 o Windows 95, hacer clic en **Todos los clientes Windows**.

Posteriormente hacer clic en **Siguiente**.

Resumen de las selecciones

En la página **Resumen de las selecciones**, se deben observar y confirmar las opciones que se hayan seleccionado. Si ha sido seleccionado **Sólo clientes Windows 2000 y Windows XP** en la página anterior, aparecerá el mensaje siguiente:

Agregar impresoras a este servidor utilizando el Asistente para agregar impresoras.

Si ha sido seleccionado **Todos los clientes Windows** en la página anterior, aparecerá el siguiente mensaje:

Agregar impresoras a este servidor utilizando el Asistente para agregar impresoras.

Agregar controladores de impresora a este servidor utilizando el Asistente para agregar controladores de impresora.

Para aplicar las selecciones que aparecen en la página **Resumen de las selecciones**, hacer clic en **Siguiente**.

Utilizar el Asistente para agregar impresoras

Después de hacer clic en **Siguiente**, el Asistente para configurar su servidor ejecutará el Asistente para agregar impresoras tantas veces como impresoras se deseen agregar. Si se finaliza el asistente y se selecciona compartir al menos una impresora, el servidor se podrá utilizar como servidor de impresión. Si se cancela este asistente, el servicio de Cola de impresión permanecerá instalado. Si se cancela el Asistente para agregar impresoras y no hay ninguna impresora compartida, el servidor no agregará la función de servidor de impresión.

Si la impresora que se desea compartir es compatible con Plug and Play, no es necesario ejecutar el Asistente para agregar impresoras. Las impresoras Plug and Play completarán los pasos de este asistente automáticamente. Si la impresora que se desea compartir es compatible

con Plug and Play, hacer clic en **Cancelar**. En este caso la impresora utilizada para ilustrar éste ejemplo es una impresora Plug and Play, por lo cual no es necesario realizar el proceso anterior. Ver Figura 81.

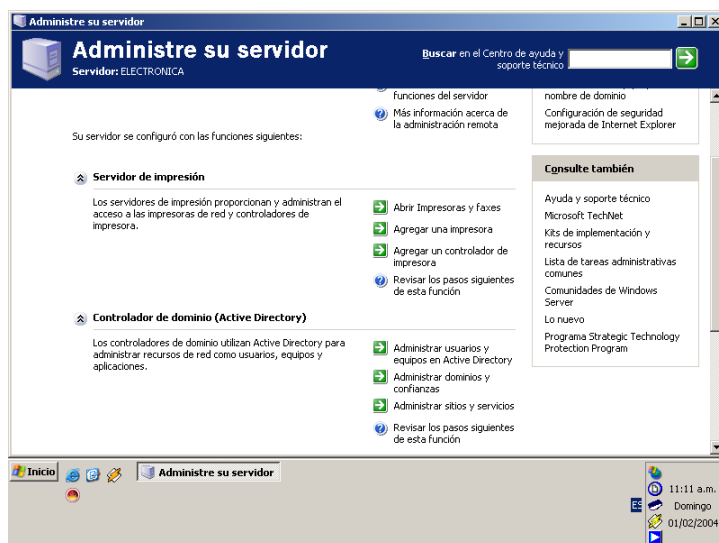


Figura 81.

Publicar una carpeta compartida.

Se pueden publicar carpetas compartidas en el Directorio Activo utilizando Usuarios y Equipos de Active Directory. Para hacer accesible una carpeta compartida, primero se debe compartir esta carpeta, y después se puede publicar en el Directorio Activo.

Para publicar una carpeta compartida, se deben seguir los siguientes pasos:

1.-Dentro de la consola Usuarios y equipos de Active Directory, dar un clic con el botón derecho en la unidad organizativa donde se quiere publicar la carpeta compartida, dar un clic sobre nuevo, y después dar un clic sobre Carpeta compartida. En el campo **Nombre de carpeta compartida**, escribir el nombre de la carpeta. Ver Figura 82.

