UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

CAMPUS ARAGON

MIGRACION E IMPLEMENTACION DE WINDOWS 2000 SERVER EN UNA RED CORPORATIVA

T E S I S

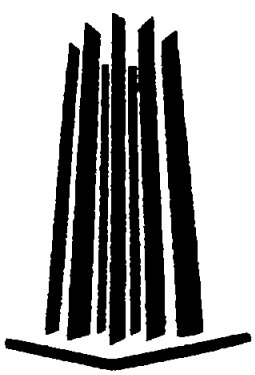
QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACION

P R E S E N T A N :

OVIDIO CERVANTES LAZCANO

MARIO MARTINEZ REYES



ASESOR: ING. SILVIA VEGA MUYTOY

SAN JUAN DE ARAGON, EDO. DE MEXICO **2004**

PROYECTO DE TESIS
MIGRACIÓN E IMPLEMENTACIÓN DE WINDOWS 2000 SERVER EN UNA RED CORPORATIVA

PROBLEMÁTICA: Operatibilidad y seguridad que existe en el Sistema Operativo Windows NT 4.0

OBJETIVO: Migrar al Sistema Operativo Windows 2000 Server para ofrecer dentro de la red una mejor administración en la transmisión de datos, compatibilidad (software-hardware) y seguridad (información y Bases de Datos).

Agradecimientos:

Ovidio Cervantes Lazcano agradece:

Agradezco a mi Madre: Ma. De Lourdes Lazcano Nieto

Por todo su apoyo incondicional para mi formación profesional, por todos sus desvelos y sacrificios. Por que siempre me enseño no importa la forma en que caigas importa la forma en que te levantes y triunfes.

Agradezco a mi Tía: Ma. Del Carmen Patricia Esquivel Nieto

Por todos su apoyo moral, económico y siempre fue incondicional. Para mí es como una 2da. Madre. Siempre estuvo conmigo apoyándome y luchando por que me esforzara a ser mejor día a día.

Agradezco a mi Abuela: Josefina Nieto Tinoco, quien con su sabiduría siempre me supo guiar por el camino del éxito y del trabajo para ser de mi Un hombre de bien.

Agradezco a mi Hermana Ma. De Lourdes Cervantes Lazcano *quien siempre me apoya en los momentos difíciles y sin su apoyo no hubiera lograr concluir mis estudios.*

Agradezco a mi cuñado Salvador Chávez Carmona *quien siempre me da ánimos para seguir adelante y nunca derrotarme. Para mí es como un hermano.*

Agradezco a mis sobrinos: Salvador Manuel Chávez Cervantes, Patricia Desire Chávez Cervantes, Ma. de Lourdes Nancy Chávez Cervantes y el más pequeño Uriel Ramses Chávez Cervantes.

Por que para mí siempre han sido como mis hijos y los he visto crecer desde que nacieron ya que para ellos siempre soy su tío, me quieren y me respetan.

Agradezco a mi Amigo y Hermano: Mario Martínez Reyes *quien siempre ha estado conmigo en las buenas y en las malas, quien me apoya en este proyecto que juntos terminamos y ha crecido conmigo.*

Esta Tesis también la dedico a mi Asesor y sinodales quien sin ellos no hubiera sido posible este Proyecto:

ING. SILVIA VEGA MUYTOY

ING. IMELDA DE LA LUZ FLORES DÍAZ

ING. FERNANDO MARTÍNEZ ITURBE

ING. RICARDO GITIÉRREZ OROZO

M. EN C. DAVID MOISÉS TERÁN PÉREZ

Esta Tesis la dedico en especial a todas esas personas que no creyeron en nosotros y que pensaban que no lo íbamos a lograr. A todas ellas Gracias por que nos motivaron a realizarlo mejor.

AGRADECIMIENTOS

A MIS PADRES:

MARIA DE JESÚS REYES DE MARTÍNEZ

JOSE JAVIER MARTÍNEZ GARCÍA

POR TODO EL APOYO Y AMOR INCONDICIONAL QUE SIEMPRE ME HAN DADO. ADEMAS DE QUE SON UN EJEMPLO A SEGUIR POR SU ENTREGA Y DEDICACIÓN POR EL TRABAJO Y LA FAMILIA. SU SOLA PRESENCIA ES UNA MOTIVACIÓN SUFICIENTE PARA REALIZAR TODOS LOS SUEÑOS QUE TENGO. GRACIAS POR TODO, LOS AMO.

A MIS PADRES ADOPTIVOS:

GRACIELA NAVARRO RAMÍREZ

PEDRO MERCADO CURIEL

PROFRA. ELSA SERRANO CABRERA

PROF. SALVADOR SÁNCHEZ ZAVALA

MARICELA ZAMORA BRIONES

MARIO FLORES

MIGUEL ANGÉL ROMERO DÍAZ

ARACELI MARTÍNEZ GARCÍA

POR QUE SU APOYO, AMOR, AMISTAD Y GUÍA HAN SIDO BASE FUNDAMENTAL Y DETERMINANTE PARA LA FORMACIÓN QUE TENGO Y LOS LOGROS QUE HE ALCANZADO.

A MIS HERMANOS:

JULIO MARTÍNEZ REYES

JAVIER MARTÍNEZ REYES

POR SU APOYO Y EJEMPLO DE QUE NO PODEMOS LIMITARNOS AL ESTÁNDAR DE LO QUE SE PUEDE HACER, SINO LO QUE SE DEBE HACER.

A MI NOVIA:

ROSARIO RUBIO DELGADO

YA QUE SU APOYO Y AMOR HAN SIDO DETERMINANTES EN LA REALIZACIÓN DE VARIOS SUEÑOS.

A MI AMIGO:

OVIDIO CERVANTES LAZCANO

POR LA EXPERIENCIA QUE ME BRINDO Y SOBRE TODO POR DARME LA OPORTUNIDAD DE SER SU AMIGO.

A MIS ASESORES Y PROFESORES:

ING. SILVIA VEGA MUYTOY

ING. IMELDA DE LA LUZ FLORES DÍAZ

ING. FERNANDO MARTÍNEZ ITURBE

ING. RICARDO GITIÉRREZ OROZO

M. EN C. DAVID MOISÉS TERÁN PÉREZ

POR MOSTRARME UNA AMPLIA GAMA DE POSIBILIDADES.

A TODAS LAS PERSONAS ANTES MENCIONADAS LES DOY LAS GRACIAS, POR QUE CON SU EJEMPLO ME HAN ENSEÑADO QUE LA SUPERACIÓN NO ES UNA ESCALERA DE UN SOLO PISO, SI NO QUE ES UN CAMINO INTERMINABLE Y DETERMINANTE EN LA VIDA.

ADEMÁS DE QUE SU PRESENCIA ES MOTIVACIÓN PARA SER UNA PERSONA MEJOR EN TODOS LOS SENTIDOS CADA DÍA.

ATT: MARIO MARTÍNEZ REYES

MCP EN WINDOWS XP

MCSA: SECURITY

MCSA EN WINDOWS 2000 SERVER Y WINDOWS SERVER 2003

" EL SABER Y LA INFORMACIÓN TE HARÁN LIBRE "

MIGRACIÓN E IMPLEMENTACIÓN DE WINDOWS 2000 SERVER EN UNA RED CORPORATIVA

CAPITULO I
REQUERIMIENTOS, INSTALACIÓN Y CONFIGURACIÓN

CAPITULO II
COMPATIBILIDAD Y CONECTIVIDAD CON OTROS SISTEMAS OPERATIVOS

CAPITULO III
SEGURIDAD

CAPITULO IV
ADMINISTRACIÓN, MANTENIMIENTO Y SOPORTE DE LA RED

ANTECEDENTES

La compañía más importante de software a nivel mundial Microsoft, durante el transcurso de los últimos años comenzó a comprender el futuro de los sistemas operativos de red. En las condiciones pasadas los sistemas operativos de red se manipulaban por medio de una larga y difícil lista de comandos para poder interactuar con algún equipo de cómputo en la red, copiar un archivo o un directorio resultaba sumamente complicado y tedioso, solamente existían 2 sistemas operativos en ese mercado como lo eran UNIX (En sus diferentes versiones) y NOVELL NETWORK.

Ambos sistemas abarcaban el mundo de las redes, con el paso de los años los usuarios comenzaron a pedir más y más de cada uno de los sistemas operativos, por lo que se requería que evolucionaran. Microsoft al darse cuenta de lo importante que era un sistema operativo de red con una plataforma mucho más amigable que las demás decidió lanzar un prototipo de sistema operativo gráfico como lo fue el sistema Windows 3.11 para trabajo en grupo, al ir creciendo poco a poco la evolución del software la compañía apostó por nuevas mejoras en cada uno de sus sistemas operativos, al lanzar la versión de Windows 95, la compañía pensó en una mejora de su Sistema Operativo de red, así que se evocó a la tarea de lanzar al mercado el sistema operativo Windows NT 4.0 (Que substituyo al Windows NT 3.51), en versiones como son Windows NT Server 4.0 (versiones para el servidor) y para el usuario final Windows NT workstation 4.0 (Sistema Operativo para una estación de trabajo) este incluía una nueva metodología ya que fue programado en su totalidad en lenguaje C, este sistema permitía un control más claro de la red creando dominios, grupos y relaciones de confianza, la herencia de permisos y demás, ayudaron a aportar una amplia gama de beneficios en la administración de la red.

Con el paso de los años las compañías de equipos PC decidieron apostar hacia una tecnología que se venía manejando en los equipos maquintosh como lo eran los famosos puertos USB (Universal Serial Bus, Puerto Serial Universal), dichos puertos permitían un traslado de datos sin ocupar una dirección lógica ni una interrupción del sistema, dichos puertos lograban conectar a las PC, escáner, cámaras de video, impresoras y un sin fin de dispositivos de una manera rápida y concisa, Microsoft experimento la compatibilidad de dicho hardware en su sistema operativo de hogar Windows 95 segunda edición, en donde contenía el software para dicho dispositivo. Bastaba con conectar el dispositivo y el equipo lo reconocía al instante y solicitaba el driver de instalación y lo instalaba sin necesidad de reiniciar el equipo, dicha mejora se vio más acentuada en Windows 98 y ME. Pero las estaciones de trabajo con NT y Servidores no contenían dicha característica, se comenzaron a detectar fallas en NT e incompatibilidad (Como una tan clara como lo son los dispositivos USB).

Al instalar una tarjeta de red en NT resultaba un poco fastidioso ya que no se sabía con exactitud el puerto de entrada y salida al que se conectaba ni la interrupción, pues no contenía una herramienta como el administrador de dispositivos de Windows 95 y 98, el administrador de red tenía que mover las tarjetas PCI e ISA las veces que fueran necesarias para poder dar de alta alguna tarjeta y que no entrara en conflicto con algún dispositivo del sistema que ocupara la misma entrada, salida e interrupción.

Microsoft comenzó a darse cuenta de las ventajas que tendría unificar un sistema operativo de red y un sistema operativo casero, sería el sistema operativo ideal pudiéndose crear un sin fin de mejoras tanto para el usuario como para el administrador de la red.

La evolución que poco a poco empezo a tener la industria de Internet en el mercado mundial comenzó a poner a Microsoft a la vanguardia, ya que esta ha sido una de las compañías que más ha estado interesada en el uso y desarrollo de Internet a nivel mundial.

Cada día más usuarios deseaban poder estar navegando en Internet y crear sus hojas web, así como diseñar sus propias cuentas de correo electrónico para poder tener una transferencia de información más eficaz en tiempo real, no importando la parte del mundo donde uno se pueda ubicar, comenzaron entonces a surgir problemas con NT pues no había logrado tal evolución y se tenia que contar con software de terceras personas para poder explotar la herramienta de Internet.

Conforme pasaba el tiempo la gente comenzó a darse cuenta que un sistema operativo con una plataforma gráfica podría ser mucho más fácil de aprender que unos 100 comandos y no poder solucionar sus problemas, los fabricantes de hardware comenzaron a apostar hacia los sistemas operativos de Microsoft que resultaban ser más amigables a los usuarios finales y en su idioma.

CONDICIONES ACTUALES DEL SISTEMA

En la actualidad NT a demostrado tener un sin fin de errores en sus características de seguridad, creación de usuarios y permisos, el sistema NO es compatible con sistemas USB y en ciertos casos carece de las herramientas claves de uso.

Los usuarios de Windows NT poco a poco comenzaron a exigir más y más a este sistema y también a darse cuenta de las fallas en las que se podía caer (Vuelos de memoria, Pantallas azules con errores y Equipos pasmados).

La seguridad no es su punto fuerte, por lo que comenzaron a surgir a nivel mundial más y más notificaciones de ataques de hackers a varios servidores y redes.

Esta tesis esta basada en una compañía de telefonía celular, dicha empresa utiliza Windows NT Server 4.0 en sus servidores y en sus estaciones de trabajo Windows NT Workstation en su mayoría y la otra parte de los equipos utiliza Windows 95 y Windows 98.

La empresa a comenzado a notar problemas en sus sistemas operativos, los servidores tienen muchas limitaciones de seguridad y resulta complicado configurar algún servicio o recurso, constantemente los servidores sufren de pantallas azules (volcados de memoria) quedan pasmados y es necesario reiniciarlos.

Las estaciones de trabajo con Windows NT Workstation no son compatibles con dispositivos USB, no se puede tener una administración de los dispositivos como con Windows 95 y 98.

En estaciones de trabajo con Windows 95 y 98 resulta sumamente complicado el poder compartir recursos en red, si uno desea accesar a una carpeta compartida de más de 8 o 9 caracteres como titulo no se visualiza la carpeta y hay que buscar el equipo por medio de la dirección IP y no por el nombre del equipo.

Los controladores de impresión de la impresora 4050N y 4050TN resultan sumamente dificiles de que Windows NT los reconozca y sean compatibles con la aplicación que se tiene en la empresa llamada Citrix, ya que si se selecciona dicho driver si permite poder imprimir en red en aplicaciones locales, pero no en las aplicaciones de Citrix por la red.

Con Windows NT Workstation los equipos comienzan a mandar pantallas azules como en los servidores y en algunos casos es necesario volver a instalar todo el sistema operativo del equipo, lo cual provoca un atraso de tiempo para los ingenieros de sitio y el usuario de entre 24 a 48 horas en repararse.

Como Windows 95 y 98 no tiene un visor de sucesos efectivo que permita indicar al usuario si algún intruso esta accesando a alguna de sus carpetas de red. En esta empresa se han reportado muchos usuarios que les gusta conectarse a diferentes equipos para poder visualizar información que no es la suya.

En algunos casos resulta sumamente complicado poder ingresar un equipo al dominio en NT porque no sólo se configura el dominio y demás, sino que en algunos casos es necesario darle al equipo una dirección IP fija y no por DHCP como se debería de hacer.

EXPERIENCIA PERSONAL

A lo largo de 6 años, logramos tener experiencia con sistemas operativos de Microsoft desde la versión 6.22, Windows 3.1, 3.11, 95, 98, ME, NT, XP y Windows 2000, laboramos en las áreas de soporte técnico y call center para diferentes empresas, tuvimos la oportunidad de estar en una de las empresas de telefonía celular a nivel nacional y logramos captar los avances que se obtuvieron al migrar su red de NT a Windows 2000.

En este proyecto de tesis daremos los pros y contras de migrar una red Windows NT a una red Windows 2000. Con apoyo de diferentes autores, así como de varias direcciones de Internet y nuestra experiencia personal.

CAPITULO 1
REQUERIMIENTOS, INSTALACIÓN Y CONFIGURACIÓN.

1.1 REQUERIMIENTOS DEL SISTEMA

Los requerimientos mínimos del equipo para migrarlo a Windows 2000 son los siguientes:

1.- Procesador Pentium a 166 MHZ o superior (Se admiten múltiples procesadores, se incluyen los procesadores Pentium II, Pentium III, Pentium IV y Xeon, y los procesadores equivalentes como son Citrix y AMD.

2.- 64 MB de RAM como mínimo, se recomienda 128 MB, 8 GB como máximo para la versión Advanced Server y 4 GB para la versión server.

3.- Espacio en Disco Duro 850MB para la instalación más el doble de memoria RAM que tenga el equipo, Por ejemplo si el sistema tiene 128 MB de RAM, necesitaría 1.106MB (850MB+256). Si es una instalación de red en vez de una instalación de CD-ROM, deben incluir otros 200 MB para los archivos de instalación temporales. Si es una actualización de un controlador de dominio y se esta distribuyendo al mismo tiempo Active Directory, asegurarse de disponer de mucho más espacio en disco porque el proceso de actualización utiliza hasta 10 veces más espacio que la base de datos de cuentas de usuarios.

4.- 1 monitor VGA

5.- 1 Teclado

6.- Un ratón o cualquier otro dispositivo de apuntar, es opcional, pero sin un ratón o puntero será más difícil trabajar.

7.- Para una instalación desde el CD-ROM, una unidad de 12X como mínimo, y una unidad de 3 ½, a menos que el sistema sea capaz de iniciar desde CD-ROM

8.- Para la instalación de red, una tarjeta de red compatible con Windows 2000 que se encuentre en la lista de hardware, así como una copia de Windows 2000 en un servidor en alguna parte donde se realizará la instalación.

1.2 COMPATIBILIDAD

Quizá la documentación más importante de Windows 2000 sea la lista de compatibilidad de Hardware. Esta es la lista de todo el hardware compatible con Windows 2000. Es la lista de los sistemas, las tarjetas de red, los controladores de disco, impresoras y otros dispositivos, la dirección es http://www.microsoft.com/hwtest/hcl/

Es recomendable que los controladores de red, audio, vídeo y sonido del equipo tengan los controladores compatibles con Windows 2000, evitando así perdidas de información y de tiempo antes de migrar algún equipo a la nueva versión, en caso de no poseerlos verificar con el fabricante si cuenta con dichos controladores.

1.3 INFRAESTRUCTURA

La red de la compañía celular de que se habla es una WAN ya que posee una cobertura en el ámbito nacional muy grande, consta de los siguientes puntos en la República Mexicana: 2 puntos centrales en el D.F. uno se encuentra ubicado en el edificio corporativo que se encuentra al centro de la ciudad de México y el megacentro que se encuentra ubicado en Tlalnepantla a las orillas del D.F., posee otros puntos como son: Celaya, Irapuato, Tijuana, Querétaro, Guadalajara, Monterrey, León, Puebla, Acapulco y Toluca (ver la figura 1.1).

Se comunican a estos puntos vía satelite por medio de un enlace de microondas y cada punto posee un servidor principal que replica o se comunica con cada uno de los servidores y con el PDC (Servidor Principal de Dominio) y el BDC (Servidor Secundario de Dominio), ambos se encuentran ubicados en el Megacentro de Tlalnepantla. Todos los edificios se encuentran cableados con cable par trenzado nivel 5 y conectados a varios switches de la marca CISCO. El edificio de Tlalnepantla posee cableado en su SAE (Sala Principal de operaciones donde se concentran todos los servidores) de fibra óptica. El tipo de enlace que se utiliza en la red es un E1.

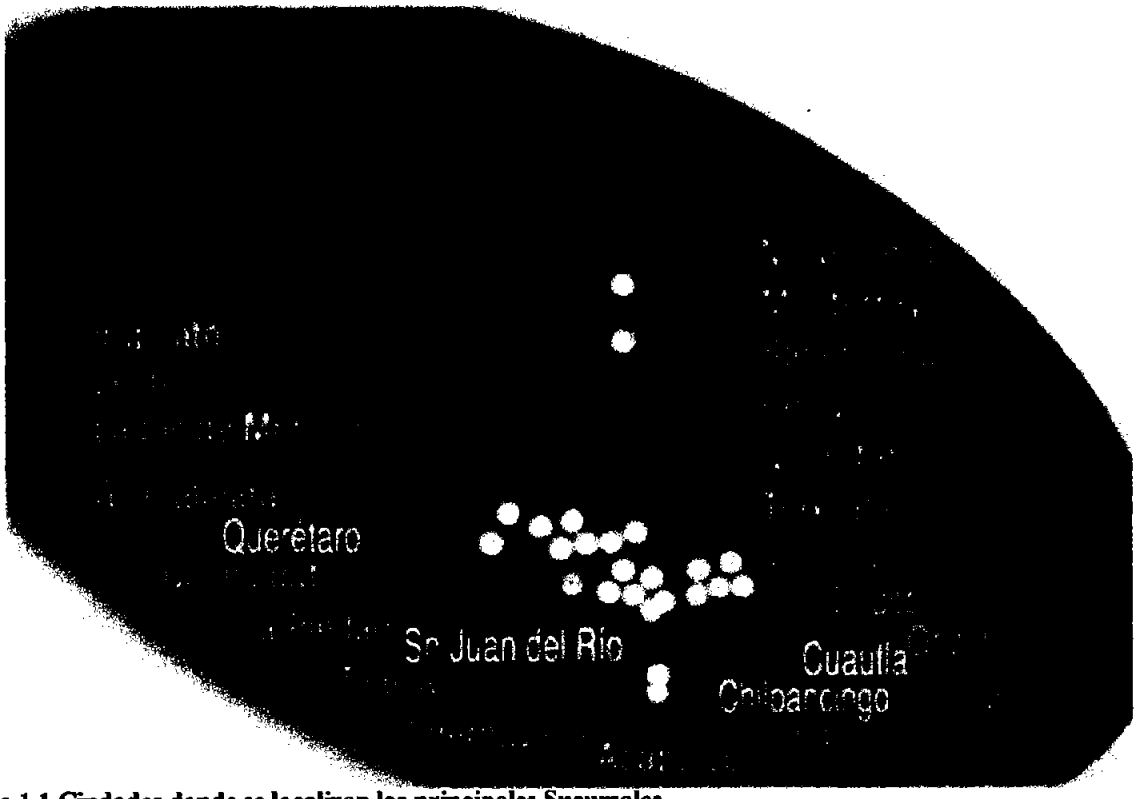


Figura 1.1 Ciudades donde se localizan las principales Sucursales.

1.4 ACTUALIZACIÓN A WINDOWS 2000

Para realizar la actualización a Windows 2000 se puede llevar a cabo desde sistemas operativos Windows 95, Windows 98 o en Windows NT, puede instalarse desde un disco de 3 ½ o una unidad de CD ROM, lo mejor es colocar el CD ROM en la unidad y reinicia el equipo. El CD ROM iniciará Windows 2000 y comenzará el proceso de instalación.

Para la instalación desde disco local o un disco remoto, ejecutar WINNT.EXE desde Windows 95, Windows 98 o Windows NT, o ejecutar WINNT.EXE desde el símbolo del sistema. De esta forma se crea una copia de seguridad en el sistema de los archivos con que se inicia desde el CD ROM; a continuación el sistema se reiniciará y comenzará la instalación en el mismo punto como si el CD-ROM se hubiera iniciado al principio. Una nota muy importante es que la partición del sistema debe de existir antes de poder instalar Windows 2000.

Básicamente, el programa WINNT copia todos los archivos al disco, y estos no se pueden quitar durante la instalación, por lo que el sistema no puede volver a dividir los discos duros durante la instalación si se ha iniciado esta utilizando WINNT.

El proceso de inicio de Windows 2000 tiene que averiguar que clase de medios de discos está disponible para la instalación. Básicamente, se examina la máquina y busca todos los adaptadores IDE y SCSI del sistema. Si estaban disponibles éstos de la máquina cuando salió al mercado Windows 2000, no abra ningún problema, y el sistema detectará el adaptador SCSI y se reiniciará. En caso contrario, puede que necesite un disco del fabricante de hardware para cargar los controladores. Justo al principio del proceso se debe de pulsar la tecla F6 para instalar un adaptador de otro fabricante. Sino se carga el adaptador desde los medios de instalación de Windows 2000, debe de utilizar obligatoriamente esta opción para configurar los controladores necesarios y complementar el proceso de inicio.

Si no es posible iniciar Windows 2000, la instalación finalizara con un mensaje INNACCESIBLE_BOOT_DEVICE (dispositivo de booteo inaccesible). Este mensaje aparece cuando no se puede iniciar Windows 2000 desde la partición que se ha configurado para iniciar.

Si ya existe un sistema operativo, aparece la pregunta si la instalación deberá ser nueva o una actualización de la versión anterior.

Posteriormente aparecerá un acuerdo de la licencia debe de aceptarse en caso contrario se suspende la instalación (En esta licencia aparecerán los términos de Microsoft sobre el uso de sus productos hacia los usuarios).

Para una instalación nueva (En caso de que no existiese un sistema operativo) pedirá que se cree en el disco una partición nueva con la capacidad que se desee. Señalar con las flechas y presionar la letra C creará una nueva partición y con seleccionar la partición y con la letra D, se podrá eliminar la partición que se elija (ver la figura 1.2).

Figura 1.2 El programa de instalación debe saber donde instalar el sistema operativo. En este caso, sólo hay un disco, así que se pulsa la tecla C para crear una partición.

Después de elegir la partición el sistema iniciará la fase de instalación en donde comenzará a copiar archivos hacia el disco duro en el directorio de Windows 2000 C:\Winnt (ver la figura 1.3). Al terminar de copiar los archivos el sistema se reiniciará y comenzará la fase de instalación de archivos.

Figura 1.3 Aparece la pantalla de copia de archivos cuando el sistema copia en el disco los archivos necesarios para ejecutar Windows 2000.

Durante la actualización del sistema Windows NT, se eliminará la mayor parte de la instalación de Windows NT, por lo menos con respecto a los archivos del sistema y los reemplazara por archivos de Windows 2000, La actualización conservará la configuración del usuario y del sistema así como el registro de las aplicaciones, de modo que no es necesario volver a instalar las aplicaciones después de la instalación.

Hay que tener en cuenta que Windows 2000 no utiliza los mismos controladores que Windows NT por lo que es posible que algunos controladores de sonido, vídeo e impresión que funcionaban en NT no lleguen a funcionar en Windows 2000. El mismo criterio se utiliza para Windows 98 y 95.

1.5 INSTALACIÓN DE WINDOWS 2000

Después de que se copio Windows 2000 en el disco duro y se reinicio el sistema comenzará la parte de configuración de Windows 2000, en esta parte Windows 2000 comenzará a buscar y detectar todos los dispositivos del equipo, si los controladores de los dispositivos los tiene Windows 2000 los instalara y continuara con el proceso de configuración. Este proceso es el más largo ya que puede durar entre 15 minutos y media hora en instalar el sistema operativo en el equipo. El sistema parpadeara varias veces mientras el sistema examina la clase de hardware de vídeo que existe. El sistema se detendrá unos minuto mientras examina los puertos seriales del sistema.

Si el sistema se queda bloqueado, sin actividad de mouse ni de teclado por un periodo mayor a 15 minutos será necesario reiniciar el equipo, esto puede ser porque algún dispositivo esta en conflicto o no se tiene el driver adecuado. A continuación el sistema le pedirá la configuración regional de instalación y la clase de teclado que utilizará, la siguiente pantalla pedirá ciertos datos sobre a nombre de quien se registrara la licencia (nombre del usuario y organización), posteriormente deberá introducir el nombre del administrador local y la contraseña debiendo de recordar que debe ser un nombre fácil de recordar para evitar futuras catástrofes. Después solicitará el nombre de la máquina y el dominio o grupo de trabajo al que pertenecerá dicho equipo, Posteriormente solicitara si se desea instalar algún componente opcional como: accesorios y utilerías, comunicaciones, juegos, multimedia, servicios de Certificate Server, servicios de Cluster Server, servicios de Internet Information Services y demás servicios.

El siguiente paso es el proceso de configuración de la red. La nueva configuración predeterminada de Windows 2000 incluye servicios simples de TCP/IP, Compartir impresoras y archivos para redes Microsoft y el cliente para redes Microsoft (ver la figura 1.4). Para seleccionar los componentes que se necesiten es necesario escoger la opción de configuración personalizada, en donde se pueden elegir a gusto cada uno de los servicios de red que se requieren.

Una vez seleccionada toda la información de red, hacer clic en siguiente y el servidor pedirá que se especifique que papel desempeña el equipo en el esquema general de la red, un servidor puede ser un servidor independiente o pertenecer a un dominio (ver la figura 1.5). Si el servidor no se encuentra en ningún dominio o si no hay una red elegir la opción de no y continuar el proceso (esto es con el fin de evitar conflictos en la configuración del equipo).

Cuando se termine de configurar la red, Windows 2000 configurara el resto del sistema operativo. Esto implica principalmente la necesidad de instalar componentes en el registro y quitar los archivos temporales.

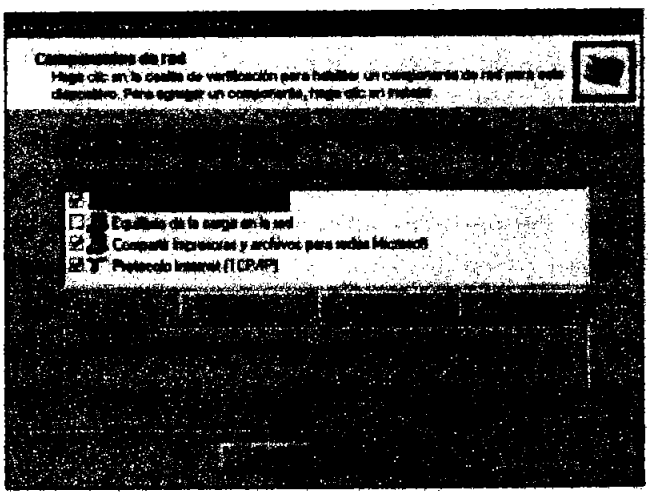


Figura 1.4 Así es como se establece la configuración de la red durante la instalación. Hacer clic en el botón Instalar para agregar componentes.

1.6 CONFIGURACIÓN DE LA RED

Después de que la instalación de Windows 2000 complete el proceso de copia de archivos en modo texto, reiniciará el sistema y comenzará la fase de configuración.

Para esta parte del proceso es necesario ingresar al equipo que se le esta instalando Windows 2000 (Para la terminal de trabajo Windows 2000 Profesional y para un servidor Windows 2000 Advanced Server) y verificar que se esté validando correctamente en el dominio de la red a la que pertenece . Esto se logra ingresando con el nombre de usuario y contraseña con la que un usuario ingresaba anteriormente. Windows 2000 configura el equipo para que se valide en la red y permita poder realizar las mismas tareas que el usuario venía realizando anteriormente.

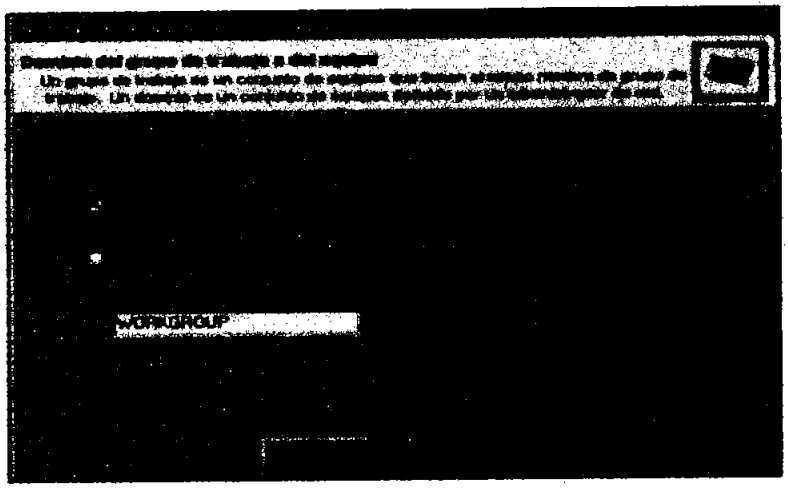


Figura 1.5 Este cuadro de diálogo le permite decidir si el equipo formará parte de un dominio y seleccionar el dominio que utilizará.

Para checar en el equipo que se esté validando en la red, se debe de ver dentro del icono de Entorno de Red (Dando 2 clics sobre el) donde se pueden ver todos los dominios de las redes disponibles, en caso de que no se vieran es necesario checar la configuración de red, esto se logra verificando en las propiedades de red que se tengan instalados los siguientes servicios:

*Cliente para redes Microsoft
*Protocolo TCP/IP (La dirección IP debe de ser proporcionada por DHCP que da una IP aleatoria y no fija)
*Compartir Impresoras y Archivos para redes Microsoft

También en la parte de hardware es necesario revisar con la herramienta Administrador de dispositivos que la tarjeta de red se encuentra activada y sin ningún conflicto, por otro lado es necesario verificar que el cableado tipo 5 par trenzado tenga continuidad y verificar que el nodo que este conectado al equipo se encuentre activo.

1.7 MIGRACIÓN DE SISTEMAS EXISTENTES

Las aplicaciones que se migraron junto con el sistema operativo de cada equipo son pequeñas bases de datos realizados en la plataforma de Oracle las cuales fueron migradas sin ningún problema, en estas bases de datos se consulta el estatus de los radios, cancelaciones, facturaciones, ordenes de reparación, bajas y altas de servicios, roaming nacional e internacional y demás. Estas aplicaciones se migraron sin ningún problema, junto con la suite de aplicaciones de Microsoft Office 97 o 2000 (Según el que tenga instalado el usuario en su equipo de computo). No presentaron falla y la migración fue transparente en todos los sentidos.

Estas pequeñas bases de datos se comunican con servidores que corren con sistemas operativos UNIX y algunos con NOVELL que más tarde se explicara en otros capítulos.

1.8 ACTIVE DIRECTORY

El sistema Active Directory es probablemente la más importante de las nuevas características de Windows 2000. Integra toda la administración de cuentas de usuario y agrupa los datos en bases de datos no centralizados. Además Active Directory se integra con Microsoft Exchange (aplicación para poder administrar el correo electrónico), esto ayuda a eliminar la duplicación del esfuerzo entre la administración de las listas de distribución de correo electrónico y los grupos de seguridad que tienden a solaparse mucho.

Windows NT utiliza un modelo de replicación de dominio principal, lo que significa que un servidor desempeña todas las tareas de replicación de la información de seguridad del usuario para todos los servidores en la red que puedan manejar inicios de sesión. Con Active Directory no existe un controlador principal, todos los servidores son igualmente capaces de almacenar y realizar cambios.

Esto permite al sistema ser más escalable porque un servidor no tiene que servir de punto central para distribuir los cambios. También permite mayor migración tras error y cambios de configuración más fáciles, porque cualquier servidor puede ser un controlador de dominio y cualquier controlador de dominio se puede volver a convertir en un servidor sencillo.

Microsoft decidió diseñar Active Directory (Directorio Activo) e implementarlo en Windows 2000 como una de las partes fuertes en la mejora de seguridad de dicho sistema operativo, El Directorio Activo es el componente insignia llamado a solucionar los problemas de escalabilidad, extensibilidad, administración y grado de apertura del directorio de NT 4.0. Este no podía satisfacer las necesidades de grandes organizaciones dada su limitación de 20,000 usuarios por dominio y el hecho de que la replica entre el servidor primario (PDC) y el servidor secundario (BDC) era de tipo uno a varios. En Windows 2000, un dominio de Active Directory (AD) puede contener más de un millón de objetos y, en la mayoría de los casos, no necesita de un PDC. Los cambios que ocurren con cualquier controlador de dominio se propagan hacia el resto. Es posible configurar a medida esta replica multimaestro para ajustar el rendimiento y el consumo de ancho de banda en organizaciones con gran dispersión geográfica. Para conseguirlo es posible crear un nuevo objeto llamado NT denominado Sede (Site), que se relaciona con las subredes IP, las sedes permiten poder superar los dominios (que suelen definirse en base a criterios organizativos) de las divisiones geográficas.

La administración es mucho más potente con el AD. Para empezar, ahora es posible organizar los equipos y los usuarios en una jerarquía que replique la verdadera estructura organizativa de la empresa. Dentro de un dominio las unidades organizativas (OU) son las que proporcionan dicha estructura. Los Dominios han dejado de estar en un sólo nivel, ya que ahora pueden tener dominios Padre e Hijos (exceptuando el dominio Raíz, que carece de dominio padre). También es posible asignar privilegios de administración individuales en cualquier nivel.

Windows 2000 da solución a muchos problemas de seguridad de versiones anteriores. Con una configuración de red adecuada Windows 2000 no enviará contraseñas cifradas a la red si no que usará en su lugar la autentificación Kerberos, que utiliza un sistema de desafió-respuesta que no requiere enviar al servidor una contraseña.

1.9 CONTROL DE USUARIOS

El control de los usuarios se puede llevar de una manera amigable con la herramienta que proporciona Windows 2000 que se llama MMC (Microsoft Management Console-consola de administración de Microsoft), por medio de esta herramienta se puede controlar la administración de los usuarios, la administración de discos, los servicios de inicio y detención.

Las cuentas de cada uno de los usuarios tienen diferentes características y al momento de ingresar a la red le otorga el acceso a ciertos recursos de la misma, únicamente el administrador posee los recursos para poder administrar la red en su totalidad, cada una de las cuentas posee ciertos atributos (ver la figura 1.6).

Con la herramienta MMC es fácil administrar el acceso de los usuarios a los recursos correspondientes, por lo que es necesario tener una buena planeación y a una nueva cuenta que se ha creado otorgarle los recursos que necesita, Por ejemplo si tiene al usuario Juan Pérez su cuenta es jperez, se le debe de agregar al grupo de trabajo de vendedores ya que el esta laborando en el área de ventas teniendo acceso a ciertas carpetas que están en el servidor primario y utiliza la impresora 3 que esta en el piso donde el desempeña sus actividades, la gente de este grupo no tiene servicio de Internet.

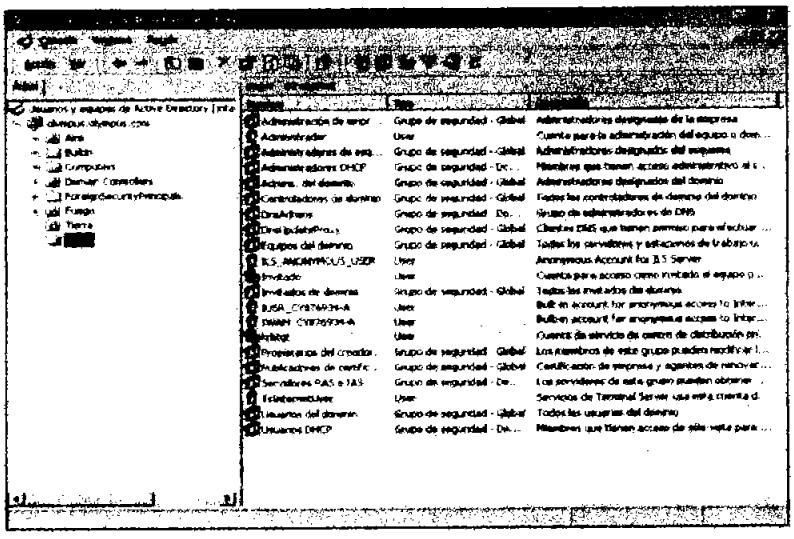


Figura 1.6 Un listado de las cuentas predeterminadas de usuario y grupo.

Cada grupo que se encontraba ya establecido desde Windows NT posee ciertas características y una cuenta puede ser integrada a varios grupos según el perfil de los usuarios, de esta manera se logra una mejora en la seguridad además de que se permite una organización jerárquica entre los usuarios.

Entre los diferentes grupos que se encuentran ya preestablecidos desde Windows NT 4.0 se encuentran los siguientes:

Grupo de Administradores.- Controlan toda la red y pueden hacer uso de carpetas e información que requieran de cualquier servidor así como también poder ver cualquier información de cualquier equipo en la red, así como poder administrar, como su nombre lo indica administran cualquier equipo en la misma, así como también pueden administrar cualquier impresora, posee acceso total a Internet y a cualquier recurso de la red.

Grupo de Help Desk.- Personal de Soporte Técnico, poseen algunos permisos de impresión y depuración de ciertas impresoras, poseen acceso a Internet y pueden dar de alta equipos en el dominio de la red, no pueden accesar a los servidores, ni poseen permisos de administración en equipos de la red.

Grupo de Gerentes.- Personas que desempeñan el puesto de gerencia, poseen permisos para imprimir en las impresoras que necesiten, tienen permisos de lectura y escritura en algunas carpetas de servidores, pueden consultar información de ciertos equipos y poseen permisos de Internet.

Grupo de Facturación.- Poseen permisos únicamente de impresión en equipos de su área, no tiene acceso a Internet, y sólo tienen permisos de lectura en algunos servidores.

Grupo de Producción.- Poseen permisos de impresión únicamente a 2 impresoras de su área, tiene acceso a un servidor con permisos de lectura y escritura en una carpeta determinada, no tienen acceso a Internet.

Grupo de Ventas.- Posen permisos de Impresión únicamente a las impresoras asignadas a su area, no tienen permisos de Internet y sólo tiene permisos de lectura en una carpeta de un servidor.

Grupo de Atención a Clientes.- Poseen permisos de lectura en un servidor y de escritura en otro, No tienen acceso más que a una impresora de su área y no pueden accesar a Internet.

Debe de tenerse cuidado que cada usuario este asignado al grupo que le corresponde y no a uno que no lo es, por ejemplo un vendedor no debe de estar en el Grupo Gerentes porque tendrá acceso al servicio de Internet, así como al uso de impresoras que no están ubicados en su área de trabajo ni de carpetas que estén en otros servidores.

A usuarios del área de Facturación y Producción que sus equipos cuentan con Windows 95 o 98 se asignó una política para que sólo pudieran ingresar a sus equipos en su turno correspondiente, con la ayuda de MMC se logro ver en las propiedades del usuario la asignación de un horario de trabajo para que no realice un mal uso de su cuenta de red o trate alguna persona de su área ingresar con su cuenta en un horario que no le corresponde.

Ya se tienen preestablecidas políticas y procedimientos en el área de Sistemas para llevar un control de los usuarios, de otra manera el uso de la red se vería manejado en una forma arbitraria y poco considerable (ver la figura 1.7).

Si algún usuario se encuentra realizando un uso indebido de su clave de la red para dañar un equipo propio o alguno que se localice en la red, inmediatamente la clave de red será deshabilitada para evitar que llegue a dañar algún equipo en la red y será habilitada únicamente si el jefe inmediato lo autoriza y se hace responsable del uso adecuado de dicha clave.

Cuando un usuario va a ingresar a la compañía se le crea su clave de red de manera apropiada a su perfil, y si ese usuario causa baja se avisa a el área de Sistemas para que dicha clave sea eliminada evitándose así desastres y malos usos.

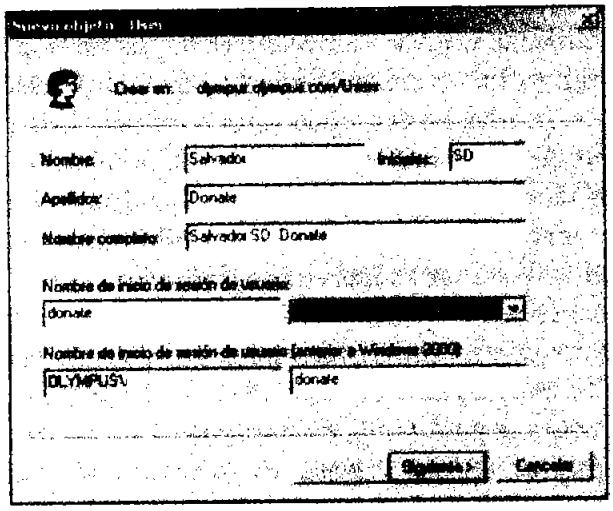


Figura 1.7 Pantalla de creación de usuarios.

1.10 IMPRESIÓN

Windows 2000 y todos los demás sistemas operativos de Windows, utilizan un concepto de microcontrolador para crear controladores de dispositivos, básicamente el sistema operativo proporciona aplicaciones con todos los aspectos básicos de cómo hacer de interfaz con ciertos tipos de dispositivos y a continuación, necesita que un controlador implemente características muy específicas para realizar estas operaciones.

Se utilizan varios métodos distintos para poder comunicarse con las impresoras. Incluyendo el uso de los puertos paralelos, serie, USB, E/S directa de archivo, conexiones de red de Windows 2000, puertos de impresión TCP/IP y puertos LPR.

La mayoría de impresoras que se manejan en esta red son las siguientes: impresora HP Láser jet modelos 4000, 4000tn, 4050tn, 5000, 2100, 5si, los modelos de inyección de tinta que se utilizan son los siguientes: HP Deskjet 610c, 660C, 2100C y Epson 9000.

Al haber migrado los sistemas operativos a Windows 2000 se noto una gran mejora en la impresión ya que los drivers con Windows NT no son muy compatibles con las impresoras 4000 o 4050x, al migrar los equipos a Windows 2000 el servidor de impresión asigno el driver que trae de fábrica y evito muchos problemas de impresión con aplicaciones como Office 97 o 2000, ya que en ocasiones la vista previa marcaba una hoja bien delineada para imprimirla en Excel o Word pero al momento de imprimirla ocupaba más tamaño que el que nos había mostrado la vista previa lo cual provocaba que la impresión saliera entrecortada en 2 hojas o más, siendo que se había mostrado en una sola hoja de la vista previa.

El servidor de impresión no sólo trae sus drivers compatibles con cualquier sistema operativo Microsoft, si no que también permite agregar los driver que nosotros necesitemos o se actualice desde Internet en la página del fabricante de la impresora o desde el sitio de Microsoft (ver la figura 1.8).

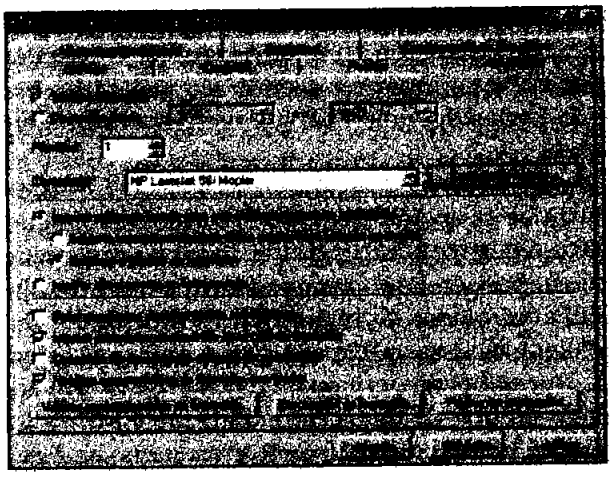


Figura 1.8 La ficha Avanzadas de la página de Propiedades de la Impresora muestra las opciones de configuración predeterminadas.

Las impresoras Deskjet en sistemas NT presentaron ciertas fallas con el driver, su impresión es difícil de conseguir y además no siempre se logra que la impresora imprima si se encuentra instalada desde un servidor de impresión o si encuentra compartida a muchos usuarios. Con Windows 2000 busca el driver y lo instala lo cual facilita la impresión y permite poderse compartir los recursos a muchos usuarios sin tener que batallar en localizar el driver.

Para que Windows 2000 utilice una impresora es necesario crear una cola de impresión. Una cola de impresión es una estructura que contiene las tareas de impresión justo antes de que vayan al papel. Es un modo de hacer que las tareas esperen en línea antes de pasar a la cola de impresión (ver la figura 1.9). Una cola de impresión puede enviar la salida a una o más impresoras. Todo el grupo de impresoras debe de ser idéntico o como mínimo, que todas utilicen los mismos controladores. El hecho de agregar más impresoras implica que los trabajos se puedan procesar más rápidamente y un posible trabajo grande no impedirá que se impriman las tareas de una sola página. Se aconseja que todas las impresoras que compartan una misma cola de impresión estén ubicadas en el mismo lugar, de modo que todos los usuarios sepan donde recoger la salida impresa. También se recomienda disponer de gran cantidad de consumibles de repuesto en esta área, ya que si los usuarios desean imprimir gran cantidad de páginas, el toner se gastara rápidamente.