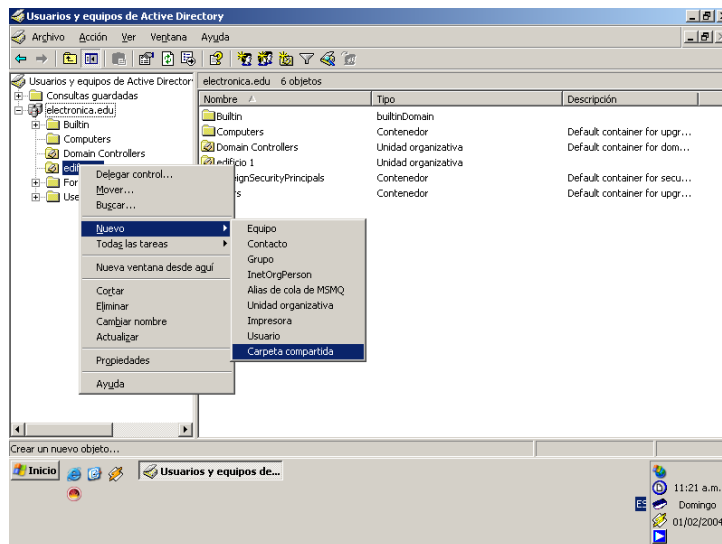


Figura 82.

2.-En el campo de ruta UNC, escribir el UNC que se quiere publicar dentro del Directorio Activo.

La ruta UNC es el nombre completo en Windows 2000 de un recurso de red que sigue la siguiente sintaxis **\\nombredelservidor\recursocompartido**. Ver Figura 83.

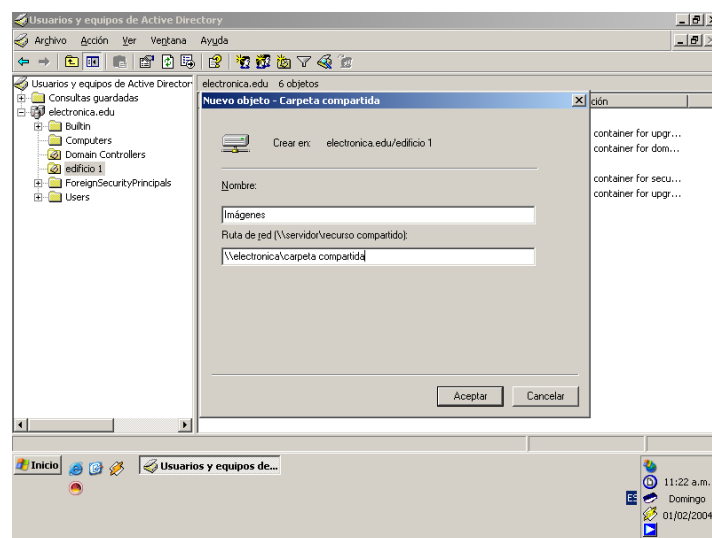


Figura 83.

Cuando se implementan carpetas e impresoras publicadas, es importante entender la diferencia entre el objeto que es publicado en el Directorio Activo y el recurso compartido actual, tal como una carpeta o una impresora. Entendiendo esta diferencia permite solucionar fácilmente los problemas presentados cuando un usuario no puede acceder a los recursos publicados.

El objeto que es publicado en el Directorio Activo está completamente separado del recurso que representa. En otras palabras, cuando se publica una impresora o una carpeta compartida

en el Directorio Activo, existen dos objetos distintos, uno es la carpeta o impresora compartidos y el otro es el objeto publicado. El objeto publicado contiene una referencia a la locación del recurso compartido. Cuando un usuario accede al objeto publicado, el usuario es redirigido al recurso compartido. Ahora se puede acceder al recurso publicado de la siguiente forma:

1.-Seleccionar el recurso publicado. Ver Figura 84.

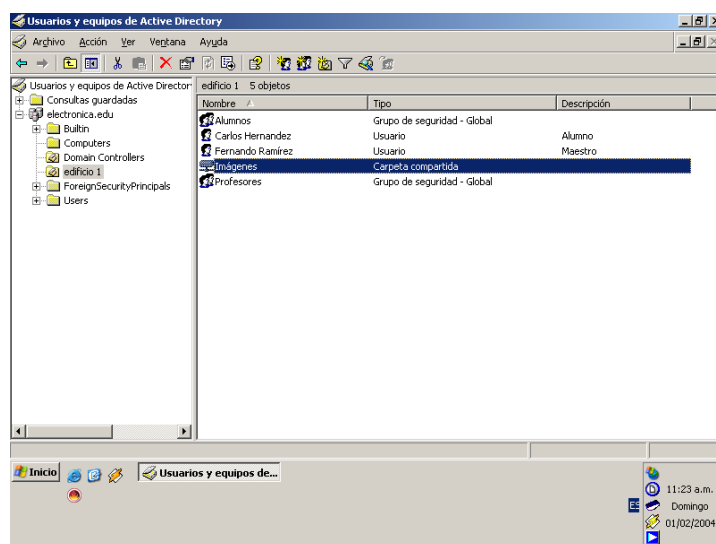


Figura 84.

2.-Dar un clic con el botón derecho del *mouse* y dar un clic en **Explorar**. Ver Figura 85.

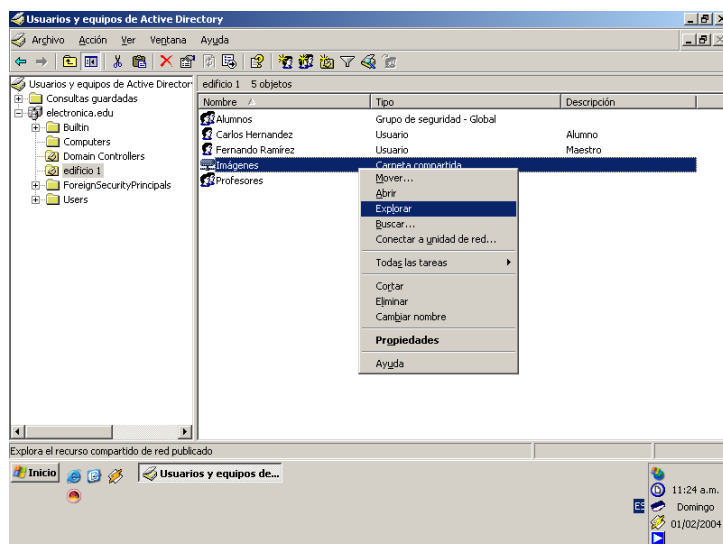


Figura 85.

3.-Por último se abre una página de explorador, en la cual del lado izquierdo se puede observar la dirección de red en donde está localizado el recurso compartido y del lado derecho se observará el contenido de la carpeta compartida. Ver Figura 86.

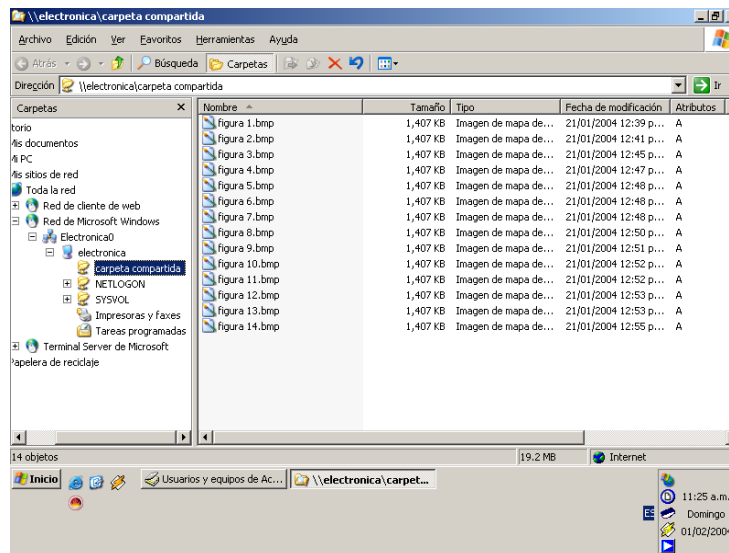


Figura 86.

Seguridad en el Directorio Activo.

El control de acceso es el proceso de autenticación de usuarios, grupos y computadoras para acceder objetos en la red.

Cada objeto dentro del Directorio Activo es asociado con un único descriptor de seguridad que define los permisos de accesos que son requeridos para leer o actualizar las propiedades del objeto. Los permisos son asignados en el nivel propiedad. Los componentes básicos del modelo de control de acceso son *Security principals*, *Security identifiers (SIDs)* y *Security descriptors*.

Security Pirncipals.

Es en donde se pueden asignar permisos . Ejemplos de éste componente son, cuentas de usuario, grupo de seguridad y de computadoras .

Security Identifiers(SIDs).

Es un valor que autentica únicamente a una cuenta de usuario, grupo, servicio o de computadora dentro de una organización. Cada cuenta es editada con un SID cuando es creada. Los mecanismos de control de acceso identifican los *security principals* más por su SID que por su nombre. Después de que un SID es editado para una cuenta, nunca es reutilizado para otra cuenta.

Security Descriptors.

Es una estructura de información que contiene la información de seguridad asociada con un objeto asegurable. Un *security descriptor* identifica al dueño de un objeto por medio de su

SID. Si los permisos son configurados para el objeto, su *security descriptor* contiene una lista de control de acceso discrecional, (*DACL, Discretionary Access Control List*).

Los usuarios son capaces de acceder un recurso cuando ha sido verificado su lista DACL de los permisos asignados contra los accesos requeridos por el usuario. Este proceso es conocido como Autorización.