Para las impresoras locales, las colas de impresión son locales, Para una impresora de red, las colas se crean en un servidor y las tareas se envían a la red. Una tarea se envía a una cola y, posteriormente, se envía desde la cola de impresión a la impresora.

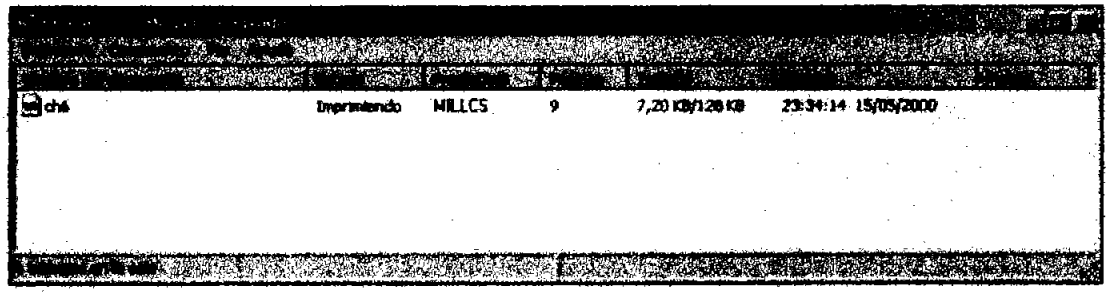


Figura 1.9 Ésta es una vista de una cola de impresión a una impresora en el servidor MILLICS con un documento, esperando que se imprima.

El administrador de impresión es la herramienta que se utiliza para administrar documentos dentro de una cola de impresión. Esto significa que pueden ver el estado de las tareas en la cola de impresión, y si el usuario tiene los permisos adecuados cambiar el orden de los objetos en la cola de impresión e incluso quitar tareas de la cola de impresión.

Una de las fallas más comunes a las que nos enfrentamos a diario es que existen usuarios que comenzaban a mandar a imprimir documentos muy grandes en las impresoras láser jet 4050 o 4000, al mandar tantos documentos comenzaban a saturar la cola de impresión de manera tal que si un usuario mandaba un documento nunca salía y se desesperaba y lo volvía a enviar 3 o 4 veces, esto sucedida junto con los usuarios que hacían el uso de la impresora, lo que provocaba que ésta se saturará. Se tenía que eliminar el documento que se encontraba atorando el documento en la cola de impresión y al poco rato se restablecía la impresión, para solucionar este problema se recomienda al usuario enviar su documento en pequeños bloques o enviarlo por completo en horarios donde no tenga mucha demanda la impresora o se le instala otra que estuviera cerca de su área y que no tuviera tanta demanda de impresión.

Figura 1.10 La ficha Compartir de un cuadro de diálogo Propiedades de la impresora.

Otra posible falla a la que nos enfrentamos es que en las impresoras Deskjet 660 o 600 que se tenían disponibles instaladas en equipos con Windows NT Workstation para algunos supervisores y gerentes no permitían poder compartir esta impresora en red con sus compañeros en red, al momento de mandar a imprimir desde otro equipo mencionaba un error indicando que la cola de impresión tuvo una falla o avería ya que no se detectaba la impresora activa, al migrar dichos equipos a Windows 2000 profesional, la falla no volvió a presentarse (ver la figura 1.10).

Windows 2000 posee drivers más actualizados que las versiones anteriores como NT o 3.11, también cuenta con una opción en agregar para poder agregar más drivers de impresión actualizados y poder utilizarlos en el servidor de impresión.

1.11 PROTOCOLOS

Un protocolo es aquel elemento que nos permite poder dar una descripción formal de los mensajes y reglas para que una máquina se pueda comunicar dentro de una red con otros equipos.

Windows 2000 admite la mayoría de los protocolos de comunicación estándar de la industria dentro de los cuales los más utilizados en una red son los siguientes:

TCP/IP (*TRANSMISION CONTROL PROTOCOL / INTERNET PROTOCOL*).- Protocolo de control de transmisión /Protocolo de Internet, creado por el departamento de defensa de los E.U. para las comunicaciones LAN /WAN sobre Arpanet.

IPX/SPX (*INTERNET PACKET EXCHANGE / SEQUENTIAL PACKET EXCHANGE*).- Protocolo de Intercambio de paquetes /Intercambio de paquetes secuenciados, creado por NOVELL para NETWARE.

NetBEUI.- Fue el primer intento de IBM y Microsoft de crear un protocolo para LAN basado en NetBIOS (Network Basic Input / Output System) Sistema básico de entrada y salida de red.

DLC (Data Link Control).- Control de Vínculos de Datos, creado por HP.

Apple Talk.- Protocolo Creado por la compañía Apple para permitir comunicaciones entre los equipos maquintosh y los periféricos de Apple.

Cualquiera de los protocolos de red se puede agregar desde el Panel de control, conexiones de red y acceso telefónico, en esa parte se selecciona Mis Sitios de Red, se eligen propiedades y se selecciona agregar y se marca el Protocolo de red (ver la figura 1.11) y seleccionamos el que sea de nuestro agrado, otra de las ventajas que posee Windows 2000 es la siguiente: Permite poder agregar y quitar protocolos mientras el servidor sigue funcionando. Esto no puede parecer de gran éxito pero cuando una migración o una transferencia requiere un cambio temporal de protocolos es muy útil ya que acorta el tiempo, La tecnología de agregar, detener o quitar protocolos mientras el servidor esta en ejecución es de gran ayuda a la hora de solucionar los problemas.

Es muy difícil un asunto de comunicaciones si se tiene que reiniciar el sistema cada vez que se agrega o cambia un Protocolo. Si el servidor esta ejecutando cualquier clase de aplicación grande, puede ser casi imposible. Una máquina con Exchange o SQL Server puede tardar casi una hora en reiniciarse.

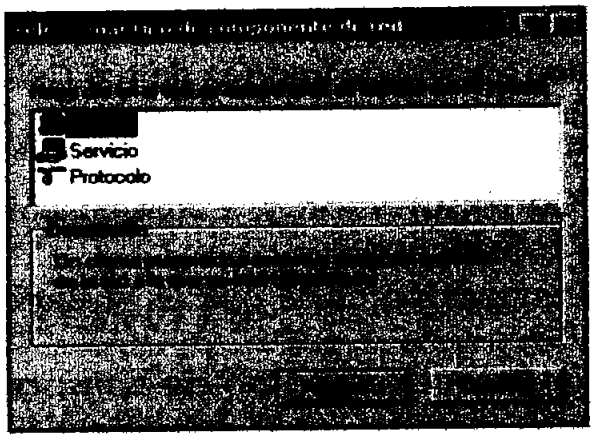


Figura 1.11 Cuadro de diálogo Seleccionar tipo de componente de red.

Los protocolos con los que más se trabajan es TCP/IP en los equipos que se van a ingresar a la red de la compañía de Telefonía, y activando la opción de DHCP puede asignar una IP aleatoria a un equipo, aunque en la red existen equipos como los servidores, enrutadores y switches que debe de poseer una dirección IP fija y no aleatoria.

Una Ventaja que resalta con la migración de NT a 2000 es que en algunas estaciones de trabajo constantemente se salían del dominio, varias ocasiones se verifico el cable de red, el nodo, la tarjeta de red y continuaba presentando la falla, se verificaba en la configuración y supuestamente el equipo se encontraba dentro del dominio, pero al accesar al icono de entorno de red y dar 2 clics sobre el icono toda la red, únicamente desplegaba el equipo del usuario, entonces se metía el equipo a un grupo de trabajo y después nuevamente se ingresaba el equipo nuevamente al dominio (después de cada paso se reiniciaba el equipo), esta falla era muy común y con Windows 2000 el equipo ya no se salió del dominio.

Algunos Ingenieros de sitio comentaron que posiblemente el segmento donde se encontraba el usuario se encontraba dañado, pero a sus compañeros no les presentaba dicha falla y como se menciono anteriormente se reviso el nodo, su cable de red y la tarjeta.

Con la facilidad y flexibilidad de agregar protocolos, se puede estar tentado de agregar todo protocolo que caiga en sus manos, si hablar 2 idiomas es bueno, entonces hablar 5 idiomas debe de ser grandioso. Sin embargo debe de considerarse que el sistema no obtiene simplemente la posibilidad de hablar un nuevo idioma por tener el protocolo instalado, si no que el sistema acepta hablarlo cada vez que habla. La sobrecarga en un servidor y en la red se incrementa proporcionalmente de forma real por cada protocolo que se agrega, sólo porque pueda hacerse no significa que deba hacerse. La situación ideal es tener instalados en el servidor tan pocos protocolos como sea posible.

Brevemente se mencionará que TCP/IP es un protocolo universal que la gran mayoría de los Sistemas Operativos de Red actuales utilizan de los cuales se pueden mencionar:

Microsoft Windows 2000, XP, NT 9x
Novell Netware 4.x y 5.x
UNIX
Digital VMS y PathWorks
IBM AS/400 y Main Frame System.

TCP/IP no es el único protocolo que se puede utilizar en Windows 2000, pero los otros protocolos son secundarios en la mayoría de las redes. Si Windows 2000 o Windows NT son un NOS (Network Operation System) o sea un Sistema Operativo de Red primario se debe elegir el protocolo TCP/IP.

1.12 Servicios de Internet Information Services

La avanzada tecnología que ha logrado desarrollar Microsoft hacia los servidores de Internet empezaron con la tecnología IIS (Internet Information Services) que significa " Servidor de Información de Internet", Microsoft decidió unir varias tecnologías hacia este nuevo concepto, incluyendo la de servidor Web, servidor FTP y un servidor de grupo de noticias. Con IIS se logra fusionar dicha tecnología en uno sólo .

La tecnología IIS es un concepto nuevo en Windows 2000, aunque cabe hacer mención sobre el pasado de este nuevo servicio que comienza de la siguiente manera:

Esta Tecnología nace con la versión NT 3.51 como un servicio de Servidor Web del Protocolo de Transferencia de Hipertexto (HTTP, *Hypertext Transfer Protocol*) y como un servidor del protocolo de transferencia de archivos (FTP, File Transfer Protocol) el cual era sumamente limitado. Antes de comercializar la versión de Windows NT 3.51, Microsoft ofrecía muy poca compatibilidad con Internet dentro de su Sistema Operativo.

La versión 2.0 se comercializó con Windows NT 4.0 en julio de 1996, lo que muchos consideran la esencia de IIS de hoy en día, su compatibilidad con Páginas Active Server (ASP , Active Server Pages) , Microsoft introdujo el concepto de ASP en su lanzamiento de la versión 3.0 de IIS, que se incluyo junto con la actualización de Internet Explorer y varias utilidades multimedia como parte de la actualización del 3er. Service Pack de Windows NT Server 4.0, al ver el éxito que se podía tener en el mercado Microsoft lanza la versión IIS 4.0 la cual se distribuyo al público con el nombre de Option Pack para Windows NT la cual se distribuía de manera gratuita para el sistema operativo Windows NT 4.0, La versión 4.0 de IIS se ha mantenido en los Service Pack 4, 5 y 6 .

Windows 2000 incluye otra versión de IIS, la cual resulta más interesante que sus antecesoras, la versión IIS 5.0, ésta introduce nuevas caracteristicas de seguridad y escalabilidad entre las que sobresalen:

- Mejoras en la página de Active Server
- Cambios Administrativos, Incluyendo compatibilidad total con la tecnología de la MMC (Microsoft Management Console), una administración remota y un registro y seguimiento de errores mejorado.
- Numerosos cambios de registro
- Seguridad Incluyendo integración completa con el cifrado basado en Kerberos de Windows 2000
- Rendimiento incluyendo una solución en el sondeo de sockets.
- Una documentación profundamente mejorada. Incluyendo la utilidad de ayuda basada en HTML, que facilita la búsqueda por toda la documentación, así como un índice de temas mejorados.

Antes de comenzar a utilizar IIS 5.0 como proveedor de servicios de Internet (ISP, *Internet Services Provider*) o web master virtual, se debe de tomar en cuenta que IIS 5.0 sólo funciona con la serie de Sistemas Operativos de Windows 2000 que son la versión profesional para estaciones de trabajo, la versión Server para Servidores de Trabajo, la versión Advanced Server para servidores que sobrepasen los 32 procesadores y la versión Windows 2000 Datacenter Server para servidores que lleguen a manejar redes gigantescas, cabe mencionar que la versión de IIS 5.0 que posee la versión profesional se encuentra limitada a comparación de las versiones Server y Advanced Server, por que su limitación consiste en su incapacidad para admitir algunos de los sucesos orientados a la transacción y a la seguridad .

Desde el punto de vista de Hardware debe de asegurarse que cumpla con los requerimientos ya antes mencionados.

Cabe mencionar que IIS 5.0, se instala automáticamente en su equipo, cuando instala Windows 2000 Server, si se trata de una instalación limpia del Sistema Operativo (esto es cuando el equipo al que se le va a instalar no tiene instalado algún sistema operativo en el equipo). Si esta actualizando una versión existente de Windows NT o de Windows 9x o de Windows NT Workstation instalado, entonces Windows le actualizara automáticamente a IIS 5.0.

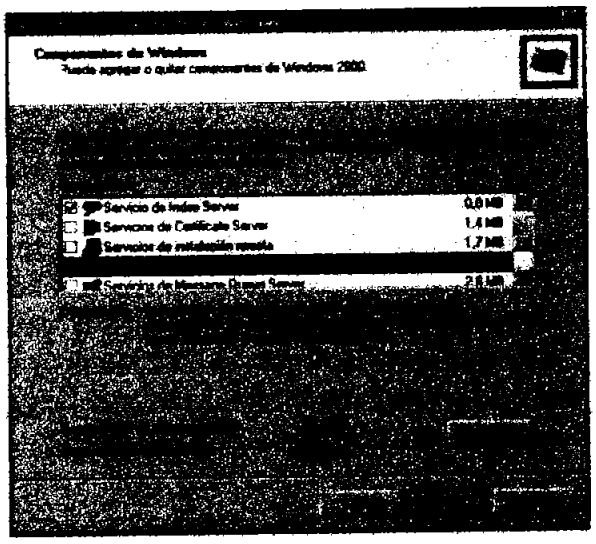


Figura 1.12 Agregar nuevos componentes de Windows.

Si se esta actualizando desde una versión existente de Windows NT o de Windows 9x y nunca ha tenido instalado una versión de IIS, debe iniciar el asistente para componentes de Windows, como se indica a continuación:

1. Hacer clic en el botón de inicio, elegir configuración, y a continuación hacer clic en el panel de control. Aparece la ventana Panel de Control de Windows 2000.

2. Hacer doble clic en el icono de Agregar o Quitar programas y aparecerá la ventana Agregar o quitar programas.

3. Hacer clic en la opción de Agregar o Quitar componentes de Windows (ver la figura 1.12), que aparece en la esquina inferior izquierda de esta ventana, aparece el cuadro de diálogo Asistente para componentes de Windows.

4. Seleccionar la opción de Servicios de Internet Information Services (IIS) en el cuadro de diálogo Asistente para componentes de Windows. De los muchos cuadros que aparecen en dicho cuadro se selecciona el de Internet Information Services (recordar que consta de los servicios básicos de Web, FTP y del servidor de grupo de noticias), que son necesarios para que todos los servicios de Internet funcionen adecuadamente, para instalar estos servicios active sus respectivas casillas de verificación(ver la figura 1.13). Si una casilla de verificación esta activada, pero tiene el fondo gris, esa opción no se ha seleccionado completamente (es decir no se han instalado todas las opciones que incluye) para examinar con detalle las distintas opciones que aparecen en cualquiera de estos servicios, hacer clic en el botón de Detalles.

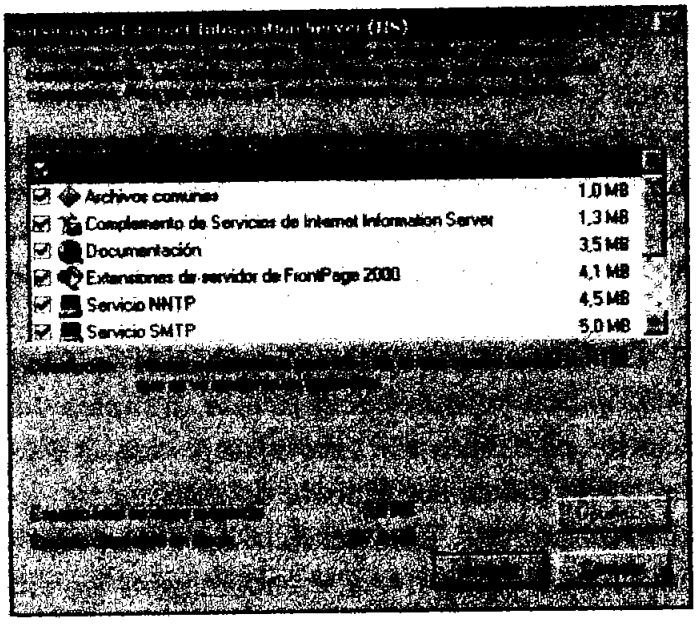


Figura 1.13 Cuadro de diálogo para agregar un componente de los Servicios de Internet Information Server (IIS).

A continuación se mencionarán algunos de los servicios de IIS como son:

ADMINISTRADOR DE SERVICIOS DE INTERNET (HTML). - Esta es la versión basada en Web de la herramienta de administración complemento de servicios de Internet Information Server.

ARCHIVOS COMUNES.- Estos son los archivos principales que componen el sistema básico de IIS.

COMPLEMENTO DE SERVICIOS DE INTERNET INFORMATION SERVER.- Se trata de la Interfaz de la consola de administración necesaria para administrar completamente IIS.

DOCUMENTACIÓN.- Esta es la Información General de IIS, ASP, Web y FTP.

EXTENSIONES DE SERVIDOR DE FRONTPAGE 2000. - Sirve para usar Microsoft Front Page y Microsoft Visual InterDev 6.0 con herramientas de creación, desarrollo y administración para los sitios de Internet.

SERVICIO NNTP.- Proporciona la compatibilidad para el protocolo de transferencia de noticias de red (NNTP, Network News Transfer Protocol), que se utiliza para correo electrónico.

SERVIDOR DE PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS (FTP). - Incluye los archivos binarios necesarios para instalar los servicios de servidor FTP.

SERVIDOR WORLD WIDE WEB.- Es la parte fundamental de IIS, y Proporciona compatibilidad con el servidor Web básico. Cuando esta Instalado este servicio, nunca se puede desactivar ya que si lo hace, podría bloquear completamente el IIS.

VISUAL INTERDEV RAD DEPLOYMENT SUPPORT.- (Soporte Visual para el Despliegue RAD). Mediante esta opción puede distribuir de forma remota varias aplicaciones en el servidor de Internet, Debería utilizar esta opción con cuidado y sólo en servidores de desarrollo. Nunca se debe instalar o hacer uso de esta herramienta en servidores IIS de producción, debido a los muchos riesgos de seguridad intrínseca que conlleva.

5.- Una vez que se hayan seleccionado todo los componentes que se quiera instalar Hacer clic en el botón Aceptar para guardar las opciones elegidas y volver al cuadro de diálogo Asistente para componentes de Windows.

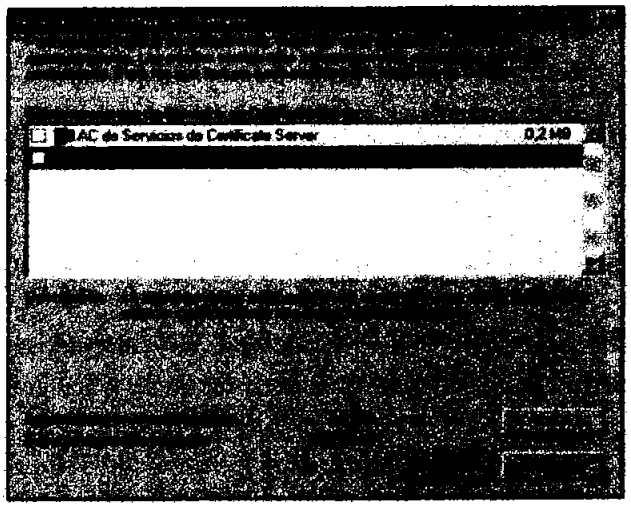


Figura 1.14 Agregar componentes de Servicios de Certificate Server.

A continuación el área que se debe de examinar a detalle es la opción Servicios de Certificate Server. Parara examinar la breve lista de opciones que incluye este servicio hacer clic en el botón de Detalles, y aparecerá el cuadro de diálogo Servicios de Certificate Server (ver la figura 1.14), las opciones detalladas de este cuadro son las siguientes:

AC de Servicio de Certificate Server. Estos son los archivos principales de la entidad emisora de certificados de Servicios de Certificate Server. Si se piensa configurar el sitio Web para utilizar la capa de Sockets segura (SSL, Secure Socket Layer) o se desea utilizar firmas digitales en el sitio, entonces se deberán comprar estas tecnologías o bien utilizar el servicio de Entidad Emisora de certificados de Windows 2000, que se puede instalar mediante la opción de Servicios de Cerficate Server. La mayoría de las organizaciones suelen utilizar este servicio para las Intranet

Compat. de Inscripción Web de Servicios de Certificate Server.- Esta sencilla utilidad permite publicar páginas Web en el sito desde el que cualquiera (con los permisos adecuados) puede descargar copias de sus certificados para utilizarlos como sus aplicaciones (es de suponer que va a funcionar sólo con la instalación del servidor Web).

6.- Una vez elegidas las opciones que se deseen, activando las casillas de verificación apropiadas, hacer clic en el botón Aceptar para guardar las modificaciones y volver al cuadro de diálogo Servicios de Internet Information Server (IIS) (ver la figura 1.15). A continuación, hacer clic en el botón de Aceptar para Iniciar el proceso de Instalación, Este proceso puede tardar entre un minuto o poco más de entre 10 a 15 minutos, dependiendo de muchos factores, como puede ser el número total de opciones seleccionadas, la cantidad de memoria disponible, etc.

7.- Hacer clic en el botón de Finalizar para salir del asistente para componentes de Windows y volver al cuadro de diálogo Agregar o Quitar Programas. Quizá se tenga que reiniciar el equipo, dependiendo de las opciones seleccionadas.

Existen varias formas de Administrar un entorno IIS, una de las maneras más sencillas de poder administrar IIS es el servicio Básico, la cual podemos accesar a ella desde la siguiente ruta: Dar un clic a inicio, luego programas, después Herramientas Administrativas, y a continuación Administración de Servicios de Internet, Aparece la ventana de Internet Information Services.

Existen 3 partes principales en esta ventana: La Barra de Menús, el panel izquierdo y el derecho; La Barra de menús contiene los menús desplegables Acción y Ver junto con los botones Atrás, Adelante, Subir un nivel, Mostrar u ocultar Árbol de la consola /Favoritos, Propiedades, Actualizar, Ayuda, Agregar un equipo a la lista de, Iniciar Elemento y Pausar el elemento. Desde esta barra de Menús se pueden administrar las actividades generales de servidores virtuales FTP, Web, SMTP y NNTP.

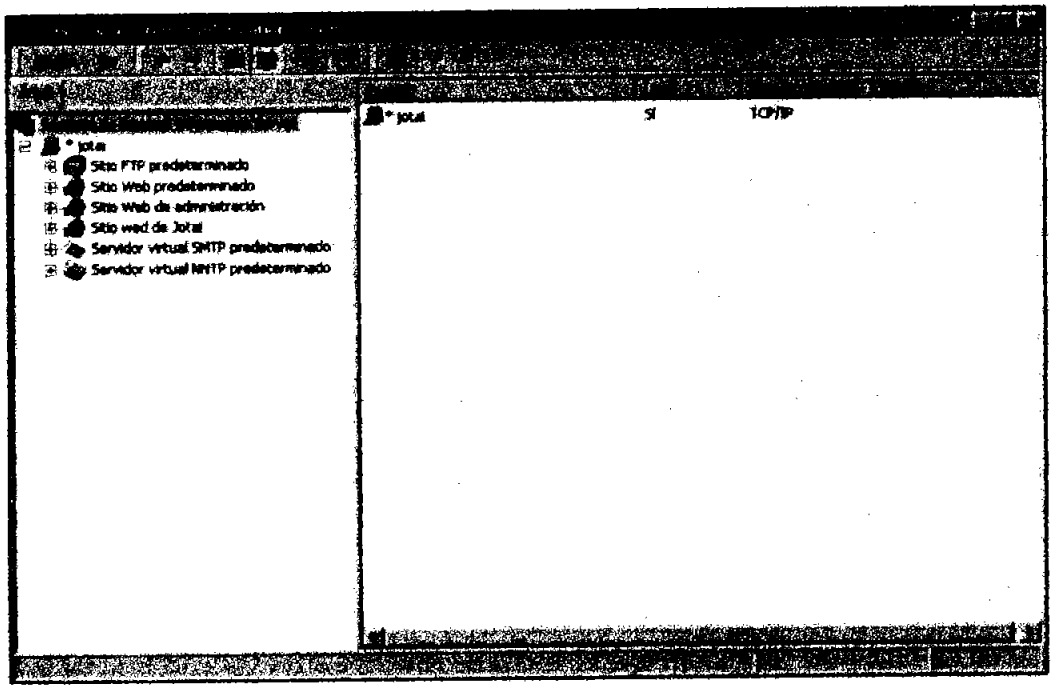


Figura 1.15 Uso de la ventana Servicios de Internet Information Server.

El panel del lado izquierdo es quizá la parte más importante de la consola, tiene al menos una ficha denominada Árbol, que contiene la mayoría de la información que interesa al administrador, se pueden utilizar los iconos de nivel superior para modificar los siguientes elementos:

- Servicios de Internet Information Server.- Este elemento permite conectarse a uno o más servidores IIS que se encuentran dentro del dominio o catálogo global (un servidor enumerado que aparece en Active Directory). El panel derecho incluye toda la información seleccionada inicialmente por lo que se haya elegido en el panel izquierdo (ver la figura 1.16).

- Nombre _Equipo.- Este es el nombre del equipo del servidor IIS que contiene los distintos sitios FTP, SMTP, NNTP y Web. Siempre habrá presentes uno o más nombres de equipo bajo el icono Servicios de Internet Information Server.

- Sitio FTP predeterminado.- Esta área se utiliza para modificar los atributos del sitio del protocolo de Transferencia de Archivos que podría existir dentro de los límites de control de este servidor IIS. Esto podría incluir sitios ubicados físicamente en el mismo equipo que el sistema operativo Windows 2000 Server, o podrían ser otros equipos separados físicamente ubicados en cualquier parte dentro del dominio de Windows 2000.

- Sitio Web predeterminado.- Esta área se utiliza para modificar los atributos para los sitios Web que podrían existir dentro de los límites de control de este servidor IIS. Esto incluye sitios que están ubicados físicamente en el mismo equipo que el Sistema Operativo Windows 2000 Server y cualquier directorio virtual almacenado en cualquier otra parte.

- Sitio Web de Administración.- El sitio Web de administración se puede concebir como el lugar donde se administran los archivos globales para todos los sitios Web controlados por esta instalación de IIS, incluyendo la capacidad para definir múltiples identidades para este servidor.

- Servidor Virtual SMTP predeterminado.- Este es el sistema de correo electrónico compatible con POP3 con el que es compatible IIS, que se configura mediante las opciones de esta ventana.

- Servidor Virtual NNTP predeterminado.- Este es el sistema de información de noticias de red con el que es compatible IIS, que se configura mediante las opciones de esta misma ventana.

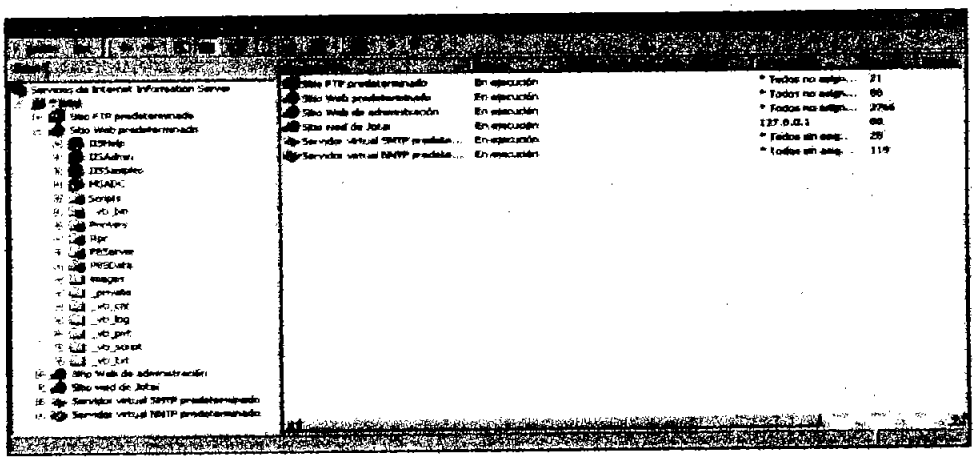


Figura 1.16 Sitios IIS instalados.

En la empresa de telefonía se cuenta con una hoja de Intranet para que los usuarios conozcan las políticas y procedimientos con los que se maneja la empresa así como algunos manuales de teléfonos celulares, aplicaciones y bases de datos y formatos para adquisición de algún producto o servicios que requiera alguno de los departamentos.

1.13 SERVIDOR DE CORREO EXCHANGE

Al Servidor de Correo Electrónico no se le suele atribuir la importancia suficiente dentro de una organización como se le tiene en realidad. Los sistemas de correo electrónico de hace apenas 4 años consistían principalmente, en lo que suele denominarse sistemas de mensajes de archivos sin formato. De tal forma era que cualquier usuario tenía permisos sobre un archivo, de enviar y recibir un archivo adjunto, en el servidor se creaba una copia del mismo archivo cada vez que se enviaba o recibía, se puede mencionar que no era lo mejor por las siguientes razones:

- Todos los usuarios del sistema debían de tener acceso al archivo, esto significa que cualquier usuario puede corromper o destruir el archivo.

- Se debía realizar un mantenimiento de archivos, tanto si se iniciaba de forma manual como mediante un archivo por lotes. Como es el único archivo, esto sólo se podía realizar cuando los usuarios no hubieran iniciado una sesión de correo electrónico.

- La copia de seguridad es del tipo todo o nada. Si fuese necesario restaurar los datos de un usuario, sería necesario restaurar todos los datos de todos los usuarios.

Exchange es un sistema de mensajerías compuesto de 2 partes básicas: Una sólida base de datos relacional y una estructura de directorio jerárquica con tres años de vida. La combinación de estos 2 elementos permite que el sistema sea sólido y se pueda utilizar a la vez que sigue siendo ágil para el trabajo. Mediante el Sistema de Base de Datos Jet, el servidor Exchange permite que el sistema administre el sistema de correo electrónico como si fuera una base de datos. Muchas fuentes de datos están en sitios distintos, pero se pueden utilizar todos los datos para proporcionar servicios. Un ejemplo de esta ventaja es el hecho de que un mensaje que se envía desde un usuario a un grupo de usuarios dentro del sistema de Exchange sólo se guarda una vez. Cualquier usuario que recibe el mensaje lo recupera de un almacén común. Imaginemos el espacio que se ahorra si se envía un archivo adjunto de 1MB a 25 Personas (25x1=25Mb pero si todos tiene el archivo en la misma ubicación seria 1MB).

La base de datos Jet también es útil porque realiza su propio mantenimiento. Los archivos de la base de datos crean primero el espacio, y a continuación rellenan ese espacio. Es muy difícil liberar espacio. Resulta complicado medir el tamaño de la base de datos al igual que mantener este tamaño, resulta confortante que la base de datos Jet ajuste su propio tamaño y compruebe la coherencia de los datos.

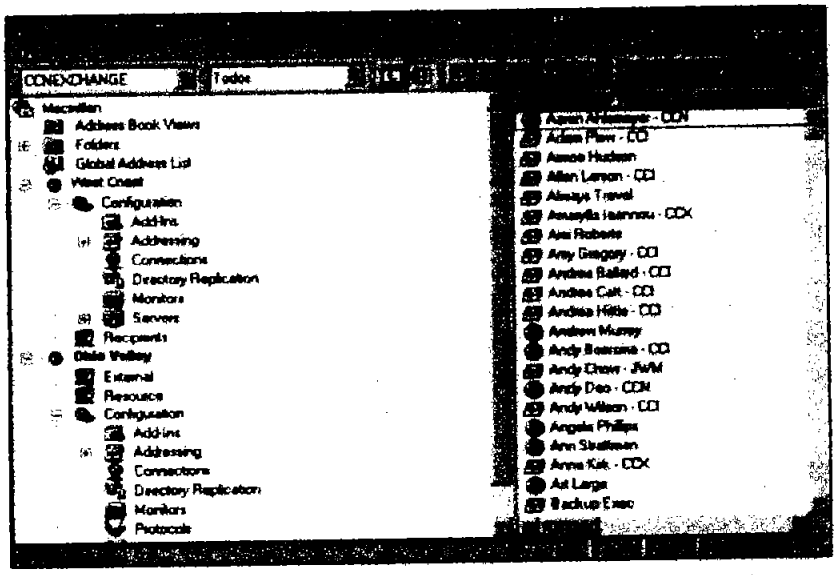


Figura 1.17 El directorio en el sistema Exchange.

En la empresa de telefonía celular la gran mayoría de las personas que laboran en ella poseen una cuenta de red y una cuenta de correo electrónico, esto es con el fin de que puedan desempeñar su trabajo satisfactoriamente, Por ejemplo un vendedor necesita conectarse a la red para poder laborar en una hoja de cálculo y en un procesador de palabras realizar una cotización de algún equipo, con la cuenta de correo puede enviar a su cliente dicha información por Internet y recibir una respuesta por el mismo medio, de esta manera se minimizan costos y se acelera cada proceso en la empresa.

La creación de cuentas de correo se realiza con Microsoft Exchange, los administradores de la red únicamente pueden realizar dicha función, cuando un usuario ingresa a la empresa su jefe inmediato tramita con recursos humanos su nombre de usuario y su contraseña de red, esta solicitud llega al Área de Redes donde los administradores crean y administran dichas cuentas, con dicha cuenta únicamente pueden enviar y recibir máximo 2MB de información, para algunos coordinadores es de 5MB y para gerentes de Área es ilimitado. La razón es que los gerentes envían y reciben bastante información con gráficos los cuales incrementan su capacidad de enviar y recibir MB.

La estructura de directorios de Exchange es bastante parecida a la de Active Directory. Incluso existe el concepto de sitio en el directorio Exchange. Aunque no existe una coincidencia exacta entre un sistema y otro (ver la figura 1.17).

El concepto de Objeto contenedor existe en forma de sitios y contenedores de recipientes. El directorio se aplica a través de la organización igual que lo hace el dominio, las tareas y responsabilidades administrativas se pueden conceder a objetos contenedor del sistema. Esto quiere decir que la información donde se almacena todos los correos es un archivo con extensión *. pst que se crea al momento de configurar el equipo localmente dentro de una computadora pero también se crea dicho archivo dentro del servidor, lo cual quiere decir que si se pierde el almacén de información pública no significa que se pierdan los almacenes de información privada. Si se pierde un único buzón de correo no significa que todos han perdidos sus correos.

Dentro de Exchange y Outlook (La interfaz de usuario de Exchange) (ver la figura 1.18), se mantiene el concepto de carpeta personal (archivo con extensión *. pst que se guarda localmente en el equipo) o carpeta buzón de correo en el servidor. La lista de tareas, calendarios, diarios y archivos se guardan todos en dichas carpetas, el concepto de carpeta pública es crear otra carpeta más que exista en un espacio en el que todos pueden tener acceso.

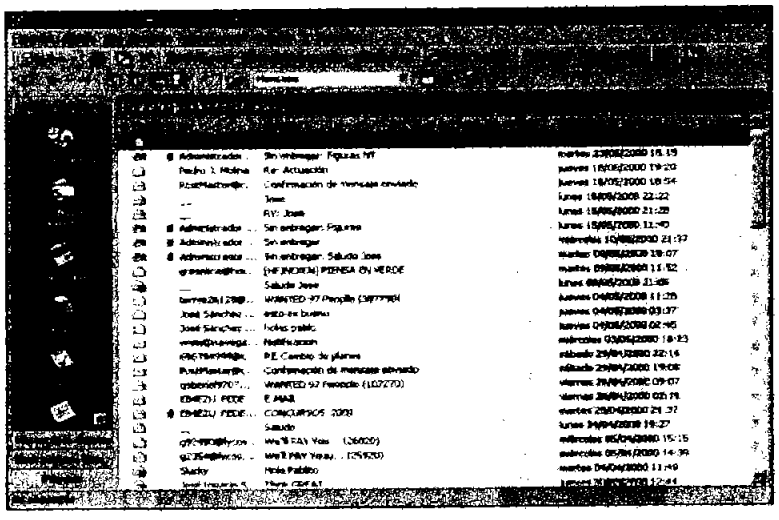


Figura 1.18 El cliente de Outlook.

Inicialmente el administrador crea una carpeta, pero a partir de ahí las carpetas pertenecen en realidad a los usuarios, incluso un administrador no puede crear una carpeta pública (a parte de la primer carpeta) en el programa de Exchange del administrador.

En la compañía de telefonía dicha carpeta se reservaba el acceso a ciertas salas de junta, así como existían comunicados de prensa e información de índole general que los usuarios podían depositar en dicha carpeta. Los usuarios pueden crear una carpeta dentro de la carpeta pública si así lo deseaban, pero la administración corresponde a los administradores de la red, de esta manera se lograba que el usuario lograra tener conversaciones privadas o foros de intercambio de ideas y opiniones.

La conectividad con Internet es muy importante para Exchange, al igual que la familia Windows Server, Microsoft ha hecho que la conectividad con internet sea parte del sistema .

El concepto de Conectividad con Internet puede significar muchas cosas en lo que concierne al correo electrónico, algunos protocolos de internet se instalan automáticamente, pero muchos servicios no. No existe una confianza en que sólo aparezcan los protocolos SMTP y POP en la interfaz administrativa de Exchange y que el sistema de Correo Electrónico este conectado a internet. Algunos de los términos que se utilizan para hablar de la conectividad del correo electrónico son:

- POP.- (Protocolo del Correo-Post Office Protocol). Proporciona una conexión de cliente con el servidor a través de internet para leer el correo.

- SMTP.- (Protocolo de Servicio de Transferencia de Correo-Services Mail Transfer Protocol). Proporciona una conexión desde un servidor de correo electrónico de internet para intercambio de correo.

- LDAP.- (Protocolo de Acceso al Directorio Ligero/pesado-Lightweight Directory Access Protocol). Permite que un origen externo tenga acceso a una lista de usuarios en el servidor sin ningún otro tipo de acceso.

- Cliente HTTP.- Permite tener acceso al correo electrónico a través de la Web.

- NNTP.- (Protocolo de Transferencia de Noticias en Red-Network News Transfer Protocol). Se usa para publicar los tablones de noticias públicos en internet para la discusión abierta y el intercambio de ideas (ver la figura 1.19).

- X 400. - Permite crear conexiones privadas entre sistemas Exchange mediante internet como una WAN de bajo costo.

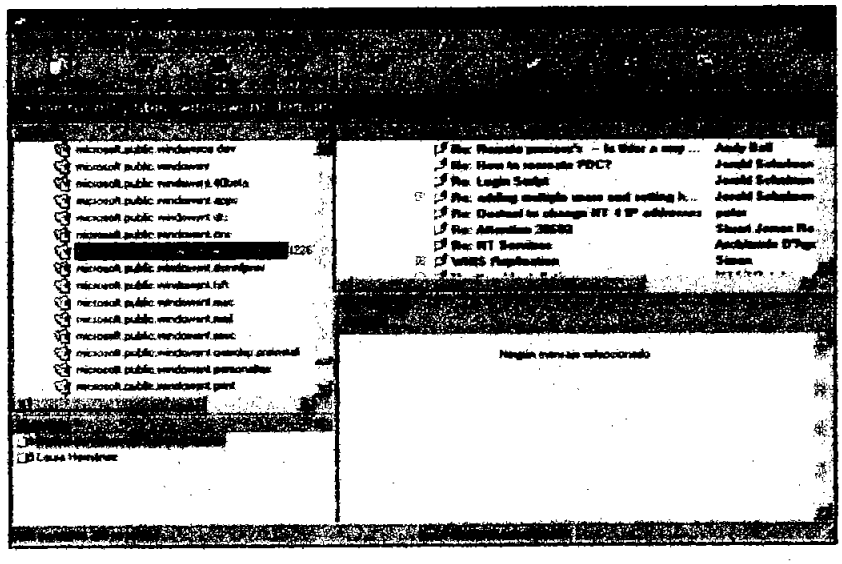


Figura 1.19 El lect

Exchange proporciona estos servicios de conectividad sin ningún software adicional, lo que le convierte en un valioso Host de correo de internet, En la empresa telefónica se utiliza el servicio SMTP y cada región posee un servidor de correo que es administrado vía remota con un software de la compañía funk technology llamado proxy con el cual se conectan al servidor desde el SAE de la ciudad de México y verifican que no sufra ninguna caída de enlace, no importando la región, sólo en un caso extremo se desplazaría un administrador hacia el lugar para corregir la falla pero que normalmente esto nunca sucede.

Con las herramientas que se proporcionan se permite poder utilizar Exchange como un Host SMTP, se realiza una implementación muy buena de un protocolo de forma bastante simple, permite utilizar al administrador una herramienta de administración para realizar algunas tareas complicadas con relativa facilidad. Por ejemplo, permite poder seleccionar algunos URL específicos que puedan enviar y recibir correo dentro de la compañía. Esto hace que el servidor se establezca como un sistema de correo electrónico privado que utiliza internet como una WAN. También permite al sistema bloquear grupos particularmente molestos que podrían enviar correo masivo con malas intenciones en el servidor (ver la figura 1.20).

En la empresa una dirección específica de correo comenzó a enviar el virus sircam32 causando daños en los equipos ya que se alojaba con forma de un archivo de imagen y dañaba varios archivos del sistema, con apoyo de dicha herramienta no se permite poder recibir correo electrónico desde dicha dirección para que no propague el virus en la red, ya que éste se mete en la lista de correos y se auto envía, además daña archivos de imágenes y archivos del Sistema Operativo de esa manera se implemento dicha función.

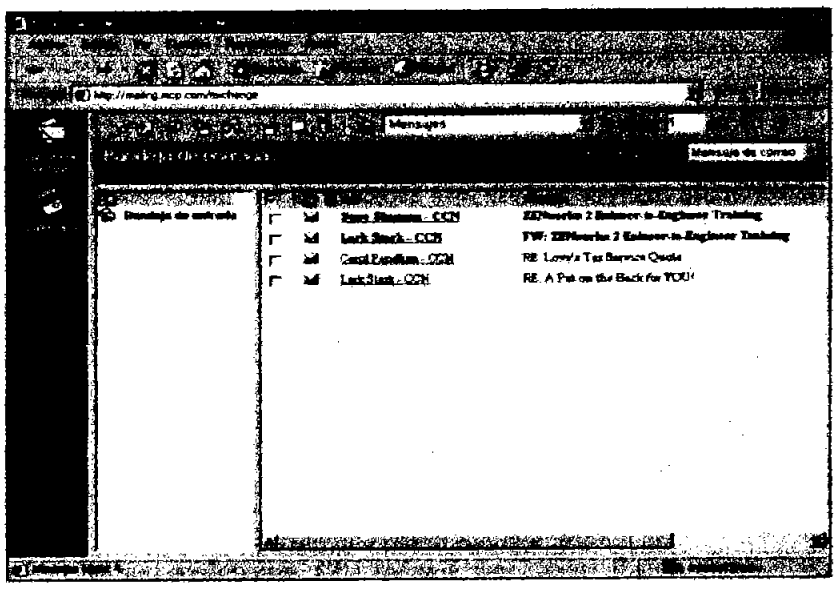


Figura 1.20 El cliente web de Outlook.

RESUMEN

En él capitulo I se mostró los requerimientos mínimos para realizar la migración de Windows NT a Windows 2000 Server, entre las ventajas que se tuvieron en la empresa de telefonía fueron:

- COMPATIBILIDAD 100 % CON DISPOSITIVOS USB
- SERVICIO DE DHCP
- CONTROLADORES DE IMPRESORAS COMPATIBLES

No se reportaron fallas en la migración del sistema operativo Windows NT al Sistema Windows 2000 Server.

Al realizar la migración la empresa de telefonía no presentó perdidas de información, con Windows 2000 se cuenta con un visor de sucesos poderoso que permite poder visualizar cualquier error de seguridad en las aplicaciones y en el sistema, es más seguro y más detallado que el que se tenia en Windows NT anteriormente

El sistema operativo Windows 2000 fue 100% compatible con IIS (Internet Información Services) que nos permite poder administrar herramientas para poder montar hojas Web en Internet, en la empresa de telefonía se tiene montada una pequeña intranet que se administra con IIS.

Microsoft Exchange fue 100% compatible con Windows 2000 el cual proporciona una poderosa herramienta como lo es la MMC (Microsoft Manager Console) La cual nos permite poder administrar usuarios , equipos , servicios y aplicaciones en una consola centralizada que es 100 % compatible con Microsoft Exchange (Software de administración y creación de correo electrónico de Microsoft).

La configuración de impresoras y dispositivos usb ahora es más fácil, además de que Windows 2000 proporciona una lista mucho mas amplia de drivers y controladores tanto de impresoras como de escaners, tarjetas de red y otros dispositivos de hardware.

La actualización permitió poder compartir impresoras, archivos y carpetas de una manera más ágil y confiable, ya no se presentaron problemas al ingresar equipos nuevos a la red, constantemente los equipos nuevos no se podían acceder al dominio. Con Windows 2000 se mejora notablemente esto.

El servicio de DHCP permite poder asignar direcciones IP de forma aleatoria a los equipos y no hubo ningún problema en su configuración a diferencia de Windows NT.

Las estaciones de trabajo que se migraron a Windows 2000 profesional desde Windows 95 y 98 se migraron de una forma ágil y no presentaron falla alguna además de que no se perdió ninguna información.

Los servidores trabajaron de una forma mucho más estable en comparación con Windows NT.

CAPITULO II
COMPATIBILIDAD Y CONECTIVIDAD CON OTROS SISTEMAS OPERATIVOS

La opción de un sistema operativo de red es una decisión estratégica, a largo plazo manejada por las demandas que las organizaciones tienen para manejar una plataforma sólida en donde construir las soluciones comerciales necesarias en una red.

Administrar y compartir datos, información e impresión son los requisitos vitales, las organizaciones hoy están confiando en el sistema operativo de red, el software del servidor puede proporcionar muchos servicios adicionales como:

- Ejecutar las aplicaciones comerciales y mantener una infraestructura para la próxima generación de aplicaciones distribuidas.
- Utilizar Internet y sitios de Intranet.
- Proveer una infraestructura de comunicaciones comprensiva para proporcionar los servicios como el acceso remoto a través de la gestión de redes privadas virtuales (VPN) y acceso a RAS (Remote Access Service-servicio de acceso remoto), a las conexiones.
- Proveer un directorio comprensivo y servicios de dirección de escritorio.