Se controlan los accesos a los recursos en dos formas:

- 1.- Requiriendo a los usuarios su firma utilizando un conjunto de credenciales de seguridad verificables. Éstas credenciales son entonces comparadas contra un conjunto de permisos asignados a los objetos del Directorio Activo y los recursos de la red, tales como carpetas compartidas y archivos en sistema NTFS (Network File System, Sistema de Archivos en red).
- 2.-Permitiendo acceso solamente a aquellos recursos que el usuario tiene permiso de utilizar. Después que ha sido autenticada la identidad única del usuario por Windows 2003 y el Directorio Activo entonces el usuario puede recibir el acceso a recursos específicos en la red desde cualquier computadora en cualquier dominio de la organización.

Permisos.

Un permiso es una autorización asignada por un dueño para que los usuarios puedan ejecutar una operación en un objeto específico, tal como una cuenta de usuario.

Permitir y denegar permisos.

Si se deniega un permiso a un usuario para obtener acceso a un objeto, el usuario no tendrá ese permiso, aún cuando es permitido este acceso al grupo de usuarios al cual pertenece el usuario.

Se pueden denegar permisos de forma implícita o explícita como sigue:

- 1.-Cuando un permiso para ejecutar una operación no es explícitamente asignada, entonces es implícitamente denegada.
- 2.-Los permisos pueden ser explícitamente denegados.

Permisos estándar y especiales.

Se pueden asignar permisos estándar y permisos especiales sobre los objetos. Los permisos estándar son los permisos más frecuentemente asignados. Los permisos especiales proveen un grado más fino de control para asignar accesos a los objetos.

La siguiente tabla lista los permisos estándar que están disponibles para la mayoría de los objetos, y el tipo de acceso que cada permiso proporciona al usuario.

Permiso.	Permite al usuario.
-----------------	----------------------------

Control completo.	Cambiar permisos y tomar posesión de objetos, además de ejecutar todas las tareas que son permitidas por todos los demás permisos estándar.
Lectura.	Ver objetos, atributos, al dueño del objeto y los permisos del Directorio Activo.
Escritura.	Cambiar atributos del objeto.
Crear todos los objetos hijos.	Sumar cualquier tipo de objeto hijo en una unidad organizativa.
Borrar todos los objetos hijos.	Borrar cualquier tipo de objeto hijo en una unidad organizativa.

Política de Grupo.

La política de Grupo es la tecnología que permite definir el ambiente de escritorio para un usuario. Al utilizar una política de grupo es posible:

- 1.-Centralizar políticas al configurar una política de grupo para una organización entera a nivel de sitio o dominio, o descentralizar configuraciones de políticas de grupo aplicando una política de grupo para cada departamento a nivel unidad organizativa.
- 2.-Asegurar que los usuarios tengan el ambiente de usuario que necesitan para ejecutar su trabajo. Se puede asegurar que los usuarios tengan una configuración de política de grupo la cual controle los valores de aplicación y configuración del sistema en el registro, un *script* puede modificar el entorno de usuario y de computadora, las instalaciones de software automatizadas, y valores de seguridad para computadoras locales, dominios y redes. También se puede controlar en donde son almacenadas las carpetas de los usuarios.
- 3.-Utilizando una política de grupo, se puede prevenir que los usuarios hagan cambios en la configuración del sistema lo cual puede provocar que una computadora se vuelva inoperable, o también se puede prevenir que los usuarios instalen aplicaciones que no necesitan para realizar su trabajo.
- 4.-Puede asegurarse que los requerimientos de seguridad aplicados a todos los usuarios concuerden con la seguridad requerida por la compañía, o que todos los usuarios tengan instalado un conjunto de aplicaciones en particular.

Para poder implementar una política de grupo se debe dar un clic con el botón derecho del *mouse* sobre el nombre del dominio, a continuación se debe dar un clic sobre **Propiedades**. Ver Figura 87.

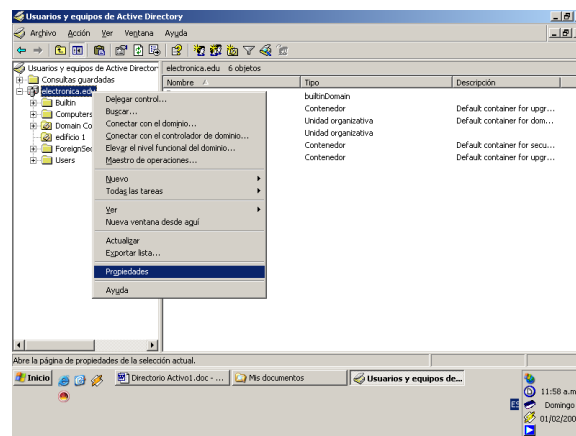


Figura 87.

A continuación se abre una pantalla mostrando las propiedades de la política de grupo y se observarán las políticas de grupo activas, por *default* existe una política de grupo del dominio. Ver figura 88.

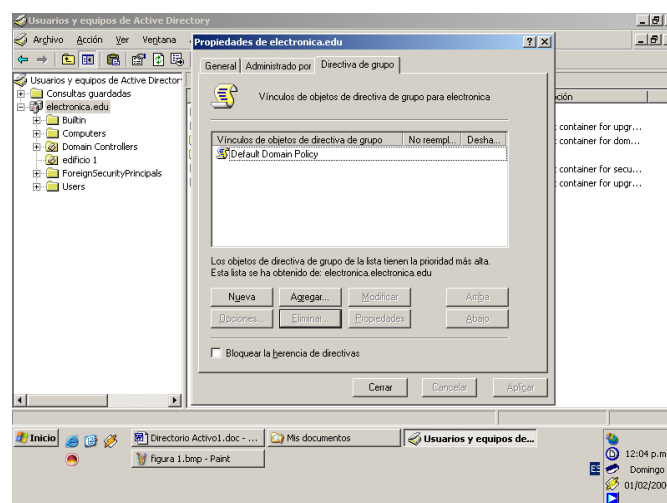


Figura 88.

Para crear una nueva política de grupo se debe dar un clic sobre **Nueva** y posteriormente se debe nombrar a ésta nueva política de grupo. Ver Figura 89.

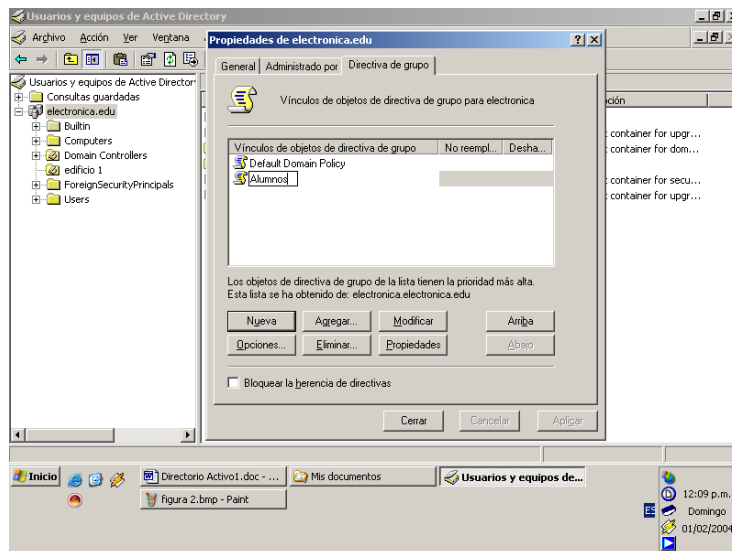


Figura 89.

Posteriormente para agregar y denegar permisos se debe seleccionar la política de grupo a modificar y se debe dar un clic sobre **Modificar** y aparecerá una pantalla en la cual aparecerán todos los tipos de política de grupo que pueden modificarse. Ver Figura 90.

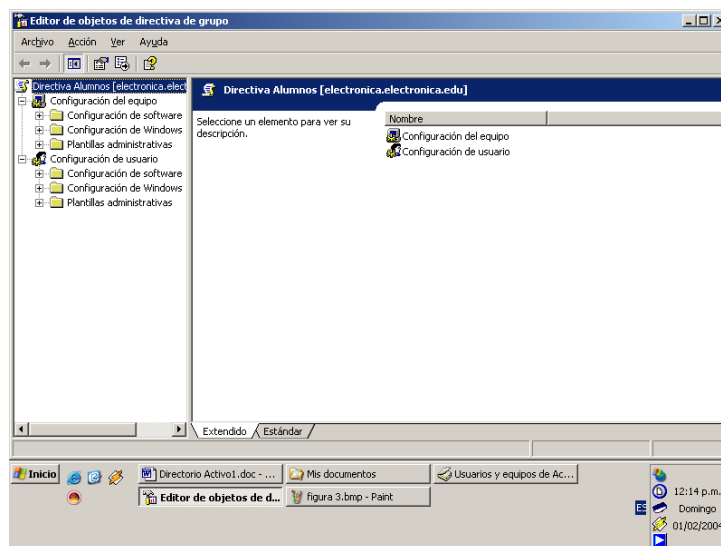


Figura 90.