2.1 CONECTIVIDAD CON NETWARE.

Uno de los competidores más fuertes que posee Microsoft es sin duda el sistema operativo de red NOVELL NETWARE, NETWARE comenzó como uno de los sistemas operativos de red pioneros en la industria, antiguamente la gran mayoría de las redes se manejaba con dicho sistema operativo, éste controlaba la mayor parte del mercado en el ámbito mundial.

Microsoft siendo visionario comenzó a desarrollar un sistema operativo de red confiable y de múltiples tareas, que logra tener una infraestructura donde se combinaran todos los servicios. Netware posee un servicio de directorios (servicio de directorio de Netware o NDS (Netware Directory Services) con seis años de experiencia que quizás es una de sus cartas más fuertes en dicho sistema operativo.

Netware se creo como un sistema operativo de servidor, los usuarios nunca se sentaran delante de un servidor Netware para escribir direcciones o llenar informes de gastos. Por esta y otras razones mucha gente considera a Netware más seriamente para utilizarlo como un sistema operativo de red en sus empresas.

La primera herramienta que se utiliza en un ambiente Windows para integrar un servidor en un entorno Netware es el servicio de Puerta de Enlace para Netware. Este servicio permite a los usuarios de un dominio Windows interactuar perfectamente con un servidor Netware sin necesidad de conectarse directamente a ese servidor.

2.1.1. DIFERENCIAS CONCEPTUALES

Entre algunas de las diferencias que existen entre Novell Netware y Windows 2000 una de la más notable es lo que Microsoft llamo un servicio de directorios nadie en la industria lo llamo un servicio de directorios. De hecho lo que Microsoft llamo un servicio de directorios no fue un servicio de directorios jerárquicos. El servicio de directorios de Novell Netware es un servicio de directorios de varios niveles, jerárquicos y orientado a objetos.

La compartición de carpetas es la forma más básica de trabajo en la red que existe, y es una de las grandes diferencias entre Windows y Netware. Las diferencias en la forma en que los usuarios tienen acceso a la estructura de los archivos y en la forma en que Netware y Windows ponen a su disposición el recurso compartido y estructuran el directorio son muy marcadas.

En un ambiente Windows como ya se ha explicado, se pueden crear recursos compartidos en cualquier punto de la estructura de directorios. Un administrador puede elegir cualquier directorio en el servidor y decidir compartirlo.

En un ambiente Netware los recursos compartidos no se llaman recursos, se llaman volúmenes, esto se debe a que los recursos compartidos que muestran un servidor Netware son realmente los volúmenes de disco creados en los servidores. Cada volumen que se crea y se monta en un servidor Netware puede ponerse a su disposición del usuario base. Sin embargo, los directorios no se pueden publicar como entidades independientes.

En orden a compensar esta diferencia se debe de comprender que cuando se conecta a un servidor Netware, el usuario tiene la posibilidad de crear asignaciones de unidades que apunten a cualquier directorio del servidor. Tales asignaciones se denominan asignaciones de raíz.

Para explicar la diferencia se puede comparar la forma en que un usuario debe tener acceso al mismo directorio en cada tipo de servidor.

2.1.2. SERVICIO DE DIRECTORIO DE NETWARE

Existen 3 diferencias importantes en la estructura de directorios de Novell:

- Delegación de Autoridad. Netware proporciona delegación de autoridad directamente a cualquier objeto sobre otro objeto cualquiera del directorio. Active Directory ofrece delegación de autoridad a cualquier objeto de usuario sobre los objetos contenedores.

- Particionamiento y replicación. Las particiones de Netware están separadas a lo largo de la línea contenedor. Las particiones de Active Directory y su replicación están basadas en las líneas de sitio (segmentación de la red).

- Conversión de Nomenclatura. La conversión de nomenclatura de Netware es libre y no sigue ningún modelo de búsqueda. El directorio se basa exclusivamente en la estructura de directorios de la combinación X.500. Active Directory esta estrechamente relacionado con la conversión de nomenclatura de DNS (Domain Name Service-servicio de nombre de dominio). Los 2 sistemas se pueden incorporar al estándar LDAP (Light-weight Directory Access Protocol-protocolo ligero de acceso al directorio), de Internet para descubrir objetos de directorio.

La conversión de un directorio Netware a Active Directory de Microsoft seria prácticamente imposible si el administrador tuviera que hacerlo manualmente. Si el directorio es lo suficientemente grande, es mejor que el administrador comience a crearlo desde cero en lugar de intentar convertirlo. Afortunadamente Microsoft proporciona una herramienta llamada Herramienta de Migración para servicios de directorio.

Al igual que la antigua herramienta de migración de Netware que incluía Windows NT, esta herramienta lo que hace es sacar los usuarios, grupos e información de los servidores Netware. Se puede utilizar para volver a colocar a los servidores Netware o simplemente para replicar la información del usuario y del grupo de trabajo desde el entorno Netware en el que existe. En cualquier caso, ahorra mucho tiempo.

La herramienta de migración se puede instalar durante la instalación inicial de Windows 2000 o posterior. La instalación es simplemente cuestión de agregar el servicio desde el panel de control. Agregar o quitar programas, en Agregar o Quitar componentes, seleccionar Herramienta de Migración para servicios de directorio. Una vez instalada ésta aparecerá en Inicio, Programas, Herramientas Administrativas.

2.1.3. SERVICIOS DE PUERTA DE ENLACE CON NETWARE

El servicio de Puerta de Enlace para Netware es justamente eso, un servicio de red que se ejecuta en un servidor Windows y crea una puerta de enlace a servidores Netware. El proceso implica que un administrador cree una combinación al recurso compartido del servidor de Netware (impresión o unidad), y a continuación, se compartan los recursos como si fuera un recurso compartido del servidor Windows. La ventaja de este proceso es que los usuarios del dominio Windows no tienen que instalar software de Cliente Netware y no tiene que ser administrado desde la perspectiva de NETWARE.

Recordemos que lo primero que se debe de tomar en cuenta es si el servidor esta preparado para recibir al usuario que se conecte al servicio de la puerta de enlace. Un grupo llamado NTGATEWAY debe de existir en el servidor de Netware al igual que una cuenta de usuario que es un miembro de un grupo que se utiliza mediante el servicio de Puerta de Enlace.

Una vez que el servidor Netware considera que la cuenta es parte del grupo NTGATEWAY, el siguiente paso es instalar el servicio de puerta de enlace. Para instalar este servicio se debe hacer lo siguiente:

1. Hacer clic en el botón secundario en Mis Sitios de Red y elegir Propiedades.

2. Hacer clic con el botón secundario en una conexión de red existente y elegir propiedades.

3. Elegir el botón Instalar. Hacer clic en Cliente y, a continuación, hacer clic en el botón agregar.

4. Se enumeran los servicios de Puerta de Enlace(y cliente) para Netware (ver la figura 2.1), Seleccionarlos y Elegir aceptar (recordar que el protocolo para poderse conectar a un servidor Netware es NWLINK y seleccionar servicios de Gateway para Network).

5. Elegir Cerrar en la pantalla propiedades, Una vez instalado el servicio se debe de configurar para tener acceso a los recursos del servidor Netware. Se le preguntara por las preferencias para esta conexión.

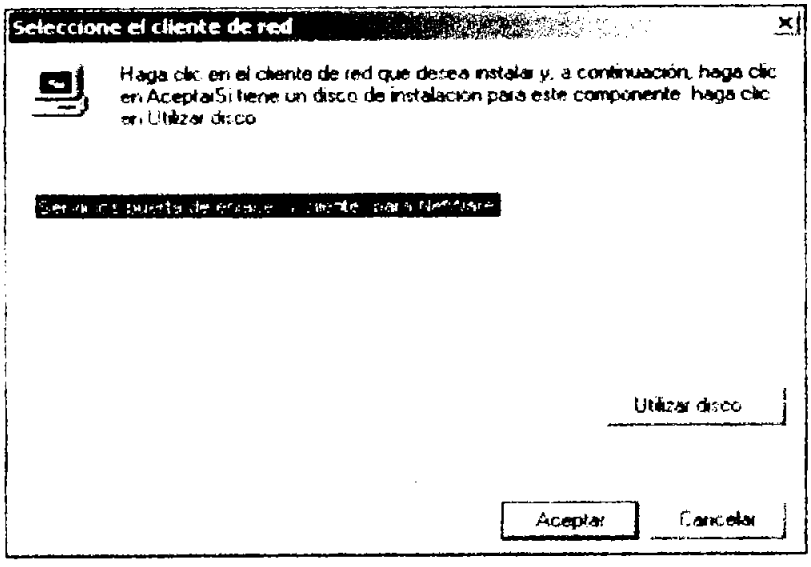


Figura 2.1 Pantalla de instalación del cliente para el Servicio puerta de enlace (y cliente) para Netware.

Antes de crear un recurso, debe estar habilitada la puerta de enlace, para hacerlo simplemente activar la casilla de verificación Activar Puerta de Enlace en el cuadro de diálogo Configuración de Puerta de Enlace. A continuación escribir el nombre de usuario y la contraseña creados en el entorno Netware para esta puerta de enlace, tener en cuenta que esta cuenta se escribirá en el registro cada vez que se inicie el servidor, sin intervención humana. El sistema esta ahora preparado para comenzar a crear recursos compartidos. Para crear un recurso compartido hacer lo siguiente:

1. Hacer clic en el botón Agregar, aparecerá la ventana Nuevo recurso compartido.

2. En el campo Nombre de Recurso Compartido escribir el nombre del recurso como aparece desde el servidor de Windows. A continuación pulsar TAB.

3. En el campo Ruta de acceso a la red, escribir la ruta UNC al recurso del servidor de Netware al que debe de conectarse (por ejemplo \\servidor1\vol1). A continuación, pulsar la tecla TAB.

4. Si se desea que aparezca algún comentario para el cliente Windows, escríbalo en el campo comentario y presionar la tecla TAB.

5. Hacer clic en la flecha que aparece hacia abajo situada al lado de la unidad de disco y seleccionar la letra para la conexión con la puerta de enlace. A continuación pulsar la tecla TAB.

6. Si se desea limitar el número de usuarios que pueden utilizar la conexión (con el fin de controlar el número de licencias o el ancho de banda), activar el botón de opción Permitir y escribir un número en el cuadro que indique el número de usuarios que se permiten en un momento determinado.

7. Hacer clic en Aceptar para terminar la configuración de la puerta de enlace.

2.1.4 SERVICIOS DE ARCHIVO E IMPRESIÓN PARA NETWARE.

La compartición de ficheros es la forma más básica de trabajo en red que existe, y es una de las grandes diferencias entre Windows y Netware. Las diferencias están en la forma en que los usuarios tienen acceso a la estructura de archivos y en la forma en que Netware y Windows ponen a su disposición el recurso compartido y estructuran el directorio.

Una característica muy útil para el administrador es la posibilidad de establecer cuotas en la cantidad de almacenamiento que los usuarios tienen en el servidor. Hace unos años, los servidores de Windows no podían controlar esa capacidad. Una forma particularmente desagradable de saturar un servidor era que un empleado descontento copiara más archivos al servidor de los que el servidor tuviera la capacidad de almacenar. Un Administrador con sentido común no pondrá los archivos del sistema en una unidad compartida, pero en un servidor de archivos sin capacidad para almacenar archivos es bastante inútil. Windows 2000 y Netware tienen hoy en día posibilidad de establecer cuotas de disco. Sin embargo existe una gran diferencia en como se realiza.

Una cuota de disco en Windows 2000 es un límite o una advertencia que se le pone a un usuario sobre la capacidad de información que puede colocar en el disco. Cuando se establece una cuota, se puede hacer que sucedan 2 acciones. La primera es que se pueda detener al usuario y no se le permita colocar más información en el disco. Segunda es que se puede escribir un suceso en el registro de sucesos. Estas acciones son independientes para permitir a los administradores avisar que el usuario ha excedido el límite evitando así la posible interrupción de una tarea importante con el fin de imponer la limitación.

Cuando a los usuarios se les impone un límite, también se les puede establecer el límite de advertencia. Este es el momento en el que se le indica que ha alcanzado un cierto porcentaje de la máxima disponibilidad de almacenamiento de sus cuentas.

En un ambiente Netware, los límites se pueden establecer en cualquier punto en la estructura del directorio. De aqui que los administradores puedan establecer un límite a la cantidad de espacio que un usuario tiene en su propio directorio raíz (ver la figura 2.2). La diferencia es que luego el usuario es capaz de cambiar directorios y tener un límite diferente. Si el administrador quiere limitar por ejemplo, la cantidad de información que pueda el usuario guardar en sus directorios raíz en el servidor, pero permite guardar más información en carpetas de departamentos, puede hacerlo.

La ventaja del sistema Windows es que evita que un Hacker llene un disco desde una dirección incontrolada. La ventaja del sistema Netware es que permite más flexibilidad pero mucho menos control.

Desde la perspectiva del usuario la conexión a las impresoras compartidas en estos 2 sistemas operativos es la misma, Los usuarios en el ambiente de Windows 95/98 no notaran la diferencia de conectarse a un servidor de impresión de Netware que al de Windows 2000. El usuario tiene acceso simplemente agregando la impresora y apuntando al recurso compartido de red. Las diferencias técnicas entre ambos sistemas son mínimas.

La diferencia aparece cuando se conecta un cliente de Windows 2000 o de Windows NT , en un ambiente de Windows NT/2000, los controladores se entregan a un cliente de Windows NT/2000 automáticamente cuando el cliente elige la impresora desde entorno de red. Los servidores Netware son capaces de distribuir controladores a éstos y a otros clientes pero en el ambiente de Windows se hace este proceso de forma más compacta, Los clientes de Windows 95/98 también son capaces de distribuir controladores desde el servidor Windows NT/2000, pero al igual que el servidor de Netware deben de configurarlo.

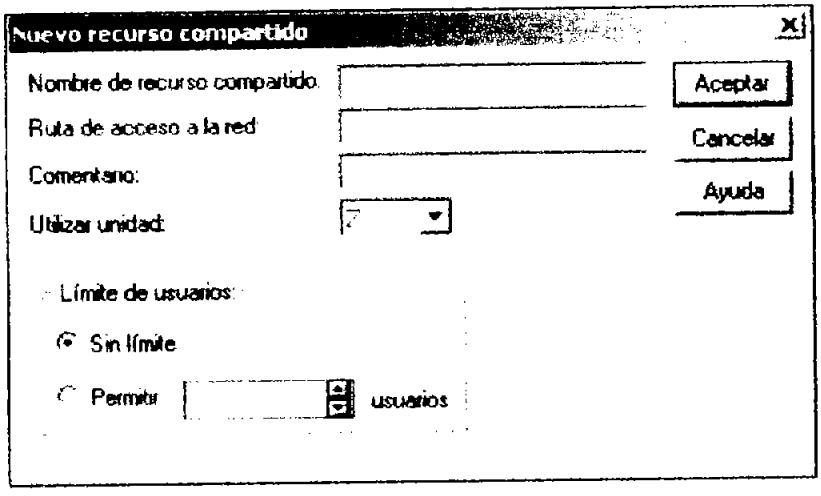


Figura 2.2 La ventana Nuevo recurso compartido para la puerta de enlace.

Si el cliente Netware se instala en un cliente Windows, entonces los servidores de impresión Netware responden al comando NET USE de Windows con NET USE LPT1 \\nombre_recurso_compartido_impresión. Sin embargo, el comando natural en el entorno Netware es CAPTURE, el comando CAPTURE es muy similar al comando NET USE en el sentido de que el usuario deberá saber el nombre del servidor de impresión y el nombre del recurso compartido (Llamado Cola u Objeto de impresión).

2.1.5. CONECTIVIDAD Y CONVIVENCIA.

Dependiendo que plataforma se este utilizando y a que recursos de la red se necesita accesar, será necesario utilizar NWLINK junto con otras herramientas, la siguiente tabla lista diferentes opciones para utilizar NWLINK:

PLATAFORMA	EJECUTANDO	PARA PERMITIR EL ACCESO A
WINDOWS 2000	NWLINK	APLICACIONES CLIENTE / SERVIDOR EJECUTÁNDOSE EN UN SERVIDOR NETWARE
WINDOWS 2000	NWLINK Y SERVICIOS PARA CLIENTES NETWARE O NWLINK Y PUERTA DE ENLACE PARA NETWORK	SERVIDORES NETWARE PARA ARCHIVOS Y SERVICIOS DE IMPRESIÓN
CLIENTE DE NETWARE	IPX CON NETBIOS O SOPORTE PARA SOCKETS WINDOWS	COMPUTADORAS EJECUTANDO WINDOWS 2000 (CON NWLINK INSTALADO) EJECUTANDO APLICACIONES IPX COMO MICROSOFT SQL SERVER
CLIENTE DE NETWARE	IPX	COMPUTADORAS EJECUTANDO WINDOWS 2000 SERVER (CON NWLINK INSTALADO Y SERVICIOS DE ARCHIVOS E IMPRESIÓN PARA NETWARE).

Los servidores de Netware son bastante parecidos a los servidores de Windows ya que tienen muchos niveles diferentes de conexión. El tipo de conexión necesaria para hacer uso de todos los servicios disponibles en el servidor se llama conexión nativa.

Para comprender la diferencia entre una conexión nativa y otras conexiones, servirá de ayuda hacer uso del concepto de una conexión Web en Internet frente a una conexión desde un cliente Windows que se conectará a un recurso compartido. Un cliente Web da acceso a un único proceso y no es capaz de asignar una impresora a recursos compartidos de impresión o unidades. Los usuarios nativos en los sistemas Netware pueden utilizar completamente las utilidades nativas de Netware, como mostrar los servidores disponibles de Netware, enviar mensajes a otros usuarios Netware y asignar recursos compartidos de Netware mediante letras de unidades locales (Asignaciones) y rutas de acceso a impresora (captura).

Cuando se conectan a servidores Netware, tienen 2 formas básicas de conexiones nativa:

- Enlace
- NDS

La conexión en forma de enlace se parece bastante a la conexión a un grupo de trabajo de Windows NT. Los usuarios se conectan a cada servidor de forma individual y cada servidor tiene sus propios usuarios y una lista de grupo; NDS utiliza la forma de conexión que se utiliza en Active Directory. un usuario se conecta al directorio, y a continuación se le permite tener acceso a los recursos que ofrece el directorio.

Tanto Netware como Windows 2000 contienen servicios de directorio jerárquicos, pero tienen sus diferencias. Las diferencias básicas de estos servicios son desde el aspecto filosófico de tres elementos: Particionamiento y replicación, delegación de autoridad sobre objetos en el directorio y la adhesión a la convención de nombres al sistema DNS, funcionalmente los dos se utilizan con el mismo propósito.

Novell Netware 5.0 mantiene el apoyo a dos sistemas de archivo: el Sistema de Archivo NetWare (NWFS.- Netware File System) y los Servicios de Almacenamiento Novell (NSS.- Novell Storage Services).

NWFS es la última aplicación del mismo sistema de archivo de 32-bits que ha servido a Novell durante muchos años en las versiones anteriores de NetWare. En la versión 5.0, su aplicación es muy similar que lo encontrado en la versión 4.1 y 4.11. Debutando en el mercado con NetWare 5.0, NSS representa la próxima generación de Novell, el sistema de archivo de 64 bits que se quiere como un reemplazo eventual NWFS.

NWFS se mantiene en NetWare 5.0 por dos razones primarias:

- Los archivos del sistema operativo deben residir en un volumen de NWFS

- NWFS proporciona versiones anteriores de NetWare a la compatibilidad dirigida hacia atrás cuando usó un guión de actualización de lugar. El sistema operativo archiva que ellos no pueden guardarse en un volumen de NSS.

El apoyo de Namespace determina los tipos de archivos y directorios que pueden guardarse en un volumen. Por defecto, NWFS sólo apoya a MS-DOS 8.3 (sistema operativo carácter archivo nombres). Pueden instalarse los módulos del loadable separados y pueden utilizarse para mantener el apoyo Windows 95, OS/2, Windows NT, el sistema de Archivo de Red de UNIX (NFS.-Network File System) y Apple Macintosh (archivo de vía LONG.NAM, NFS.NAM, y MAC.NAM.

Debe notarse que para cada módulo del namespace cargado, se requiere una entrada separada dentro del sistema del archivo para guardar huella de información del namespace para cada archivo físico y directorio.

En un sistema con todos los espacios del nombre instalados, se harán cinco entradas del directorio–uno para cada namespace. NSS, en contraste, el apoyo para el namespace por defecto no requiere las entradas del directorio separadas.

Por lo que se refiere a el valor-agregado del sistema de archivo, NetWare 5.0 proporciona lo siguiente en el NWFS:

La Compresión de Archivo (File Compresión).- proporciona compresión de datos de archivos y directorios en todos los volúmenes. Esto permite guardar los datos en menos espacio al que normalmente se requeriría espacio del disco reservado para el usuario terminal.

La Asignación de Subalterno de bloque (Block Sub-Allocation).- permite al sistema operativo poder utilizar el espacio sin usar dentro de cada bloque físico; guardar la información adicional, produciendo en el espacio del disco menos gasto sobre todo en los sistemas con el tamaño del bloque grande.

Recuperación de Archivos (Salvaje Undelete).- proporciona protección de recuperación de archivos borrados para todos los archivos, permitiéndoles a los usuarios recuperar los archivos y directorios que se anularon accidentalmente dentro de una cantidad razonable de tiempo.

Arreglo en caliente (Hot Fix).- proporciona la redirección de los datos a un área para prevenir la corrupción de los datos en caso de errores de los medios de comunicación que pueden ocurrir en el disco. Esto permite al servidor seguir corriendo, en caso de que los errores de los medios de comunicación de disco sean menores, permite ahorrar tiempo al administrador de la red para un óptimo desempeño.

2.1.6.-HERRAMIENTAS DE MIGRACIÓN PARA SERVICIOS DE DIRECTORIO.

La conversión de un directorio de Netware a Active Directory de Microsoft sería prácticamente imposible si el administrador tuviera que hacerlo manualmente. Si el directorio es suficientemente grande, es mejor que el administrador comience a crearlo desde cero en lugar de intentar convertirlo. Afortunadamente Microsoft proporciona una herramienta llamada Herramienta de Migración para servicios de directorio.

Al igual que la antigua herramienta que poseía Windows NT, esta herramienta lo que hace es sacar todos los usuarios, grupos e información de los servidores Netware. Se puede utilizar para volver a colocar servidores Netware o simplemente para replicar la información del usuario y del grupo desde el entorno Netware en el que existe. En cualquier caso, ahorra mucho tiempo.

Una de las mejores características de esta herramienta es su capacidad para ejecutar un modelo de la migración antes de copiar un usuario una pieza simple de datos. Esto permite al administrador estar preparado para cualquier complicación antes de que suceda.

La Herramienta de Migración se puede instalar durante la instalación inicial de Windows 2000 o posterior. La instalación es simple solo es cuestión de agregar el servicio desde el panel de control Agregar o Quitar Programas en Agregar o quitar componentes de Windows.

Una vez instalada la herramienta, aparecerá en el menú Inicio, Programas, Herramientas Administrativas. La ventana que se abre permite poder crear un proyecto nuevo (ver la figura 2.3).

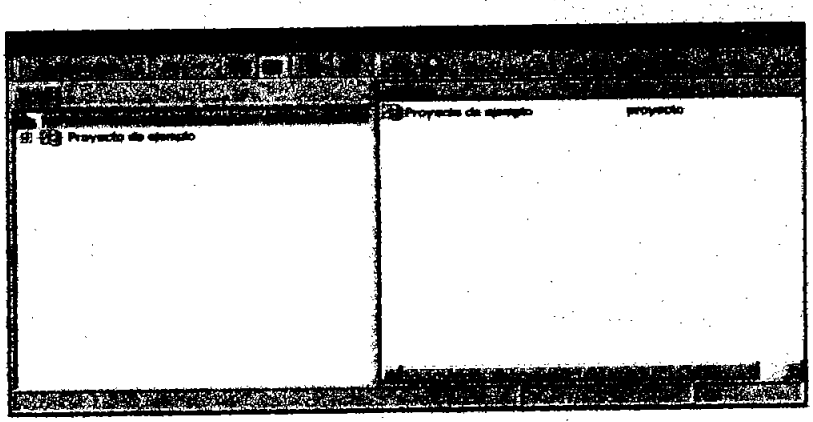


Figura 2.3 Pantalla inicial de la herramienta de migración.

Antes de crear un proyecto, se debe establecer las opciones que guiaran el proyecto a través de la información que encontrara. Las opciones tienen en cuenta las diferencias y complicaciones que pueden existir en los 2 sistemas y permite al administrador controlar dichas diferencias.

Estas son las fichas de opciones:

- **GENERAL.-** En esta ficha se define la ubicación del archivo de proyectos así como el filtrado de objetos que se mostrarán durante el proyecto (ver la figura 2.4). Si decide no activar la casilla de verificación Mostrar sólo los objetos que se admiten en los Asistentes para configurar y descubrir, aparecerán los objetos que no se pueden agregar al directorio activo. Esto puede servir de ayuda como una comprobación real para los elementos que no se utilizarán.

- **DESCUBRIR ENTORNO DE NOVELL.-** Para controlar el objeto predeterminado del enlace de la organización creado en el proyecto, debe escribir en el Nombre predeterminado del **enlace** de la organización (ver la figura 2.5). Si se agrega un número máximo de objetos que aparecen en la vista puede que se detenga el proyecto una vez que alcance un número no controlable de objetos. Sin embargo, este número puede detener un proyecto y no permitir que finalice. Es mejor usar esta opción como una manera de alterar el tamaño del proyecto y no como un regulador de proceso.

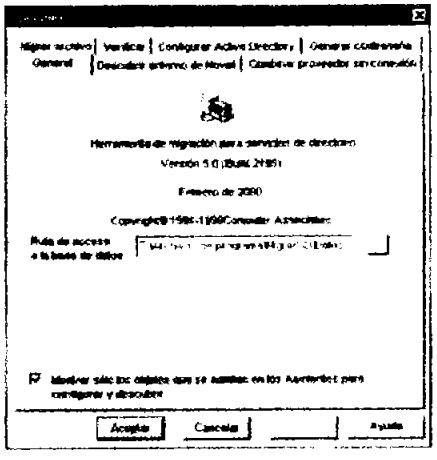


Figura 2.4 Opciones de la ficha General.

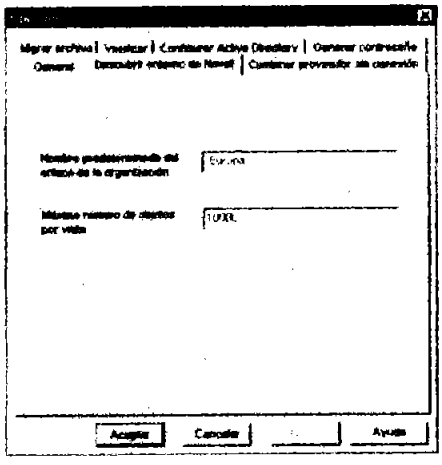


Figura 2.5 Descubrimiento del entorno Novell.

- **MIGRAR ARCHIVO.-** Cuando migre archivos y directorios, puede haber directorios duplicados y archivos que existan en los servidores del proyecto. Cuando suceda esto, es posible definir reglas que le indiquen al sistema como comportarse. Si estas opciones no se han definido manualmente, es posible sobre escribir los directorios y archivos.

- **VERIFICAR MÉTRICA DE ÁRBOL.-** Al igual que el Árbol NDS se migra a Active Directory, se hace una comprobación de las dependencias de usuarios y grupo. Durante esta comprobación el administrador puede controlar el número y valor de los objetos que se colocaran en el directorio.

- **CONFIGURAR ACTIVE DIRECTORY.-** Los objetos de dirección existentes pueden estar duplicados al igual que los objeto de archivos, en estas ocasiones es necesario establecer reglas que le indiquen a la herramienta de migración como manejar el proceso (ver la figura 2.6). Este mismo concepto se establece en la ficha Combinar proveedor sin conexión. La diferencia entre un objeto con un sólo valor o con valores múltiples es que un objeto con valores múltiples puede conectar varios objetos. Los objetos como los miembros de un grupo se consideran con valores múltiples.

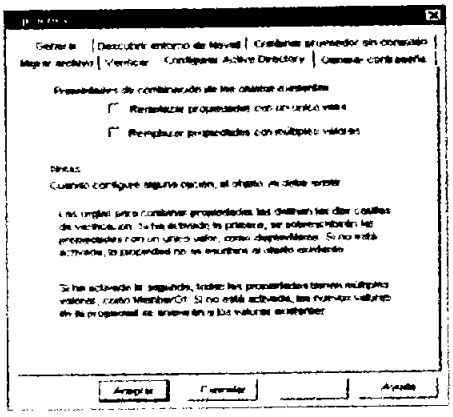


Figura 2.6 Ficha Configurar Active Directory.

- **GENERAR CONTRASEÑA.-** Cuando se realiza la migración, Windows no puede leer las contraseñas en el árbol NDS de Netware incluso con los permisos adecuados del administrador. Por ello, un Administrador debe establecer una regla para controlar las contraseñas que se darán a los usuarios para la primera conexión, es posible no crear contraseñas, crear una contraseña aleatoria, crear una contraseña a partir del nombre de usuario o asignar a todos los usuarios la misma contraseña. Una vez que se crea la contraseña (o no), el administrador puede avisar a los usuarios para que cambien las contraseñas todos a la vez (ver la figura 2.7).

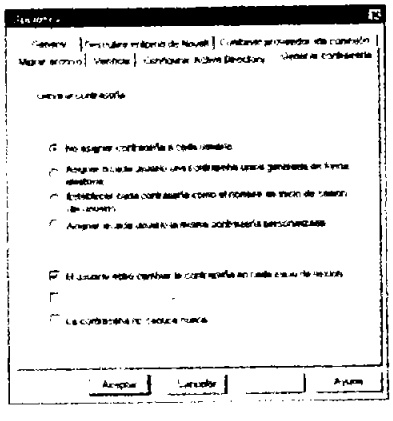


Figura 2.7 Ficha General contraseña

Una vez establecidas las opciones, la creación del proyecto es sumamente sencillo. Para crear el proyecto hacer lo siguiente:

1. Elegir el menú Acción, y a continuación, Nuevo Proyecto.

2. Introduzca el nombre del proyecto en el espacio que se le ofrece y pulsar Enter.

Ahora el proyecto debe de llenarse con los recursos que se necesitan para migrar. También debe de especificar dónde los migrará. Realizando lo anterior el proyecto recibe el nombre de "Creación de vistas". Una vista es una vista gráfica o herramienta que se puede utilizar para recopilar los objetos que se migrarán. Los objetos extra o incompatibles no aparecerán enumerados y pueden provocar problemas en entornos grandes (ver la figura 2.8).

La primera vista a crear es Ver desde Netware. Ésta es la vista inicial de los objetos de descubrimiento o NDS que se migraran. Esto permite al Administrador del proyecto moverse a través de objetos de descubrimiento o el árbol NDS de objetos.

Para crear la vista Ver desde Netware, hacer lo siguiente:

1. Hacer clic con el botón secundario en el proyecto, elegir Nuevo y a continuación hacer clic en Ver desde Netware.
2. Introducir el nombre de la vista, nombre del autor y una descripción opcional y hacer clic en siguiente. Aparecerá una lista de los servidores disponibles.
3. Seleccionar el objeto de Enlace o servidor NDS y a continuación, hacer doble clic en los Árboles.
4. Hacer clic en un árbol y luego hacer doble clic en el árbol para mostrar sus objetos contenedor.
5. Hacer clic en un objeto contenedor y a continuación, hacer doble clic en el contenedor para mostrar los objetos secundarios.
6. Después de seleccionar un objeto, Hacer clic en Agregar contexto para definir el contexto de descubrimiento a nivel del objeto seleccionado, aparecerá en el panel Detalles del cuadro de diálogo.
7. Hacer clic en Siguiente y el cuadro de diálogo mostrará un resumen del nombre de la vista y del contexto especificado para la operación de descubrimiento.
8. Hacer clic en Finalizar y un cuadro de diálogo mostrará los mensajes de procesamiento.

Una vez creada una vista del recurso Netware, la herramienta de migración se llenara con los objetos que se puedan migrar. El proceso de migrar estos objetos es sencillo.

Lo más importante que hay que tener en cuenta mientras se mueven objetos es la relación entre el tipo de objeto y el objeto al que se mueve o se desplaza.

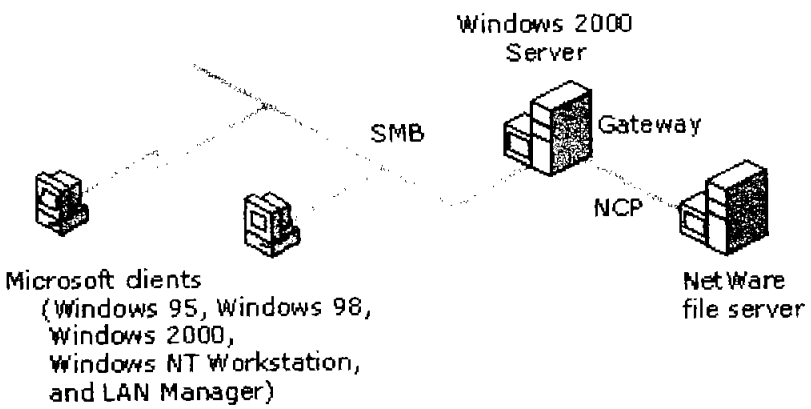


Figura 2.8 Creación de un nuevo Proyecto.

Para migrar archivos de un servidor a otro o de varios servidores a un servidor también deberán realizarse con la herramienta de migración. Se pueden migrar archivos y directorios con esta Herramienta y mover los atributos y permisos junto con los datos. Esto puede ser una tarea difícil o imposible sin esta utilidad (ver la figura 2.9).

Debe de utilizar el asistente para migración de archivos. Este asistente le guiara paso por paso a través del proceso de seleccionar y copiar. Para Inicializar el asistente hacer lo siguiente:

1. Hacer clic con el botón secundario en el objeto Herramientas de migración para servicios de directorio, o en un volumen de objeto en la consola Migración de Servicios de Directorio y elegir Todas las Tareas y a continuación Copiar Archivos.
2. Cuando se inicie el asistente seleccionar Siguiente.
3. Seleccionar Sí, migrar archivos. A continuación, hacer clic en Siguiente.
4. Para mostrar todos los volúmenes y directorios de la configuración Netware hacer doble clic en volúmenes de origen.
5. Hacer clic en un volumen de origen o directorio y arrastrarlo sobre el recurso compartido.
6. Hacer clic en Siguiente.
7. Seleccionar un elemento de la vista origen y a continuación, hacer clic en Eliminar para quitar el objeto, o bien hacer clic en Modificar para mostrar un cuadro de diálogo de modificación.
8. Hacer clic en Examinar al lado del directorio de destino. Aparecerá una lista de ubicaciones de directorios disponibles. Seleccionar un directorio de destino.
9. Habilitar Crear Recurso Compartido para crear una nueva ubicación del recurso. A continuación hacer clic en Siguiente.
10. Hacer clic en siguiente para migrar todos los archivos. De esta forma regresara al cuadro de diálogo de modificación para migrar recursos y archivos compartidos. Hacer clic otra vez en siguiente, se le pedirá que actualice los objetos del volumen individual o hacer clic en seleccionar todo.
11. Hacer clic en comprobar espacio de disco para asegurarse de que hay suficiente espacio de disco para llevar a cabo la migración de archivos planificada. A continuación Hacer clic en siguiente.
12. Hacer clic en Actualizar o No Actualizar. A continuación, Hacer clic en siguiente. Se pedirá que termine la migración. Hacer clic en Finalizar para iniciar la migración.

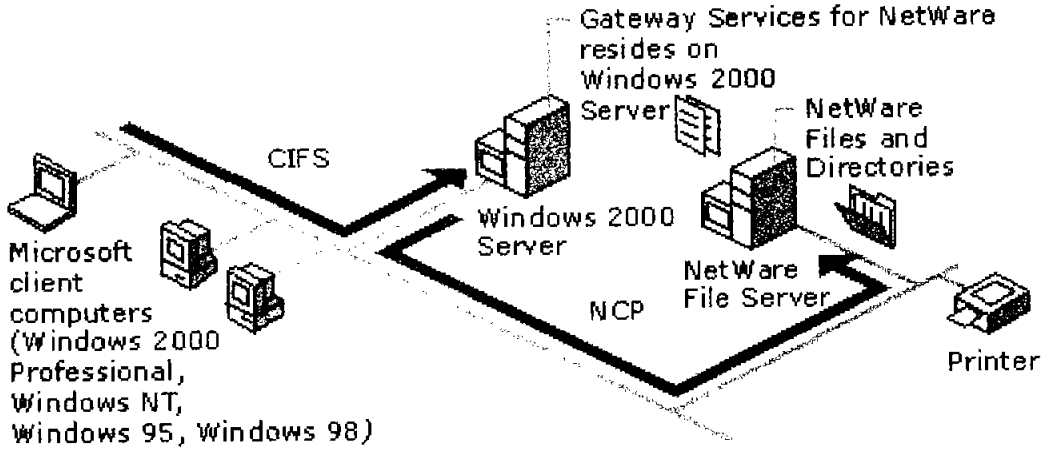


Figura 2.9 Red trabajando con Novell Netware y Windows 2000.

TABLA DE COMPARACIÓN

CARACTERÍSTICAS	Netware 5.0		Windows NT	Windows 2000
	NWFS	NSS	NTFS	NTFS5
INTEGRANDO NOMBRES DE ESPACIO		X	X	X
REDUCCIÓN DE ARCHIVOS				
LA ASIGNACION DE SUBALTERNO DE BLOQUE	X		X	X
SALVAJE UNDELETE(RECUPERACIÓN DE ARCH.)	X		X	X
HOT FIX	X			
SPANNING	X		X	X
MIRRORING(ARREGLO DE DISCO ESPEJO)	X		X	X
DUPLEXING(ARREGLO DE DISCO DUPLEX)	X		X	X
ARREGLO DE DISCO SIN PARIDAD			X	X
ARREGLO DE DISCO CON PARIDAD	X		X	X
HSM/RSM APLS	X			X
SOFTWARE DE BACK UP INTEGRADO	X		X	X
ARCHIVO ESPARCIDO				X
CAMBIO DE VOLUMEN				X
PUNTO DE UNIÓN				X
DISTRIBUCIÓN DE LIGAS RASTREADO				X
CUOTAS DE DISCO	X			X
DESCRIPTOR DE DISCOS				X
ADMINISTRADOR DE DISCOS EN LINEA				X
ADMINISTRADOR DE ALMACENAMIENTO REMOVIBLE				X
ADMINISTRADOR DE ALMACENAMIENTO JERÁRQUICO				X
SOPORTE AL DEFRAGMENTADOR DE DISCOS				X
SOPORTE I20				X
CANAL DE FIBRA				X
IEEE 1394				X
ARCHIVO DE SISTEMA DISTRIBUIDOS				X
SOPORTE CGI		X	X	X
JAVA SCRIPT SERVER SOPORTE SCRIPT			X	X
INTEGRACIÓN DE SERVICIOS DE			X	X

COMPONENTES				
REDIRECCIONAMIENTO		X	X	X
CONTENIDO DE EXPIRACION HTTP			X	X
EXTENSIONES PARA SERVIDOR FRONTPAGE			X	X
SOPORTE A PLUG AND PLAY				X
CONFIGURACIÓN DE CAMBIOS QUE NECESITE REINICIAR		X	X	
SOPORTE A ADMINISTRADOR DE ENERGÍA				X

2.2.- CONECTIVIDAD CON UNIX

Uno de los puntos fuertes de Windows 2000 es su capacidad para poderse conectar a diferentes sistemas operativos y entornos. UNIX es, y seguirá siendo El sistema operativo que se ejecute en Internet.

En la empresa de telefonía se tienen conectadas las bases de datos de radios, accesorios, cobranza, tiempo aire, existencias y demás creadas en diferentes aplicaciones y programas que se encuentran ejecutándose en una pequeña red de UNIX, al parecer las bases de datos en UNIX poseen mucho menos riesgo a caídas en el servidor que otro sistema operativo, muchas de ellas han sido diseñadas en E.U., por programadores en diferentes lenguajes como Oracle. Los servidores con Windows 2000 deben de conectarse al servidor de UNIX para tener acceso a las bases de datos y así repartirlas hacia las diferentes estaciones de trabajo que necesite el usuario. Aquí explicaremos la conectividad que existe entre los servidores con Windows 2000 y el servidor de UNIX.

Windows 2000 y UNIX son sistemas operativos muy diferentes Windows 2000 lo crea y soporta la compañía Microsoft. Por ello cada instalación de Windows 2000 es muy similar a todas las demás instalaciones y el software que funciona en una máquina funcionara siempre en otra máquina, suponiendo que tenga la misma arquitectura de microprocesador. En el ambiente Windows hay un directorio estándar para los archivos DLL (%SYSTEMROOT%\\Winnt\\System32), directorios estándar para programas cliente (\Archivos de Programa) y un formato estándar para guardar información de configuración (el registro). Estos estándares junto con una gran base de usuarios consolidada, facilita y hace más rentable la programación para plataformas Windows de lo que sería sin estándares. Eso también reduce enormemente los costos de servicios técnico, ya que un conjunto de máquinas que ejecuten Windows son bastante similares, y si una requiere un cambio en el registro para solucionar cierto problema, el resto de equipos probablemente necesitara el mismo cambio.

Los sistemas Windows también son compatibles a nivel binario dentro de la misma arquitectura. En otras palabras un programa que se ejecuta en Windows 98 se ejecutara casi seguro en Windows 2000 (Sobre Hardware Intel) sin problemas.

En el mundo UNIX las cosas no son tan sencillas. Al principio UNIX lo creó AT&T y fue un sistema de código libre, de esta forma quien tenía UNIX podía hacerle modificaciones. Últimamente después de la desintegración de AT&T, a la compañía se le permitió vender UNIX..

Así algunas personas en la Universidad de California en Berkeley USA crearon desde cero un nuevo sistema operativo del tipo UNIX llamado Free-BSD. La palabra Free en el nombre hace referencia al hecho de que el código no se derivaba del de AT&T, por lo que estaba libre de los derechos de autor de AT&T.

Las versiones actuales de BSD (Berkeley System Development-Desarrollo de Sistemas de Berkeley), incluye Free-BSD y Net-BSD.

Al mismo tiempo, un estudiante finlandés: Linus Torvalds, estaba probando encontrar un sistema operativo bueno y barato para su estación de trabajo. Su problema era que AT&T todavía era propietario de UNIX que era muy caro en ese entonces, y los sistemas operativos de otros fabricantes no cumplían con sus necesidades. Por ello realizo algo que mucha gente hubiese deseado hacer: construyo su propio sistema operativo llamado LINUX. Después de muchos años de investigación y desarrollo Linux es uno de los sistemas operativos dominantes en Internet. Linux está disponible en varias versiones diferentes, que distribuyen tanto compañías comerciales como no comerciales, incluyendo a RedHat, Caldera y SuE.

Además de Free-BSD y Linux, los vendedores de estaciones de trabajo UNIX normalmente tienen su propia versión de UNIX. Incluyendo al gigante SUN (SunOS), Data General(DG/UX) y Hewlett Packard(HP/UX), sólo por nombrar unos pocos. Cada uno de éstos forman parte de AT&T System V original y de las variantes de BSD y las unifica.

A mediados de los años ochenta los fabricantes de UNIX decidieron adherirse a un estándar. Pero existen grandes diferencias en elementos críticos como el inicio del sistema operativo(System V Init o BSD Init), las localizaciones y formatos de archivos de registros, y los formatos de la información de configuración, ubicaciones y nombres de archivo. Por desgracia muchas de las diferencias existen hoy en día, tienden a no ser compatibles a nivel binario de una versión a otra, incluso dentro de la misma arquitectura. Es más los archivos de registros y los archivos de configuración están normalmente en sitios diferentes en máquinas diferentes.

2.2.1.-DIFERENCIAS CONCEPTUALES

Windows 2000 Server se ha diseñado para ser un servidor de empresa escalable que proporcione archivos, impresión y servicios de aplicación a estaciones de trabajo que ejecuten Windows. UNIX esta diseñado para funcionar tanto de cliente como servidor y para conectarse con otros clientes UNIX. Como resultado hay diferentes aproximaciones relacionadas con los problemas de las cuentas de usuario, seguridad y servicios de directorio.

Las cuenta de usuario son la forma en que un sistema operativo decide que usuarios pueden realizar que operaciones. Windows 2000 tiene un administrador de grupo al que pueden asignar varios usuarios, lo que esencialmente permite a dichos usuarios controlar todos los aspectos de la máquina. En el ambiente UNIX, hay una cuenta llamada root que tiene un nivel similar de permisos. En Windows 2000 las cuentas de usuario se almacenan en el registro, mientras que en el ambiente UNIX las cuentas se almacenan en un fichero de texto, como cualquier otra pieza de configuración de información. Los usuarios se definen en un archivo de texto, normalmente llamado passwd, que tiene un formato dependiente del sistema que normalmente incluye el nombre, pertenencia a un grupo y a una versión cifrada de la contraseña, el directorio raíz y el shell que ejecutará el usuario cuando inicie o finalice la sesión.

En la mayoría de los sistemas, las cuentas de usuario existen en cada sistema UNIX al que el usuario tiene acceso y existen varios esquemas para copiar información de cuentas sobre la red.

UNIX tiene una noción similar a la de Windows 2000 en cuanto al uso de grupos. **Los grupos** permiten a un conjunto de usuarios tener acceso a un conjunto de recursos sin tener que dar a cada usuario acceso a los recursos de forma individual. Al igual que Windows 2000 las cuentas de usuarios en Sistemas Operativos del tipo UNIX pueden asignarse a varios grupos.

Toda la seguridad de UNIX se basa en el concepto de archivo. En un Archivo de disco se pueden establecer tres niveles de seguridad:

*Propietario
*Grupo
*Todos

Cada Archivo es propiedad de un usuario especifico y de un grupo especifico. Se pueden establecer tres atributos en cada nivel: lectura, escritura y ejecución.

Una de las ventajas que posee UNIX es la siguiente: Permite a un usuario leer y escribir en un archivo, pero sólo desde un determinado programa (Por ejemplo si el usuario esta escribiendo datos en el archivo con un formato que se pueda corromper fácilmente). El programa se iniciará siendo propiedad de un usuario que tenga acceso al archivo y los usuarios individuales no tendrán acceso al archivo. Otro tipo de uso es el siguiente: Si un programa se debe de ejecutar durante horas específicas; por ejemplo, los juegos sólo se pueden ejecutar fuera de horas de trabajo, los programas de juego se podrían asignar a una cuenta que sólo se pueda iniciar fuera de horas de oficina y entonces el bit se establecería para que cualquiera pueda ejecutarlo.

Otra nota interesante en la seguridad UNIX: todo en UNIX es un archivo, por tanto si alguien quiere escuchar un archivo de sonido, el archivo de sonido se envía al dispositivo de sonido, que esta asociado, a un archivo llamado /dev/audio en algunos tipos de UNIX. Esto también implica que el usuario que ejecuta el archivo tiene acceso de escritura al archivo /dev/audio.

2.2.2 TELNET

TELNET proporciona servicios de terminal sobre una red, se utiliza ampliamente en el ambiente UNIX para ejecución y administración remota. Como la mayoría de las estaciones de trabajo tiene un Shell de comandos muy cómodo y potente, TELNET es una herramienta muy poderosa que permite a los administradores realizar cualquier cambio en la configuración de cualquier máquina, desde iniciar y detener servicios, hasta cambiar configuraciones y direcciones IP. TELNET es como sentarse delante de la consola.

Windows 2000 Proporciona dos versiones de TELNET. Una versión de TELNET en modo consola: normalmente se encuentra en %SYSTEMROOT%\\SYSTEM32\telnetc.exe y es un cliente TELNET en modo consola básico. Éste es un cliente estándar por lo que se maneja desde la línea de comandos. Para iniciarlo ir a inicio, dar clic en Ejecutar y escriba TELNET, y opcionalmente el nombre de la máquina a conectar; ejemplo: TELNET X, para conectarse a una máquina llamada X (ver la figura 2.10).

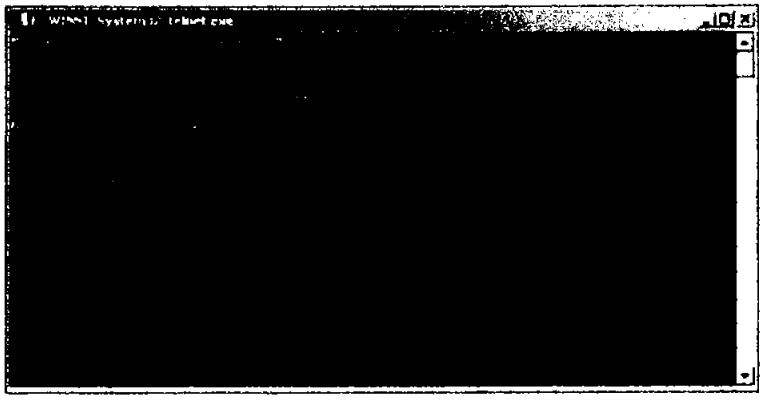


Figura 2.10 La ventana telnet de modo carácter, en modo consola. Esta consola se prepara para conectar con la máquina "kermit" mediante el comando open.

El TELNET basado en consola se ejecuta en 2 modos. El modo consola tiene una línea de comandos que aparece de la siguiente forma:

Microsoft TELNET>

Esta línea de comandos significa que el sistema está en modo de consola. Para ver una lista de comandos que pueda usar en la consola utilice el comando help, que mostrará lo siguiente:

Microsoft TELNET>help

Los comandos se pueden abreviar, los comandos permitidos son:

close	cierra la conexión actual
display	muestra los parámetros de visualización
open	conectarse a un sitio
quit	salir de TELNET
set	establecer opciones
status	escribe la información de estado
unset	desactivar opciones

Hay varios comandos básicos de la consola necesarios para poder utilizar TELNET. Si no aparece un nombre de equipo en la línea de comandos, el comando open abrirá una conexión. Por ello TELNET sé inicializa simplemente escribiendo TELNET en el cuadro de diálogo de Inicio, dar clic en Ejecutar, si escribe open X se iniciará una sesión con la máquina llamada X, los demás comandos se aplicaran por sí mismos.

Después de inicializar el cliente TELNET, ira automáticamente a modo conectado, para volver al modo consola mientras se sigue conectado se debe de teclear Ctrl+](Esto es un corchete). Para volver al modo conectado, pulsar Enter en una línea en blanco. Para cerrar una consola TELNET, hacer clic en cierre la sesión y en la consola escriba quit.

El otro cliente de TELNET es una interfaz gráfica que se encuentra normalmente en %SYSTEMROOT%\\SYSTEM32\TELNET.EXE. Ofrece dos emulaciones de terminal diferentes VT-100/ANSI y VT-52. La emulación VT-100/ANSI es la que más se utiliza y es establecida en forma predeterminada. Para tener acceso a estas 2 opciones de configuración:

Utilizar el menú Terminal, hacer clic en Preferencias (ver la figura 2.11), la pantalla de configuración también permite poder cambiar el color del fondo, así como la fuente y las propiedades de la fuente.

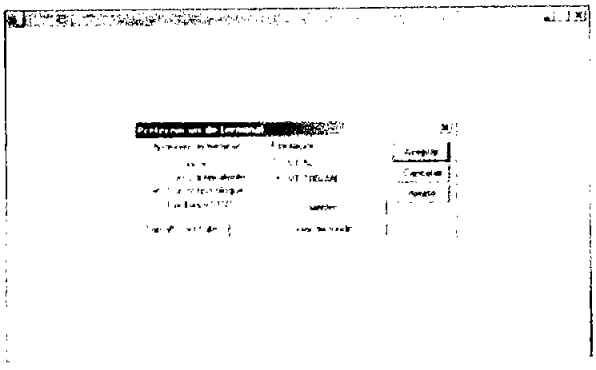


Figura 2.11 El Telnet gráfico con la ventana Preferencias de terminal abierta.

El Acceso remoto vía TELNET.- Los servicios para UNIX mantienen a un servidor del TELNET y cliente del TELNET Windows. TELNET es un protocolo basado en TCP/IP que permite conectar las estaciones de Trabajo remotas a una computadora. El servidor de TELNET y el Cliente proporcionan una manera para acceder y administrar a las computadoras basadas en Windows remotamente.

El Servidor de TELNET.- Con el servidor del TELNET para Windows, los usuarios de UNIX pueden conectar a las computadoras de Windows para ejecutar los programas o administrar a la computadora. Esto les permite a los administradores manejar a las computadoras de Windows sin dejar su estación de trabajo.

El servidor de TELNET apoya a un nuevo tipo terminal llamado VTNT que apoya el acceso a la funcionalidad completa de la Consola de Windows. El servidor de TELNET también apoya el esquema de autenticación NTLM que permite a los Servicios de UNIX y a otros clientes del TELNET que apoyan NTLM para conectarse sin enviar una contraseña encima de la red. El servidor de TELNET apoya dos modos de funcionamientos, modo de consola y el modo gráfico.

El servidor de TELNET anota una variedad de actividades telnet-relacionadas, como intervenir, supervisando las sesiones del TELNET y enviar los mensajes a las conexiones del TELNET; le permite al usuario guardar aplicaciones que incluso corren después de desconectar.

El Cliente de TELNET.- Con el cliente de TELNET para Windows, los usuarios de Windows pueden conectarse a un UNIX remotamente o a la computadora basada en Windows y ejecuta los programas remotamente. El cliente de TELNET apoya una variedad de emuladores terminales incluso VT100, ANSI, y VTNT. También apoya autenticación que usa NTLM. Proporciona los rasgos para anotar la sesión entera del TELNET a un archivo. También apoya una variedad de opciones que son aplicables al conectarse a los servidores de TELNET.

2.2.3.- FTP

El protocolo FTP permite la transferencia de archivos desde servidores a clientes. FTP se basa en una serie de comandos para cambiar al directorio correcto e iniciar las transferencias de archivos. El archivo toma un Id, y una contraseña de usuario y trabaja dentro de la noción d seguridad de archivo del sistema operativo para determinar que archivos se pueden leer y si se aceptara o no un archivo de entrada, recordemos que por medio de IIS (Internet Information Services) se puede configurar correctamente dicho servicio en nuestro servidor. En la Empresa de telefonía se utiliza una pequeña hoja en la Intranet donde se pueden descargar manuales, folletos y Políticas y Procedimientos para todos los trabajadores de la compañía, por medio de este servicio se conectan a servidores UNIX para descargar datos e información para uso de las distintas areas de la empresa.

Existen varios Clientes diferentes de FTP, Windows NT incluye 2, para tener acceso al primero, vaya al explorador Web y escriba una dirección URL de FTP, como por ejemplo **ftp://ftp.x.com**, esto proporciona una interfaz de usuario gráfica familiar para FTP, que se vera como una ventana normal de Internet Explorer (ver la figura 2.12).

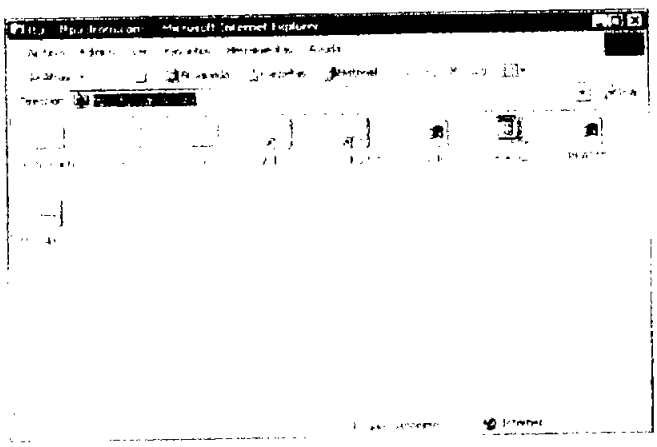


Figura 2.12 Esta es una sesión FTP al popular sitio ftp.cdrom.com. Puede tener acceso a ella escribiendo ftp://ftp.cdrom.com en el cuadro de diálogo Inicio, Ejecutar.

El otro cliente FTP es el cliente de línea de comandos y se puede iniciar desde el símbolo del sistema (o menú inicio) escribiendo ftp<dirección>, la dirección es exactamente el nombre de la máquina a la que se puede enviar la petición FTP.

Con cualquiera de los 2 métodos, se trasmiten los nombres de usuario y contraseña sobre la red en formato de texto simple, por lo que cualquiera que posee un analizador de red, como Network General Sniffer o el monitor de Red de Microsoft, podrá ver las contraseñas y utilizarlas.

La Herramienta de Sniffer se utiliza en la red para monitorear los sitios de Internet no autorizados a los que los usuarios están logrando el acceso así como también detecta si algunas máquinas están en una zona de juegos en Internet, esto se logra cuando el equipo comienza a mandar varias peticiones al servidor y comienza accesar a direcciones IP no autorizadas. Al usuario que se le encuentra utilizando mal uso de dichos servicios es reportado a su jefe inmediato y si reincide se le toma una sanción administrativa.

A continuación se explican los comandos FTP habituales:

- **OPEN**.- Se utiliza para abrir una conexión (Por ejemplo OPEN FTP:X.COM abrirá una sesión con el servidor FTP de la compañía X).
- **USER**.- El nombre de usuario que se usa para autentificar la sesión. Esté es el usuario genérico "anonymous" con la contraseña (tradicionalmente) "guest", o es un Id. de usuario real.
- **PASSWORD**.- Normalmente abreviado como PASS, el comando PASSWORD se usa para transmitir una contraseña. Tenga en cuenta que al igual que el protocolo TELNET, FTP trasmite contraseñas en texto normal sobre la red y en algunas redes es vulnerable a ataques de piratas informáticos que usan software de rastreo en la red (en esta red no sucedió así, ya que con la herramienta de Sniffer se detecta quien esta realizando un mal uso).
- **BINARY**.- A menudo abreviado como BIN, este comando indica a FTP que use transferencia de ficheros binaria. La mayoría de los servidores usan ASCII como mecanismo estándar de transferencia de ficheros. Como ASCII es un estándar de 7 Bits, cualquier archivo binario enviado con el mecanismo de transferencia ASCII se corromperá. Éste es un comando de establecimiento de modo, por lo que después de este comando, todas las trasferencias se realizaran en modo binario hasta que se use el comando BINARY.
- **HASH**.- Este comando le indica a FTP que muestre una almohadilla(#) por cada 1,024 bytes transferidos. Esta es una buena forma para sesiones interactivas, con el fin de asegurarse de que la transferencia no se ha detenido.
- **CD**.- Cambiar directorio Este comando cambia del directorio actual al directorio destino en el servidor. Funciona igual que el comando CD de la línea de comandos.
- **LDC** (Local Change Directory, Cambiar Directorio Local). - Este comando cambia el directorio local del cliente a la trayectoria especificada.
- **LS o DIR**.- Lista el contenido de un directorio dado, o si no se especifica directorio, lista el contenido del directorio actual. Se admiten las opciones de tipo UNIX, como ls–l para listados de direcciones largas y ls -C para directorios en columnas (tener en cuenta que las opciones distinguen entre mayúsculas y minúsculas). Sin embargo el comando ls–l foot.txt creará una lista de directorio y colocara la lista en un archivo llamado foot.txt en el directorio actual. Esto es útil porque permite redireccionar la salida; por ello, los comandos como ls –l more se pueden utilizar para páginar la salida.
- **GET**.- El comando GET va seguido del nombre del archivo a transferir al cliente. El comando GET obtendrá un archivo. No obtendrá un directorio y no usará comodines. Por ejemplo, el comando GET *.* probara a encontrar un archivo llamado *.* y probará a transferirlo. No encontrara ninguno y la transferencia fallara. La característica de GET es que permite especificar un archivo de destino, por ello, GET ARCHIVO1 MIARCHIVO obtendrá el archivo llamado ARCHIVO1 y lo escribirá en un archivo llamado MIARCHIVO.
- **PUT**.- El comando PUT va seguido del nombre de archivo que se va a transferir al servidor. Al igual que el comando GET, el comando PUT no utiliza comodines.
- **MGET y MPUT**.- La M viene de Múltiple. De aquí que MGET obtuviere varios archivos y aceptara comodines, y MPUT colocara varios archivos en el servidor y también aceptara comodines. Los comodines son estándares de UNIX.
- **DELETE Y MDELETE**.- Normalmente abreviados como DEL y MDEL son los comandos de eliminación. DEL funciona con archivos individuales, mientras que MDEL funciona como comodines.
- ¡. Este comando inicializara un shell de comandos dentro de la sesión FTP.
- **QUIT**.- Este comando cerrara FTP.

La pregunta que se hace mucha gente en la compañía es: ¿Por que molestarse con tantos comandos si existe una interfaz gráfica?, La respuesta es la siguiente Por que en muchos casos el programa FTP debe ejecutarse como un proceso por lotes (Por ejemplo para obtener una copia de las transacciones del día anterior para importarla a la base de datos de SQL Server).

En ese caso es planificar la secuencia con el comando AT o cualquier otro servicio de planificación. Para realizar lo anterior, se debe crear un archivo ordinario de texto con el bloc de notas y escribir en el los comandos que necesitara FTP para ejecutarse, por ejemplo:

```
OPEN FTP.X.COM
USER anonymous
                    Guest
CD / bussys
                    GET LEAME.TXT
                    Quit
```

Cualquier combinación de los comandos listados funcionara dentro de una secuencia de comandos de FTP, por lo que los archivos se pueden enviar o recibir, Esto es muy útil para procesos por lotes nocturnos cuando es necesario obtener un archivo de cualquier máquina UNIX, pero también funciona con cualquier otra máquina que pueda ejecutar FTP.

2.2.4 MANEJO DE DISCOS

Se diseñan Servicios Microsoft para UNIX para facilitar la interoperabilidad entre los sistemas operativos Windows 2000 y UNIX. Los Administradores están buscando las soluciones para integrar una red heterogénea e información de la porción transparentemente entre las computadoras UNIX y Windows. Los usuarios deben enfrentar los pocos impedimentos moviendose entre computadoras que ejecutan los sistemas operativos diferentes en la misma red. Igualmente importante es que el costo de administración debe minimizarse.

Con Microsoft Windows 2000 los nuevos rasgos han agregado y mejorado la fiabilidad, disponibilidad, y escalabilidad, varios negocios se han integrado a las computadoras Windows en las redes de su empresa que tradicionalmente utilizaban UNIX.

Debido al Costo Total favorable de Funcionamiento (TCO) de computadoras que utilizan diferentes versiones de Windows, ellos están utilizando estas computadoras donde una vez se usaron las computadoras basadas en sistema operativo UNIX.

Sin embargo, muchos negocios tienen las inversiones significantes en los bancos de datos basados en UNIX, aplicaciones comerciales, y servidores que no se reemplazarán durante algún tiempo y se migrarán a Windows. Los clientes tienen una necesidad comercial genuina de hacer que los ambientes Windows y UNIX interactúen entre sí.

Para utilizar todo un sin fin de herramientas que Windows 2000 Server proporciona para poder trabajar con UNIX basta con instalar los servicios para UNIX (ver la figura 2.13). Estos servicios se pueden instalar desde agregar desde Mis Sitios de Red, y elegir propiedades, en el botón instalar elegir Servicios para UNIX. y posteriormente dar clic en finalizar.

Los servicios para UNIX versión 2 incluye Korn Shell para Windows y un juego de aproximadamente 60 utilidades de UNIX. Estas utilidades han estado disponibles en las computadoras de UNIX, y los usuarios de UNIX están muy familiarizados con ellos. El propósito de proporcionar estas utilidades es aliviar la tarea de programadores y administradores del sistema que migran a Windows desde las computadoras basadas en UNIX.

Los servicios para las utilidades de UNIX son útiles para hacer muchas tareas administrativas repetitivas. Éstos incluyen supervisar los procesos o ver el uso del disco y el espacio disponible. Utilidades que les permiten a administradores hacer las tareas repetitivas incluyen: ps, kill y cima para la dirección del proceso, y el du y df por el espacio en disco a supervisar. Los programadores usan las utilidades de orden-línea para una variedad de propósitos, por ejemplo, utilidades como el hallazgo, grep, o diff al procesar los archivos.

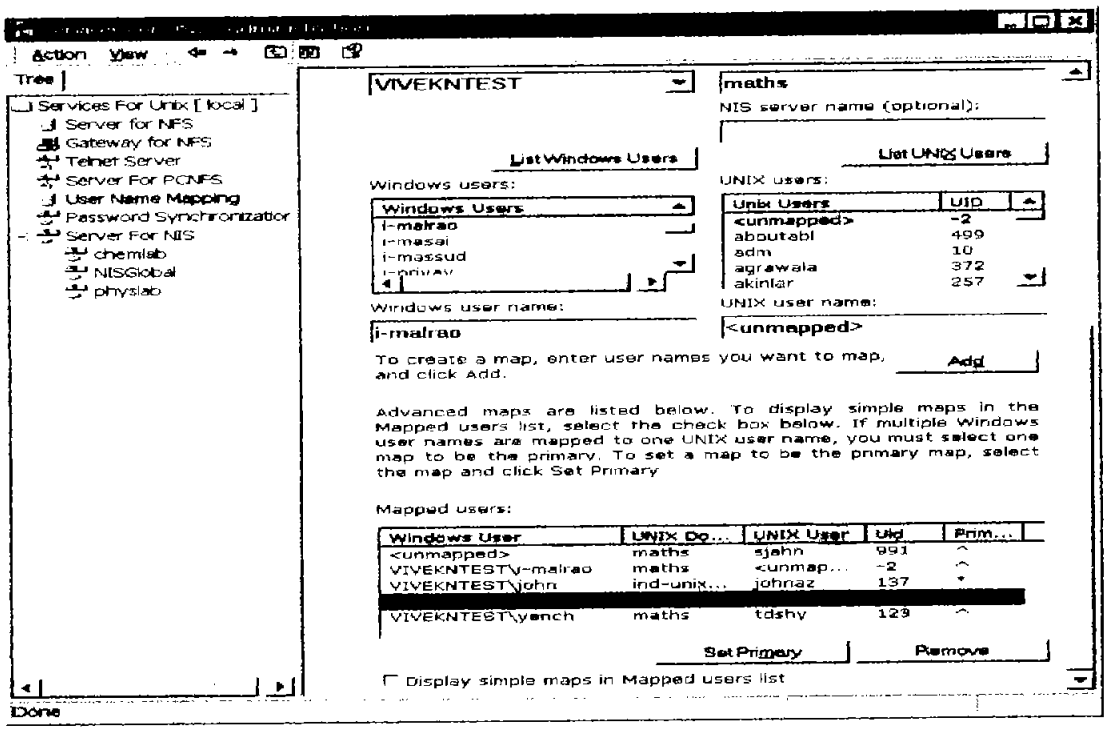


Figura 2.13 Ventana Servicios de Administración para UNIX.

La tecnología UNIX a comienzo de los años setenta logro un gran desarrollo en la administración de discos, la herramienta que vemos en Windows 2000 como el Administrador de Discos (ésta tecnología que en UNIX se llama montar una unidad en un directorio), permite cambiar la letra de la unidad de un disco duro o hacerlo parte de un directorio desde la raíz. El disco puede montarse en varias ubicaciones y en diferentes sistemas de archivos.

2.2.5 TCP/IP

TCP/IP es compatible con muchos mecanismos diferentes de conexión entre clientes y servidores. UNIX dispone de muchos mecanismos estándar distintos que usa para conectar servidores a clientes, incluyendo Xwindows (Interfaz gráfica de UNIX que simula un entorno Windows para ejecutar programas de forma remota) y otros protocolos propietarios. Un examen exhaustivo del archivo SERVICES que se encuentra en %SYSTEMROOT%\system32\drivers\etc, muestra una lista de los puestos estándar que utilizan los sistemas UNIX para comunicar diferentes tipos de información. El archivo muestra una lista de los puertos bien conocidos asignados por la autoridad de números asignados de Internet(IANA, Internet Assigned Numbers Autority). Todas las aplicaciones que se utilizan actualmente tienen asignadas números de puertos para que no colisionen entre sí y el número de puertos se adjunta al paquete IP, de manera que los servicios de red puedan enrutar cada paquete al programa correcto.

UTILIDADES TCP/IP.- Windows 2000 utiliza tres tipos de utilidades basadas en TCP/IP que son; Utilidades de Conectividad que se pueden usar para actuar y utilizar los recursos como los sistemas de UNIX, Utilidades de diagnostico que se pueden utilizar para descubrir y resolver problemas en una red TCP/IP. Servidor de software que proporciona la impresión y publicación de los servicios a los clientes TCP/IP basados en Windows 2000.

UTILIDADES DE CONEXIÓN

UTILIDAD	DESCRIPCIÓN
FTP	Transfiere archivos de cualquier tamaño entre un equipo Windows 2000 y cualquier computadora que ejecute el comando FTP Software de servidor.
Lpr	Envía los trabajos de la impresión a impresoras de UNIX remotas manejadas por el Demonio de Línea de Impresión (LPD), el software de servidor de impresión.
Rcp	Copia archivos entre una computadora con Windows 2000 y computadoras que ejecutan el Protocolo de Copia Remoto (RCP) el software del servidor.
Rexec	Ejecuta los procesos en las computadoras remotas.
Rsh	Ejecuta comandos en una computadora que ejecuta el Shell Remoto(RSH).
Tftp	Transfiere pequeños archivos desde una computadora con Windows 2000 a cualquier computadora que ejecute El protocolo de Traslado de Archivo Trivial (TFTP).
TELNET	Usa Terminales basadas en Autenticación remota para acceder a dispositivos de la red

UTILERIAS DE DIAGNOSTICO

UTILERIAS	DESCRIPCIÓN
Arp	Despliegues y modifica el Protocolo de Resolución de Dirección (ARP) en un escondite. Este escondite es una mesa local usada por Windows 2000 para resolver las direcciones de IP a los medios de comunicación para que acceda direcciones del mando usadas en la red local.
HostName	Regresa el nombre del Host de la computadora local
Ipconfig	Despliega la configuración de TCP/IP actual, también usado para liberar y renovar las Configuraciones de TCP/IP asignadas por DHCP.
Lpq	Obtiene la información de la cola de impresión para computadoras ejecutando el Demonio de Línea de Impresión (Line Printer Daemon, LPD).
Nbtstat	Despliega el NETBIOS local con la tabla de nombres, una tabla de nombres de NETBIOS registrada por las aplicaciones y los NETBIOS nombran un escondite, un escondite local que lista nombres de computadora NETBIOS que se han resuelto a las direcciones de IP.
Netstat	Despliega la información de la sesión del protocolo TCP/IP
Nslookup	Checa las grabaciones, seudónimos de organizador de dominio, servicios de organizador de dominio, e información del sistema operativo preguntando los servidores de DNS.
Ping	Verifica la configuración y comprueba la conexión IP
Route	Despliega o modifica la tabla de la ruta local
Tracert	Traza la ruta de un paquete hacia su destino
Pathping	Traza la ruta del paquete hacia un destino e informa de los despliegues sobre las pérdidas del paquete para cada segmento en el camino.

SOFTWARE BASADO EN SERVIDOR

SOFTWARE DE SERVIDOR	DESCRIPCIÓN
TCP/IP SERVICIOS DE IMPRESIÓN	Ofrece el servicio de Impresión TCP/IP, Line Printer Daemon (LPD) imprimiendo el servicio para las computadoras Windows 2000 corriente. Este servicio les permite a las computadoras de UNIX enviar los trabajos de impresión a las computadoras Windows 2000 corriente usando la Línea de Impresión Remoto (Lpr).
Internet Information Services (IIS)	IIS ofrece el software de servidor para proveer el servicio de Web, Gopher y FTP para proporcionar los servicios de la públicación TCP/IP, IIS proporciona a Windows 2000 Server un sitio Web listo para utilizar un número de conexiones ilimitadas.
Punto de Servicio de Web	Se proporciona a Windows 2000 Profesional para proporcionar los servicios de públicación de Web similar a IIS pero sirve solo para menos de 10 conexiones simultáneas.

2.2.6 SERVICIOS DE DIRECTORIO

El Sistema de Archivos de red (NFS, Network File System) es un conjunto de protocolos diseñado por SUN Microsystems que permite la compartición de archivos con estaciones de Trabajo. Es el mismo concepto que montar una unidad de red en Windows pero funciona de forma diferente. Para que una máquina actúe como servidor, debe de tener un conjunto de unidades compartidas de red y el servidor establece la seguridad y los privilegios para las unidades compartidas según sea necesario. Cuando el cliente inicia una conexión, la seguridad se valida y la compartición se monta en un directorio específico en UNIX.

UNIX utiliza la barra inclinada hacia adelante exclusivamente como delimitador de directorio. De ahí que la trayectoria /home/milles no es una serie de parámetros de línea de comandos; es realmente un directorio

Los sistemas operativos de tipo UNIX usan una jerarquía simple para todo el sistema de archivos. Es muy similar a la forma en que funcionan los sistemas Microsoft, excepto que no hay concepto de letra de unidad.

Los sistemas UNIX por el contrario tienen diferentes unidades "montadas" desde la raiz. El dispositivo de inicio principal se monta normalmente como raíz o root, llamado */*, si hay otra partición en ese disco debe montarse en /data y un usuario que ejecute un comando como cd /data estará automáticamente buscando datos en otro disco o partición. Para algunos usuarios, este sistema tiene más sentido que tener que cambiar contextos de dispositivos todo el tiempo.

Los servicios de directorio como Active Directory y NDS, son la espina dorsal de la seguridad de las empresas. Estos sistemas permiten al administrador central manejar toda la seguridad, lo que es una gran ventaja. La seguridad en otros sistemas se establece una vez, en un sitio y se distribuye ella misma a través de la red.

Los sistemas del tipo UNIX son pioneros en la historia de los servicios de directorio, SUN Microsystems comenzó con lo que ahora se conoce como *Páginas Amarillas*, Alguna compañía de teléfonos se enfado por este nombre y para no tener problemas se cambio por NIS, Network Information System (Sistema de Información de la red). NIS permite a los nombres de usuario y a las contraseñas fluir dentro de un dominio de contexto, de forma que los usuarios puedan acceder a los recursos dentro de un dominio sin tener una cuenta de acceso individual en cada máquina del dominio. NIS, sin embargo, es en gran parte un sistema de transporte. No maneja autenticación de usuario, en cambio maneja el desplazamiento de los nombres de usuario y contraseñas (y, opcionalmente, otra información) sobre la red para permitir los cambios de autenticación.

Windows Proporciona tres sevicios diferentes: El servidor para NFS, Cliente para NFS, y Puerta de Enlace (Gateway) para NFS. NFS proporciona acceso que usa autenticación de Windows y un Servicio que archiva para el rasgo de UNIX llamado la Cartografía de Nombre de Usuario(Called User Name Mapping).

Los servidores de NFS basados en Windows 2000 tienen que identificar a los usuarios pidiendo las demandas de NFS basado solamente en identificación de NFS normal que consiste en una Identificación del usuario (*UID*) y la Identificación de grupo (GID). Desde que las computadoras basadas en Windows y dominios no usan UIDs y GIDs para la identificación, una cartografía se necesita de UIDs y GIDs para contener las demandas de NFS a los nombres de usuario de Windows. Windows se basó en que los clientes de NFS necesitan trazar el nombre del usuario de Windows pidiendo a UID/GID antes de remitir una demanda de NFS. De Igual manera, una entrada de NFS necesita traducir al usuario de Windows que nombra a UNIX UIDs y GIDs mientras remite las demandas de sistema de archivo a los servidores de NFS.

El servidor para NFS es un servidor de NFS llevado a cabo en un servidor Windows 2000. Les permite a los clientes de NFS en UNIX acceder los archivos que se encuentran en las computadoras basadas en Windows. de la misma manera archiva en otro UNIX para poder accederse a los servidores de NFS. Para los usuarios de NFS basado en UNIX, este proceso es completamente transparente. El archivo del acceso nivelado es determinado por el UID del usuario o GID así como por las Estaciones de Windows que se manejan por las listas de acceso (Listas de Control de Acceso, ACLs). El Servidor para NFS soporta todos los sistemas de archivo basado en Windows incluso la FAT, CDFS, y NTFS.

La puerta de Enlace, Entrada o Gateway para NFS permite el acceso a NFS, comparte para las computadoras sin NFS un software de instalación en ellas. Esto es útil para Windows que opera a las computadoras sin el Cliente para NFS instalado en ellas. La entrada para NFS actúa como una entrada entre la red Windows y la red UNIX. La entrada para NFS comparte y exporta como las porciones de Windows. Las computadoras basadas en Windows acceden a NFS usando la gestión de redes basada en Windows vía la porción que se exportó por la Entrada para NFS.

La entrada para NFS también usa La Cartografía de Nombre de Usuario(Called User Name Mapping), para trazar las credenciales basadas en Windows a UNIX UIDs o GIDs antes de remitir las demandas de acceso de archivo a los servidores de NFS. Cada demanda de la entrada de un usuario separado se identifica propiamente y se trazan los nombres de usuario de Windows a los usuarios de UNIX correspondientes antes de que remitiera al servidor de NFS. Esto asegura que clientes que acceden los servidores de NFS de las máquinas con el software de cliente de NFS, consiguen los mismos privilegios que ellos recibirían de los clientes UNIX de NFS. Subsecuentemente acceder a la entrada para las porciones de NFS se proporciona usando la gestión de redes basadas en Windows, estas demandas que usan las credenciales basadas en Windows se autentifican. Los Administradores pueden exportar NFS y Windows comparte usando una herramienta simple que le permite al administrador especificar el servidor de NFS y el nombre de la porción basada en Windows con que esta porción de NFS debe exportarse.

Con NFS pueden accesar utilizando estándares de sintaxis NFS normales como por ejemplo: \\nombredeelservidor\nombredelaruta. También los usuarios pueden buscar o mapear unidades de red con volúmenes NFS y accesar a todos los recursos NFS desde mis sitios de red, Microsoft recomienda instalar en los servidores de UNIX el software llamado SAMBA , este software se utiliza si un servidor de UNIX requiere conectarse a un servidor de Windows 2000 Server, con esta utilerías el servidor UNIX puede de una manera transparente compartir datos con equipos Windows. Si se desea descargar dicho software e instalarse en el servidor UNIX la dirección es la siguiente: www.samba.org.

UTILIDADES INSTALADAS CON EL CLIENTE PARA NFS:

Grep	Búsqueda de Archivos para los modelos y resultados del despliegue en pantalla que contiene ese modelo
Ps	Las listas procesan su estatus
Sed	Copia nombres de archivos a un rendimiento normal, Edita según el script de comandos.
Sh	Invoca el Shell de Korn.
Tar	Crea los archivos de la cinta o agrega o extrae archivos.
Vi	Invoca al Editor de texto vi

2.3.- CONECTIVIDAD CON OTROS SISTEMAS OPERATIVOS

Además de poderse conectar con Novell y UNIX, como se menciono anteriormente Windows 2000 permite poderse con otros sistemas operativos por medio de protocolos, como ya mencionamos anteriormente con TCP/IP se puede conectar a servidores UNIX y con NWLINK se puede conectar a servidores Novell (ver la figura 2.14).

Con el protocolo DLC se puede conectar con servidores grandes como son los de la compañía IBM AS400.

Con el protocolo Appletalk que se encuentre instalado en el servidor de Windows 2000 se puede lograr conectar a una red de computadoras Apple, también se puede instalar el Cliente y servicios para Maquintosh y lograr tener acceso a los archivos e impresoras de Maquintosh.

Con el Protocolo NetBEUI es posible conectarse a redes Microsoft.

La necesidad de mejorar la administración de la red y el clamor por el estado real en el mundo de la PC empresarial ha provocado la necesidad de una forma más creativa de tener acceso a diferentes tipos de redes, servidores y mainframes.

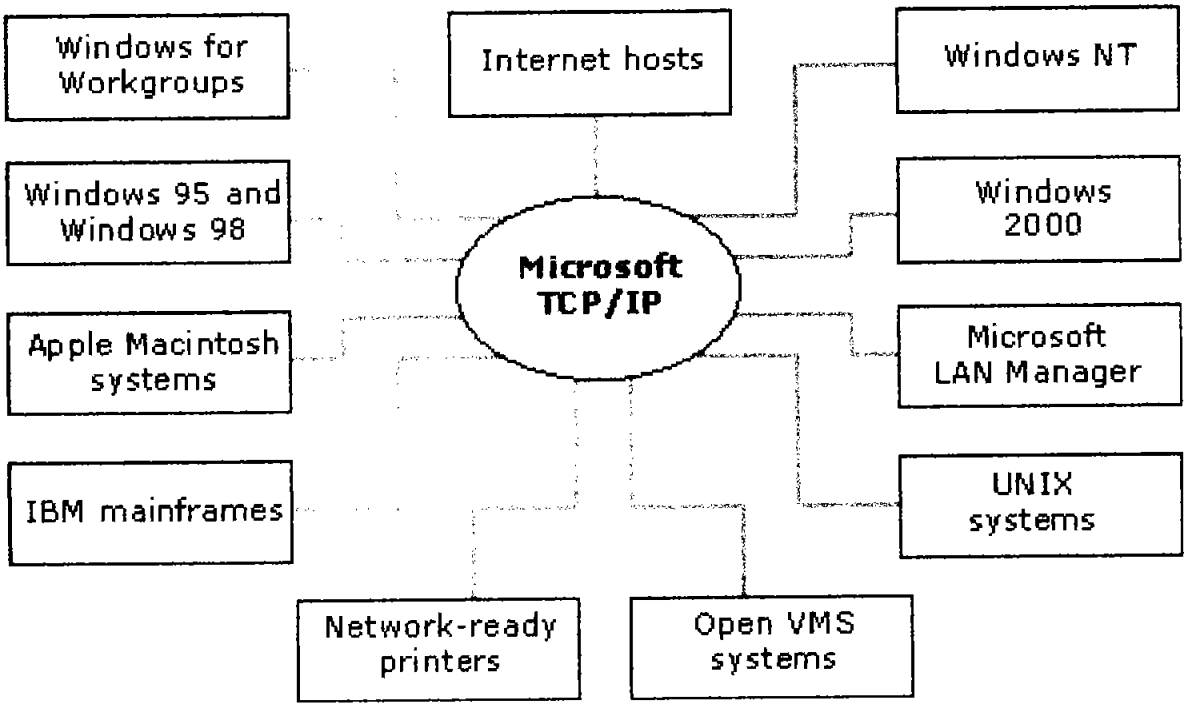


Figura 2.14 Compatibilidad con otros Sistemas Operativos.

2.4.- UNA VISION HACIA EL FUTURO

En un futuro no muy lejano veremos una integración de sistemas operativos de red, una mejor administración tanto de recursos y medidas de seguridad mucho más extensas y seguras, Los sistemas operativos del futuro traerán un soporte mucho más amplio y una interfaz gráfica mucho más amigable, la idea es que el mundo de la computación pueda evolucionar de una manera útil y practica para todos los seres humanos, actualmente todavía no existe esa compatibilidad al 100% entre un sistema operativo y otro, pero con el paso de los años y la evolución que sé esta llevando en materia de tecnología no dude que en el futuro cualquier sistema de red se pueda integrar hacia cualquier PC.

La evolución que ha tenido Internet esta obligando a los administradores de red a migrar y buscar muchas herramientas para lograr una integración de su red hacia los servicios de Internet. Los creadores de software de red como Microsoft están preocupados debido a la demanda que solicitan día con día los usuarios, esperemos en un futuro poder lograr ver dicha integración en nuestras vidas.

RESUMEN

En este capitulo observamos como la red con Windows 2000 Server puede comunicarse con una red Novell Netware 5.0 o con una red Unix, para compartir bases de datos y aplicaciones.

Windows 2000 Server ha evolucionado tanto que permite a los usuarios de Novell poder comunicarse con la red de Microsoft, aunque trata de tener diferencias conceptuales y lógicas, Windows 2000 fue creado para poder ser una herramienta confiable de Administración en una red, además de que ya se puede comunicar con otras redes como Apple y AS400,

En la empresa de telefonía la comunicación entre estos 3 tipos de sistemas operativos de red resulta útil y valiosa para los usuarios, ya que acceder a datos, información y recursos de cada uno de los diferentes sistemas operativos de red resulta necesario.

En la empresa de telefonía se prefiere utilizar Windows 2000 Server ya que además de ser muy amigable en su plataforma grafica permite a los usuarios él poder adquirir su información de una manera eficaz y rápida.

A pesar de que Microsoft no haya comenzado su carrera creando sistemas operativos de red con el paso de los años ha evolucionado hasta Windows 2000 Server que sé esta volviendo muy popular en el mercado.

En las tablas comparativas se muestra las ventajas y desventajas que puede tener Windows 2000 con Novell y UNIX (Aunque en ellas se ve una clara ventaja de Windows 2000 Server)

Las herramientas y servicios que Microsoft ha creado para que se comunique con diferentes redes resultan muy útiles, aunque en el futuro las encontraremos mucho más mejoradas y de una mayor facilidad en los próximos sistemas operativos que Microsoft diseñe.

En la empresa de Telefonía los servicios de puerta de enlace de Novell permitieron tener una comunicación con la red Novell para poder trabajar con las bases de datos que maneja la pequeña red Novell.

Además la comunicación con el ambiente de UNIX fue trasparente y no presento falla, basto con dar de alta la puerta de enlace y se logro la comunicación con la red UNIX para acceder a sus diferentes bases de datos.

CAPITULO 3
SEGURIDAD

El desafío para un administrador de una red es mantener la información siempre disponible para los usuarios autorizados y al mismo tiempo, no disponible para aquellos que no lo están.

En el presente capítulo se mostrara las diferencias conceptuales entre el manejo de la administración y seguridad de datos entre Windows NT y 2000.

Windows 2000 implementa muchas de las más nuevas tecnologías de seguridad que hay en el mercado. Entre ellas, los certificados y claves, protocolos de autenticación como Kerberos, soporte para smart cards y sistema de cifrado de datos

Windows 2000 Server se hizo con el propósito de mejorar el desempeño y productividad de los servicios del sistema operativo y aumentar sus prestaciones, mejorando su protección a los archivos del sistema, la eliminación de los 45 escenarios más comunes de reinicio, y la resolución y recuperación más sencillas de problemas.

3.1 CONCEPTOS BÁSICOS DE DIRECTORIOS Y ACCESOS

3.1.1 CONCEPTO DE GRUPO DE TRABAJO Y DE DOMINIO

Grupos de Trabajo: Es un conjunto de máquinas compartiendo los mismos recursos de una red. En redes punto a punto integradas por computadoras con Windows 3.11, 95 y 98, se organizan las computadoras en grupos de trabajo, un grupo de trabajo es un conjunto de equipos que pueden examinarse mutuamente los directorios a través de la red, pero que no comparten una base de datos de directorio común, cada computadora lleva el registro de los usuarios que trabajan en ella y el control de acceso por medio de claves que se asocian a los subdirectorios que se comparten.

Es decir que el control administrativo esta distribuido en cada computadora, un conjunto de máquinas compartiendo los mismos recursos de una red. Agregar una computadora a un grupo de trabajo se denomina unirse a un grupo. Durante la instalación, también tiene que decidir si la computadora se unirá a un Grupo de trabajo (Workgroup) o a un Dominio (Domain).

Son para grupos pequeños de computadoras de implantación sencilla. Cada máquina guarda su sistema de control de acceso a sus recursos. Cada una almacena el control de los usuarios que la accesan. No requieren un servidor NT, como controlador de dominio.

Si se esta instalando Windows 2000 Pro, sólo debe indicar el nombre del grupo al que se unirá. Si instala Windows 2000 Server, este se unirá como un servidor autónomo (se llama servidor autónomo al equipo corriendo Windows 2000 Server que no esta unido a ningún dominio. En este caso, no sólo puede ingresar el nombre del grupo al que va a unirse sino también crear un grupo propio

Dominio: Un dominio es un espacio de nombre (namespace) con el que se identifica un recurso en una red IP. Cada espacio de nombre esta indisolublemente unido a una dirección IP que le es única.

El Controlador de Dominios (domain controller) es el servidor encargado de administrar los nombres y direcciones IP de una parte o toda la red. Al igual que un grupo de trabajo es un agrupamiento de computadoras, pero en que el control de la seguridad y la información de las cuentas de usuarios están centralizadas en una base de datos, este control se almacena en una base de datos llamada "Directorio". El directorio contiene toda la información administrativa de un dominio.

En otras palabras, un dominio es un grupo lógico (fisicamente las computadoras pueden estar en cualquier parte del mundo y conectadas por medio de cualquier tipo de conexión) que provee una colección de cuentas de usuario y una base de datos de seguridad que hace que cada computadora del grupo sea reconocida por el resto de las computadoras del dominio. Se dice que una computadora participa de un dominio (esta unida a él) cuando utiliza la base de datos de seguridad de un dominio para validarse y autenticar la identidad o las credenciales al ingresar a él.

El Servidor de Nombres de Dominio (Domain Name Server –DNS) es un servicio que transforma las direcciones IP en nombres de dominio. Estas direcciones son números con formato 0.0.0.0, por ejemplo 169.254.0.2, cuyo mayor valor es 255 (255.255.255.255) que se "traducen" a nombres como Microsoft.com o miempresa.com.ar

Para unir una computadora a un dominio, el controlador tiene que estar activo y el servidor de nombres en funcionamiento. El administrador de la red deberá informar cual es el nombre del dominio al cual se esta uniendo la nueva computadora. A su vez, en el controlador de dominios se debe crear una cuenta de usuario, es decir, asignar un nombre de usuario y una contraseña. Si usted tiene privilegios de administrador, puede crear la cuenta de usuario en el mismo momento de la instalación.

Además de la cuenta de usuario, existe la cuenta de computadora, necesaria para acceder a los recursos de una red Microsoft. Un equipo puede tener más de una cuenta de usuario, pero necesita por lo menos una de computadora para la red. Si se actualiza el equipo sobre NT 4, la cuenta ya había sido creada y no hará falta este paso. Sí es necesario cuando se actualiza desde Windows 95/98 o MS-DOS o se instala en una máquina vacía. Por otra parte, si se establece un equipo con doble booteo, se deberá crear una cuenta de computadora para cada sistema operativo.

3.1.2 TIPOS DE SERVIDORES NT

PDC: Primary Domain Controller (Controlador Primario de Dominio), es la computadora que contiene la base de datos "Directorio", sólo puede haber una en un dominio y sólo puede ser un servidor NT

BDC: Backup Domain Controller, (Controlador de Dominio de Respaldo), son aquellas computadoras que contienen una copia de respaldo del directorio, la cual se sincroniza periódicamente con la principal, pueden apoyar al PDC cuando este tiene mucha carga de trabajo, pueden haber varios BDC dentro de un dominio

Independientes: Puede haber servidores NT que no contienen información administrativa de la red, si no que sólo ofrecen la función de compartir software y hardware, éstos son servidores independientes o servidores miembros.

DOMINIO NT: Un dominio de NT es un grupo de usuarios y computadoras donde el registro y control de los usuarios se centraliza en una base de datos llamada directorio la cual reside en un NT Server formando así una unidad administrativa (se puede tener en una misma red –generalmente organizaciones muy grandes- varios dominios; campus sur, campus norte con sus respectivos grupos y usuarios) (ver la figura 3.1).

En un domino de Windows NT los usuarios pueden estar incluidos en más de un grupo de usuarios o pueden ser usuarios que no pertenecen a ningún grupo.

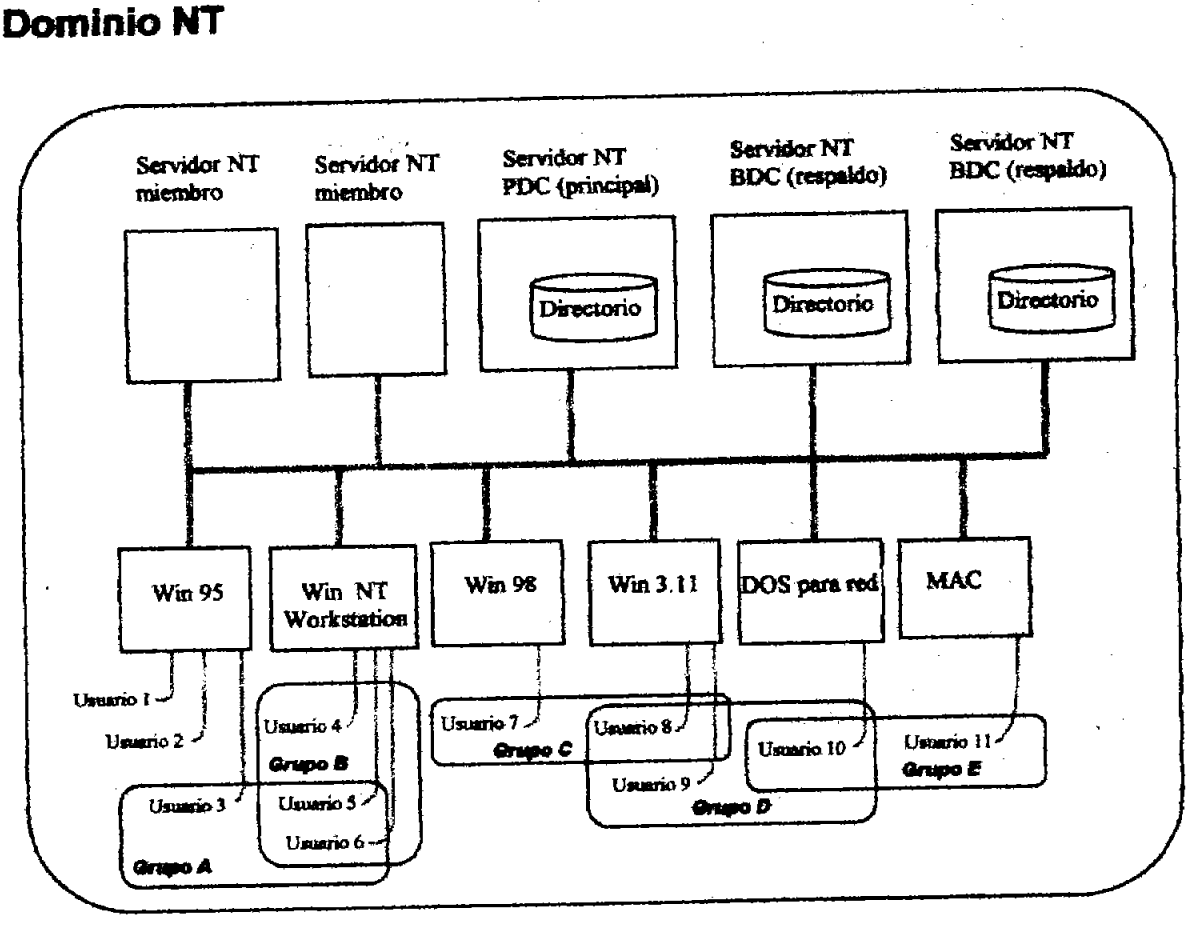


Figura 3.1 Estructura de un Dominio en NT.