Tipos de políticas de grupo.

Los valores que se pueden configurar con una política de grupo son los siguientes:

1.-Plantillas administrativas. Son valores basados en registro para la configuración de valores de aplicación y de entornos de escritorio. Éstos valores incluyen los componentes del sistema

operativo y las aplicaciones a las cuales el usuario puede tener acceso, el grado de acceso a las opciones del **Panel de Control** y el control de archivos de usuario fuera de línea.

2.-Seguridad. Son valores para la configuración de una computadora local, dominio, y valores de seguridad de red, dar de alta una cuenta y políticas de auditoria, y el control de derechos de usuario. Por ejemplo, se pueden configurar el numero máximo de intentos fallidos de firma que una cuenta de usuario puede realizar antes de ser bloqueada.

3.-Instalación de seguridad. Son valores para la centralización de la administración de las instalaciones de software, actualizaciones y desinstalaciones. Se puede hacer que las aplicaciones se instalen automáticamente en la computadora del usuario, puede ser automáticamente actualizada, o ser automáticamente borrada.

4.-Scripts. Se pueden especificar los *scripts* a ejecutarse cuando una computadora se enciende y cuando se apaga, cuando un usuario se conecta o se desconecta. Se pueden especificar *scripts* para ejecutar operaciones tipo batch, controlar múltiples *scripts* y determinar el orden en que se ejecutarán. Para más información sobre *scripts* visitar la siguiente página de Internet <http://msdn.microsoft.com/scripting/>

5.-Servicios de instalación remota. Son valores que controlan las opciones disponibles a los usuarios cuando se está ejecutando el Asistente de instalación del cliente usado por los servicios de instalación remota (RIS, *Remote Installation Services*).

6.-Mantenimiento del explorador de Internet. Son valores para administrar y personalizar el Explorador de Internet.

7.-Redireccionamiento de carpetas. Son valores para el almacenamiento de carpetas específicas de un perfil de usuario en un servidor de red. Los valores crean un enlace entre el perfil y va hacia la carpeta de red compartida, pero las carpetas aparecen localmente. El usuario puede tener acceso a la carpeta desde cualquier computadora de la red. Por ejemplo se puede redireccionar la carpeta de usuario **Mis Documentos** hacia una carpeta de red compartida.

Plantillas administrativas.

Las plantillas administrativas son una colección de valores de política de grupo que modifican los valores de los registros. Se utilizan las plantillas administrativas en una política de grupo para configurar los valores basados en registros que controlan el ambiente de trabajo del usuario. Esto incluye el control de los valores de escritorio, opciones de interfase, componentes del sistema operativo y los valores por *default* para las aplicaciones del usuario.

Las plantillas administrativas modifican los valores localizados en las siguientes locaciones de registro:

1.-**HKEY_ LOCAL_MACHINE (HKLM)**. Cuando una computadora se enciende los valores de la política de grupo contenidos dentro de la porción de política de grupo en la Configuración de la Computadora que son aplicados a la computadora son escritos en **SOFTWARE\Policies** o en **SOFTWARE\Microsoft\Windows\CurrentVersion\Policies**.

2.-**HKEY_CURRENT_USER (HKCU)**. Cuando un usuario se firma en una computadora, las políticas de grupo contenidas en la porción de la configuración del usuario que son aplicadas al usuario se escriben en **SOFTWARE\Policies** o **SOFTWARE\Microsoft\Windows\CurrentVersion\Policies**.

Las plantillas administrativas están organizadas en siete tipos, en los cuales hay configuraciones para usuarios y computadoras. Los valores de computadora están enfocados en la administración del sistema operativo y los valores de usuario están enfocados en como los usuarios pueden afectar su entorno de escritorio.

Para acceder al **Editor de registro**, se da un clic en **Inicio**, dar un clic en **Ejecutar** y escribir el siguiente comando **regedit**; después se accede a los registros indicados anteriormente.

La siguiente tabla muestra los tipos de valores en las plantillas administrativas.

<i>Tipo de Valor</i>	<i>Controla</i>	<i>Disponible para</i>
Componentes	Las partes de usuarios, sus herramientas y	Computadoras y

De Windows	componentes a los cuales el usuario puede tener acceso	Usuarios
Sistema	Procesos de conexión y desconexión, escritura en disco	Computadoras y Usuarios
Red	Las propiedades de conexiones de red.	Computadoras y Usuarios
Impresoras	Los valores de impresora que fuerzan a las impresoras para ser publicadas en el Directorio Activo y deshabilitar impresión basada en Web.	Computadoras y Usuarios
Menú inicio & Barra de tareas	Lo que los usuarios pueden acceder en el menú Inicio y hacer de solo lectura a la Barra de tareas	Usuarios
Escritorio	Al Active Desktop , incluyendo lo que aparece en el escritorio y lo que los usuarios pueden hacer en la carpeta Mis Documentos	Usuarios
Panel de Control	El uso de Agregar/quitar Programas, impresoras y monitor en el Panel de Control	Usuarios

Tabla 1.