Para cada equipo con Windows que haya en la red, es necesario especificar si participará en un dominio o en un grupo de trabajo. Los miembros de un grupo de trabajo sólo inician sesiones en cuentas de una estación de trabajo y comparten recursos con los equipos de su grupo. En la mayoría de los casos, será conveniente que cada estación de trabajo participe en un dominio.

Los servidores miembros pueden participar en un dominio, aunque no es obligatorio. Un servidor miembro no participa en un dominio, sólo tiene su propia base de datos de usuarios y procesa por si mismo las peticiones de inicio de sesión. No comparte información de cuentas con ningún otro equipo y no permite el acceso a cuentas de dominio. Sólo es posible iniciar sesión con cuentas de usuario creadas en el servidor y sólo se puede asignar derechos y permisos para usar los recursos del servidor.

Estos servidores tienen los mismos tipos de cuentas de usuario y de grupos locales incorporados que los equipos con Windows NT Workstation (no los tipos de cuentas de grupo incorporados de los controladores de dominio de Windows NT Server).

Los equipos con Windows NT Workstation, Windows NT Server, Windows para Trabajo en Grupo o Windows 95 pueden configurarse para participar en un dominio o en un grupo de trabajo. Al configurarse para el funcionamiento en red, se especifica un nombre de equipo y un nombre de grupo de trabajo. Si este coincide con el nombre de un dominio, el nombre del equipo aparecerá en la lista de examen del dominio y podrá examinar los equipos con Windows NT Server y Windows NT Workstation, tanto si participan en un dominio como en un grupo de trabajo. Para determinar si un equipo participa en un dominio o en un grupo de trabajo en la instalación debe especificar que el equipo iniciará una sesión en un dominio de Windows NT Server o que lo hará en un grupo de trabajo.

3.1.3 CUENTAS, DERECHOS Y PERMISOS

Cuentas de Usuarios: Permiten tener acceso a los recursos del dominio. Cada persona que participa en un dominio debe tener una cuenta de usuario para iniciar una sesión en la red y utilizar recursos del dominio tales como archivos, directorios e impresoras.

Un administrador crea una cuenta de usuario asignando un nombre de usuario a una cuenta, especificando los datos identificativos del usuario y definiendo los derechos del usuario en el sistema. Entonces, Windows NT Server asignara a la nueva cuenta un identificador único de seguridad (SID).

Derechos de usuario: Controlan las acciones del usuario. Los derechos de usuario son reglas que determinan las acciones que puede realizar un nuevo usuario en los controladores de dominio, en las estaciones de trabajo o en los servidores miembros. Además, los derechos controlan si un usuario puede iniciar una sesión en un equipo directamente (localmente) o a través de la red, agregar usuarios a un grupo de estaciones de trabajo o de dominios, eliminar usuarios, etc.

Cuentas de grupo: Windows tiene incorporados varios grupos predefinidos los cuales tienen ya asignados conjuntos de derechos de usuario, normalmente los administradores asignan los derechos de usuario agregando las cuentas de usuario a uno de los grupos predefinidos o creando un grupo nuevo y asignándole derechos de usuario específicos de ese grupo. Los usuarios que se agregan posteriormente a un grupo reciben automáticamente todos los derechos asignados a la cuenta de grupo. Los usuarios individuales pueden recibir determinados derechos de usuario; sin embargo, la mayoría de los administradores prefieren controlar las acciones por grupos, en lugar de por usuarios individuales.

Puede haber 2 tipos de cuentas de grupo:

Grupo Global: Esta formado por varias cuentas de usuario de un dominio que se agrupan bajo un nombre de cuenta de grupo. Un grupo global sólo puede contener cuentas de usuario de un mismo dominio (el dominio donde se creo el grupo global). El termino "global" indica que el grupo puede recibir derechos y permisos para utilizar recursos de múltiples dominios. Los grupos globales sólo pueden contener cuentas de usuario y solamente pueden crearse en un dominio (no en una estación de trabajo, ni en un servidor miembro).

Grupo Local: Esta formado por cuentas de usuario y grupos globales de uno o más dominios, agrupados bajo un nombre de cuenta. Es posible agregar al grupo local usuarios y grupos globales que no sean del dominio local siempre y cuando pertenezcan a un dominio en el que se confía.

El termino "local" indica que el grupo sólo puede recibir derechos y permisos para utilizar recursos de un único dominio (el local). Los grupos locales pueden contener usuarios y grupos globales, pero no otros grupos locales.

Los controladores de dominio de Windows NT Server contienen grupos locales incorporados que determinan lo que los usuarios pueden hacer en el dominio al iniciar una sesión en esos controladores. Los equipos con Windows NT Workstation y los servidores miembros que ejecutan Windows NT Server cuentan con grupos locales incorporados que determinan lo que los usuarios pueden hacer en el equipo local.

Los derechos asignados a los grupos incorporados de un controlador de dominio proporcionan distintas capacidades a los usuarios del dominio, como sugieren los nombres de los grupos: Administradores, Operadores de cuentas, Operadores de servidores, Operadores de copia, Operadores de impresión, Usuarios, Invitados y Duplicadores.

Los grupos locales incorporados para las estaciones de trabajo y los servidores miembros son Administradores, Operadores de copia, Usuarios avanzados, Usuarios, Invitados y Duplicadores.

Cuentas de Equipo: Cada equipo con Windows NT Workstation o Windows NT Server que participa en un dominio tiene su propia cuenta en la base de datos de directorio, llamada cuenta de equipo. Las cuentas de equipo se crean cuando el equipo se identifica por primera vez en el dominio al configurar la red durante la instalación. Las cuentas de equipo permiten a los administradores controlar de forma remota las estaciones de trabajo y los servidores miembros. También afectan a la relación entre una estación de trabajo y los servidores de dominio, y a la relación entre el controlador principal y los controladores de reserva.

Los equipos clientes que ejecutan sistemas operativos distintos de Windows NT Workstation o Windows NT Server pueden interactuar con equipos de un dominio de Windows NT Server. Sin embargo, no tendrán cuentas de equipo en el dominio y, por tanto, no contarán con la seguridad de inicio de sesión de Windows NT Workstation. Sus usuarios pueden tener cuentas de usuario almacenadas en la base de datos de directorio, pero el equipo propiamente dicho no tendrá seguridad de inicio de sesión que proteja el acceso a sus propios recursos.

Cuentas de dominio y cuentas de estación de trabajo: Los equipos que ejecutan Windows NT Workstation y los servidores miembros (equipos que ejecutan Windows NT Server que no son controladores de dominio) mantienen cuentas de usuario, grupos y directivas de seguridad independientes de los del dominio. Las cuentas incorporadas de tales equipos proporcionan derechos incorporados sobre el equipo, similares a los derechos que proporcionan las mismas cuentas incorporadas a nivel de dominio.

Cuando se configura un controlador de dominio, sus cuentas incorporadas proporcionan al administrador algunos derechos administrativos. Cuando se configura una estación de trabajo o un servidor miembro, sus cuentas incorporadas proporcionan al administrador derechos administrativos. Para adquirir el nivel de control apropiado sobre una estación de trabajo, un servidor miembro o un dominio, el administrador decide las cuentas de usuario que agrega a los distintos grupos incorporados.

Permisos: Controlan el acceso a los recursos del dominio. Los permisos son normas que regulan que usuarios pueden utilizar objetos (como directorios, archivos e impresoras) y de que forma pueden hacerlo. El propietario de un objeto establece los permisos sobre dicho objeto. De forma similar a lo que ocurre con los derechos de usuario, los permisos sobre un objeto se aplican a todos los miembros de los grupos a los que se conceden.

Conjuntamente, las cuentas de usuario, los derechos de usuario y los permisos sobre recursos permiten establecer los accesos y restricciones adecuados para cada usuario.

Cuenta Administrador: La cuenta Administrador ofrece al usuario derechos automáticos para realizar tareas de administración de dominio en un controlador de dominio, una estación de trabajo o un servidor miembro que resida en dicho dominio o en un dominio que confía. La persona que instala es quien define la contraseña de administrador, esta contraseña debe apuntarse y guardarse en un lugar seguro.

La cuenta de usuario Administrador es miembro del grupo local Administradores del controlador de domino, estación de trabajo o servidor miembro. La cuenta Administrador nunca se puede eliminar, desactivar ni quitar del grupo local Administradores, lo cual asegura que nunca pueda bloquearse a sí mismo fuera del equipo eliminando o desactivando todas las cuentas administrativas.

Cuenta invitado: La cuenta invitado la utilizan para los inicios de sesión aquellas personas que no tienen una cuenta en el equipo, en el dominio o en cualquiera de los dominios en los que confía el dominio del equipo. Un usuario cuya cuenta esté desactivada (pero no eliminada) también puede usar la cuenta Invitado. La cuenta Invitado no requiere contraseña y se puede usar para dos tipos de inicio de sesión: inicios de sesión de invitado local e inicios de sesión de invitado de red.

Se puede configurar cada dominio y cada equipo para permitir ambos tipos de inicios de sesión de invitado, un único tipo o ninguno. La cuenta Invitado queda desactivada de forma predeterminada cuando se instala Windows NT Server o Windows NT Workstation, pero la puede reactivar.

Los Invitados no tienen derechos predefinidos sobre un controlador de dominio.

Un inicio de sesión de invitado local tiene lugar cuando un usuario inicia una sesión interactiva en un equipo con Windows NT Workstation o en un servidor miembro con Windows NT Server y especifica Invitado como nombre de usuario en el cuadro de diálogo información de inicio de sesión. Como la cuenta Invitado en estos equipos (pero no en los controladores de dominio) tiene el derecho incorporado de iniciar sesiones en modo local, el usuario Invitado puede trabajar en dicho equipo (sujeto a los derechos y permisos asignados a la cuenta Invitado) y usarlo para tener acceso a la red.

Un inicio de sesión de invitado de red tiene lugar en un equipo que utilice la cuenta Invitado cuando un usuario ha iniciado una sesión interactiva en una cuenta de dominio o en una cuenta de equipo local (como en el caso de un miembro de un grupo de trabajo) e intenta conectar con el equipo que usa la cuenta Invitado:

Un equipo con Windows NT Workstation en un grupo de trabajo o en un dominio
Un servidor miembro
Un controlador de dominio
Un equipo cliente LAN Manager 2.x

En el caso de un grupo de trabajo, el equipo al que se tiene acceso considera el nombre de equipo como un nombre de dominio. El equipo al que se conecte podría no reconocer la cuenta del usuario por alguna de las siguientes razones:

- No se confía en el dominio especificado como el que contiene la cuenta de usuario y el usuario no tiene una cuenta en el dominio o en la base de datos de directorio del equipo al que se está teniendo acceso. Este caso siempre se aplica a un equipo de grupo de trabajo porque este tipo de equipos no usan relaciones de confianza y el equipo al que se está conectando trata el nombre del equipo como un nombre de dominio. Se confía en el dominio especificado como el que contiene la cuenta de usuario pero el usuario no tiene cuenta en el dominio en el que se confía.

- El dominio es el mismo que el dominio del equipo al que se conecta y el usuario no tiene una cuenta en el dominio o en la base de datos de directorio del equipo al que se conecta (si no es un controlador de dominio).

- Un inicio de sesión de Invitado de red sólo se aprueba si la cuenta Invitado del equipo de destino está activada y no tiene definida una contraseña. El usuario Invitado tiene entonces todos los derechos, permisos y pertenencia a grupos del equipo que se haya asignado a la cuenta Invitado, incluso aunque no haya especificado Invitado como su nombre de usuario.

Se sugiere para permitir los inicios de sesión de invitado local pero no los de invitado de red, active la cuenta Invitado, pero revoque el derecho Acceder a este equipo desde la red en el Administrador de usuarios para dominios.

Para permitir los inicios de sesión de invitado de red pero no las de invitado local, active la cuenta Invitado y revoque el derecho Inicio de sesión local. (Asegúrese de que Invitado tenga el derecho Acceder a este equipo desde la red).

3.1.4 RELACIONES DE CONFIANZA

En una relación de confianza unidireccional, un dominio confía en los usuarios del otro dominio, permitiéndoles utilizar sus recursos. Más específicamente, un dominio confía en que los controladores del otro dominio validen las cuentas de usuario para que utilicen sus recursos. Los recursos que pasan a estar disponibles se encuentran en el dominio que confía y las cuentas que pueden usarlos se encuentran en el dominio en el que se confía. Sin embargo, si las cuentas de usuario del dominio que confía precisan utilizar recursos situados en el dominio en el que se confía, será necesaria una relación de confianza bidireccional.

Una relación de confianza bidireccional está formada por dos relaciones de confianza unidireccionales, de modo que cada dominio confía en las cuentas de usuario del otro. Los usuarios pueden iniciar una sesión en el dominio que contenga sus cuentas desde equipos de cualquiera de los dos dominios. Cada dominio puede contener cuentas y recursos. Es posible utilizar las cuentas de usuario globales y los grupos globales en cualquier dominio para conceder derechos y permisos sobre recursos de ambos. Es decir, ambos son dominios en los que se confía. El uso de los recursos de cualquier dominio, con o sin relaciones de confianza, estará siempre sujeto a los permisos que tengan asociados.

3.1.5 INICIO DE SESIÓN EN UN DOMINIO DE NT

Una computadora al iniciar una sesión de red en un dominio de NT, hace una autentificación o proceso de Logon, requiriendo una cuenta de usuario y una contraseña, los cuales son buscados en la base de datos Directorio, en un servidor NT (el PDC), si ya se ha dado de alta dicho usuario, coincide su contraseña y se tiene activado el acceso a dicho usuario, se permite el inicio de sesión.

Si el inicio de sesión se hace desde un equipo con Windows 3.11 o Windows 95 o 98, y no se autentifica al usuario, puede entrar de todas formas (oprimiendo "Cancelar" o ESC) a una sesión de Windows, con funciones de red limitadas, pero si estamos iniciando en un equipo con Windows NT Workstation o Server, no es posible entrar al sistema. Mediante la edición de las políticas o directivas del sistema se puede negar el inicio de sesión en Windows 95-98 si no se ha validado al usuario desde un servidor NT controlador del dominio.

3.2 KERBEROS

Kerberos es un sistema de identificación de usuarios desarrollado por el MIT que utiliza criptografía de clave simétrica para asegurar la identificación del usuario y la seguridad.

Consiste en un servidor central que verifica la identidad de los usuarios y autoriza el acceso a los recursos enviando claves específicas. Cada petición de un recurso va acompañada de un ticket. Si el ticket es válido se autoriza el acceso al recurso, y en caso contrario, se deniega.

Directiva Kerberos. Permite definir las directivas por las que se regirá este protocolo de autentificación. Entre ellas se encuentran los siguientes subnodos: Edad máxima de renovación de ticket, Vigencia máxima del ticket de servicio, Vigencia máxima del ticket de usuario, etc.

Windows 2000 autentifica a los usuarios y aplicaciones mediante el uso de dos protocolos: Kerberos V5 o NTLM (NT LAN Manager-Administrador de LAN NT). El protocolo Kerberos v5 es el predeterminado para equipos donde se ejecuta Windows 2000 y para aquellos que tienen instalado el software de cliente de Windows 2000. Con este protocolo el cliente solicita un vale (que contiene datos cifrados que incluyen una contraseña para confirmar la identidad del usuario al servicio solicitado) a un controlador de dominio. Este vale es emitido por un intermediario en el que confían el cliente y el servidor. El cliente presenta este vale de confianza al servidor de dominio que confía para proceder a su autentificación.

EL protocolo Kerberos es un estándar de autenticación de Internet y Windows 2000 soporta su versión 5. Se ha constituido en el protocolo nativo de autenticación de Windows 2000. Cada servidor Active Directory tiene corriendo automáticamente el servicio Kerberos Key Distribution Center (Llave de Distribución Central Kerberos), y todos los sistemas Windows 2000 soportan el protocolo como clientes.

Ticket de identificación: Cada usuario que se identifica en un sistema Windows 2000 recibe un ticket, una especie de entrada que le permite ser identificado y acceder a los recursos de la red que esa entrada le asigna. La información del ticket está cifrada y contiene tanto la información de la identidad como la de autentificación.

El ticket, así como válida el usuario frente a un determinado recurso, también válida el recurso frente al usuario. De esa manera, no sólo no es necesaria la autenticación ante cada paso del usuario, es decir, ante cada recurso accedido, sino que tampoco es posible usurpar una identidad.

Al ser Kerberos un estándar de Internet, se facilita la administración en el caso de redes heterogéneas, no sólo por que no es necesaria una infraestructura especial para soportarlo sino porque cualquier cliente o servidor que soporte Kerberos puede participar. Los administradores no necesitan saber exactamente como funciona Kerberos ya que éste es manejado transparentemente por el sistema operativo.

Kerberos es ofrecido, además, a los desarrolladores y aplicaciones para que hagan uso de sus prestaciones a través de SSPI (Security Support Provider Interface-Proveedor de la Interface de Soporte de Seguridad). SSPI ofrece una API (Application Program Interface-Interface de Programación de Aplicaciones), para crear conexiones autenticadas. Los métodos de autenticación permanecen ocultos por lo que el desarrollador puede elegir otras SSPI sin problemas de compatibilidad. En otras palabras, así como Windows 2000 viene con la SSPI de Kerberos, otros sistemas de seguridad que ofrezcan SSPI pueden ser utilizados.

En la versión de Windows 2000, Kerberos versión 5 es el protocolo de seguridad primario. Kerberos verifica tanto la identidad del usuario como la integridad de los datos de sesión, los servicios están instalados en cada controlador de dominio, y un cliente se instala en cada estación de trabajo y servidor Windows 2000. Una autenticación Kerberos inicial de usuario proporciona al usuario una sola conexión a los recursos de la empresa.

Además de la seguridad mejorada, Kerberos permite:

- Relaciones verdaderas transitivas para la autenticación entre dominios.
- Credenciales de autenticación emitidas por un servicio Kerberos son aceptadas por todos los servicios de éste dentro del árbol de dominio. También, credenciales emitidas por un servicio Kerberos en un campo de árboles de dominio son aceptadas por todos los servicios dentro del campo.
- Autenticación mutua de cliente y servidor
- Se autentifican el cliente y servidor en la sesión de Kerberos.
- Procesos de autenticación eficaz
- Windows 2000 Server puede verificar las credenciales del cliente sin consultar el servicio Kerberos en el controlador de dominio.

Autenticación delegada para transacciones cliente/servidor multinivel. En algunas arquitecturas de aplicación, una transacción de cliente necesita transitar servidores múltiples. En este caso, el servidor actual puede autenticar el servidor solicitado en nombre del cliente.

Credenciales Kerberos: El protocolo de autenticación principal para un dominio de Windows 2000 Server es la autenticación Kerberos. Las credenciales Kerberos constan de un nombre de dominio y usuario (que pueden ser nombres fáciles de Internet, como BobbyB@Microsoft.com), así como de una contraseña encriptada estilo Kerberos. Cuando el usuario se conecta al sistema, Windows 2000 obtiene una o más boletas Kerberos para conectarse a los servicios de red. Las boletas representan credenciales de red del usuario en una autenticación basada en Kerberos.

Windows 2000 administra automáticamente la memoria caché de boletas Kerberos para conexiones a todos los servicios de red. Las boletas tienen un tiempo de caducidad y ocasionalmente necesitan ser renovadas. La expiración y renovación de boletas son manejadas por el proveedor de seguridad de Kerberos y los servicios de aplicaciones asociados. La mayoría de los servicios, como el Redireccionador de sistemas de archivos, automáticamente mantendrán actualizadas las boletas de sesión. La renovación regular de boletas proporciona una seguridad agregada de sesión al cambiar periódicamente las claves de la misma.

3.3 NTLM

Si alguno de los equipos no admite el protocolo Kerberos V5, se utilizará el protocolo NTLM. Cuando un cliente intenta acceder a recursos de un servidor de otro dominio con la autentificación NTLM, el servidor que contiene el recurso debe ponerse en contacto con un controlador de dominio del cliente para comprobar las credenciales de la cuenta.

Credenciales NTLM: Los clientes utilizan el protocolo de autenticación NTLM para cuentas o servidores que ejecutan versiones anteriores de Windows NT. Por ejemplo, la autenticación NTLM se utiliza para conectarse a una sección compartida de archivos remotos en un servidor basado en Windows NT 4.0, o para conectar un cliente basado en este último a una sección compartida de archivos de servidor basada en Windows 2000. Las credenciales NTLM constan del nombre de dominio, el nombre del usuario y la contraseña encriptada introducida una vez durante la conexión inicial.

Transición sin problemas: La transición de la autenticación NTLM utilizada en Windows NT 3.5x/4.0 a la autenticación de dominios Kerberos será muy fácil. Los servicios de Windows NT pueden soportar conexiones de cliente o servidor utilizando cualquier protocolo de seguridad. La negociación de seguridad, a través del nivel SSPI o del protocolo de la aplicación, proporciona otra forma de seleccionar la mejor opción de las opciones disponibles de protocolo de seguridad. La transición de los servicios basados en la empresa utilizando la autenticación Kerberos a los servicios basados en Internet utilizando la autenticación de claves públicas, es totalmente transparente para el usuario.

Windows 2000 proporciona soporte para varias credenciales de usuario haciendo posible el uso de la tecnología de autenticación de claves secretas para los servicios de aplicaciones empresariales con tecnología de muy alto rendimiento y seguridad de claves públicas al conectarse a servidores basados en Internet. En vez de depender de una sola tecnología y protocolo de autenticación, Windows 2000 utilizará varios protocolos según sea necesario para cumplir los requerimientos de aplicaciones y de la comunidad de usuarios con el objeto de proporcionar computación segura en red.

3.4 EL DIRECTORIO ACTIVO

Es la nueva organización administrativa de toda la red. El Directorio Activo (Active Directory-AD), contiene toda la información de los elementos que forman parte de la red, centraliza la administración de usuarios, impresoras, estaciones de trabajo, servidores, aunque la red este distribuida en localizaciones distantes unas de otras. En si, el Active Directory se ajusta a la organización en árbol, que siguen los nombres de dominio en internet. Esto es, dentro de un dominio se pueden crear subdominios, y dentro de estas, unidades organizativas, que representan los elementos finales de la red, como usuarios, impresoras, etc.

Elimina la existencia de controladores, el principal de dominio (PDC) y el de respaldo (BDC), dando lugar a controladores de dominio en general. Ahora todos estos controladores tienen una copia de la base de datos del directorio.

Además dentro de los subdominios pueden existir controladores de dominio que sólo tiene información de los elementos pertenecientes a ese subdominio.

Active Directory: (AD) es el servicio de directorios incluido en Windows 2000. Servicio de Directorios: es un servicio de red que identifica todos los recursos en ella y los hace accesibles a los usuarios y a las aplicaciones.

El elemento principal del Active Directory es el directorio, que almacena información sobre los recursos de la red y sobre los servicios que hacen disponible la información. Los recursos almacenados en el directorio, como los datos del usuario, impresoras, servidores, bases de datos, grupos, computadoras y políticas de sistema, se denominan objetos. Active Directory organiza los recursos jerárquicamente en dominios.

Dominio: Un dominio (domain) es una agrupación lógica de servidores y otros recursos de la red bajo un mismo nombre de dominio.

Cada dominio incluye uno o más controladores de dominio (domain controllers), que son máquinas que almacenan una réplica completa de un directorio de dominio. Para simplificar la administración; todos los controladores de un dominio son pares y cada vez que se hace algún cambio en alguno de los controladores, el resto se actualiza automáticamente. Más aun, Active Directory permite tener un sólo punto de ingreso a la red, y por lo tanto, un sólo lugar de administración de la red. Un administrador esta en condiciones de manejar todos los dominios desde un mismo lugar.

El directorio de Active Directory almacena la información organizándola en secciones que permiten recopilar un gran número de objetos. Este sistema de secciones permite expandir el directorio a medida que la información a almacenar es mayor, generalmente a resultas del crecimiento de la empresa o de la ampliación de la red.

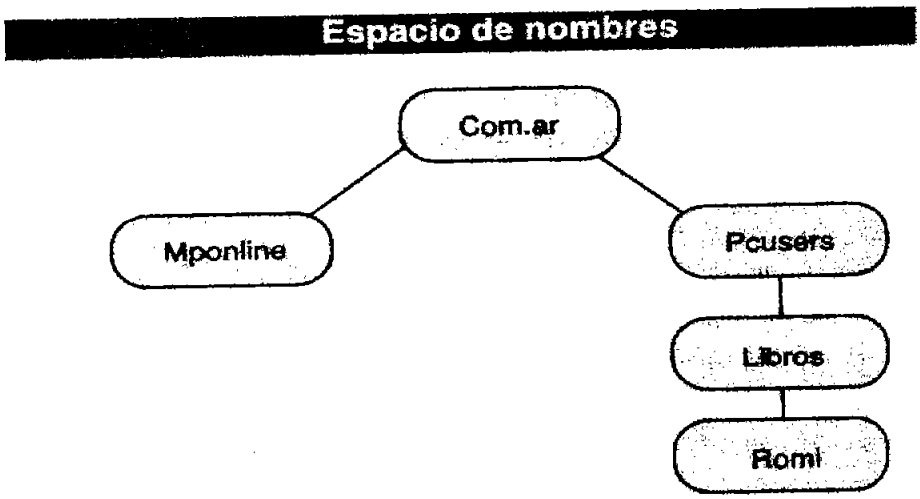


Figura 3.2 El espacio de nombres de Active Directory es semejante al DNS, es decir, al que se usa en Internet.

A semejanza de lo que sucede con Internet, Active Directory integra el concepto de espacio de nombres (namespace), lo que permite unificar, y de esa manera, facilitar la administración de múltiples espacios de nombre que hoy existen en los entornos empresariales con combinaciones muy heterogéneas de hardware y software (ver la figura 3.2).

Precisamente por su cercanía con los mecanismos de Internet, Active Directory usa DNS (Domain Name System) para su sistema de nombres y puede intercambiar información con cualquier aplicación o directorio que use LDAP (Lighweight Directory Access Protocol-Protocolo de Acceso al Directorio Ligero-Pesado) o HTTP (Hypertext Transfer Protocol-Protocolo de Transferencia de Hipertexto).

Active Directory, usa LDAP para intercambiar información también con cualquier otro sistema de directorios que soporte LDAP versiones 2 y 3, como es el caso de Novell Directories Services (NDS), del sistema operativo Novell Netware.

3.4.1 SERVICIO DNS

Para que Active Directory y el software asociado pueda funcionar correctamente, debe instalar y configurar el servicio DNS (Domain Name System-Sistema de Nombres de Dominio). Como Windows 2000 usa DNS como su servicio de nombres y ubicaciones, los nombres de dominios de Active Directory también son nombres DNS. Es más, si la red esta compuesta exclusivamente por equipos corriendo cualquier versión de Windows 2000 –y eventualmente, Windows 98-, se puede instalar y configurar DDNS (Dynamic DNS-Sistema de Nombres de Dominio Dinámico), para que asigne dinámicamente las direcciones y actualice las tablas DNS automáticamente, lo que elimina la necesidad de otros servicios como WINS (Windows Internet Naming Service-Servicio de Nombres de Internet de Windows).

HTTP es el protocolo estándar que se usa para mostrar páginas web en Internet. Esto significa que cada objeto de Active Directory puede mostrarse en una página HTML, en un explorador, con lo cual es posible unificar la interfase para casi todas las aplicaciones de la red.

Dado que Active Directory soporta varios de los formatos de nombre estándar, el usuario localiza los recursos de varias maneras:

- RFC 822. Este formato es el clásico del correo electrónico, por lo que se puede usar la forma recurso@dominio para referirse a un recurso determinado.

- UNC. Los nombres definidos por UNC (Universal Naming Convention-Convención Universal de Nombres) son los que se conocen comúnmente como direcciones de red: \\domino\servidor\archivo.ext.

- HTTP. Los nombres http, también llamados URL (Universal Resourse Locator-Localizador Universal de Recursos) son los que estamos acostumbrados a usar en Internet: http://subdominio.dominio/página.

- LDAP (Lightweight Directory Access Protocol-Protocolo Ligero de Acceso a Directorio. Con algunas variantes, la dirección LDAP es básicamente semejante a la HTTP.

3.4.2 ESTRUCTURA DE ACTIVE DIRECTORY

Debido a la gran variedad de entornos, por un lado, y a la flexibilidad de Active Directory, por el otro, antes de implementar Active Directory, se necesita, más que nunca, un buen diseño previo. Por otra parte, un buen diseño previo, que contemple no sólo las prestaciones de Active Directory sino también la posible escalabilidad de la corporación, hace que la administración posterior de la red sea mucho más fácil que en otros entornos.

Como Active Directory permite separar completamente la estructura lógica de la jerarquía del dominio de la estructura física, se pueden crear tanto estructuras centralizadas desde un departamento de Tecnologías de Información hasta organizaciones altamente descentralizadas donde cada unidad está enfocada a un objetivo específico.

En Active Directory los recursos se organizan en una estructura lógica que posibilita distintos tipos de agrupamientos. Precisamente una de las ventajas de agrupar lógicamente los recursos es la de poder encontrar el que se busca por nombre y no por ubicación. De esta manera, la estructura física de la red queda transparente para el usuario.

Objeto: es un conjunto de atributos particulares, bajo un nombre específico, que representa un recurso individual de la red. Los atributos se refieren a las características del objeto. Así, los atributos de una cuenta de usuario pueden ser el nombre, departamento y dirección de e-mail y los de una impresora, si es láser y si es color. Algunos objetos funcionan también como contenedores: un dominio, por ejemplo, es un objeto contenedor.

Clases: Las agrupaciones lógicas de objetos son las clases. Una clase pueden constituirla todas las cuentas de usuario, las impresoras, los grupos, etc.

Unidades Organizacionales: (UO – Organizational Units) son contenedores que se usan para agrupar objetos de un dominio en grupos administrativos lógicos. Cada Unidad Organizacional contiene distintos objetos y cada domino tiene su propia lógica de agrupación en Unidades Organizacionales.

La unidad central de la estructura lógica del Active Directory es el dominio. Agrupando los objetos en uno o más dominios es posible representar la propia organización de la empresa. Todos los objetos de la red existen dentro de un dominio, dentro del cual, teóricamente, se pueden albergar hasta 10 millones de objetos.

Un dominio es a la vez un límite de seguridad. El acceso a los objetos se controla por medio de Listas de Control de Acceso (ACL –Access Control Lists), que contienen los permisos asociados con los objetos. Estas listas controlan cómo se accede a los objetos y quiénes y de qué manera lo hacen. Todas las políticas de seguridad y configuraciones –derechos administrativos, comparticiones, ACLs, etc.- no pasan de un dominio al otro. El administrador del dominio tiene derechos absolutos de control sólo sobre su dominio.

Árbol: Un árbol es una agrupación de uno o más dominios que comparte un espacio de nombres contiguos. Para nombrar un árbol hay que recurrir a los estándares DNS.

Todos los dominios de un árbol comparten un catálogo global, que es el depósito central de toda la información relacionada con los objetos de un árbol.

Catálogo global: es un servicio que, entre otras cosas, almacena los atributos de un objeto más comúnmente usados en una operación de búsqueda, por lo que se puede usar para localizar los objetos en cualquier lugar de la red.

Al instalar Active Directory en el primer controlador de domino de un bosque, este controlador se convierte, automáticamente en el servidor del catálogo global. El contenido del catálogo se actualiza constantemente como parte del proceso de replicación.

Todos los dominios de un árbol comparten un esquema, que es una definición formal de todos los tipos de objetos que es posible almacenar en una implementación de Active Directory. El esquema mantiene una especie de lista de las definiciones más comunes de los objetos, así como de sus propiedades. Es factible definir nuevos tipos de objetos o atribuirles nuevas propiedades o atributos a objetos existentes y el esquema –a través del snap-in (complemento): Administrador de esquemas- se extiende para cubrir las nuevas funcionalidades. Como el esquema se almacena en el catálogo global, cada vez que se extiende mediante nuevos atributos o nuevas clases, las extensiones están disponibles inmediatamente.

Bosque: Un bosque (forest) es una agrupación de árboles que no comparten un espacio de nombres contiguos. Todos los árboles de un bosque comparten un esquema común, así como todos los dominios comparten un catálogo global. Sin embargo, los dominios de un bosque pueden operar independientemente, pero el bosque se encarga de establecer comunicación a través de toda la organización (ver la figura 3.3).

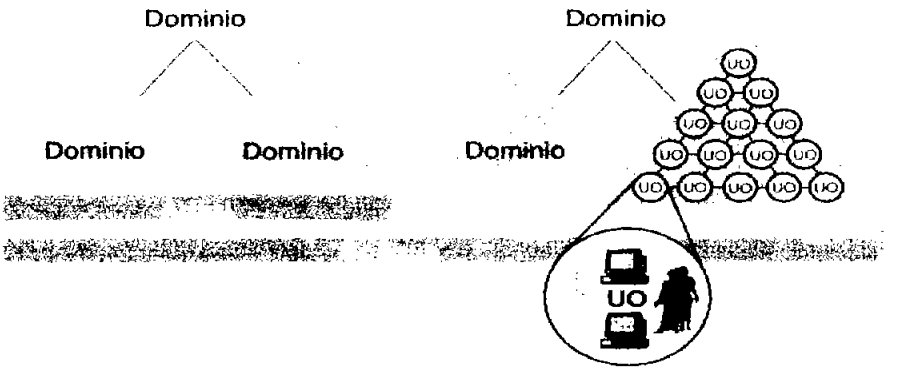


Figura 3.3 Estructura de un bosque.

Estructura Física de Active Directory: La estructura física de Active Directory está basada en sitios. Un sitio es la combinación de una o más subredes comunicadas mediante IP. Los sitios sólo tienen objetos computadora y objetos conexión, y no son parte del espacio de nombres. Un dominio individual puede extenderse por múltiples sitios y un sitio puede incluir computadoras y usuarios pertenecientes a varios dominios.

Relaciones de Confianza: Como se definió anteriormente un árbol de dominios es una agrupación jerárquica que se crea agregando uno o más dominios hijos a un dominio padre existente. Todos los dominios de un árbol comparten el mismo directorio de Active Directory. Sin embargo, los controladores de dominio sólo almacenan la parte de Active Directory que contiene los objetos de ese dominio. No hay una base de datos maestra que almacene toda la información de todos los dominios del árbol. En cambio, como todos los dominios comparten un directorio, los usuarios pueden ubicar y usar los recursos de la red en cualquier dominio, siempre que tengan los permisos requeridos para acceder a ese recurso.

Precisamente, la estructura de árbol permite establecer permisos y restricciones sobre la base de una unidad organizativa o de un sólo dominio. Para eso, en la etapa de diseño y planificación es necesario tener en cuenta no sólo el flujo de permisos a través de la jerarquía de Active Directory sino también el sistema de relaciones de confianza.

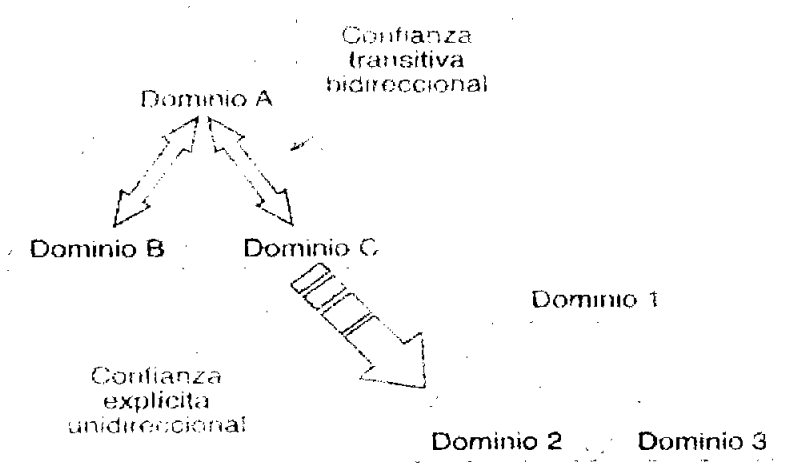


Figura 3.4 Mediante las relaciones de confianza es posible autenticar a un usuario dentro y fuera de un dominio determinado.

Una relación de confianza (trust relationship) es el vínculo que se establece entre 2 dominios entre los cuales el que confía acepta las autenticaciones del domino confiado (ver la figura 3.4). Existen 2 formas de relaciones de confianza:

- Confianza transitiva bidireccional (two-way transitive trust). Ésta es una prestación provista por el protocolo de autenticación Kerberos. Es la relación entre dominios hijos y padres dentro de un árbol y entre los dominios de alto nivel de un bosque. Estas relaciones se establecen y mantienen automáticamente. La confianza transitiva implica que si un dominio A confía en uno B, y éste a su vez en un C, entonces A automáticamente confía en C al ser también bidireccional, C confía en A. Cada dominio que se une al árbol tiene establecidas inmediatamente las relaciones de confianza con el resto de los dominios.

- Confianza explícita unidireccional (explicit one-way trust). Es la relación entre dominios que no son parte del mismo árbol. Esta forma se provee por compatibilidad con dominios de otros sistemas operativos como Windows NT u otros, lo que permite configurar relaciones de confianza entre dominios de otros árboles.

Como todos los dominios de un árbol confían unos en otros, un árbol permite que el usuario acceda a toda la red como si estuviera en un dominio simple. El usuario puede loguearse en un dominio y usar los recursos de otro, mientras posea los permisos necesarios.

Para esto, cada dominio funciona como una demarcación de seguridad en la cual los miembros del grupo de administradores de dominio sólo tienen autoridad sobre los objetos de su dominio, así como los miembros del grupo de Administradores en el domino raíz no tienen, por defecto –se les puede asignar luego- privilegios fuera de ese dominio.

Replicación y Actualización: Active Directory incluye una prestación llamada replicación, que asegura que los cambios en un controlador de dominio se reflejen en el resto de los controladores de dominio dentro de un mismo dominio.

Cada controlador de dominio almacena una copia completa (réplica) de toda la información del mismo, administra los cambios de esa información y réplica esos cambios en el resto de los controladores de dominio de ese dominio. Asimismo, dichos controladores replican todos los objetos en un dominio a cada uno de los otros. Cuando se hace un cambio en Active Directory, en realidad se esta haciendo el cambio en un controlador de dominio. Éste luego replica el cambio al resto de los controladores. Se puede definir cada cuando se lleva a cabo la replicación y que cantidad de información se replica en cada vez.

La densidad del tráfico de la red depende de la cantidad de servidores de catálogo global que haya en un bosque o en un árbol. Se puede tener más de un servidor de catálogo global, por cuestiones de seguridad y redundancia, pero hay que definir exactamente la cantidad de servidores en función de soportar el tráfico ya que a mayor cantidad de servidores, hay más rapidez en las respuestas a solicitudes o a búsquedas, pero es mayor el tráfico.

Active Directory usa un tipo de replicación llamada multimaster (multimaestro), que significa en realidad, que ninguno de los controladores de dominio es el controlador maestro -ni siquiera el que alberga el servidor de catálogo global- sino que, como se dijo anteriormente, todos los controladores son pares (peers) y poseen la misma información y la misma capacidad de administración. Aunque por cortos periodos la información en los diversos controladores sea distinta -el tiempo entre 2 sincronizaciones- tener más de un controlador de dominio provee tolerancia a fallos, ya que si un controlador de dominio está fuera de línea, cualquier otro puede tomar sus funciones.

3.4.3 INSTALAR Y CONFIGURAR ACTIVE DIRECTORY

Lo primero que hay que tener en cuenta es que Active Directory sólo puede existir en particiones formateadas con NTFS. Eso significa que un servidor que va a ser controlador de dominio no sólo puede ser un equipo con doble booteo, sino que, además, se deberán convertir las particiones FAT, y FAT32 a NTFS antes de proseguir con el trabajo.

Ahora se utilizará el Asistente para instalación de Active Directory, el que permitirá llevar a cabo las siguientes tareas:

- Agregar un controlador de dominio a un dominio existente.
- Crear el primer controlador de dominio de un nuevo dominio.
- Crear un nuevo dominio hijo (child).
- Crear un nuevo árbol de dominios.

Para arrancar el Asistente para instalación de Active Directory hacer clic en Programas/Herramientas Administrativas/Configurar su servidor.

Alternativamente, para instalar Active Directory puede ingresar dcpromo.exe en la caja de diálogo Ejecutar del menú del botón Inicio. Sin embargo, debe tener cuidado, ya que con dcpromo también puede eliminar Active Directory del controlador de dominio y degradarlo a servidor autónomo. Asimismo, si borra todos los controladores de dominio en un dominio, desaparecerá la base de datos de éste, por lo cual el dominio dejará de existir.

Si se escoge crear el primer controlador de dominio para el nuevo dominio, primero se debe crear el dominio. En ese caso, también, se pueden crear dominios hijos y árboles. El nuevo hijo será un subdominio del principal. Si se crea un nuevo árbol, se creará un nuevo dominio que no será parte del recién creado.

Se pueden crear nuevos árboles para un bosque existente o crear el nuevo bosque.

Si elige añadir un controlador de dominio a un dominio existente, estará creando un controlador de dominio par (peer). Crear controladores de dominio para agregar a los ya presentes tiene sentido por redundancia y para reducir el tráfico entre los que ya están.

Instalar Active Directory crea 2 componentes básicos:

- Base de Datos. La base de datos es el directorio de un nuevo dominio. Junto con ella se crean también los informes (logs) de la base de datos. Ambos se almacenan en la subcarpeta \Ntds de la carpeta de instalación de Windows, aunque se recomienda, para un mejor rendimiento, almacenar la base de datos y los informes de la base de datos en discos diferentes.

- Volumen de sistema compartido (Shared System Volume). Es una estructura de carpetas que existe en todos los controladores de dominio de Windows 2000. Almacena scripts, políticas del sistema y otros objetos referidos no sólo al controlador de dominio actual, sino también a toda la red. La ubicación predeterminada es la carpeta \Sysvol y debe estar ubicada en una partición o volumen formateado con NTFS.

La actualización del volumen de sistema compartido ocurre al mismo tiempo que la replicación de Active Directory –de hecho forman parte del mismo proceso- por lo que al crear un volumen, la primera vez hay que esperar por lo menos 2 ciclos de replicación para que éste contenga toda la información actualizada.

Cuando se instala por primera vez un controlador de dominio –o se actualiza uno existente a Windows 2000 Server-, éste se crea en modo mixto (mixed mode). Este modo permite al controlador interactuar con otros controladores que estén corriendo otras versiones de Windows, típicamente NT Server 4.0. Éstos reciben el nombre de controladores de bajo nivel (down-level domain controllers).

Si toda la red ha sido actualizada a Windows 2000 y no tiene pensado añadir controladores de bajo nivel, puede convertir los controladores a modo nativo. Este modo, además de permitirle contar con todos los beneficios de Active Directory, tiene algunas condiciones. No se soportan más los controladores de bajo nivel, y el que aparecía como controlador de dominio maestro, no lo es más, ya que todos los controladores de dominio, como dijimos anteriormente, son pares. Más aún, si se han convertido los controladores de dominio al modo nativo, no puede volver luego al modo mixto.

3.4.4 CUENTAS DE USUARIO Y GRUPOS

La cuenta de Usuario es la que permite que un operador pueda ingresar (log on-loguearse) a un dominio y tenga acceso a los diferentes recursos de una red. Windows 2000 permite crear 2 tipos de cuentas de usuario, una de Dominio y otra Local

Con una cuenta de Usuario de Dominio, éste ingresa al dominio y tiene acceso a todos los recursos de cualquier parte de la red. Usando el nombre de usuario y contraseña, Windows autentica al usuario, crea una ficha (token) de acceso con la información del usuario, su seguridad, sus permisos y restricciones.

La cuenta de usuario se mantiene en la copia de la base de datos de Active Directory (el Directorio) de un controlador de dominio y éste replica la información a todos los controladores. De esa manera, todos los controladores en un árbol pueden autenticar al usuario (ver la figura 3.5).

La cuenta de Usuario Local permite ingresar y tener acceso a los recursos sólo en la computadora en la que se ha creado la cuenta. La información se almacena sólo en la base de datos de seguridad local. No hay replicación y por lo tanto, no hay autenticación por el resto del árbol.

No se recomienda crear usuarios locales en computadoras que son parte de un dominio, ya que éstos no reconocen esas cuentas.

Windows 2000 crea automáticamente una serie de cuentas llamadas built-in (predeterminadas), como Administrador e Invitado.

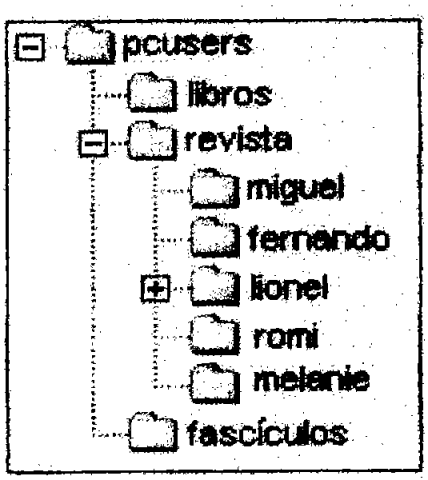


Figura 3.5 Las relaciones entre el dominio, el subdominio y los usuarios en Active Directory se pueden simbolizar de la misma manera como se puede hacer con carpetas y subcarpetas.

Es posible cambiar de nombre la cuenta Administrador pero no puede borrarla. Más aún, por seguridad se recomienda renombrarla con algún nombre que no de una idea de los privilegios de administrador, de modo que se impide que cualquier usuario no autorizado ingrese en la cuenta del administrador, al no saber cuál es exactamente. Lo mismo ocurre con la cuenta Invitado que, además, está desactivada por defecto.

Para crear cuentas de usuario de dominio se usa el snap-in Administración de directorios. Hacer clic con el botón derecho del mouse en Usuarios y seleccionar Nuevo Usuario. En la caja de diálogo que se abre, ingresar el o los nombres completos, el nombre de usuario que corresponde a la Unidad Organizativa y el que eventualmente, puede usarse para ingresar desde clientes de bajo nivel como Windows NT y 98.

En forma predeterminada se agrega el nombre del dominio desde el cual se está creando la cuenta, pero ese se puede cambiar si se crea un usuario de otro dominio.

Luego hay que ingresar la contraseña dos veces para confirmarla. Mediante los casilleros de chequeo apropiados es posible definir si se permite que el usuario cambie mandatoriamente la contraseña –la primera vez que ingrese, estará obligado a cambiar la contraseña por una de su elección – o por el contrario no puede modificarla. Asimismo, es posible determinar que la contraseña no venza nunca.

Luego de crear la cuenta, puede cliquear con el botón derecho en ella para seleccionar Propiedades y definir diversas características tales como los datos personales del usuario, horario en el que se le permite ingresar, propiedades de la cuenta, propiedades de marcado telefónico, etc.

Un grupo es una colección de cuentas de Usuario. Al asignar permisos y restricciones a un grupo, se puede facilitar la administración de los usuarios individuales simplemente asignándolo a un grupo determinado.

Windows 2000 utiliza 2 tipos de grupos:

- Los grupos de seguridad se utilizan para propósitos relacionados con la seguridad de la red, tal como puede ser el asignar permisos, etc.

- El grupo de distribución, en el que las aplicaciones se pueden usar para actividades no relacionadas con la seguridad como enviar e-mails.

Ambos tipos de grupos se almacenan en la base de datos de Active Directory. Los grupos de seguridad se administran mediante ámbitos (scopes).

Los grupos globales suelen servir para reunir usuarios que comparten similares niveles de permisos y acceden aproximadamente a los mismos recursos de la red. Los grupos globales se pueden usar para signar permisos para recursos ubicados en cualquier dominio, pero sólo se pueden agregar miembros del dominio en el que fue creado el grupo.

Los grupos de seguridad de dominio local, en cambio se usan más para asignación de permisos a recursos. Se agregan usuarios de cualquier dominio pero sólo se asignarán permisos a recursos disponibles en el dominio en el que se creó el grupo.

Los grupos de seguridad universales permiten asignar permisos para usar múltiples recursos en varios dominios. Se agrega a cualquier usuario y se da acceso a cualquier recurso, pero sólo puede hacerse si los controladores de dominios están en modo nativo.Los grupos pueden ser tanto globales como locales, según el tipo de cuentas capaces de manejar.

Para crear un grupo seleccionar Usuarios y, haciendo clic en la opción Nuevo/Grupo del menú Acción, en la caja de diálogo que se abre, asignar nombre al grupo y definir el tipo y el ámbito. Luego hacer clic con el botón derecho del mouse en el nombre del grupo que acaba de crear y seleccionar propiedades. En la hoja de Propiedades es posible añadir los distintos usuarios o computadoras y cambiar el ámbito, entre otras cosas.

3.5.- MICROSOFT MANAGEMENT CONSOLE (MMC)

La consola de administración de Microsoft (Microsoft Management Console-MMC), es el nuevo espacio de centralización de control de Windows. Esta herramienta de configuración hace la tarea de contenedor para todos los componentes de administración y configuración de Windows 2000.

MMC provee un método estandarizado para crear, abrir y guardar herramientas administrativas, llamada consola.

Consola: En este contexto, es un conjunto determinado de herramientas en una misma interfase.

MMC no posee en sí misma capacidades administrativas sino que "hospeda" un tipo especial de aplicaciones llamadas snap-ins o complementos, cada uno de los cuales sí puede usarse para tareas administrativas.

Las ventajas de MMC se sintetizan en 3 puntos:

- Llevar a cabo la mayor parte de las tareas administrativas desde MMC ahorra tiempo por cuanto todo se hace en una misma interfase, cualquiera que sea la labor.

- Usar consolas para llevar a cabo la mayor parte de las tareas administrativas permite crear herramientas específicas para cada usuario, es decir, sólo aquellas autorizadas por el administrador.

- Hay snap-ins preparados para administración remota y eso permite centralizar la administración desde una sola computadora.

Las consolas pueden tener uno o más snap-ins y se guardan como archivos con la extensión MSC. Estos archivos almacenan tanto la configuración de la consola como la de cada snap-in, por lo que pueden abrirse y conservar parámetros aún desde computadoras remotas.

MMC tiene opciones que permiten la creación de distintas consolas para que otros administradores o usuarios puedan ejecutar acciones específicas.

Cada consola tiene un árbol (console tree) que a la manera del Explorador, muestra la organización jerárquica de los snap-ins instalados en esa consola. El panel derecho presenta el contenido de cada snap-in seleccionado, ya sea un informe en el caso de los que se dedican a reportes de funcionamiento, o controles de ejecución en el caso de programas.

Los menús Acción y Ver cambian sus opciones según el contenido o función de los snap-ins. Éstas son las aplicaciones diseñadas para ser usadas mediante MMC. Hay 2 tipos de complementos: independientes y extensiones.

Los Complementos Independientes (Stand-alone snap-ins) son conocidos simplemente como snap-ins. Cada uno de ellos provee una función o un conjunto determinado de funciones. Cada versión de Windows 2000 viene con un grupo de consolas predeterminadas, la mayor parte de ellas con distintos subconjuntos de snap-ins. Como es obvio, aquellas funciones de administración de red que necesita Windows 2000 Server, no estarán en Windows 2000 Pro.

Las Extensiones de Complementos, conocidos simplemente como extensiones, proveen funcionalidades adicionales a otros snap-ins. Se diseñaron para añadir funciones a snap-ins independientes, basados en las que éste ya cumple. Cuando se crea una consola y se desea añadir extensiones, sólo aparecerán aquellas relacionadas o compatibles con el snap-in seleccionado.

Si se añaden snap-ins con extensiones. Éstas se instalaran automáticamente, a menos que explícitamente se eliminen o se deshabiliten algunas.

Una misma extensión, incluso, puede agregarse a varios snap-ins, mientras cumplan con el requisito de la compatibilidad. Finalmente digamos que en ocasiones, algunas extensiones pueden funcionar como un snap-in independiente.

Las consolas tienen 2 maneras de operar:

- El modo Usuario. No permite a los usuarios agregar, quitar o modificar la configuración de la consola. Este modo tiene, además, 3 opciones: Acceso completo (todo el árbol disponible, capacidad de abrir varias ventanas y navegar entre los snap-ins), Acceso delegado, ventanas múltiples (se pueden abrir varias ventanas pero no todo el árbol esta disponible) y Acceso delegado, ventana única (no se puede abrir más de una ventana y hay porciones del árbol restringidas).

- El modo Autor. Admite acceso completo a toda la funcionalidad de MMC. Guardar la consola en este modo habilita agregar o quitar snap-ins, la creación de ventanas, ver todas las porciones del árbol de la consola y guardar el archivo MSC.

Como se dijo al principio, Windows 2000 trae varias consolas preconfiguradas, las que permiten la mayor parte de las tareas administrativas (ver la figura 3.6). Éstas contienen los snap-ins más comúnmente usados y aparecen en Programas/ Herramientas Administrativas del menú del botón Inicio.

Por su parte, las consolas que aparecen en Herramientas Administrativas serán distintas, según se trate de Windows 2000 Pro o de Windows 2000 Server. Cuando se instalan componentes adicionales a Windows, también se añaden las consolas preconfiguradas, como en el caso de agregar el servicio de Domain Name Server o Internet Information Services. En ambos procedimientos se instalan las consolas de control de DNS y de IIS.

Aún cuando las preconfiguradas no se pueden modificar, sí es posible crear consolas nuevas con cualquiera de los snap-ins instalados en el sistema, más otros que pudiesen ser agregados por otros fabricantes.

Quizás el administrador desee crear consolas personalizadas con los servicios que usa más frecuentemente. Puede guardarlas como un archivo para reutilizarlas cada vez que las necesite, distribuirlas entre otros administradores o centralizar varias tareas administrativas distintas en una sola consola utilizable desde cualquier equipo de la red.

Además crear consolas personalizadas tiene la ventaja de no tener que pasar de una preconfigurada a otra en medio del trabajo.

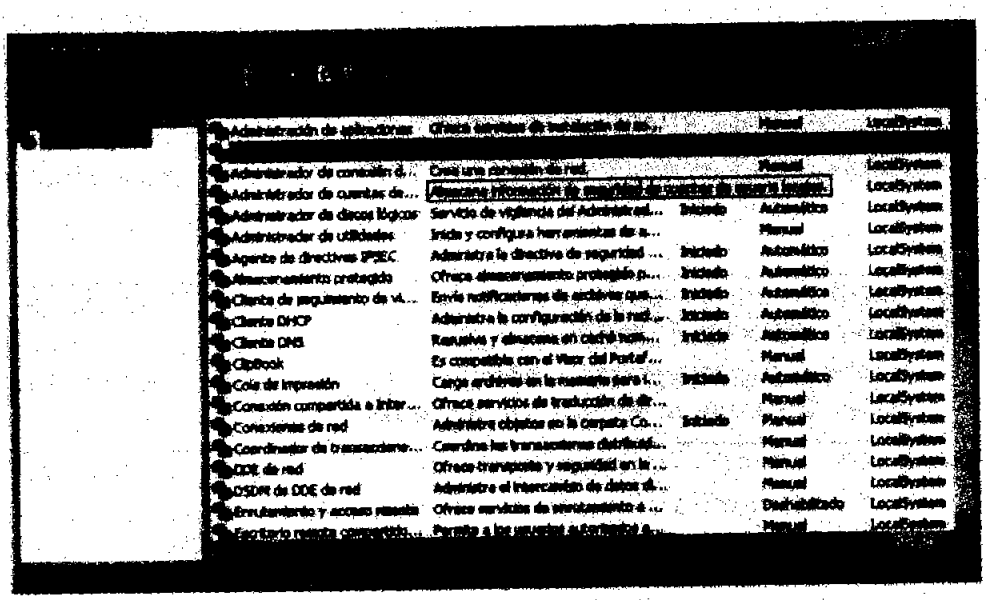


Figura 3.6 Windows viene con varias consolas predeterminadas.

Para usar las preconfiguradas, sólo hay que hacer clic en Programas/Herramientas Administrativas y elegir la que se va a usar.

La otra opción es arrancar las consolas haciendo doble clic en los archivos MSC guardados. Generalmente las consolas preconfiguradas van a estar en la carpeta \WINNT\system32, suponiendo que \WINNT sea el nombre de la carpeta de instalación de Windows.

3.6- RESPALDO DE INFORMACIÓN (ESPEJOS)

Se entiende por conjunto de espejos a 2 particiones de 2 discos duros distintos que se configuran para que una sea idéntica a la otra.

La partición espejo no aparece en la Administración de discos y sólo sirve para reflejar los datos de la otra partición (que entrara en funcionamiento cuando la primera partición falle).

Este método hace que el nivel de seguridad sea alto (RAID 1) aunque no se evitan los virus ya que estarían grabados en ambas particiones.

Se pueden dar 2 configuraciones:

- Los 2 discos duros están conectados al mismo controlador (en este caso, si falla el controlador dejará de funcionar el conjunto de espejos).

- Los 2 discos duros están conectados a controladores distintos (en este caso, si falla un controlador el conjunto de espejos seguirá funcionando con el otro controlador).

3.6.1 ADMINISTRACIÓN DE VOLÚMENES

Los volúmenes dinámicos son un nuevo concepto introducido en Windows 2000

Volúmenes Dinámicos. Se trata de espacios de almacenamiento que proveen la misma funcionalidad que las particiones pero que pueden ser configurados sin rebootear el sistema.

A diferencia de las particiones, no están limitados a cuatro por disco rígido. Los administradores crean, extienden y espejean volúmenes sin reiniciar el servidor, por lo que no es necesario interrumpir la tarea de éste mientras está en trabajando.

Asimismo, la administración se puede hacer a través de la red, a diferencia de lo que sucedía en versiones anteriores, en las que las tareas de administración de volúmenes requerían la presencia del administrador en el equipo local.

Las particiones creadas con Windows NT, 95, 98 y MS-DOS se consideran almacenamiento básico. Windows 2000 soporta este tipo de particiones por cuestiones de compatibilidad. Los volúmenes básicos no pueden extenderse, espejearse o crearse en forma seccionada. Sin embargo, pueden convertirse en dinámicos en cualquier momento.

La herramienta para gestionar el sistema de volúmenes de Windows es el Administrador de discos. A él se accede desde Programas/Herramientas administrativas/Administración de equipos, desplegando la rama Almacenamiento.

Si lo desea, puede crear una consola con las herramientas de disco (Administrador y Desfragmentador) con la herramienta MMC. Asimismo, si en lugar de definir la máquina como local, ingresa el nombre de otra de las máquinas de la red, podrá administrarla desde la cual está trabajando.

Windows 2000 seguirá soportando particiones y discos lógicos en volúmenes heredados, pero si la compatibilidad no es un tema, se recomienda que los administradores los actualicen a volúmenes dinámicos.

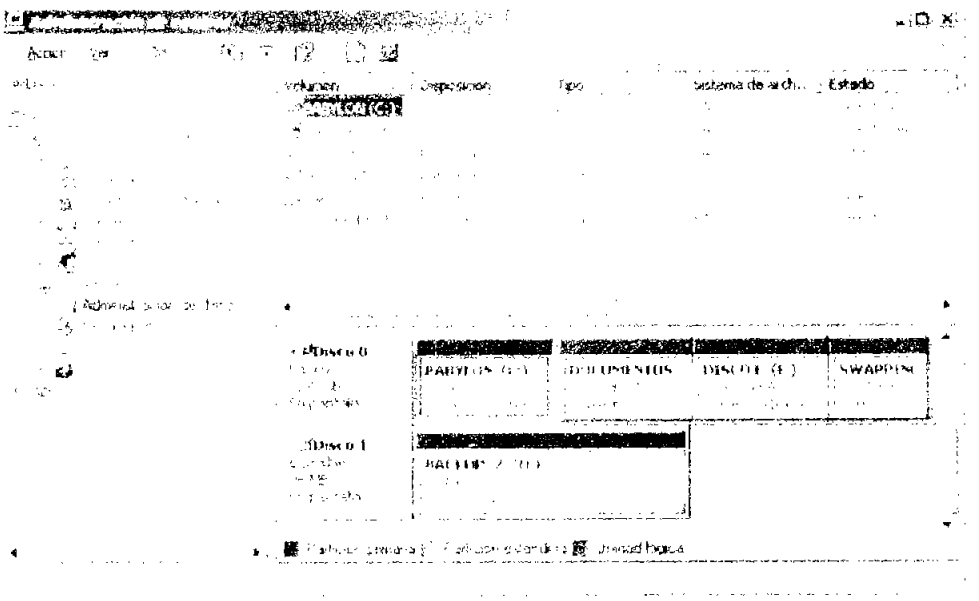


Figura 3.7 Si tiene doble booteo con otro sistema operativo, no podrá convertir a volumen dinámico ya que el otro sistema operativo no será capaz de "ver" el volumen.

Desde el Administrador de discos, se puede:

- Agregar nuevos discos.
- Crear nuevos volúmenes.
- Marcar particiones como activas.
- Añadir, eliminar y extender volúmenes.
- Crear y eliminar volúmenes seccionados.
- Crear, eliminar y reparar conjuntos RAID 1 y RAID 5.
- Convertir particiones básicas en dinámicas y viceversa.

Para convertir un volumen básico en uno dinámico, una vez que está en el snap-in de Administración de discos (ver la figura 3.7), hacer clic con el botón derecho del mouse en la unidad elegida y seleccionar Actualizar a Disco dinámico. Siga las instrucciones de las pantallas.

Si no encuentra este comando en el menú contextual, es posible que este seleccionando un volumen (partición) y no una unidad; que el volumen ya sea dinámico o que este usando una computadora portátil, ya que en ésta última no es posible crear este tipo de volúmenes.

Para que la actualización tenga éxito, todo disco a actualizar debe contener por lo menos 1 MB de espacio sin usar. Administración de discos reserva automáticamente este espacio al crear particiones o volúmenes en un disco, pero los hechos con otros sistemas operativos pueden no tener este espacio.

Los volúmenes dinámicos no deben contener particiones o unidades lógicas. Además no acceden a ser leídos por otros sistemas operativos tales como Windows 95/98 o MS-DOS, aún si están formateados con FAT.

Después de actualizar un volumen a dinámico, no se restauran las particiones a básico. Para hacerlo, debe borrar todos los volúmenes dinámicos del disco y usar el comando Restaurar a Disco Básico.

Tipos de volúmenes: Los discos básicos se pueden dividir en particiones primarias y extendidas. Las particiones funcionan como unidades físicas de almacenamiento separadas. Un disco básico puede tener hasta 4 particiones primarias o hasta 3 primarias y 1 extendida (ver la figura 3.8).

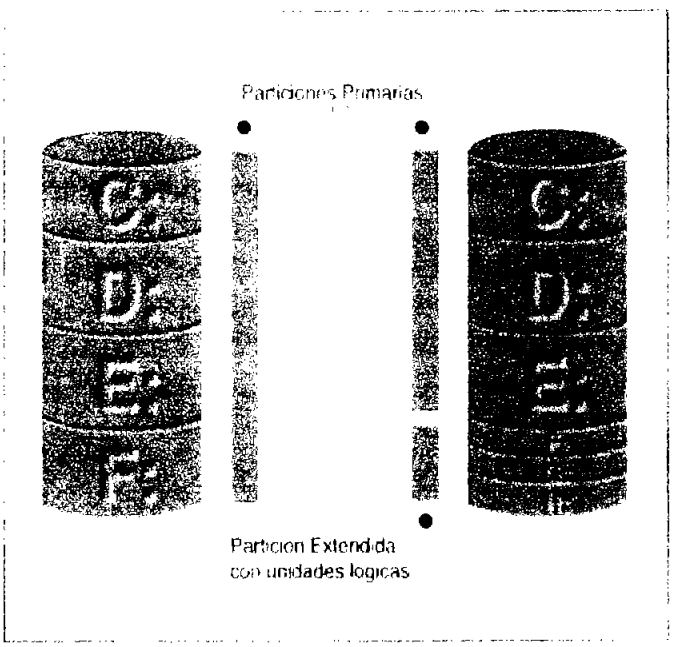


Figura 3.8 Las particiones primarias pueden ser 4 por disco, por eso las extendidas con discos lógicos amplían las posibilidades.

Sólo una partición primaria puede marcarse como partición activa –partición activa es aquella en la que el hardware busca los archivos para bootear el sistema operativo- y Windows 2000 sólo puede usar particiones primarias para arrancar la computadora. Solamente una partición por disco puede declarase activa por vez. El sistema de archivos con que se formatea una partición depende del sistema operativo que se instalara en ella.

Las particiones extendidas se crean del espacio libre. Puede haber una sola por disco, por lo que es importante incluir todo el espacio libre en la unidad. Las particiones extendidas por sí solas no son operativas hasta que se las divide en segmentos, cada uno de los cuales recibe el nombre de unidad lógica. A cada unidad lógica se le asigna una letra y se le da el formato que corresponde.

Para Windows 2000, una partición de sistema es la partición activa que contiene los archivos específicos para cargar el sistema operativo. La partición de inicio (boot partition) es la partición primaria o extendida que almacena los archivos del sistema operativo.

Particiones iguales. Es posible que ambas, partición de sistema y de inicio sean la misma. Pero si bien la de inicio puede ser cualquier unidad (física o lógica), la de sistema sólo puede ser la activa.

Al convertir discos básicos a volúmenes dinámicos, es decir, volúmenes de Windows 2000, es posible aumentar la seguridad del sistema. Una cualidad que sólo se encuentra en volúmenes dinámicos es la tolerancia a errores (fault tolerance), la habilidad del sistema operativo o del hardware para responder a eventos catastróficos sin perdida de los datos.

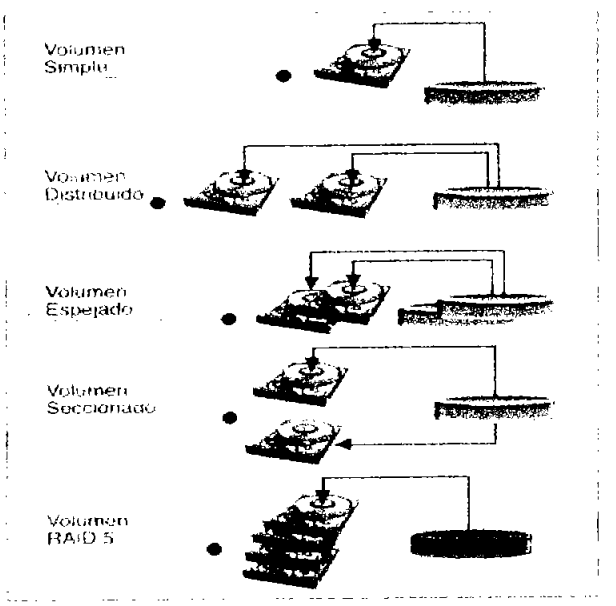


Figura 3.9 Los distintos tipos de volúmenes sólo se pueden hacer si se convierte un disco básico en un volumen dinámico.

Hay 5 tipos de volúmenes dinámicos (ver la figura 3.9):

- El volumen simple contiene espacio de un sólo disco.

- El volumen distribuido (spanned) incluye espacio de varios discos (hasta 32). En un volumen distribuido, los datos comienzan a escribirse en el primer disco hasta que el espacio se llena completamente, con lo cual empieza a escribirse el segundo y así sucesivamente. Un volumen distribuido no tiene tolerancia a errores, por lo que sí un disco del volumen falla, falla todo el volumen.

- El volumen espejado o reflejado (mirrored) consiste en dos copias idénticas de un volumen simple, cada una en un disco duro separado. Los volúmenes reflejados ofrecen tolerancia a errores, ya que si se pierde un disco, la información sobrevive en su "espejo".

- Un volumen seccionado (striped) combina áreas de espacio libre de múltiples discos –hasta 32- en un sólo volumen lógico. La razón de mantener un volumen seccionado tiene que ver con el rendimiento, ya que todos los datos se escriben en todos los discos a la misma tasa, pero si un disco falla, el volumen estero se cae.

- Un volumen RAID 5 (Redundant Array of Independent Disk-Matriz Redundante de Discos Económicos) es seccionado, pero con tolerancia a errores. Windows 2000 añade una banda de información de paridad en cada partición del volumen. Windows usa luego esa información de paridad para reconstruir los datos en caso de que un disco físico falle. Se necesita un mínimo de 3 discos para crear un volumen RAID 5.

Windows 2000 Pro puede usar volúmenes distribuidos, espejeados o seccionados con y sin paridad creados con Windows NT Server 4.0 pero no puede crearlos; tampoco puede extender un volumen on line (en línea), así que para hacer cambios en un disco básico, se deberá rebootear. Sin embargo, creando un snap-in capaz de manejar discos remotos, un administrador puede crear y administrar todo tipo de volúmenes desde Windows 2000 Pro.

Particiones Primarias vs. Extendidas. Los dispositivos de almacenamiento extraíble sólo pueden contener particiones primarias. No se pueden crear particiones extendidas, unidades lógicas o volúmenes dinámicos en unidades removibles. Tampoco marcar una partición primaria en un disco removible como activa.

3.7.- MEDIDAS DE SEGURIDAD

3.7.1 CLAVES PÚBLICAS Y PRIVADAS

Toda transacción de negocios requiere que cada parte esté segura de la identidad de la otra. La firma, en el caso de una tarjeta de crédito, por ejemplo, es una forma de validación ya que es teóricamente imposible que otra persona pueda hacer la misma firma que uno.

Hasta hace relativamente poco tiempo la seguridad no era un tema considerado ya que las redes estaban aisladas del exterior y todo usuario que se loguease en ella debía estar físicamente en el mismo edificio. Así, la autenticación de usuarios basados en su dirección IP y/o dominio era más que suficiente.

Sin embargo, en estos últimos años, la red se hizo cada vez más virtual en esencia y la conexión con el mundo exterior, vía Internet o satélite o cualquier otro medio, se hizo más la regla que la excepción. Asimismo, el par nombre de usuario/palabra clave –que generalmente viaja por la red encriptado- suele ser útil para identificar al usuario, pero no al servidor.

Para resolver esta omisión, se creó el par clave pública/clave privada. Estas claves están relacionadas entre sí, pero no hay manera de que se pueda extraer información de la otra a partir de una. Como su nombre lo indica, la clave pública es la que el usuario envía a todos sus destinatarios. Utilizándola, el que envía un mensaje puede encriptar la información. La única manera de desencriptarla es con la clave privada, que sólo obra en poder del usuario.

Como estas claves tienen una relación especial, no se puede encriptar el mensaje con la clave pública y desencriptarlo con la misma. Al mismo tiempo, la pública puede servir para enviar una firma digital que obre como identificación positiva. Se muestra a continuación un ejemplo para ver como funciona:

Alfredo necesita mandarle a Elena cierta información. Por el camino cualquiera podría interceptar el mensaje, cambiar el contenido, entonces lo que Elena recibiría, no sería válido. Alfredo utiliza la clave pública de Elena para cifrar el mensaje y su propia clave pública para insertar una firma digital que certifique que el mensaje fue enviado por Alfredo. Mientras el mensaje viaja, cualquiera puede tratar de usar la clave pública de Elena pero no podrá descifrar el mensaje. Cuando Elena lo recibe, lo desencripta usando su clave privada. Elena está segura de que el mensaje está inalterado porque ha venido cifrado y que, efectivamente, fue enviado por Alfredo porque ahí está su firma digital.

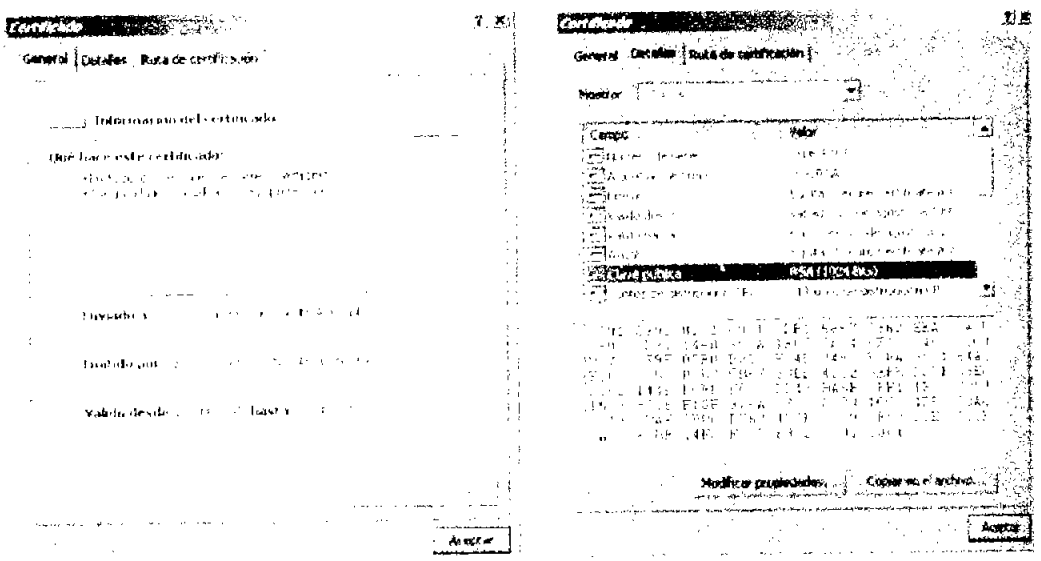


Figura 3.10 Un certificado expedido por una autoridad confiable (izquierda) provee las claves (derecha) para cifrar los mensajes, contraseñas, etc.

Cualquiera que posea el software adecuado puede generar claves públicas y privadas. Pero para que este procedimiento funcione, debe haber alguna organización que garantice que las claves públicas y privadas sean auténticas. Éstas son las Autoridades de Certificación (AC) (ver la figura 3.10). Estos organismos certifican que los pares de claves están asociados a una persona o a una asociación o entidad válida. Mantienen una copia de la clave pública y una lista de los certificados extendidos. Como es obvio, las AC deber ser organizaciones en las que se confía para llevar a cabo esta autentificación. La más conocida de ellas es VeriSign.

3.7.2 ADMINISTRACIÓN DE SEGURIDAD

Muchos aspectos de la seguridad de Windows 2000 dependen de certificados. El snap-in Certificados es la herramienta que se usa para administrar las claves y para especificar en que autoridades se confía. Cualquier certificado y su clave asociada se manejan desde este snap-in.

Muchas aplicaciones de Microsoft, incluyendo Internet Explorer, almacenan información de seguridad en el Registro, así como en ocasiones también buscan esta información en él. Como Windows 2000 viene nativamente preparado para soportar el manejo de la seguridad, las aplicaciones o servicios que la requieran pueden usar estos certificados como parte de su estructura.

El snap-in Certificados ya viene con una lista de Acs (AC-Autoridades de Certificación) que permiten ir construyendo la directiva de seguridad. El complemento también permite importar nuevas autoridades, así como aceptar una AC creada por usted para propósitos locales.

Mantener la seguridad de una red de máquinas, especialmente si es amplia, es difícil y por eso otra prestación del sistema de seguridad de Windows 2000 Server son las plantillas de seguridad (security templates). Esta herramienta, un snap-in de MMC, permite crear, editar, modificar y configurar distintas directivas de seguridad que después se aplican todas juntas a un equipo o a toda la red o a un subdominio, etc. Es muy probable que deba añadir el snap-in manualmente a una consola antes de usarlo (ver la figura 3.11).

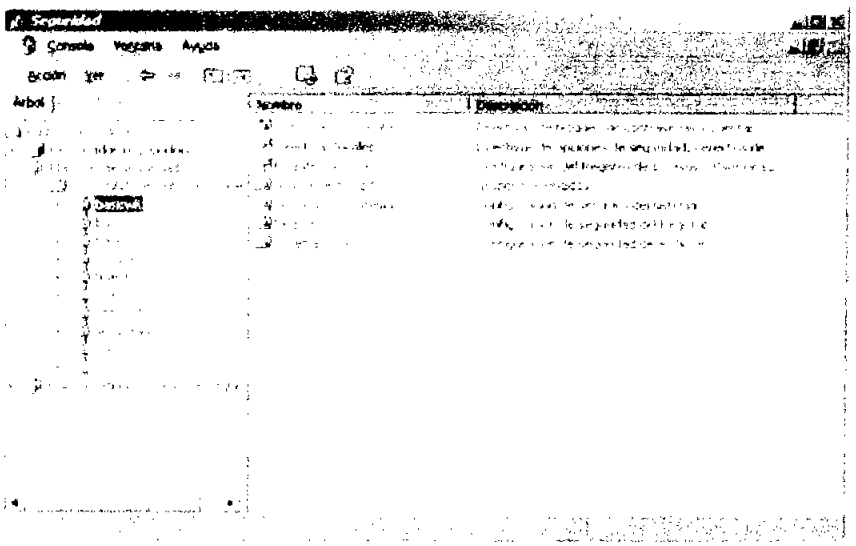


Figura 3.11 En este snap-in encontrará una buena cantidad de plantillas de seguridad para configurar sus propias directivas de seguridad.

Es factible usar las plantillas de seguridad, incluso, para analizar la seguridad de un sistema y determinar, por ejemplo, que aspectos de éste no están de acuerdo con los protocolos de seguridad de la empresa.

La funcionalidad de este complemento es semejante al Editor de directivas de grupo, a diferencia de éste, lo que se modifican son las plantillas que van a aplicarse luego, en lugar de activar la configuración ahora.

Windows 2000 viene con una buena cantidad de plantillas preparadas para asignar niveles bajos y altos en sistemas Windows 2000 Pro, Server y en controladores de dominio. Asimismo es posible usar cualquiera de las plantillas como base para crear la suya propia. Así como están, existe la posibilidad de que las plantillas no cubran exactamente los aspectos particulares de su red pero siempre es mejor tener una base que empezar de cero.

Si instala manualmente las plantillas, le conviene añadir el snap-in Configuración y análisis de seguridad, crear o abrir una base de datos de seguridad, seleccionar la plantilla que está usando su sistema y poner el snap-in a analizar su sistema.

Al finalizar la auditación se verá cada uno de los elementos que componen su esquema de seguridad y puede, incluso, exportar los resultados a un archivo de texto para llevar un registro de los análisis.

Finalmente, hay un aspecto que Windows 2000 también considera. No todos los administradores están de acuerdo o necesitan recurrir a una entidad verificadora externa para manejar su seguridad. Una de las maneras de resolver este tema es ser su propia AC y para ello, Windows 2000 viene con el Servidor de Certificados.

Durante la instalación de Windows o desde el accesorio Agregar o quitar programas del Panel de Control, Agregar o quitar Componentes de Windows, se puede instalar el Servicio de Certificate Server (Servidor de Certificados).

Durante la instalación tendrá 2 ó 4 opciones para seleccionar:

- Entidad emisora raíz de la Empresa. Es la opción a elegir si está usando Active Directory y ésta es la primera AC de la organización.
- Entidad emisora subordinada de la Empresa. Si usa Active Directory y ésta no es la primera AC, elegir esta opción.
- Entidad emisora raíz independiente. Si ésta es la primera AC de la empresa y no está usando Active Directory.
- Entidad emisora subordinada independiente. Si ya tiene una estructura de AC y no usa Active Directory.

Si durante la instalación de Certificates Server chequea el casillero Opciones avanzadas, una caja de diálogo especial aparecerá para permitirle definir el proveedor del encriptado, el algoritmo de hash (transformación) y la longitud de la clave, entre otros parámetros (ver la figura 3.2).

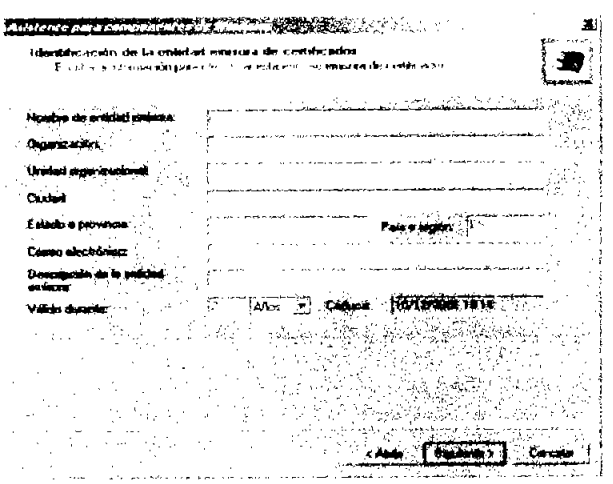


Figura 3.12 Si llena correctamente esta pantalla del Asistente de instalación de Certificate Server y concluye el procedimiento, puede empezar a entregar sus propios certificados.

El próximo paso es ingresar información de la empresa. Ésta es muy importante ya que figurará en los certificados emitidos por el Administrador, convertido en AC. Finalmente, el Asistente le pedirá que ingrese las carpetas donde almacenar los certificados. Trate en lo posible de que esas carpetas se encuentren en una partición con NTFS.

Luego de instalar el servicio, podrá administrar la creación y entrega de los certificados mediante el snap-in Autoridad de Certificación.

3.7.3 TARJETAS INTELIGENTES (SMART CARDS)

En muchos casos, para algunas organizaciones, la autenticación por técnicas de nombre de usuario y contraseña no es suficiente. Uno de los métodos más nuevos es el de la tarjeta inteligente (smart card) que el usuario lleva consigo. Es una tarjeta electrónica semejante a una de crédito, con un microprocesador, que almacena información de identidad del usuario.

Cuando se entrega una smart card, al usuario se le asigna un PIN (Personal Identification Number-Número de Identificación Personal), que lo autentica frente a la tarjeta. El usuario es la única persona que conoce el PIN, el que debe ser ingresado junto con la tarjeta, para ser validado como usuario autorizado, al poseer tanto el medio físico (la tarjeta) como el conocimiento para usarla (PIN).

Al ingresar la tarjeta en el lector, el sistema operativo utilizará el protocolo Kerberos para autenticar al usuario. La información de la tarjeta y del PIN no viajan a través de la red –una vez que Kerberos entrega el ticket ya no es necesaria- y sí lo hacen con el usuario, el puede loguearse desde cualquier máquina mientras posea el lector adecuado.

Una alternativa más económica la constituyen las tarjetas plásticas tipo de crédito, que poseen una cinta magnética. Esta cinta puede contener mucha información, incluyendo una clave personal, pero no poseen la capacidad de procesamiento que distingue a las tarjetas inteligentes.

Windows 2000 provee soporte nativo desde el sistema operativo para soportar tarjetas inteligentes como sistema de identificación de seguridad.

3.8.- POLÍTICAS Y PROCEDIMIENTOS

3.8.1 DIRECTIVAS DE GRUPO

Directivas de Grupo: Como primera definición, las directivas de grupo son un conjunto de configuraciones que se aplican sobre uno o más objetos de Active Directory. Sin embargo, también se usan para controlar los entornos de trabajo en un dominio, En una Unidad Organizacional o simplemente, en un conjunto particular de cuentas de Usuario.

Los grupos de directivas además, tienen un cierto grado de herencia. Cuando se aplican a clases, todas las subclases son tributarias de las mismas configuraciones. Uno de los usos más comunes de las directivas de grupo, es por ejemplo, crear un Escritorio común a la empresa o departamento. Esto incluye un menú del botón inicio Personalizado, una carpeta Mis Documentos específica y una serie de permisos y restricciones sobre aplicaciones y archivos.

Las directivas de grupo pueden actuar sobre una variedad de componentes de la red y de objetos de Active Directory. Entre ellos:

- Aplicaciones. Los usuarios pueden acceder a las aplicaciones bajo dos condiciones posibles. La asignación de aplicaciones, en la que a las que tienen acceso son instaladas y actualizadas automáticamente desde el servidor sin que el cliente tenga la opción de desinstalarlas. La publicación de aplicaciones en cambio, es una serie de programas que el usuario puede utilizar, pudiendo instalarlas y desinstalarlas a voluntad; aparecen en las cajas de diálogo de Agregar o quitar programas en las que, por otra parte no es posible agregar nada más.

- Archivos. Ciertos archivos van a aparecer siempre en las carpetas Mis Documentos o Escritorios de las computadoras cliente.

- Guiones (scripts). Los administradores de directivas de grupo pueden especificar archivos de comandos para ser ejecutados a intervalos determinados o ante eventos particulares (arranque o cierre del equipo o de la sesión).

- Configuración de software. Los administradores pueden configurar globalmente muchas de las definiciones en perfiles de usuarios.

- Seguridad. El administrador puede restringir el acceso a ciertas carpetas y archivos. También controlar parámetros como la cantidad de veces que un usuario puede ingresar una contraseña incorrecta o cuales son los derechos y permisos para acceder a un servidor de dominio, etc.

Si bien es posible crear y administrar directivas de grupo en entornos mixtos o heterogéneos, el mayor rendimiento se logra cuando la red está formada exclusivamente por Windows 2000.

En este caso, la conjunción de las directivas apropiadas, combinadas con los permisos de NTFS y otras prestaciones de seguridad de Windows 2000, hacen a las directivas de grupo una de las más poderosas herramientas para administrar una red con la mínima perdida de rendimiento.

Los parámetros de configuración de las directivas de grupo están contenidos en un Objeto de directivas de grupo (Group Policy Objets-GPO). Uno o más GPOs pueden aplicarse a las Unidades Organizacionales, así como una o más Unidades Organizacionales pueden ser asociadas con un mismo GPO (ver la figura 3.13).

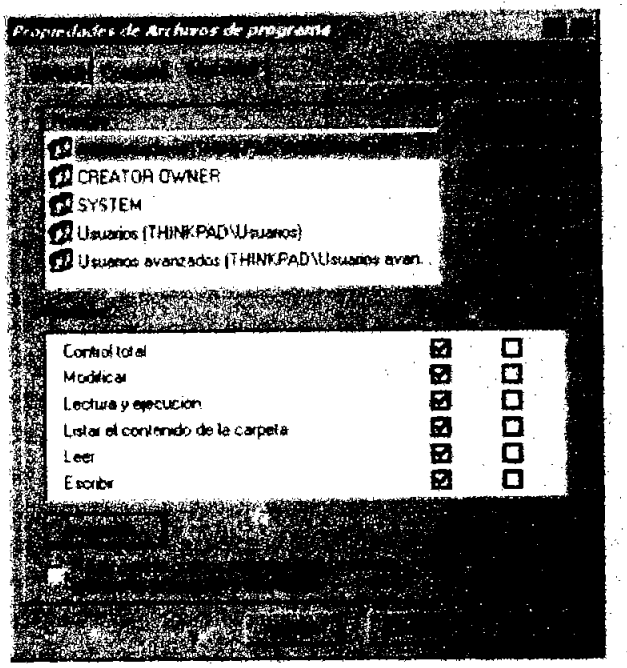


Figura 3.13 Cada objeto de directivas de grupo tiene hojas de Propiedades que permite, como en este caso, definir los permisos de acceso y asignar a grupos.

El GPO almacena la información de las directivas en dos ubicaciones. Los Contenedores de directivas de grupo son objetos de Active Directory y que contienen las propiedades de uno o más GPOs; pueden contener subcontenedores que incluyen información de grupos de usuarios y de computadoras. Las Plantillas de directivas de grupo (Group Policies Templates) constituyen una estructura de carpetas y subcarpetas en el volumen de sistema de un controlador de dominio y funcionan como contenedores de las directivas de software, scripts e información de seguridad, entre otras cosas.

Como se dijo antes, las directivas de grupo son hereditarias y acumulativas y afectan a todas las computadoras y cuentas de usuario en el contenedor de AD al cual el GPO está asociado.

El orden de herencia es Sitio, Dominio y Unidad Organizativa. Sin embargo, el orden de prioridad se establece cuanto más cerca esté la directiva de la computadora o del usuario. En otras palabras, si hay un conflicto entre dos configuraciones perteneciente una al Dominio y la otra a la Unidad Organizativa, tiene prioridad esta última por estar más cerca del objeto computadora o del objeto usuario. Y si hay un conflicto entre la directiva de la computadora y la del usuario, se aplica esta última.

En algunos casos, sin embargo, es necesario que la prioridad sea inversa, es decir, las opciones de la Unidad Organizativa tengan precedencia sobre las del usuario. En ese caso, mediante el Administrador de Active Directory es posible cambiar el orden de procesamiento.

3.8.2 TRABAJAR CON DIRECTIVAS DE GRUPO

El primer paso para crear una directiva de grupo es crear o abrir un GPO. Desde el Administrador de Active Directory, seleccionar un objeto y desde la hoja de Propiedades crear o modificar la directiva de grupo del objeto.

El resto de la tarea se lleva a cabo desde el Editor de directivas de grupo, un snap-in que puede instalarse en una consola según las instrucciones de MMC.

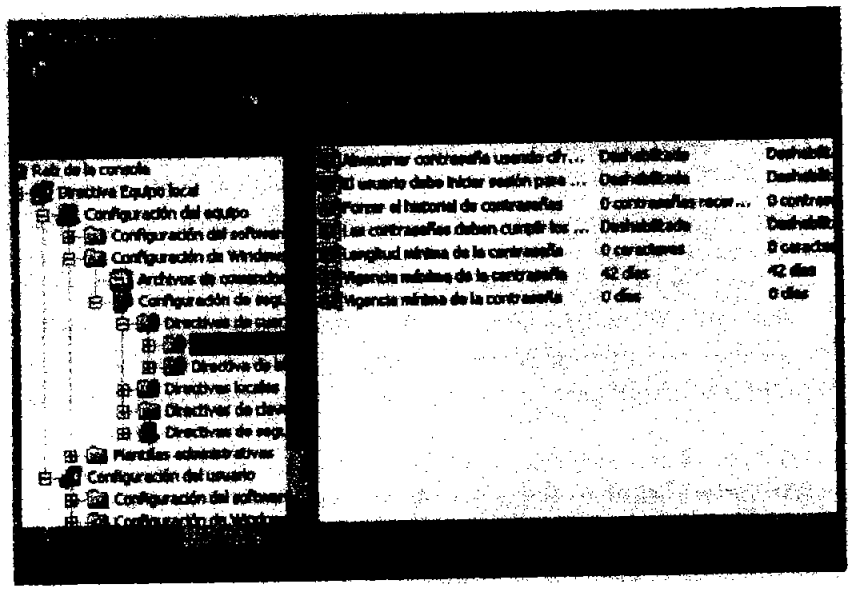


Figura 3.14 El Editor de Directivas de grupo permite configurar los múltiples parámetros que Windows 2000 ofrece para mantener la seguridad de un sistema.

En la estructura de árbol del panel izquierdo, las ramas principales son Configuración del equipo y Configuración del usuario (ver la figura 3.14).

Las carpetas de Configuración del equipo contienen parámetros que se usan para personalizar el entorno de trabajo y se activan cada vez que se enciende el equipo. De entre las directivas que se pueden configurar, se cuentan las contraseñas (cantidad de caracteres y vigencia), el software a instalar, planes de auditoria, opciones de seguridad, etc. Esta configuración se pone en marcha cada vez que se enciende la máquina independientemente de qué usuario se loguee.

De entre las prestaciones de la carpeta de Configuración del usuario, figuran la configuración de Internet Explorer, los scripts (archivos de comandos) de inicio y cierre, y los servicios de instalación de aplicaciones. Esta configuración se aplica cada vez que el usuario se loguea, independientemente de en que máquina lo haga.

Ambas carpetas tienen una subcarpeta llamada Plantillas administrativas, las que le permiten modificar innumerables definiciones, desde la apariencia del shell de Windows hasta la protección de los archivos de sistema, pasando por el comportamiento de los archivos fuera de línea y de otros componentes de Windows como el Programador de tareas.

RESUMEN

Al eliminar el PDC y el BDC de Windows NT y migrar a los Controladores de Dominio en Windows 2000, la Base de Datos de todo el AD estaba contenida en cada Controlador de Dominio y los cambios se replicaban automáticamente en cada uno de ellos.

Como pudimos apreciar en este capitulo Microsoft se preocupo mucho por la seguridad en este sistema operativo de red ya que noto con la entrada de Internet una necesidad de crear un protocolo de seguridad más estable y seguro para los usuarios. Así surge Kerberos.

Como la red de la compañía es muy extensa se aprovecharon todas las ventajas que ofrece Windows 2000.

Primero en administración, ya que con Active Directory se pudo redefinir la red en Unidades Organizacionales y asi se pudo sistematizar la red entre los departamentos, grupos y usuarios que realmente se necesitaban.

Segundo en seguridad ya que para el manejo de la información se contó con los servicios de Certificados, encriptamiento y GPO que permitían activar la seguridad en un nivel alto donde era más sensible el manejo de información; además los permisos asignados por el grupo de Administradores y el departamento de Help Desk ayudaron significativamente a la buena administración de información y recursos en la red.

Por medio de MMC se puede llegar ha tener una administración mas centralizada y ágil, provee un método estandarizado para crear, abrir y guardar herramientas administrativas. Al grupo de Help Desk se le asignaron varias MMC para poder administrar a un nivel medio la red y a un nivel alto a los recursos, grupos y usuarios de la sucursal

La Administración de discos como RAID y los espejos permitió que los servidores de mayor importancia en la red (servidores de Bases de Datos y Aplicaciones), nunca dejaran de operar y que su rendimiento se incrementara.

CAPITULO 4
ADMINISTRACIÓN, MANTENIMIENTO Y SOPORTE DE LA RED

4.1 OPTIMIZACIÓN DEL RENDIMIENTO Y HERRAMIENTAS DE MONITOREO

Windows 2000 proporciona un conjunto de herramientas administrativas que facilitan la operación del mismo.

Las herramientas Visor de sucesos, Información del sistema, Administración remota, Carpetas compartidas y Consola de rendimiento son utilizadas a medida que se necesitan y entran en lo que es la optimización y mantenimiento del sistema.

4.1.1 EL VISOR DE SUCESOS

En la terminología de Windows 2000, se dice que un suceso es cualquier incidente cuya ocurrencia es interesante conocer, y por lo tanto, notificar al usuario.