Valores para el bloqueo del escritorio.

Hay muchos valores para una política de grupo que pueden ser utilizados para personalizar el entorno del escritorio del usuario.

A continuación se describen los valores de política de grupo:

- 1.-Ocultar todos los íconos en el escritorio. Oculta todos los íconos en el escritorio, incluyendo, menús, carpetas, y accesos directos. Esto provee al usuario una interfase simple.
- 2.-No guardar cambios al salir. Deshabilita la propiedad de salvar cualquier cambio hecho en la configuración durante el proceso de firma. La configuración original es almacenada cada vez que el usuario se desconecta y se vuelve a cargar ésta configuración cuando el usuario se vuelve a conectar.
- 3.-Ocultar los discos especificados en **Mi PC**. Remueve los iconos que representan los discos seleccionados desde **Mi PC**, **Explorador de Windows** y **Mis sitios de red**. Las literales de

los discos no aparecerán en el cuadro de diálogo **Abrir** de cualquier aplicación. Ocultando discos ayuda a limitar a los usuarios para ejecutar solamente las aplicaciones que se encuentran en el menú **Inicio**.

4.-Remover el menú **Ejecutar** del menú **Inicio**. Remueve el comando **Ejecutar** del menú **Inicio**. Sin embargo, los usuarios aún pueden acceder a éste comando a través del **Administrador de tareas**.

5.-Prohibir al usuario el acceso a **Monitor** en el **Panel de control**. Previene a los usuarios de cambiar la configuración del monitor tal como, el fondo, protector de pantalla, y la apariencia. Este valor también reduce los problemas ocasionados por el usuario cuando cambia la apariencia de su escritorio.

6.-Deshabilitar y remover las ligas a **Windows update**. Remueve el comando **Windows update** del menú **Configuración**. Sin embargo, este comando todavía puede estar disponible en el **Explorador de Internet**. Al remover éste comando ayuda a prevenir a los usuarios de aplicar actualizaciones no autorizadas o hacer cambios a sus sistemas operativos.

7.-Deshabilitar cambios en la configuración de la **Barra de tareas** y del menú **Inicio**. Remueve el comando **Barra de tareas & Menú Inicio** del menú **Configuración**. Esto ayuda a prevenir a los usuarios de rechazar cualquier cambio realizado por el Administrador en el menú **Inicio**.

8.-Deshabilitar/Remover el comando **apagar**. Previene a los usuarios de apagar y reiniciar su equipo. Esto es útil en computadoras que deben estar trabajando ininterrumpidamente, tal como una computadora en una biblioteca pública.

Valores para bloquear el acceso del usuario a los recursos de red.

Es posible restringir los recursos de red a los cuales el usuario tiene acceso. A continuación se describen éstos valores:

1.-Ocultare el ícono **Mis sitios de red** del escritorio. Remueve el ícono **Mis sitios de red** del escritorio y deshabilita el soporte para convención de nombramiento universal (UNC, *Universal Naming Convention*). Utilizar los *scripts* de conexión para mapear los discos de red, se pueden controlar los recursos de red a los cuales el usuario tiene acceso.

2.-Remover **Conectarse a unidad** y **Desconectarse de unidad**. Éste valor también remueve el Asistente **Nuevo sitio de red** de **Mis sitios de red**. Sin embargo, los usuarios aún pueden conectarse a otras computadoras utilizando en comando **Ejecutar** del menú **Inicio**.

3.-Menú **Herramientas**: Deshabilitar **Opciones de Internet**...menú **Opciones**. Remueve el comando **Opciones de Internet** del **Explorador de Internet**. Esto previene a los usuarios de modificar su configuración del **Explorador de Internet**.

Implementando Plantillas Administrativas.

Para seleccionar el estado de una política de las opciones presentadas en el cuadro de diálogo **Propiedades** de la política de grupo.

A continuación se muestran los tres posibles estados de un valor de política:

- 1.-No configurado. Este estado no especifica un cambio de valor en el registro.
- 2.-Habilitado. Éste valor es aplicado y se suma al archivo *Registry.pol* apropiado.
- 3.-Deshabilitado. Éste valor no es aplicado ni tampoco sumado al archivo *Registry.pol*.