En el caso de sucesos críticos, como por ejemplo un servidor lleno o una interrupción del flujo eléctrico, puede ser que aparezca en pantalla un mensaje notificando inmediatamente al usuario. En otros casos, en los que no se requiere una atención inmediata del usuario, el suceso se almacena en un archivo de registro, sin interferir en el trabajo del usuario. Este archivo puede ser analizado a través del Visor de sucesos.

Se pueden encontrar 3 tipos de sucesos:

- Sucesos del sistema: generados por el propio sistema operativo.
- Sucesos de aplicación: generados por las aplicaciones que se ejecutan.
- Sucesos de seguridad: indicados por el usuario a través de las directivas de seguridad.

Para iniciar el Visor de sucesos de forma independiente de la consola Administración de equipos, simplemente ejecutar Visor de sucesos desde Programas, Herramientas administrativas (ver la figura 4.1).

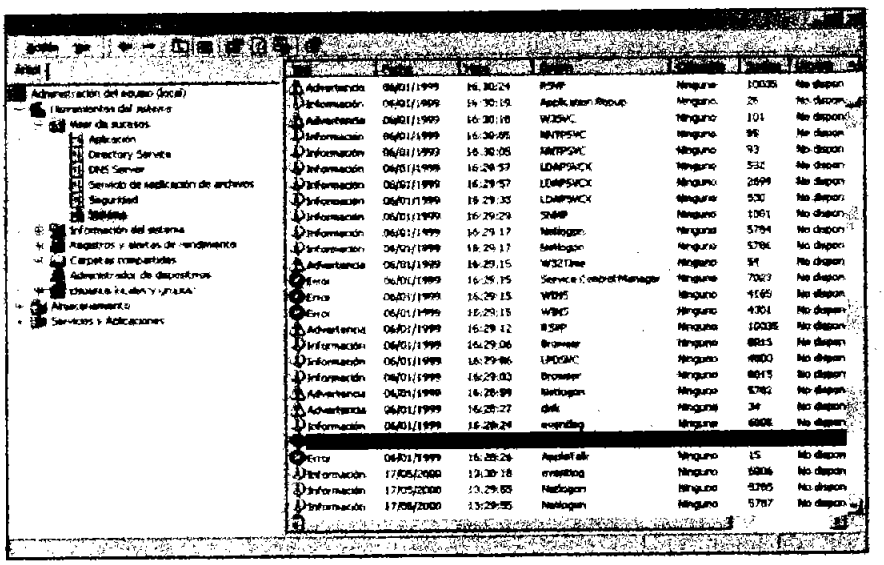


Figura 4.1 Herramienta Visor de sucesos.

Dentro del Visor de sucesos se realizan distintos registros, dependiendo de la configuración del sistema. La lista variará, pero normalmente existe una línea básica de elementos seguidos por el registro. El hecho de que aparezcan unos u otros registros depende, en gran medida, de la instalación de dichos servicios.

El registro del sistema hace un seguimiento de los sucesos que afectan el rendimiento o funcionamiento del servidor. Una vez iniciado el sistema, se inicia un registro del sistema, y el registro de sucesos guarda su propio inicio en el registro (ver la figura 4.2). Cada suceso posterior se registra y se etiqueta según el tipo y la urgencia del mensaje.

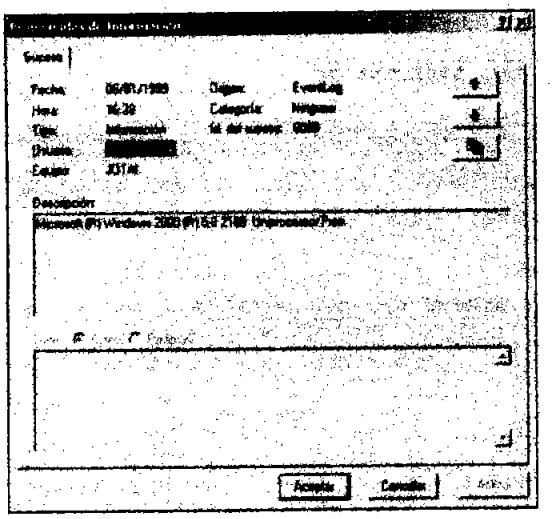


Figura 4.2 Visor de sucesos abierto.

El registro de aplicación sólo lo utilizan las aplicaciones que se han escrito para registrar elementos en el registro. En otras palabras, el sistema operativo no registra todas las aplicaciones y tampoco escribe sucesos de las mismas en el registro de aplicaciones. Considerando, por ejemplo, el paquete de aplicaciones de trabajo en grupo de Microsoft llamado Exchange. Exchange escribe muchos sucesos en el registro de aplicaciones, que indican al administrador lo que ha sucedido en la aplicación.

El registro de seguridad no registra nada, a menos que active la auditoria en una parte específica del sistema de seguridad en Windows 2000. El proceso para iniciar esta auditoría se basa en cambiar la directiva de grupo; además puede incluir un sistema predeterminado para todo el dominio.

4.1.2 INFORMACIÓN DEL SISTEMA

La información de la sección Información del sistema de la consola Administración de equipos es sólo eso, simplemente información (ver la figura 4.3). No es información que se pueda cambiar o manipular, pero es un buen recurso para encontrar la respuesta al tipo de preguntas que surge cuando aparece un problema. No es posible cambiar la información de esta interfaz, pero puede imprimirla.

La herramienta Información del sistema es ideal cuando tenemos algún problema con el hardware de nuestro equipo. En ocasiones ocurre que 2 ó más componentes de hardware intentan utilizar los mismos recursos del equipo, lo que puede producir que uno de ellos o ambos a la vez no funcionen de forma correcta. Esta situación se verifica con esta herramienta.

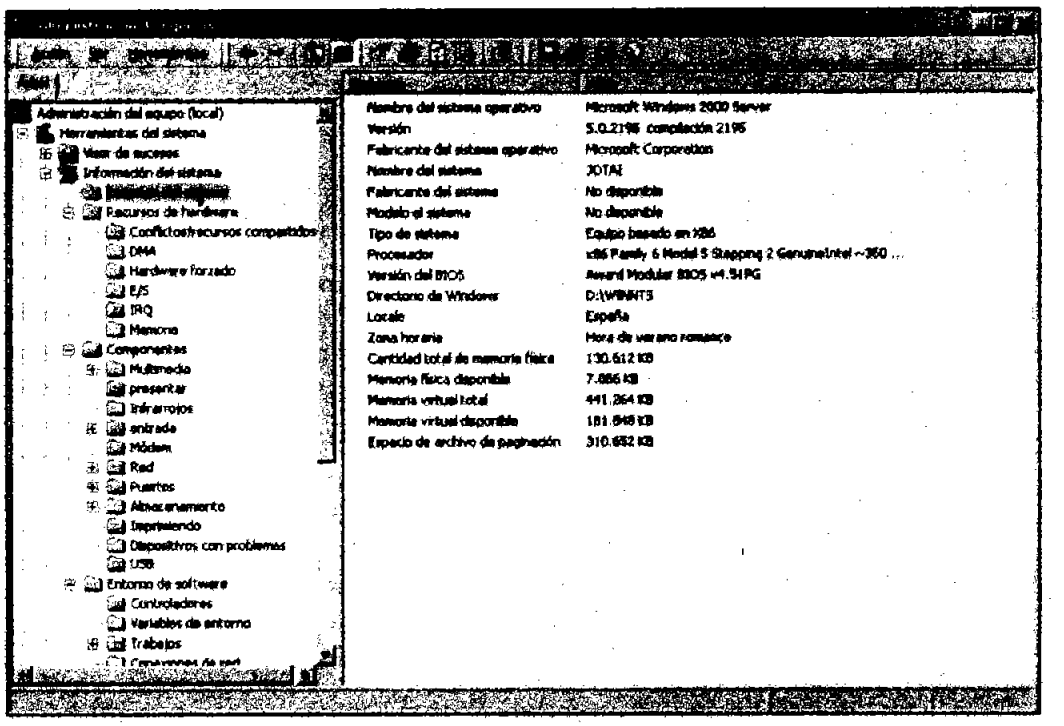


Figura 4.3 La pantalla Información del sistema expandida.

4.1.3 DESFRAGMENTADOR DE DISCO

Evitando la fragmentación de las unidades del disco duro puede mejorar de forma palpable el rendimiento de los sistemas. La fragmentación se puede dar en cualquier tipo de disco duro (EIDE, SCSI, etc.) lo mismo que en los sistemas con una sola unidad y sistemas RAID. Cuanto más se fragmenta una unidad de disco, más difícil es para el sistema operativo y las aplicaciones encontrar los archivos que necesitan para realizar cualquier operación concreta. Obviamente, si se tarda más tiempo en hallar un archivo esparcido por uno o más discos, disminuirá la velocidad general o la velocidad aparente del sistema operativo y de la aplicación. En Windows 2000 Server existe una herramienta que puede ayudar a identificar las áreas fragmentadas de la unidad del disco y a desfragmentar las unidades de disco particulares. Esa herramienta se conoce como Desfragmentador de disco.

Para tener acceso a la utilidad Desfragmentador de disco de Windows 2000, hacer clic en inicio, Programas, Accesorios, Herramientas del sistema, Desfragmentador de disco para iniciar la aplicación y ver la primera pantalla (ver la figura 4.4).

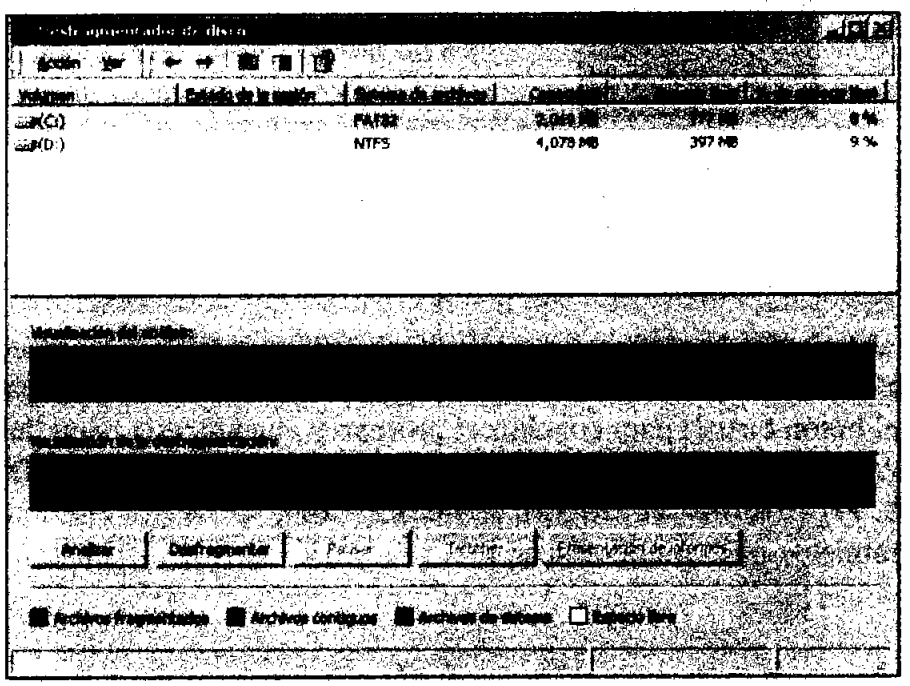


Figura 4.4 Pantalla principal del Desfragmentador de disco.

Cuando se utiliza por primera vez la herramienta Desfragmentador de disco, se verá una lista de volúmenes de unidades de disco duro disponibles en la mitad superior de la pantalla. La mitad inferior de la pantalla se dedica a los procesos de análisis y desfragmentación que deberá seleccionar para iniciar una o las dos características.

A continuación, seleccionar una unida para analizar. Para ello, hacer clic en una unidad concreta para resaltarla (esto significa que ha decidido llevar a cabo estas operaciones concretas en ese volumen particular; en este caso la unidad C:\).

Luego hacer clic en el botón Analizar (que aparece en la parte inferior izquierda de la pantalla) o en el menú Acción y seleccionar Analizar (las dos opciones hacen lo mismo) para iniciar el proceso de análisis del Desfragmentador de disco.

Cuando comience el proceso de análisis, aparecerá una línea coloreada en el área Visualización del análisis (se encuentra en la mitad inferior de la pantalla). Utilizar los cuadros inferiores de colores para descifrar exactamente lo que está sucediendo en el volumen de la unidad de disco. Es probable, si nunca ha utilizado esta herramienta en ese volumen concreto de la unidad de disco, que vea muchas areas fragmentadas en la unidad. Cuando finalice el análisis, aparecerá un pequeño cuadro de diálogo (ver la figura 4.5).

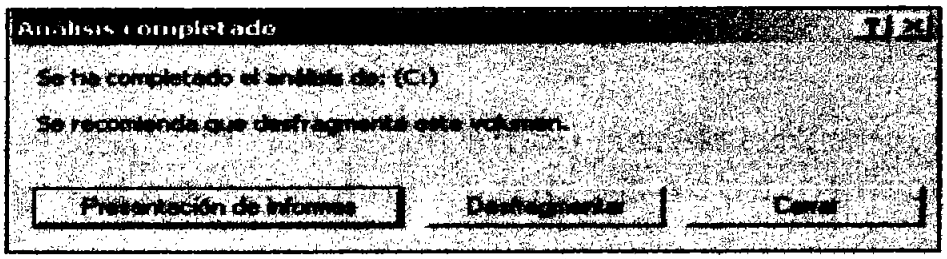


Figura 4.5 Decisión de lo que debe hacer cuando acaba la fase de análisis.

Cuando aparece la ventana de Análisis completado, se muestra una recomendación para ese volumen concreto. Es muy probable que la unidad de disco requiera desfragmentación, especialmente si se trata de un volumen que forma parte de una base de datos o de un servidor de archivos, o si es la primera vez que utiliza la herramienta Desfragmentador de disco.

Enseguida pulsar el botón Desfragmentar y de esta forma continua el proceso de desfragmentación. Cuando termine el proceso sólo basta con cerrar la ventana para salir de esta herramienta y la unidad en cuestión ya estará desfragmentada.

4.1.4 MONITOR DEL SISTEMA

Para monitorizar el rendimiento del equipo, Windows 2000 proporciona la herramienta Monitor de sistema.

El Monitor del sistema es una herramienta gráfica que mide el comportamiento de procesadores, memoria, memoria caché, subprocesos y procesos. Cada uno de ellos lleva asociado un conjunto de contadores que ofrece información sobre el uso de dispositivos, longitudes de colas, retardos y otros datos que informarán del rendimiento y su posible saturación. Entre las posibilidades se encuentran:

- Reunir datos de rendimiento en tiempo real tanto del equipo local como de cualquier otro equipo de la red.
- Ver los datos reunidos (tanto los actuales como los anteriores).
- Mostrar los datos en un gráfico imprimible, en un histograma o en una vista de informe.
- Exportar los datos a Microsoft Word u otras aplicaciones de Microsoft Office.
- Crear páginas HTML a partir de las vistas de rendimiento.

La herramienta Monitor de sistema se activa desde Inicio, Programas, Herramientas administrativas, Rendimiento.

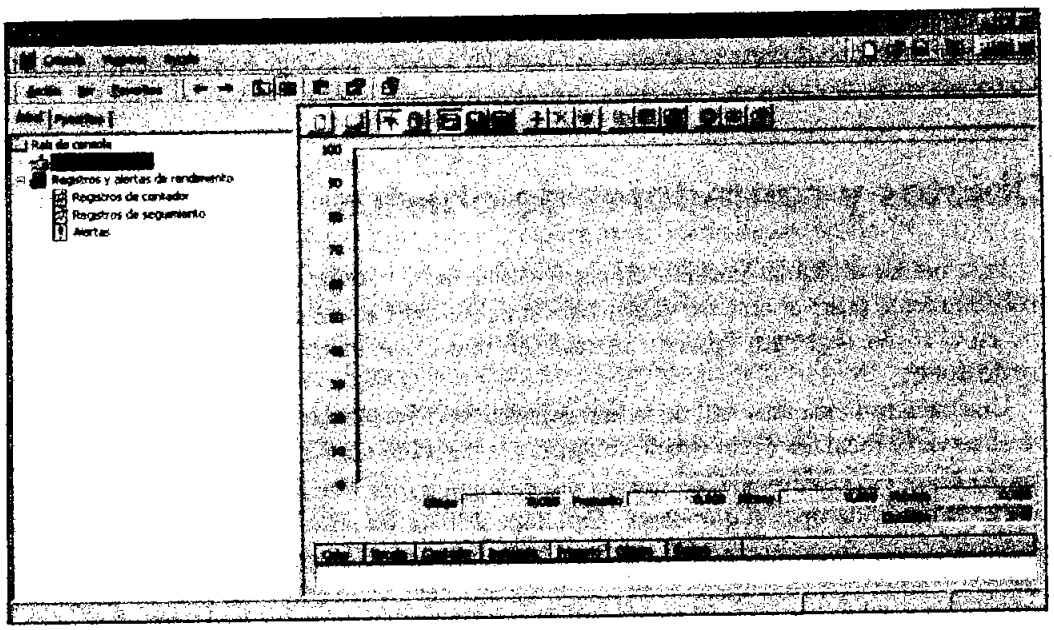


Figura 4.6 Pantalla de Monitor de sistema.

Dicha pantalla está dividida en dos paneles. En el panel izquierdo se encuentran el nodo Monitor del sistema, y en el panel derecho se muestra un eje vertical, numerado en función de una escala dada y en su parte inferior, cinco valores (ver la figura 4.6):

- Ultimo. Es el último valor leído.
- Promedio. Es la media de todos los valores leídos.
- Mínimo. Es el valor más pequeño de los leídos.
- Máximo. Es el valor mayor de los leídos.
- Duración. Muestra el tiempo que se tarda en crear un gráfico completo en la pantalla.

Para finalizar la herramienta simplemente cerrar la ventana.

4.2 RECUPERACIÓN DE INFORMACIÓN EN CASO DE DESASTRE

4.2.1 COPIA DE SEGURIDAD DE WINDOWS 2000

La utilidad Copia de seguridad de Windows 2000 Server se puede considerar posiblemente el aspecto más importante de este sistema operativo. Numerosas organizaciones carecen de planes formales de copia de seguridad, por no mencionar siquiera los planes habituales de negocios que se aplican para los servidores de los departamentos y otras aplicaciones pequeñas basadas en el servidor. Muchas organizaciones consideran que los servidores fuera de alcance y control del departamento de Tecnologías de la Información (IT) son aquellos servidores que se pueden reemplazar fácilmente y por ello, no requieren ni una copia de seguridad a nivel empresa, ni los servicios de restauración que proporcionan la mayoría de grupos de IT. Normalmente, esta forma de pensar conduce al desastre comercial cuando el servidor de una organización se bloquea y no hay forma de recuperarlo.

Las versiones anteriores de Windows NT incorporaban una utilidad de copia de seguridad y restauración en el propio sistema operativo. Aunque proporcionaba un método rudimentario con el que las compañías podían hacer sus copias de seguridad con facilidad y en última instancia, recuperar la información, el término "rápido" no se podría asociar nunca a este proceso. Debido a los constantes avances en las tecnologías de dispositivos de copia de seguridad, unidos a algunas mejoras en el mismo software de la utilidad Copia de seguridad, estos defectos de la antigua utilidad de copia de seguridad de Windows NT Server no siempre se apreciaban antes de que fuera demasiado tarde (durante un proceso de recuperación de varios días o cuando se intentaba una recuperación completa de entradas del Registro de un servidor). Ahora, sin embargo, con la última versión de Windows 2000 Server, muchos de los defectos de las versiones anteriores se han mejorado finalmente con la aplicación de una consola de recuperación, un modo seguro, un proceso de reparación de emergencia y similares.

Algunos administradores de red dejan los procesos de copias de seguridad a usuarios individuales, lo que significa que cada uno de ellos se responsabiliza de guardar sus propios archivos.

Esta forma de actuar no es buena, ya que los usuarios no dedican el tiempo ni la periodicidad necesaria para hacer la copia de seguridad adecuada de sus archivos.

Por tanto, es mucho más positivo que sea un administrador, como responsable de mantener el funcionamiento y mantenimiento del sistema, el que se encargue de las tareas de copia de seguridad o delegue en alguien que tenga los permisos necesarios, por ejemplo los Operadores de copia.

En el entorno operativo de Windows 2000 Server, sólo los administradores de sistemas o aquellos cuyas cuentas de usua io son miembros del grupo Administradores u Operadores de copia podrán hacer copias de seguridad de los archivos y carpetas del servidor.

Por lo anterior el grupo Operadores de copia debe tener el mismo grado de confianza que el de Administradores, ya que en sus manos esta la protección y recuperación de los datos del servidor.

Puede tener acceso a esta herramienta haciendo clic en Inicio, Programas, Accesorios, Herramientas del sistema, Copia de seguridad (ver la figura 4.7).

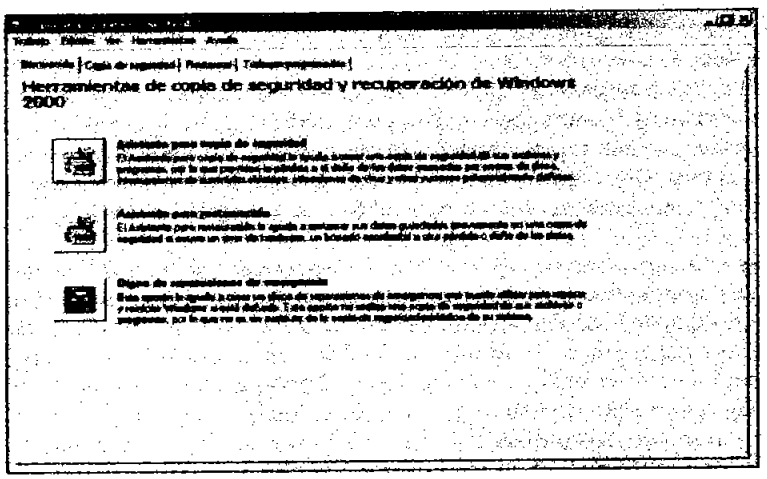


Figura 4.7 Pantalla principal de copia de seguridad de Windows 2000.

La herramienta Copia de seguridad admite cinco tipos distintos de copias de seguridad:

- Copia de seguridad **Copia.** Este tipo es útil cuando desea copiar archivos específicos de Windows 2000 Server a un dispositivo de copia de seguridad (cinta, disco, etc.) sin borrar el atributo del archivo de esos archivos específicos.

- Copia de seguridad **Diaria.** Este tipo es el que se utiliza cuando desea hacer copia de seguridad de todos los archivos que se han alterado de algún modo u otro (modificado, agregado, etc.) desde la última vez que se llevo a cabo un proceso de copia de seguridad. De nuevo, esto no marca los archivos como ya copiados, lo cual lo convierte en útil para las sesiones de copia de seguridad de cada noche.

- Copia de seguridad **Diferencial.** Este esquema de copia de seguridad permite hacer copias de seguridad de cualquier archivo o carpeta que se haya creado o modificado desde la última sesión de copia de seguridad Normal o Incremental. Muchas compañías emplean como su metodología de copia de seguridad una combinación de copias de seguridad diferenciales, incrementales y normales o diarias. Este es un método de copia de seguridad muy común porque el tiempo de restauración es mucho menor que el necesario para un esquema de copia de seguridad combinado de Normal-Incremental, debido al menor número de cintas y discos necesarios. Como desventaja, sin embargo, un esquema de seguridad Normal-Diferencial requiere más tiempo que un proceso de copia de seguridad Normal-Incremental.

- Copia de seguridad **Incremental.** Aunque este tipo de copia de seguridad puede resultar interesante al reducir considerablemente el tiempo necesario para realizar un proceso de copia de seguridad, recuerde que se necesitan cintas de copia de seguridad normales, además de todas las cintas de copia de seguridad incrementales para poder recuperar los sistemas correctamente. Las copias de seguridad incrementales dejan una marca especial en los archivos para indicar que ya se han copiado.

- Copia de seguridad **Normal.** Este proceso de copia de seguridad marca cada archivo y carpeta con un atributo especial que indica los demás tipos de copia de seguridad a los que ese archivo o carpeta en concreto han sido sometidos previamente.

El asistente de Copia de seguridad le guiara de forma sencilla y amigable el proceso y parámetros de la copia de seguridad.

4.2.2 RECUPERACIÓN DE DATOS

Muchos administradores piensan en una copia de seguridad del servidor como un método de recuperación únicamente en el caso de una pérdida total del disco duro, sin embargo, es mejor pensar en la copia de seguridad del servidor como una forma de recuperar los datos en cualquier momento. Los medios para hacer copias de seguridad pueden utilizarse para muchas formas de recuperación de datos:

- Recuperación de un error del disco duro.
- Recuperación de corrupción o pérdida de un archivo individual.
- Volver a versiones anteriores de los archivos.
- Mantenimiento de un registro para propósitos de auditoría o historial.

El error de disco duro es probablemente el uso menos habitual del proceso de recuperación. Es más frecuente que los desastres estén relacionados con errores de usuario. Estos desastres son incluso peores que el error físico. Los errores de usuario frecuentemente no se detectan durante días, semanas o incluso meses. Esto significa que la recuperación de datos desde ayer, no es lo suficientemente buena. Si la corrupción ocurrió un martes y no se encuentra hasta el lunes, la cinta de la noche anterior tiene los datos erróneos.

Sea consciente de que las cintas de copia de seguridad y las unidades de cinta fallan de la misma manera que los disquetes, cintas de vídeo o cintas de sonido. Son medios magnéticos y como tales, sólo son buenos durante un cierto tiempo. Por esta razón, entre otras, asegúrese de restaurar algún dato cualquiera de la unidad de cinta de vez en cuando. Ningún sistema es perfecto, e incluso un buen sistema puede fallar.

Nunca deja de sorprender a los ingenieros de redes cuantas veces vayan al sitio del cliente, encontrarse con que la restauración que se les está pidiendo que hagan es lo primero que se hace en el sistema. No tenga fe en ningún hombre o sistema de seguridad. Ponga a prueba su sistema de copia de seguridad y restaure el sistema por sí mismo.

4.2.3 OPCIONES PARA EL CASO DE ERROR POR HARDWARE

En cualquier máquina, las partes con mayor probabilidad de fallar son las partes móviles. En una PC, la única parte que se mueve constantemente es el disco o discos duros. Los discos duros giran como un disco en un tocadiscos desde el momento en que se encienden. Algunos discos duros se detienen para ahorrar energía, pero no debería hacer eso con los discos duros de un servidor.

El disco duro contiene todos los datos almacenados en la PC. Si toda la PC fallara y se recuperara el disco duro, sería fácil recuperar todos los datos. Esto convierte al disco duro en la pieza más importante del hardware del servidor.

Cualquier plan de recuperación de hardware debe incluir el subsistema del disco duro como parte de ese plan. Existen dos corrientes principales a la hora de implementar el hardware y que se utilizan actualmente en los servidores para seguir usando el espacio de disco duro durante un error hardware:

- La corriente más habitual consiste en utilizar el hardware administrado por RAID. Esto impidiendo que el sistema operativo se vea afectado por el fallo.

- Una solución cada vez más popular y disponible es el uso de los servidores organizados por clústeres. Esto supone la unión de dos servidores en un único subsistema de disco duro, permitiendo que alterne el control entre los dos cuando se produzca un error o cuando lo decida el administrador. Actualmente, estos sistemas se utilizan principalmente para ofrecer tolerancia a errores.

4.2.4 RAID CONTROLADA POR HARDWARE

RAID es una parte del sistema operativo Windows 2000 Server. Esta forma de RAID se conoce como RAID software porque la administración y el control de la matriz la realiza el sistema operativo. RAID controlada por hardware administra la matriz RAID en el controlador del disco duro.

La ventaja de este sistema es que el sistema operativo no consume tiempo ni energía de procesamiento cuando realiza este proceso. En las soluciones hardware, el controlador contiene el procesador y la RAM para mantener la división y la tolerancia a errores. Esto permite al sistema ejecutarse más rápidamente.

La comunicación administrativa con el controlador se mantiene a través del sistema operativo, pero esta comunicación se hace más bien con propósitos de alerta. Mediante utilidades de alerta de errores en el sistema operativo, éste puede alertar al administrador de la existencia de un error.

4.2.5 SERVIDORES ORGANIZADOS POR CLÚSTERES

La organización por clústeres de los sistemas tiene numerosos significados en el mundo de la computación. En relación con el sistema operativo, implica la unión de dos servidores en un único subsistema de disco duro y permite que alterne el control entre los dos, en función de los errores o del control del administrador.

El hardware en esta configuración suele ser más una combinación propietaria de los siguientes elementos (ver la figura 4.8):

- Un controlador del disco duro (SCSI o Canal de fibra) en cada servidor para unirse al subsistema del disco duro común.
- Un subsistema del disco duro que consta de los siguientes elementos:
  - Un controlador interno del disco duro del subsistema.
  - Discos duros.
  - Un armario o recinto cerrado.

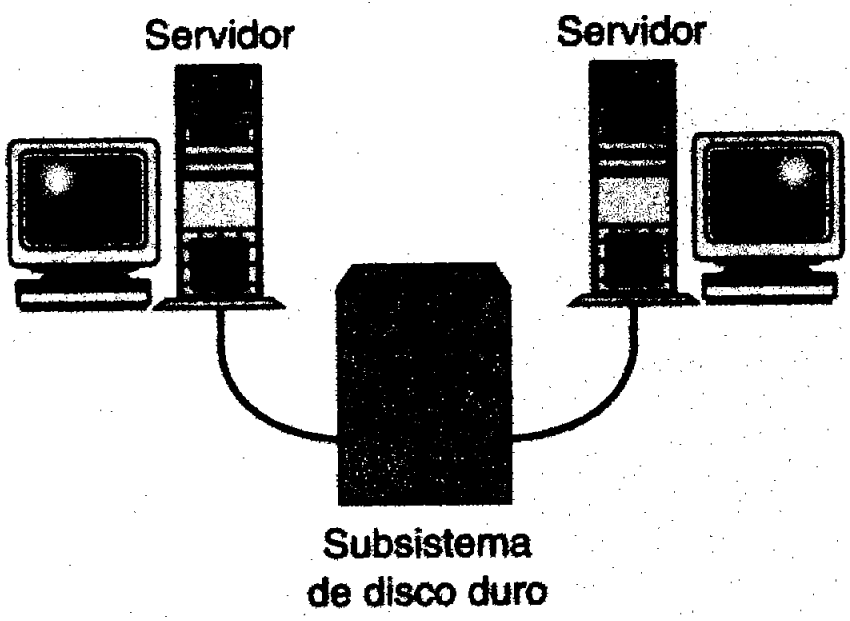
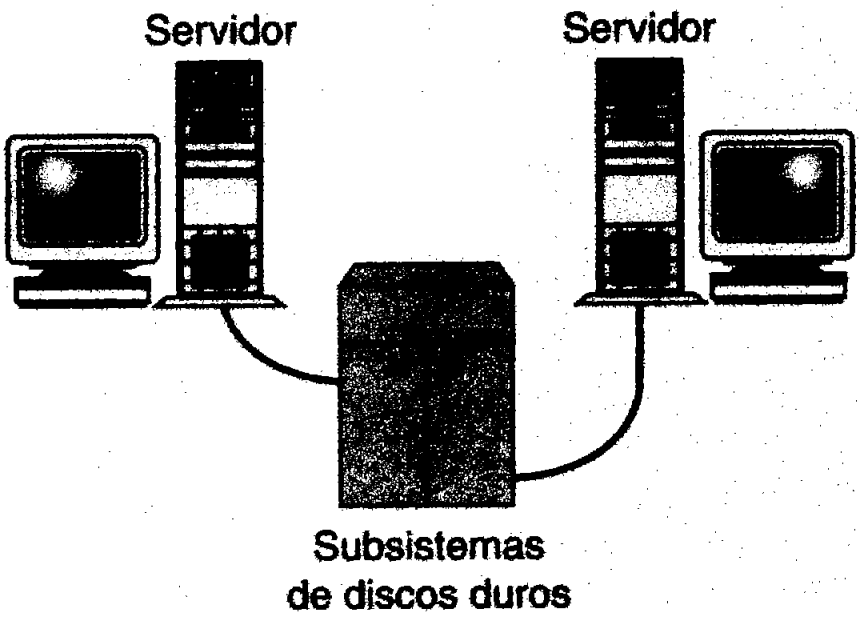


Figura 4.8 Clúster de servidores Windows.

La conexión se hace entre los servidores, y el subsistema se hace mediante SCSI o Canal de fibra, dependiendo de la implementación. El SCSI compartido es la solución más antigua y está más restringida por los límites físicos de los cables SCSI y la tecnología. El Canal de fibra es una tecnología más nueva y tiene la ventaja del cable de fibra óptica. También permite conectar múltiples servidores y periféricos (incluyendo los discos duros) a un concentrador.

La organización por clústeres de Windows en este entorno se llama frecuentemente "nada compartido", porque los sistemas no tienen acceso común a ningún almacenamiento en ningún momento (ver la figura 4.9). Un servidor tendrá siempre el control de un disco dado. Por ejemplo, si un subsistema de unidad contiene dos unidades lógicas, puede utilizar cualquiera de las siguientes combinaciones:

- El Servidor 1 controla las unidades A Y B.
- El Servidor 2 controla las unidades A y B.
- El Servidor 1 controla la unidad A y el Servidor 2 controla la unidad B.
- El Servidor 1 controla la unidad B y el Servidor 2 controla la unidad A.



Fifura 4.9 Un ejemplo de "nada compartido".

La cuestión es que en ningún momento los servidores A y B pueden controlar la unidad al mismo tiempo. Ni tampoco pueden controlar la unidad B al mismo tiempo. Los dos pueden tomar el control utilizando cualquiera de las combinaciones mencionadas anteriormente, pero no pueden compartir el control.

Una vez establecido el almacenamiento común, se puede formar el clúster. Desde el punto de vista del usuario, estos dos servidores aparecerán con un nombre común. El clúster se presenta a sí mismo a través de ese nombre como si fuera un servidor "lógico" independiente. De la misma forma que se pueden presentar espacios de disco duro independientes como un único disco duro lógico, los dos servidores y sus recursos compartidos comunes pueden presentarse como un único servidor lógico.

Los servidores A y B aparecerán como el Clúster_1 del servidor (ver la figura 4.10).

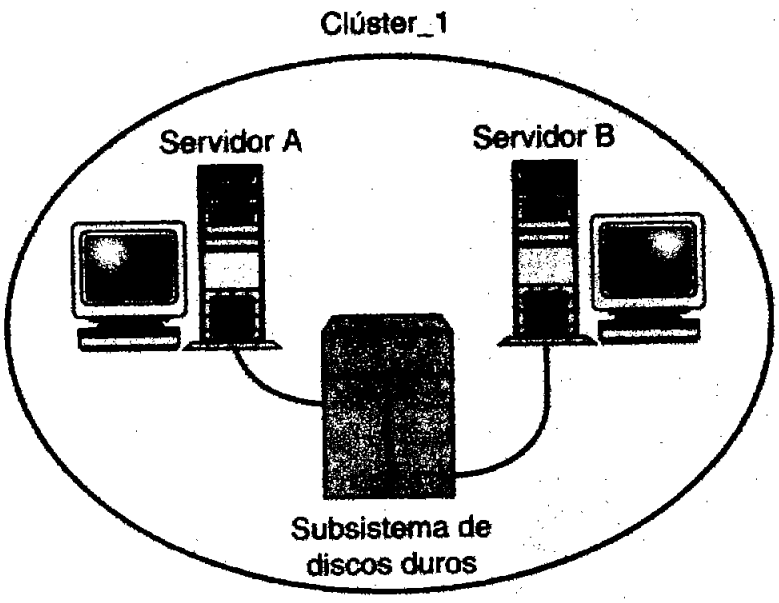


Figura 4.10 Presentación de los clústeres.

Los servidores se comunican entre sí su estado actual enviando una señal tipo "pulso" o "latido" a su asociado mediante la conexión a la red.

Cuando se produce un error en un servidor del clúster (software o hardware) el procesador se detiene, por lo que el pulso también se detendrá. Si un servidor no ve a su asociado de clúster durante un determinado periodo de tiempo, tomará el control de la parte del subsistema de disco asociado.

Como todos los recursos del clúster aparecen con un nombre de servidor lógico, los usuarios no notarán nada más que un retraso en el servicio mientras se realiza el cambio. El clúster puede incluir impresoras compartidas y disco compartidos, que tampoco se deberían detener durante el cambio. Como los recursos están en las unidades de las que toma el control el asociado del clúster, el servidor lógico continuará funcionando.

Como se mencionó anteriormente, los discos duros también pueden fallar. Por ello, es lógico controlar estos discos duros por algún tipo de RAID hardware. No tiene sentido gastar el dinero innecesariamente en hacer que los servidores estén disponibles en todo momento, para que después se produzca un error de disco duro y los recursos dejen de estar disponibles.

La recuperación de un desastre puede significar muchas cosas para una organización, desde recuperar datos perdidos en el disco duro de una secretaria, hasta una mudanza de todo el núcleo de la organización debido a un fenómeno natural. Su organización debería estar preparada para estos problemas por igual.

La recuperación de desastres requiere de algo más que simplemente hacer una copia de seguridad en una buena cinta cada noche. Necesita que haya una distribución de tareas, el equipo debe volverse a inventariar y ordenarse en prioridades, y la documentación de los recursos clave debe estar disponible en un sitio externo.

Hacer copias de seguridad no es simplemente el proceso de almacenamiento de datos en una cinta cada noche. El proceso requiere que haya más de una cinta en el plan de copias de seguridad total. Un plan para hacer copias de seguridad debe implicar varias cintas, con diferentes edades y un sitio externo de almacenamiento. Tenga en mente que la pérdida de datos o la necesidad de archivar datos no se deben sólo a la posibilidad de un fallo.

4.3 ENRUTAMIENTO Y ACCESO REMOTO (RAS)

En estos últimos años ningún segmento de la informática ha crecido tanto como el de las comunicaciones. Comenzando con los servidores de acceso remoto, siguiendo por Internet y terminando por las derivaciones actuales como las redes virtuales privadas, videoconferencias y telefonía por Internet, el soporte de protocolos de comunicación telefónica se ha impuesto como una necesidad ante la actualidad.

Enrutamiento y Acceso Remoto (Routing and Remote Access Service-RRAS). Este grupo de tecnologías permite a los usuarios conectarse a la red corporativa sobre líneas telefónicas comunes. No sólo posibilita el acceso a Internet sino que también es capaz de brindar el servicio de ISP a otros usuarios.

Enrutamiento y Acceso Remoto combina e integra las tecnologías que antes estaban separadas como Servidor de Acceso Remoto (Remote Access Server-RAS) y Acceso Telefónico a Redes (DUN-Dial-up Networking).

Windows 2000 Server tiene las herramientas para convertirse en un servidor de acceso remoto, mientras tanto Windows 95 y 98 como NT Workstation y 2000 Pro pueden ser los clientes de este tipo de acceso.

Windows 2000 soporta conexiones de líneas análogas a través de módems, conexiones por medio de líneas digitales de alta velocidad (ISDN), líneas X.25 y conexiones directas por cable (modem null).

4.3.1 UNICASTING, MULTICASTING Y NAT

Un ruteador (router) es una capa intermediaria de hardware o software que se usa para conectar redes LAN o WAN, basada en protocolos comunes a las redes que se conectan, como TCP/IP. El unicasting (también llamado unicast routing) es el reenvío de tráfico destinado a una sola ubicación en la red, de un host fuente a un host destino, usando ruteadores. Al servidor Windows 2000 encargado del enrutamiento se le conoce como Windows 2000 router (ver la figura 4.11).

Las computadoras de una red pueden enviar paquetes a otras redes reenviándolos a través del router. Éste examina el encabezado del paquete para decidir que protocolo utilizar. Windows 2000 puede rutear tráfico de IP, IPX y Apple Talk. Windows 2000, está además, preparado para que terceras partes puedan agregarle tantos protocolos nuevos como sean necesarios (ver la figura 4.12).

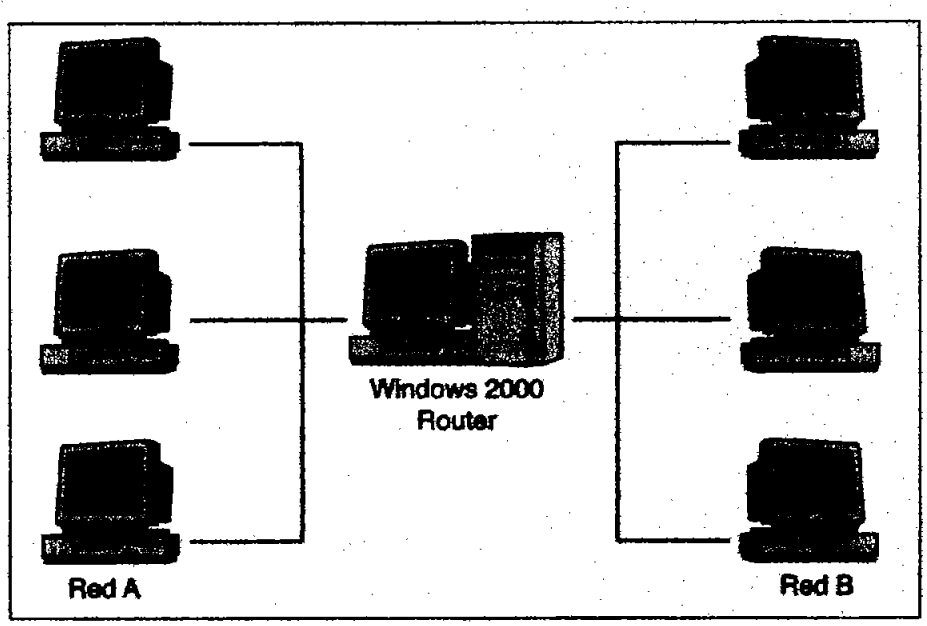


Figura 4.11 Si el ruteo es simple, no son necesarios protocolos especiales porque el router tiene contacto con las dos subredes.

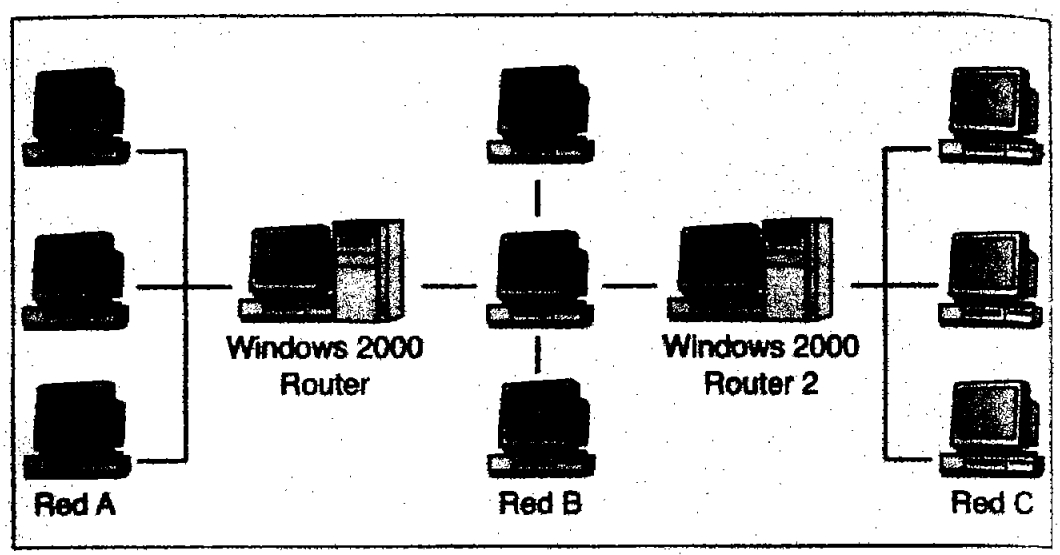


Figura 4.12 En cambio, si es más complejo, los protocolos cobran enorme importancia.

Multicasting (multicast routing and forwarding) es el envío de paquetes a través de la red a múltiples puntos. Se trata de un único paquete que se envía a múltiples direcciones utilizando IP. Aunque Windows 2000 puede manejar el reenvío (forwarding) mediante multicast, no trae los protocolos para el ruteo multicast. Sin embargo hay un modo de habilitarlo para una Intranet que se conecta a múltiples redes mediante un ruteador simple, instalando el protocolo IGMP (Protocolo de Administración de Grupo en Internet-Internet Group Management Protocol) y usándose como un proxy.

NAT (Network Address Translation-Traducción de Direcciones de Red), es el proceso en el cual se usa un proxy de manera transparente para transferir paquetes entre una red interna y una externa. Con la funcionalidad de NAT –nativa en Windows 2000- habilitada, una conexión telefónica simple es capaz de permitir que una red entera se conecte a Internet sin hacer cambios en los clientes.

El servidor debe estar configurado con direcciones IP estáticas, mientras los clientes deben definir al servidor como su puerta de enlace (gateway) predeterminada. El servidor NAT actuará como un router al reenviar los paquetes de la red interna a la externa. NAT añade la prestación adicional de reemplazar las direcciones IP privadas por direcciones IP públicas válidas.

NAT también es capaz de actuar como un proxy invertido (reverse-proxy), lo que permite a los administradores publicar páginas web o servicios de correo electrónico disponibles públicamente sin necesidad de poner los servidores en una red pública. Puede usar un rango determinado de direcciones IP públicas o asignar IPs privadas usando DHCP y actuar, incluso, como un proxy para solicitudes DNS.

Se accede a la herramienta haciendo clic en inicio, Programas, Herramientas administrativas, Enrutamiento y acceso remoto.

La primera vez que se use, se deberá establecer el o los servidores que va a controlar mediante el utilitario. Hacer clic en el menú Acción y seleccionar Agregar servidor. Mediante botones de opción, se puede elegir si se configura la máquina local, otro equipo de la red, un dominio en particular o rastrear un objeto de Active Directory.

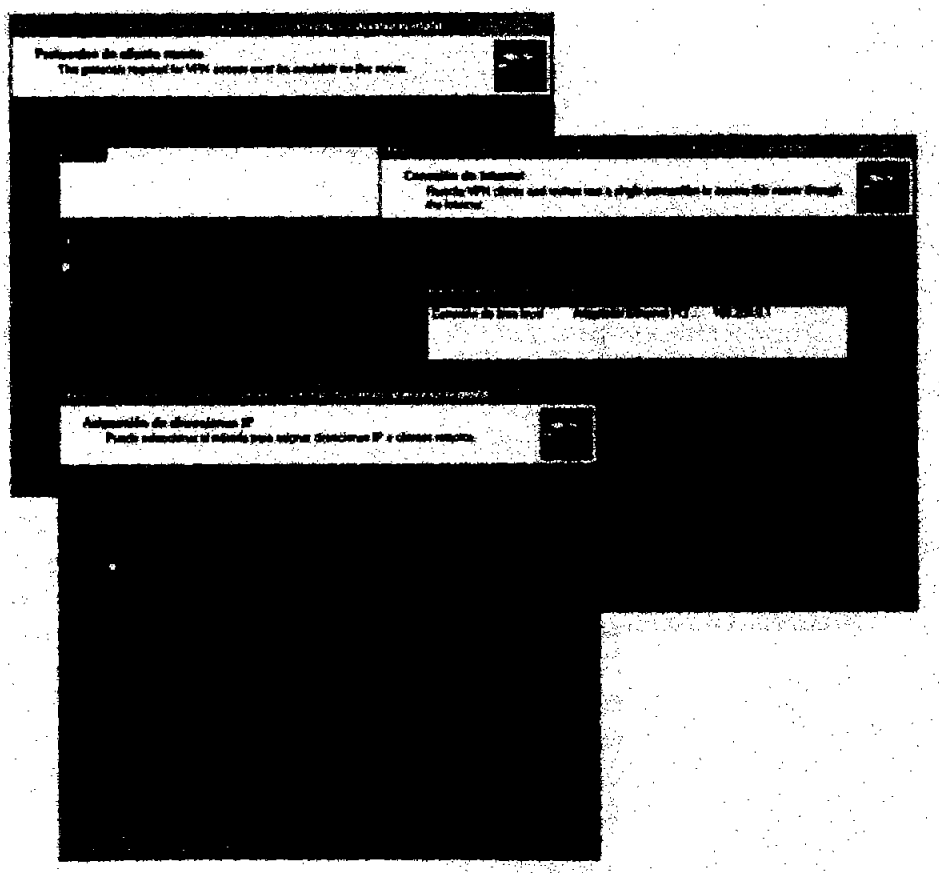


Figura 4.13 Este Asistente es el que lo guiará para transformar su equipo en un router.