¿Que es un redireccionamiento de carpeta?

Cuando se redireccionan carpetas, se cambia la locación de almacenamiento de carpetas desde un disco duro local en la computadora del usuario hacia una carpeta compartida en un servidor de archivos. Después de redireccionar una carpeta hacia un servidor de archivos, sigue apareciendo al usuario como si se estuviera almacenando en el disco duro local. Las cuatro carpetas que pueden ser redireccionadas y que son parte del perfil de usuario son: **Mis Documentos**, **Información de Aplicación**, **Escritorio**, y el menú **Inicio**.

Seleccionando las carpetas a redireccionar.

Dependiendo de las necesidades del usuario y de la red, se pueden redireccionar todos o solo algunas de las carpetas.

- 1.-**Mis Documentos** Contiene información personal del usuario. Se redirecciona para que el usuario pueda acceder a su información desde cualquier computadora, y ésta información puede ser respaldada y administrada de manera centralizada.
- 2.-**Menú Inicio**. Contiene las carpetas y accesos directos en el menú **Inicio**. Se redirecciona para que los menús **Inicio** de todos los usuarios estén estandarizados.
- 3.-**Escritorio**. Contiene todos los archivos y carpetas que un usuario coloca en el escritorio. Se redirecciona para que los usuarios tengan el mismo escritorio a pesar de la computadora en la que se firmen.

4.-Información de aplicación. Contiene la información almacenada de un usuario específico por aplicaciones. Se redirecciona para que las aplicaciones utilicen la información de un usuario específico por un usuario si importar la computadora en la cual se firman.

Una política de grupo permite estandarizar los valores de seguridad aplicando la misma plantilla de seguridad a múltiples computadoras en un solo paso. Las plantillas de seguridad son grupos de valores de seguridad que pueden ser importados en políticas de grupo o ser utilizadas para análisis.

Introducción a la administración de difusión de software.

Se pueden utilizar políticas de grupo para administrar el proceso de difusión de software de manera centralizada, o desde una locación. Se pueden aplicar políticas de grupo a usuarios o computadoras en un sitio, dominio o unidad organizativa para que automáticamente se instale, actualice o remueva software a los usuarios y computadoras en el sitio, dominio o unidad organizativa. Al aplicar una política de grupo al software, se pueden administrar las diferentes fases de difusión de software sin tener que visitar cada una de las computadoras.

Creando un punto de distribución de software.

Un punto de distribución de software es una carpeta compartida que contiene un paquete de archivos para la difusión de software. Los paquetes instaladores y los archivos del software deben estar disponibles en un punto de distribución de software, para que cuando el software haya sido instalado en una computadora local, los archivos sean copiados desde este punto hacia la computadora. Manteniendo juntos los archivos de cada aplicación simplifica la administración.

Para crear un punto de distribución de software, se deben ejecutar las siguientes tareas:

- 1.-Crear una carpeta compartida.
- 2.-Crear las carpetas de aplicación apropiadas dentro de la carpeta compartida.
- 3.-Copiar los paquetes del instalador de Windows y los archivos ejecutables de la aplicación en las carpetas apropiadas.
- 4.-Establecer el permiso apropiado a la carpeta compartida. Asignar a los usuarios el permiso de lectura para que puedan tener acceso a los archivos de instalación del software en el punto de distribución de software.

Publicando software.

Cuando se publica software, éste se hace disponible para los usuarios y para instalarlo en sus computadoras, aún cuando no existan accesos directos en los escritorios de los usuarios o en el menú **Inicio**, y no se hacen entradas de registro local. Debido a que los usuarios deben instalar el software instalado, se puede publicar el software solo para los usuarios y no para las computadoras. Los usuarios pueden instalar el software publicado en una de las dos siguientes formas:

1.-Utilizando **Agregar/Quitar Programas**. Un usuario puede abrir **Panel de Control** y dar doble clic en **Agregar/Quitar Programas** para mostrar el conjunto de aplicaciones disponibles. El usuario puede entonces seleccionar la aplicación seleccionada y dar un clic en **Instalar**.

2.-Utilizando la activación de documento. Cuando una aplicación es publicada en el Directorio Activo, las extensiones de los archivos para los documentos que soporta están registrados en el Directorio Activo. Si un usuario da doble clic en un tipo de archivo desconocido, la computadora envía una petición al Directorio Activo para determinar si existe alguna aplicación asociada con la extensión del nombre del archivo. Si el Directorio Activo contiene dicha aplicación entonces la computadora la instala.