El segundo paso es agregar los servicios que se deseé configurar. Hacer clic con el botón derecho del mouse en el nombre del servidor y seleccionar Configurar y habilitar el enrutamiento y acceso remoto (ver la figura 4.13).

El Asistente que se abre permitirá escoger que se va a configurar:

- **Servidor de conexión a Internet.** Esta opción permite establecer un servidor a través del cual se comunica el resto de la red con Internet.
- **Servidor de acceso remoto.** En este caso lo que se configura es la capacidad de recibir llamados telefónicos para conectarse con este servidor.
- **Servidor de red privada virtual.** Una manera de comunicarse con la red local a través de Internet.
- **Enrutador de red.** Como su nombre lo indica, configura este servidor como router.
- **Servidor configurado manualmente.** Esa opción habilita que el administrador configure todos los parámetros necesarios directamente desde la consola.

Si se selecciona Servidor de conexión a Internet, la siguiente caja de diálogo permitirá marcar, dependiendo de la complejidad de la red, dos servicios básicos: Conexión compartida a Internet y NAT.

Si la red es única y pequeña, seleccionar Conexión compartida a Internet (Internet Connetion Sharing-ICS), el asistente lo enviará a Conexiones de red y acceso telefónico.

Si se selecciona NAT, el Asistente ofrecerá utilizar la conexión de red existente o crear una conexión de marcado a demanda. Luego abrirá otro Asistente en el que se debe ingresar los datos de la conexión.

Para crear un Servidor de acceso remoto, seleccionar entre las opciones Básica y Avanzada. Como en el primer caso, si selecciona la opción Básica, el Asistente enviará a Conexiones de red y acceso telefónico. Si se elige la opción Avanzada, el Asistente comenzará a guiar por los protocolos y servicios que se desean implementar.

Alternativas semejantes a la opción avanzada esperan si se selecciona Red privada virtual y Enrutador de red. Finalmente Servidor configurado manualmente activará el servicio y dejará que el administrador haga el resto de las configuraciones.

4.4 ESCALABILIDAD Y ALCANCE DE LA RED

La migración y el despliegue de un sistema en red tiene tantas particularidades como empresas, corporaciones, instituciones u oficinas intervengan en la estructura de la red.

Por otra parte, cada red precisa de distintos enfoques, por cuanto no es lo mismo una red administrativa interna que una que posee conexión a Internet, que otra dentro de la cual convivan distintos sistemas operativos u otra que posea algunos integrantes portátiles.

Sin embargo hay una serie de pautas a seguir para lograr una migración exitosa –o por lo menos con la menor cantidad de incidentes posibles- la mayor parte de las cuales se llevan a cabo antes de la instalación y actualización del sistema operativo propiamente dicha.

Para describir el procedimiento de planificación de la migración, se seguirá un esquema de seis pasos propuestos por Anthony Northrup en su libro Introducing Windows 2000 Server.

Fase 1: Limpieza y depuración

Una primera idea implica hacer la migración tan simple como sea posible. Aún cuando es una buena práctica de todos los días, antes de una migración, la limpieza y depuración de una red es fundamental.

En esta etapa se trata de verificar la base de datos de las cuentas de usuario para asegurarse de que no hay cuentas duplicadas o sin uso. Elimine todas las carpetas y archivos innecesarios tanto en los servidores como en los clientes y asegúrese de tener la mayor cantidad de espacio libre disponible en los discos rígidos de sus máquinas.

Este es el momento también, de llevar a cabo esas actualizaciones de hardware que había dejado de lado. Recuerde que el soporte de hardware de Windows 2000 es mucho mejor que el de Windows NT 4, sin embargo, también lo son los requerimientos.

Fase 2: Actualización

Lo ideal sería tener la red lista para la migración antes de instalar Windows 2000. Eso se logra teniendo en cuenta algunas condiciones:

- Revisar si se puede eliminar todos los protocolos de red que no sean TCP/IP. La mayor parte de los sistemas operativos lo soportan, así que no habrá, teóricamente, problemas de compatibilidad.

- Tratar de utilizar extensamente los servicios de TCP/IP, especialmente si se tiene Windows NT 4. Hacer que los servidores y clientes utilicen WINS y, si es posible, DHCP.

- Implementar DNS y hacer que todas las máquinas lo usen. Tratar de migrar todos los servidores a Windows NT de modo de lograr luego, que la transición a Active Directory sea más fácil. Si no se pueden migrar todos, crear un subdominio administrado por un servidor NT.

- Como Windows 2000 no necesita NetBIOS, se puede facilitar la migración haciendo que todos los sistemas tengan un nombre que corresponda al de la máquina. Por ejemplo, si un sistema se llama Cuentas y tiene un FQDN como www.miempresa.com, darle al equipo un alias DNS tipo cuentas.miempresa.com.

En algún momento de esta etapa, es conveniente hacer un backup, en lo posible completo de cada disco o, por lo menos, de cada documento y aplicación importante que funcione adecuadamente.

Si está actualizando sobre Windows NT 4 Server, es conveniente por no decir imprescindible, que se tenga instalados tanto el Service Pack 4 como el Option Pack. Ambos se bajan gratuitamente desde el sitio de Microsoft: www.microsoft.com.

Fase 3: Planeamiento

Tomarse el tiempo de crear un diagrama de la nueva arquitectura, listando todo el hardware y software adicional que necesite; utilizar esta lista para crear un presupuesto y una lista de tareas.

Recordar que Windows 2000 tiene diferentes requerimientos que Windows NT 4. Por ejemplo, Windows 2000 necesita menos dominios y, por lo tanto, menos controladores de dominio, pero por el otro lado, una estructura DNS quizás necesite nuevo hardware.

En la determinación del nuevo presupuesto no contemplar sólo el valor monetario de las nuevas licencias de software o de los nuevos dispositivos de hardware que se requiera. Incluir la mano de obra de los técnicos que deban montar el equipamiento, así como el tiempo extra que los empleados necesiten para configurar o aprender nuevas tareas.

Al crear una lista de tareas detallada, hay que asegurarse de no omitir ningún paso. Distribuir esta lista de tareas de modo de que todos sepan que habrá momentos en los que la red esté fuera de línea y recursos que no estarán disponibles. Adjuntar, además, una buena línea de tiempo basada en cuántas horas se pueden necesitar para implementar cada paso. Hay que ser generoso con el tiempo y añadir un poco más para solventar imprevistos.

Finalmente, si tiene la lista de tareas y la cantidad de horas que insumirá cada una, añada a la ecuación los recursos humanos con los que cuente. Es posible que pueda llevar a cabo más de una tarea simultáneamente si posee la cantidad de personal adecuada. Windows 2000 es nuevo para todos, por lo que cierto entrenamiento y capacitación serán necesarios.

Fase 4: Testeo

En un mundo ideal, todo el software debería funcionar como se espera que lo haga. En el mundo real (y los administradores de red lo saben) las cosas casi nunca suceden como se previeron.

Una de las alternativas que existen para evitar la máxima cantidad de problemas es establecer máquinas de testeo. Separar algunas computadoras de la red, instalar Windows 2000 Server en alguna y Windows 2000 Pro en otras. Si la red va a ser heterogénea, reservar algunas para otros sistemas operativos. Instalar y probar todo el software que se usa habitualmente en la red, tanto el de administración como el de productividad.

Verificar que el pequeño modelo de red funcione de la misma manera en que lo hacía hasta el momento con Windows NT o el sistema operativo que se estuvo usando. Seguramente van aparecer problemas de configuración, de incompatibilidad o, simplemente, de incapacidad de correr. Es en la fase de testeo donde es preferible que estos problemas aparezcan.

De esta manera, no sólo se previene los que puedan surgir durante la tarea concreta, sino que se tendrá la oportunidad de intercambiar información con los soportes técnicos de los distintos software y de elaborar estrategias de contingencia para el caso de que los problemas surjan en el mundo real.

Más aún, si se puede, testear de la misma manera una muestra del hardware que se utilizará. Obviamente el tiempo de testeo dependerá de la planificación. No se debe saltear esta fase, especialmente si la migración será a gran escala, pero tampoco derrochar recursos en una tarea de testeo más allá de lo necesario.

Fase 5: Migración propiamente dicha

Si la planificación y el testeo se hicieron correctamente, esta fase, que es la de instalar y configurar Windows 2000 en todos los sistemas, deberá ser fácil y sin obstáculos. En todo caso, si aparece alguno, tendrá que ser rápidamente resuelto. El tema aquí es si la propia migración debería hacerse en uno o más pasos.

La recomendación general es que en organizaciones pequeñas, con menos de 50 equipos, la actualización podría hacerse de una sola vez. Hay que planificar hacerla fuera de horas de trabajo o cuando los riesgos por dejar fuera de línea el sistema sean mínimos.

Las organizaciones más grandes no soportan la actualización en una sola etapa. Por el contrario, en este caso la idea es trabajar en las fracciones más pequeñas posibles. Comenzar con los controladores de dominio primarios a Windows 2000 y dejarlos trabajar toda una semana antes de continuar con el próximo paso. De esta manera, lleva a cabo una última fase de testeo en un entorno de producción real.

Al terminar de actualizar todos los servidores, comenzar con los clientes, de a un departamento por cada vez. Llevando a cabo la migración en pequeños pasos, se limita la posibilidad de graves inconvenientes a relativamente pocos equipos y a una relativamente pequeña fracción de la red.

Fase 6: Determinar el resultado

No hay que quedarse tranquilo luego de haber actualizado el último de los equipos. Siempre es conveniente efectuar una serie de testeos para validar la funcionalidad de la nueva red.

Además es sabido que siempre aparecen problemas que no estaban previstos dado que el trabajo cotidiano nunca puede simularse perfectamente en un equipo de pruebas. Así se prepara también para la tarea de soporte de los usuarios. Más aún, en el peor de los casos se deberá estar preparado para volver atrás en algunos equipos, es decir, restaurar el sistema operativo anterior, que recuperará del backup que hizo durante la etapa de actualización.

Cada etapa de la migración deberá –o debería- estar perfectamente documentada. La documentación no sólo le servirá al administrador o gerente de sistemas o al responsable de la migración como información o como resumen de aprendizaje y entrenamiento, sino que también le será útil para crear documentación específica para usuarios específicos –que necesiten, por ejemplo, instrucciones para llevar a cabo backups-, una guía de resolución de problemas (si ya resolvió un problema durante la fase de testeo, se deberá poder hacerlo durante el funcionamiento final de la red) y como material para intercambiar información con el o los soportes técnicos tanto del software como del hardware.

RESUMEN

Windows 2000 proporciona un conjunto de herramientas administrativas que facilitan la operación del mismo.

Las herramientas Visor de sucesos, Información del sistema, Administración remota, Carpetas compartidas y Consola de rendimiento son utilizadas a medida que se necesitan y entran en lo que es la optimización y mantenimiento de la red.

En la empresa telefónica hay una política muy definida acerca de la prevención de fallas y errores en cualquier nivel de la red y las herramientas arriba mencionadas cumplen con esa función, ya que la empresa no puede darse el lujo de cometer errores por la cantidad de información y aplicaciones que soporta para sus clientes.

La copia de seguridad permite hacer los respaldos a la medida de lo que se quiere y se tiene dentro de cada sucursal, sin que esto lleve una carga adicional en el rendimiento de la red.

El Acceso Remoto es muy útil para el mantenimiento y soporte de la red en sucursales donde no se cuenta con el personal de Help Desk.

NAT ofrece una solución rentable y estable para el manejo de Internet, ya que permite usar una o dos cuentas del servicio y repartirlas en varias maquinas y clientes sin necesidad de costear más cuentas.

En lo que respecta a la escalabilidad y alcance de la red, basta con decir que es ilimitado, ya que Windows 2000 Server prevé y permite un crecimiento muy grande y sobre todo muy administrable y seguro.

CONCLUSIONES

Tomando en consideración el resultado de la implementación de las nuevas características que ofrece Windows 2000 se obtuvieron los siguientes resultados:

La compatibilidad con los dispositivos USB y Plug and Play fue probada con éxito, solamente en casos de modelos muy anteriores se determino en cambiar el Hardware, siendo un mínimo de dispositivos, ya que la empresa cuenta con suficiente poder adquisitivo y en general los equipos Cliente contaban como mínimo con un procesador Pentium III y los Servidores con Pentium III Xeón en adelante.

La compatibilidad con los S.O. UNIX y Novell Netware no presento problema alguno, ya que las herramientas de compatibilidad que ofrece Windows 2000 mostraron su eficacia al hacer la actualización. El Dominio y su total administración quedo a cargo de Windows 2000 Server, los servidores de impresión y de archivos montados sobre Novell Netware y las Bases de Datos que contenían los Servidores UNIX fueron integradas y administradas sobre el Dominio de Windows 2000 Server.

La creación de varios dominios permitió la desaparición de los BDC y PDC, lo que facilito una administración de los recursos de la red más centralizada y fácil de hacer, el sistema de archivos NTFS dio la ventaja de asignar una seguridad a nivel de archivo y mayor control de espacio en disco duro con las Cuotas. Se implementaron Políticas de Grupo a nivel de Dominio y Unidad Organizacional para definir y delegar actividades dentro de la red. Por ejemplo el grupo de Help Desk se le asignaron varias MMC para poder administrar las cuentas de usuarios.

Las herramientas de monitoreo ayudaron de inmediato a ubicar y definir alertas en servidores con mucha carga de trabajo y así poder revisarlo en base a las estadísticas marcadas.

En base a que desde un principio se hizo una minired de pruebas con todas las aplicaciones existentes en la red y el proceso que se hizo fue ordenado, la migración fue todo un éxito.

GLOSARIO

A

AC.- Control de Acceso (Access Control), es el mecanismo de seguridad en Windows NT y Windows 2000 que determina qué objetos se pueden accesar y utilizar en la red.

Active Directory.- Directorio Activo, el servicio del Directorio Activo incluido en Windows 2000 Server, guarda la información sobre los objetos en una red y hace esta información disponible a los usuarios y administradores de la red. El Directorio Activo permite a los usuarios de la red acceder en cualquier parte a los recursos permitidos en la red que usa un sólo proceso de logon. Les proporciona una vista jerárquica intuitiva de la red y un sólo punto de administración a administradores de la red para todos los objetos de la red.

API.- Interfaces de Programación de aplicaciones, es un juego de rutinas que una aplicación usa para pedir y llevar a cabo los servicios bajar y nivelar realizado por el sistema operativo de una computadora. Estas rutinas normalmente llevan a cabo las tareas de mantenimiento como los archivos de administración y la información desplegándose.

AppleTalk.- Es el protocolo de red necesario para implementar la compatibilidad con equipos cliente Macintosh que existen dentro de una organización y necesitan utilizar recursos ubicados en un servidor Windows 2000 Server en el que los usuarios Macintosh quieren almacenar archivos y de los que quieren recuperar o imprimir archivos.

Árbol.- Un árbol de dominio es una colección que incluye dominios y dominios subordinados en una jerarquía DNS en Windows 2000.

Arp.- Es una utilería de diagnóstico de TCP/IP de Windows 2000, despliega y modifica el Protocolo de Resolución de Dirección (ARP) el escondite.

AS.- Servidor de Autentificación, para Kerberos este tipo de servidor se refiere al Servidor de Autenticación (AS), un Servidor de Otorgación de Boletas (TGS) y un Centro de Distribución Clave (KDC), El KDC es un servicio de red que suministra boletas y claves de sesión temporales. El KDC da servicio a ambos, la boleta inicial y las solicitudes de otorgación de boletas. La parte de boleta inicial en ocasiones se conoce como AS. la parte de otorgamiento de boletas en ocasiones se conoce como TGS. Por lo tanto KDC es tanto AS como TGS según RFC 1510.

ASP.- Páginas Active Server (Active Server Page), la compatibilidad con este servicio la proporciona IIS.

B

BDC.- Controlador de Dominio de Respaldo (Backup Domain Controller), en Windows NT son aquellas computadoras que contienen una copia de respaldo del directorio, la cual se sincroniza periódicamente con la principal, pueden apoyar al PDC cuando éste tiene mucha carga de trabajo, pueden haber varios BDC dentro de un dominio.

BINARY.- A menudo abreviado como **BIN**, este comando indica a FTP que use transferencia de ficheros binaria. La mayoría de los servidores usan ASCII como mecanismo estándar de transferencia de ficheros. Como ASCII es un estándar de 7 Bits, cualquier archivo binario enviado con el mecanismo de transferencia ASCII se corromperá. Éste es un comando de establecimiento de modo, por lo que después de este comando, todas las trasferencias se realizaran en modo binario hasta que se use el comando BINARY.

Block Sub Allocation.- Dentro de Novell Netware 5.0 La Asignación de Subalterno de bloque (Block Sub-Allocation) permite al sistema operativo poder utilizar el espacio, sin usar dentro de cada bloque físico; guardar la información adicional, produciendo el espacio del disco menos gasto sobre todo en los sistemas con el tamaño del bloque grande.

Bosque.- Un bosque (forest) es una agrupación de árboles que no comparten un espacio de nombres contiguos. Todos los árboles de un bosque comparten un esquema común, así como todos los dominios comparten un catálogo global. Sin embargo, los dominios de un bosque pueden operar independientemente, pero el bosque se encarga de establecer comunicación a través de toda la organización.

C

Called Use Named Mapping.- La Cartografía de Nombre de Usuario, es usada en NFS para trazar las credenciales basadas en Windows a UNIX UIDs o GIDs antes de remitir las demandas de acceso de archivo a los servidores de NFS. Cada demanda de la entrada de un usuario separado se identifica propiamente y se trazan los nombres de usuario de Windows a los usuarios de UNIX correspondientes antes de que remitiera al servidor de NFS. Esto asegura que clientes que acceden los servidores de NFS de las máquinas con el software de cliente de NFS, consiguen los mismos privilegios que ellos recibirían de los clientes UNIX de NFS. Subsecuentemente acceda a la Entrada para las porciones de NFS se proporciona usando la gestión de redes basadas en Windows, estas demandas que usan las credenciales Basadas en Windows se autentifican.

CAPTURE.- El comando CAPTURE de Novell Netware 5.0 es muy similar al comando NET USE en el sentido en el que el usuario deberá saber el nombre del servidor de impresión y el nombre del recurso compartido (llamado Cola u Objeto de impresión), el comando Net use nos permite poder específicar al servidor al que deseemos conectarnos.

Catálogo Global.- En Windows 2000, el catálogo global es un servicio que, entre otras cosas, almacena los atributos de un objeto más comúnmente usados en una operación de búsqueda, por lo que se puede usar para localizar los objetos en cualquier lugar de la red.

CD.- En FTP, este comando cambia de el directorio actual al directorio destino en el servidor. Funciona igual que el comando CD de la línea de comandos.

CDFS.- el Sistema de Archivo de Disco Compacto (Compact Disc File System), permite a una computadora ejecutando Windows 2000 leer archivos que se encuentren en una unidad de CD ROM.

Confianza Bidireccional.- Una relación de confianza bidireccional está formada por dos relaciones de confianza unidireccionales, de modo que cada dominio confía en las cuentas de usuario del otro.

Confianza Unidireccional.- En una relación de confianza unidireccional, un dominio confía en los usuarios del otro dominio, permitiéndoles utilizar sus recursos. Más específicamente, un dominio confía en que los controladores del otro dominio validen las cuentas de usuario para que utilicen sus recursos.

Consola.- Es una herramienta que permite dividir los componentes propios de un equipo y permite al administrador supervisarlos o controlarlos.

Cuenta de Dominio.- Cuentas de dominio y cuentas de estación de trabajo: Los equipos que ejecutan Windows NT Workstation y los servidores miembros (equipos que ejecutan Windows NT Server que no son controladores de dominio) mantienen cuentas de usuario, grupos y directivas de seguridad independientes de los del dominio. Las cuentas incorporadas de tales equipos proporcionan derechos incorporados sobre el equipo, similares a los derechos que proporcionan las mismas cuentas incorporadas a nivel de dominio.

Cuentas de Estaciones de Trabajo.- Las cuentas incorporadas de tales equipos proporcionan derechos incorporados sobre el equipo, similares a los derechos que proporcionan las mismas cuentas incorporadas a nivel de dominio.

D

DEL.- En FTP es el comando para poder eliminar archivos individuales.

DELETE.- Al trabajar en FTP, el comando DELETE sirve para poder borrar directorios de Archivos.

DHCP.- Protocolo de Configuración Dinámica de Host (Dynamic Host Configuration Protocol), se utiliza para asignar las direcciones IP a las estaciones de trabajo de una red.

DLC.- Protocolo de control de Vínculos de Datos (Data Link Control), se usa principalmente para los sistemas informáticos grandes de IBM y para poder conectar impresoras de red.

DNS.- Servidor de Nombres de Dominio (Domain Name Server), es un servicio que resuelve las direcciones IP en nombres de dominio. Estas direcciones son números con formato 0.0.0.0, por ejemplo 169.254.0.2, cuyo mayor valor es 255 (255.255.255.255) que se "traducen" a nombres como Microsoft.com o miempresa.com.ar.

Drivers.- Programas que controlan algún dispositivo de un equipo de cómputo y permiten interactuar con él, por ejemplo los drivers de video, controlan una tarjeta de vídeo y permiten su instalación y manejo en un sistema operativo.

E

Enlace E1.- Enlace vía microondas, usado principalmente en Europa, transmite a una velocidad de 2.048 Mbps.

Exchange Server.- Servidor Exchange, es el software que permite poder administrar y crear las cuentas de correo electrónico que se creen en una empresa. Es una herramienta útil para cualquier administrador de una red.

Explict one way.- Confianza explícita unidireccional, es la relación entre dominios que no son del mismo árbol.

F

FAT.- Tabla de asignación de Archivos (File Alocation Table), es el sistema de archivos original usada en MS-DOS. Usa una tabla almacenada en el disco que hace seguimiento de donde residen los archivos y directorios en el disco. Almacena dos copias de estos datos al principio del disco. El sistema de Archivos FAT sólo se puede utilizar en las particiones menores de 4 GB y un archivo no puede ser mayor de 2 GB.

FAT32.- Es una versión posterior a FAT, esta versión viene incluida en Windows 95 versión OSR2, Windows 98, NT y 2000, la ventaja que tiene sobre FAT32 es que admite volúmenes de 512MB y 2 Terabytes, pero Windows 2000 únicamente puede crear particiones de hasta 32 GB.

FIREWALL.- Corta-fuego, una combinación de hardware y software que proporcionan un sistema de seguridad, normalmente sirve para prevenir el acceso no-autorizado, de fuera a una red interior o Intranet. Un cortafuego previene la comunicación directa entre la red y las computadoras externas.

FTP.- Protocolo de Archivos de Transferencia (File Transfer Protocol) es el protocolo que permite la transferencia de archivos desde servidores a clientes. FTP se basa en una serie de comandos para cambiar al directorio correcto e iniciar las transferencias de archivos.

G

GET.- En FTP, el comando GET va seguido del nombre del archivo a transferir al cliente. El comando GET obtendrá un archivo, no obtendrá un directorio y no usará comodines.

GID.- Los servidores de NFS basados en Windows 2000 tienen que identificar a los usuarios pidiendo las demandas de NFS basado solamente en identificación de NFS, GID es el identificador de grupo.

Grep.- Es una utilería para NFS, es la búsqueda de archivos para los modelos y resultados del despliegue en pantalla que contiene ese modelo.

Grupo de Distribución.- En Windows 2000 se utilizan los grupos de distribución, un grupo es una colección de cuentas de Usuario. Al asignar permisos y restricciones a un grupo, se puede facilitar la administración de los usuarios individuales simplemente asignándolo a un grupo determinado. El grupo de distribución, es aquel en donde las aplicaciones pueden usarse para actividades no relacionadas con la seguridad, como enviar correo electrónico.

Grupo de Seguridad.- Los grupos de seguridad en Windows 2000 se utilizan para propósitos relacionados con la seguridad de la red, tal como puede ser el asignar permisos, etc.

Grupo de Seguridad de Dominio Local.- Se usan más para asignación de permisos a recursos. Se agregan usuarios de cualquier dominio pero sólo se asignarán permisos a recursos disponibles en el dominio en el que se creó el grupo.

Grupo de Trabajo.- Es un conjunto de equipos que pueden examinarse mutuamente los directorios a través de la red pero que no comparten una base de datos de directorio común.

Grupo Global.- Esta formado por varias cuentas de usuario de un dominio que se agrupan bajo un nombre de cuenta de grupo. Un grupo global sólo puede contener cuentas de usuario de un mismo dominio (el dominio donde se creo el grupo global). El termino "global" indica que el grupo puede recibir derechos y permisos para utilizar recursos de múltiples dominios. Los grupos globales sólo pueden contener cuentas de usuario y sólo pueden crearse en un dominio (no en una estación de trabajo, ni en un servidor miembro).

Grupo Local.- Esta formado por cuentas de usuario y grupos globales de uno o más dominios, agrupados bajo un nombre de cuenta. Es posible agregar al grupo local usuarios y grupos globales que no sean del dominio local siempre y cuando pertenezcan a un dominio en el que se confia. .

Guest.- La cuenta invitado la utilizan para los inicios de sesión aquellas personas que no tienen una cuenta en el equipo, en el dominio o en cualquiera de los dominios en los que confía el dominio del equipo. Un usuario cuya cuenta esté desactivada (pero no eliminada) también puede usar la cuenta Invitado. La cuenta Invitado no requiere contraseña y se puede usar para dos tipos de inicio de sesión: inicios de sesión de invitado local e inicios de sesión de invitado de red.

H

HASH.- Este comando le indica a FTP que muestre una almohadilla (#) por cada 1,024 bytes transferidos. Esta es una buena forma para sesiones interactivas, con el fin de asegurarse de que la transferencia no se ha detenido.

Help Desk.- Departamento de Ayuda de Escritorio, este departamento se utiliza en algunas empresas para dar apoyo a los usuarios, resolver dudas, dar soporte en sitio y vía telefónica en cualquier software de la empresa o en equipos de cómputo, son de gran apoyo para las Áreas de Redes, tienen permisos una jerarquía debajo de un administrador de red.

HostName.- Especifica un nombre de Host para el cliente de hasta 63 caracteres de largo.

Hot Fix.- Arreglo en Caliente, utilería de Novell Netware 5.0 que proporciona la redirección de los datos a una área para prevenir la corrupción de estos en caso de errores de los medios de comunicación que ocurren en el disco. Esto permite al servidor seguir corriendo, en caso de que los errores de medios de comunicación de disco sean menores, esto permite ahorrar tiempo al administrador de la red para un óptimo desempeño.

HTTP.- Protocolo de Transferencia de Hipertexto (Hypertext Transfer Protocol), se utiliza mucho en Internet.

I

IDE.- Electrónica de Dispositivos Integrados (Integrated Drive Electronics), es el controlador de disco duro más popular.

IIS.- Servidor de Información de Internet (Internet Information Services), Microsoft decidió unir varias tecnologías hacia este nuevo concepto, incluyendo la de servidor Web, servidor FTP y un servidor de grupo de noticias con IIS se logra fusionar dicha tecnología en uno sólo.

Ipconfig.- Este comando en Windows 2000 despliega la configuración de TCP/IP actual, también usado para liberar y renovar las configuraciones de TCP/IP asignadas por DHCP.

IPX/SPX.- Protocolo de Intercambio de paquetes /Intercambio de paquetes secuenciados (Internet Packet Exchange/Sequential Packet Exchange), creado por Novell para utilizarse en redes Netware.

K

KDC.- En Windows 2000, para Kerberos, el KDC es un servicio de red que suministra boletas y claves de sesión temporales. El KDC da servicio a ambos, la boleta inicial y las solicitudes de otorgación de boletas.

KERBEROS.- EL protocolo Kerberos es un estándar de autenticación de Internet y Windows 2000 soporta su versión 5. Se ha constituido en el protocolo nativo de autenticación de Windows 2000, cada servidor Active Directory tiene corriendo automáticamente el servicio Kerberos Key Distribution Center, y todos los sistemas Windows 2000 soportan el protocolo como clientes. Kerberos es un sistema de identificación de usuarios desarrollado por el MIT que utiliza criptografía de clave simétrica para asegurar la identificación del usuario y la seguridad.

L

LDAP.- Protocolo de Acceso al Directorio Ligero-pesado(Lighweight Directory Access Protocol), Active Directory usa LDAP para intercambiar información, también con cualquier otro sistema de directorios que soporte LDAP versiones 2 y 3, como es el caso de Novell Directories Services (NDS).

LDC.- Cambiar Directorio Local (Local Change Directory), este comando en FTP cambia el directorio local del cliente a la trayectoria especificada.

Lpq.- Utilerías de Diagnóstico de TCP/IP, obtiene la información de la cola de impresión para computadoras ejecutando el Demonio de Línea de Impresión (Line Printer Daemon-LPD).

Lpr.- Utilidad de Conexión de TCP/IP, envía los trabajos de la impresión a impresoras de UNIX remotas manejadas por el Demonio de Línea de Impresión (Line Printer Daemon-LPD), al software de servidor de impresión.

LS.- En FTP, lista el contenido de un directorio dado, o si no se especifica directorio, lista el contenido del directorio actual. Se admiten las opciones de tipo UNIX, como ls–l para listados de direcciones largas y ls-C para directorios en columnas (tener en cuenta que las opciones distinguen entre mayúsculas y minúsculas).

M

MDELETE.- Comando de Eliminación en FTP para directorios, mientras que MDEL funciona como comodines.

MGET.- El comando PUT va seguido del nombre de archivo que se va a transferir al servidor. Al igual que el comando GET, el comando PUT no utiliza comodines. La M viene de Múltiple. De aquí que MGET obtuviere varios archivos y aceptara comodines, y MPUT colocara varios archivos en el servidor y también aceptara comodines. Los comodines son estándares de UNIX.

MMC.- Consola de Administración de Microsoft (Microsoft Management Console), es el nuevo espacio de centralización de control de Windows. Esta herramienta de configuración hace la tarea de contenedor para todos los componentes de administración y configuración de Windows 2000.

MPUT.- MPUT colocara varios archivos en el servidor y también aceptara comodines. Los comodines son estándares de UNIX.

N

Namespace.- Determina los tipos de archivos y directorios que pueden guardarse en un volumen Novell, es un espacio de nombre con el que se identifica un recurso en una red IP.

Nbstart.- Es una utilería de diagnóstico de TCP/IP, despliega el NETBIOS local con la tabla de nombres, una tabla de nombres de NETBIOS registrada por las aplicaciones y los NETBIOS nombran escondite.

NDS.- Es una conexión nativa de Novell Netware, utiliza la forma de conexión que se utiliza en Active Directory, un usuario se conecta al directorio, y a continuación, se le permite tener acceso a los recursos que ofrece el directorio.

NetBEUI.- Fue el primer intento de IBM y Microsoft de crear un protocolo para LAN basado en NetBIOS (Sistema Básico de Entrada y Salida de Red- Network Basic Input / Output System).

Netstart.- Utilería de Diagnóstico de TCP/IP, despliega la información de la sesión del protocolo TCP/IP.

NFS.- Sistema de Archivos de Red (Network File System), es un conjunto de protocolos diseñado por SUN Microsystems que permite la compartición de archivos con estaciones de Trabajo.

NIS.- Sistema de Información de Red (Network Information System), permite a los nombres de usuario y a las contraseñas fluir dentro de un dominio de contexto en UNIX, de forma que los usuarios puedan acceder a los recursos dentro de un dominio sin tener una cuenta de acceso individual en cada máquina del dominio. NIS, sin embargo, es en gran parte un sistema de transporte. No maneja autenticación de usuario por sí mismo, en cambio, maneja el desplazamiento de los nombres de usuario por sí mismo.

NNTP.- Protocolo de Transferencia de Noticias en Red (Network News Transfer Protocol).

Nomenclatura.- Catálogo, Lista Detallada. La conversión de nomenclatura de Netware es libre y no sigue ningún modelo de búsqueda. El directorio se basa exclusivamente en la estructura de directorios de la combinación X.500. Active Directory esta estrechamente relacionado con la conversión de nomenclatura de DNS. Los 2 sistemas se pueden incorporar al estándar LDAP de Internet para descubrir objetos de directorio.

Novell.- Es una de las compañías creadoras de software de red más importantes en el mundo.

Nslookup.- Es una utilería de diagnóstico de TCP/IP, checa las grabaciones, seudónimos de organizador de dominio, servicios de organizador de dominio, e información del sistema operativo preguntando los servidores de DNS.

NSS.- Servicio de Almacenamiento Novell (Novell Storage Services), es el sistema de archivos de Novell Netware 5.0.

NTFS.- Sistema de Archivos de Nueva Tecnología (New Technology File System), es el sistema de archivos que utiliza Windows 2000, surgió con Windows NT y es compatible con la seguridad a nivel de archivos, en la versión de NTFS que viene incluida con Windows 2000 ningún sistema operativo puede leer archivos NTFS más que Windows 2000.

NTLM.- Administrador de LAN NT (NT LAN Manager), es un protocolo heredado de Windows NT, se carga durante el inicio de Windows 2000 para permitir la administarción de clientes NT y 95/98, que existen. El proceso de autentificación de NTLM implica tres partes de la información inicial: El nombre del dominio, el nombre del usuario y la contraseña del usuario.

NWFS.- Sistema de Archivo Netware (Netware File System), es la última aplicación del mismo sistema de archivo de 32-bits que ha servido a Novell durante muchos años en las versiones anteriores de Netware.

NWLINK.- Es una versión del protocolo IPX/SPX, en Windows 2000 es un protocolo de la red normal que apoya la asignación de ruta a Servidores y Clientes de Netware. Puede comunicar equipos con Windows 2000 a servidores o clientes que se comunican con IPX/SPX para accesar a las aplicaciones.

O

GPO.- Contiene parametros de configuración de las directivas de grupo contenidas en un objeto de directivas de grupo.

OPEN.- Es un comando de FTP, se utiliza para abrir una conexión (por ejemplo OPEN FTP: X.COM abrirá una sesión con el servidor FTP de la compañía X).

Options Pack.- Paquete de Opciones, al ver el éxito que se podía tener en el mercado, Microsoft lanza la versión IIS 4.0 la cual se distribuyo al público con el nombre de Option Pack para Windows NT la cual se distribuía de manera gratuita para el sistema operativo Windows NT 4.0, la versión 4.0 de IIS se ha mantenido en los Service Pack 4, 5 y 6 .

P

Particionamiento.- El Particionamiento en un disco duro se refiere a crear y definir una partición primaria activa dentro de un disco para que pueda posteriormente dársele un formato y poder cargar un sistema operativo. Una partición esta formada por un conjunto de cilindros contiguos. La tabla de Partición se encuentra siempre en el primer sector de un disco duro que permita particiones. La tabla se prepara mediante el formato FDISK (mediante un disco de arranque del sistema operativo MS-DOS, win95, win98, WINNT), pues el espacio que el sistema operativo otorga a la FAT, al directorio raíz y al espacio de datos, depende del tamaño de la partición dada al sistema operativo.

PASSWORD.- Comando utilizado en FTP, normalmente abreviado como PASS, el comando PASSWORD se usa para transmitir una contraseña. Tenga en cuenta que al igual que el protocolo TELNET, FTP trasmite contraseñas en texto normal sobre la red y en algunas redes es vulnerable a ataques de piratas informáticos.

Pathping.- Utilería de diagnóstico de TCP/IP en Windows 2000, traza la ruta del paquete hacia un destino e informa de los despliegues sobre las pérdidas del paquete para cada segmento en la red.

PDC.- Controlador de Dominio Primario (Primary Domain Controller), en redes NT se refiere al servidor principal dentro de una red, es que el que controla y administra todos los equipos.

Perfil de Usuario.- Un perfil de usuario se crea por un administrador de red y asigna a dicho perfil el acceso a diferentes recursos de la red, dentro del perfil se encuentra la configuración personalizada del usuario dentro de un equipo como son accesos directos, protectores de pantalla, archivos de correo, mapeo de unidades de red etc.

Ping.- Utilería de diagnostico de TCP/IP en Windows 2000, verifica la configuración y comprueba la conexión IP.

POP3.- Protocolo del Correo 3 (Post Office Protocol 3), es un servicio que le permite a un cliente recuperar correo que el servidor está sosteniendo para el. La más reciente aplicación es la Versión 3, o POP3.

PUT.- Es un comando utilizado en FTP, El comando PUT va seguido del nombre de archivo que se va a transferir al servidor. Al igual que el comando GET, el comando PUT no utiliza comodines.

Q

QUIT.- Comando de FTP, este comando cerrará FTP

R

RAID.- Serie Redundante de Discos Economicos (Acronym for Redundant Array of Inexpensive Disks), un método para regularizar y categorizar en el disco duro para tolerar fallas. Seis niveles calibran varias mezclas de actuación, fiabilidad, y costo. Windows NT incluye tres de los niveles de RAID: Nivel 0, Nivel 1, y Nivel 5.

RAS.- Servicio de Acceso remoto (Remote Access Services), es un servicio que mantiene la gestión de redes, gestión remota de las estaciones móviles, y administradores del sistema que supervisan y manejan los servidores en las oficinas remotas. Los usuarios con RAS en una computadora con Windows 2000, NT y 95/98 pueden acceder a su red remotamente para diferentes servicios como son el accesar a aplicaciones e impresión, compartir archivos, correo electrónico, planificación, y banco de datos de acceso.

RCP.- Protocolo de Copia Remota (Remote Copy Protocol), es una utilidad de conexión de TCP/IP en Windows 2000, opia archivos entre una computadora con Windows 2000 y computadoras que ejecutan el RCP.

Rexec.- Es una utilidad de conexión de TCP/IP en Windows 2000, Ejecuta los procesos en las computadoras remotas.

Root.- En un ambiente UNIX, hay una cuenta llamada ***root*** que tiene un nivel similar de permisos. En Windows 2000 es el equivalente a la cuenta de usuario.

Route.- Utilería de diagnóstico de TCP/IP en Windows 2000, despliega o modifica la tabla de la ruta local.

RSH.- Utilidad de conexión de TCP/IP en Windows 2000, ejecuta comandos en una computadora que ejecuta el Shell Remoto (RSH).

S

SAE. – El SAE, es una habitación donde se encuentran concentrados los servidores principales, hubs, switch, concentradores, etc., en este lugar únicamente pueden tener acceso los administradores de la red o personal de alto nivel.

Salvaje Delete.- Utilería de Novell Netware 5.0, proporciona protección de recuperación de archivos borrados para todos los archivos, permitiéndoles a los usuarios recuperar los archivos y directorios que se anularon accidentalmente dentro de una cantidad razonable de tiempo.

SCSI.- Interface de Sistema de Computadora Pequeña (Small Computer System Interface), es un controlador de discos duros, todas las funciones de la tarjeta controladora están incorporados directamente en el drive, incluyendo la transformación de los datos desde la forma codificada.

Sh.- La utilidad Sh se encuentran instaladas con el cliente para NFS de Windows 2000, esta utilidad invoca el Shell de Korm.

SID.- Identificador de Seguridad (Security Identifiers), cuando un usuario ingresa a una computadora basada en Windows, el se identifica con un Identificador de Seguridad (SID).

Smart Cards.- Tarjeta Inteligente, es una tarjeta electrónica semejante a una de crédito, con un microprocesador, que almacena información de identidad del usuario.

SMTP.- Protocolo de Servicio de Transferencia de Correo (Services Mail Transfer Protocol), proporciona una conexión desde un servidor de correo electrónico de Internet con otro para intercambiar correo.

Snaps-ins.- Complementos, estos archivos almacenan tanto la configuración de la consola como la de cada snap-in, por lo que pueden abrirse y conservar parámetros aún desde computadoras remotas.

SSL.- Nivel de Sockets Seguro (Secure Sockets Layer), implementación de seguridad.

SSPI.- Porveedor de la Interface de Soporte de Seguridad (Security Support Provider Interface), ofrece un API para crear conexiones autenticadas.

T

Tar.- Es una utilidad que se encuentra instalada para el cliente NFS de Windows 2000, usa archivos de cinta, o agrega o extrae archivos para archivarlos.

TCP/IP.- Protocolo de Control de Transferencia/ Protocolo de Internet (Transfer Control Protocol/Internet Protocol), es el protocolo más popular y mayormente usado para Internet, creado por el departamento de defensa de los E.U. para las comunicaciones LAN /WAN sobre Arpanet.

TFTP.- El Protocolo de Transferencia de Archivo Trivial (Transfer File Trivial Protocol), es un protocolo que se usa por un servidor de IntelliMirror para transmitir los archivos iniciales de proceso de instalación

TGS.- En la tecnología del protocolo Kerberos TGS es un Servidor de otorgación de boletas.

Tracert.- Utilería de diagnóstico de TCP/IP en Windows 2000, traza la ruta de un paquete hacia su destino.

Two-way-transitieve trusht.- Confianza transitiva bidireccional, es una prestación provista por el protocolo de autenticación Kerberos. Es la relación entre dominios hijos y padres dentro de un árbol y entre los dominios de alto nivel de un bosque. Estas relaciones se establecen y mantienen automáticamente.

U

UID.- Los servidores de NFS basados en Windows 2000 tienen que identificar a los usuarios pidiendo las demandas de NFS basado solamente en identificación de NFS normal que consiste en una Identificación del Usuario.

UNC.- Convención Universal de Nombres (Universal Naming Convention), son los nombres que se conocen comúnmente como direcciones de red: \\domino\servidor\archivo.ext.

UNIX.- Sistema operativo de red creado por AT&T y fue un sistema de código libre, de esta forma quien tenía UNIX podía hacerle modificaciones. Después de la desintegración de AT&T, a la compañía se le permitió vender UNIX. Actualmente existen muchas versiones de este sistema operativo.

UO.- Unidad Organizacional (Organizational Unit-OU), son contenedores que se usan para agrupar objetos de un dominio en grupos administrativos lógicos. Cada Unidad Organizacional contiene distintos objetos y cada domino tiene su propia lógica de agrupación en Unidades Organizacionales.

USB.-(Universal Serial Bus, Bus Serial Universal), esta interface permite conectar dispositivos (Impresoras, Scaners, Cámaras de Vídeo, Palm Pilot, Impresoras, etc.) sin necesidad de tener una interrupción lógica o un puerto COM, además no es necesario reiniciar el equipo después de instalar el software de instalación.

USER.- Comando de FTP, sirve para el nombre de usuario que se usa para autentificar la sesión. Este es el usuario genérico "anonymous" con la contraseña (tradicionalmente) "guest", o es un Id. de usuario real.

V

Vi.- Utileria que se encuentra instalada con el cliente NFS de Windows 2000, invoca al editor de texto vi.

Volumen.- En ambiente Netware, los recursos compartidos no se llaman recursos, se llaman volúmenes, esto se debe a que los recursos compartidos que muestra un servidor Netware son realmente los volúmenes de disco creados en los servidores. Cada volumen que se crea y se monta en un servidor Netware puede ponerse a disposición del usuario base.

VPN.- Red Privada virtual (Virtual Prívate Networking), es la extensión de una red privada que abarca los eslabones por las redes compartido o públicas, como el Internet.

W

WAN.- Red de Área Amplia (Wide Area Network), es una red de comunicaciones que conecta a las computadoras, impresoras, y otros dispositivos geográficamente. Una WAN permite conectar un dispositivo sin importar la ubicación geográfica, normalmente este tipo de redes es de compañías muy grandes que posen varias sucursales o plantas de producción y distribución.

WWW.- World Wide Web, es el software, protocolos, convenciones, e información que habilitan el Hipertexto y públicación de multimedios y recursos en las diferentes computadoras alrededor del mundo.

X

X.400.- Protocolo utilizado para el correo electrónico. Permite crear conexiones privadas entre sistemas Exchange mediante Internet como una WAN de bajo costo.

BIBLIOGRAFÍA

D. GOLBERGER RICARDO
MICROSOFT WINDOWS 2000
MANUAL DE USO YCONFIGURACIÓN
EDITORIAL MP EDICIONES S.A.
NOVIEMBRE DEL 2000 BUENOS AIRES, ARGENTINA

MICROSOFT CORPORATION
MICROSOFT WINDOWS 2000 SERVER
CURSO OFICIAL DE CERTIFICACIÓN MCSE
EDITORIAL MCGRAW-HILL/INTERAMERICANA DE ESPAÑA
2001 MADRID, ESPAÑA

MICROSOFT CORPORATION
MANAGING A MICROSOFT WINDOWS 2000 NETWORK ENVIRONMENT
MCSA/MCSE GUÍA DE ESTUDIO OFICIAL DE CERTIFICACIÓN
EDITORIAL MCGRAW-HILL/INTERAMERICANA DE EDITORES, S.A. DE C.V.
MÉXICO

MICROSOFT CORPORATION
SEGURIDAD EN MICROSOFT WINDOWS 2000
REFERENCIA TÉCNICA
EDITORIAL MCGRAW-HILL/INTERAMERICANA DE ESPAÑA S.A.U.

R. STANEK WILLIAM
MICROSOFT WINDOWS 2000
MANUAL DEL ADMINISTRADOR
EDITORIAL MCGRAW-HILL/INTERAMERICANA DE ESPAÑA S.A.U.
2000 ESPAÑA

PETER NORTON, INFAN C HAUDHRY Y TOMAS BURKE
GUIA COMPLETA PARA MICROSOFT WINDOWS 2000 SERVER
EDITORIAL PRENTICE may

MIGUEL PARDO NIEBLA
WINDOWS 2000
EDITORIAL ANAYA MULTIMEDIA

MIGUEL ANGEL RODRÍGUEZ ALMEIDA
WINDOWS 2000
EDITORIAL MC GRAW HILL INTERAMERICANA

MANUEL BAETO VIBORA
WINDOWS 2000 SERVER
EDITORIAL MC GRAW HILL INTERAMERICANA

PHILLIPPE MATHON
WINDOWS 2000 SERVER
EDICIONES ENI.-RECURSOS INFORMATICOS

WILLIAM BOSWELL
WINDOWS 2000 SERVER
ED. ANAYA MULTIMEDIA

PETER DAVIS
APRENDIENDO MICROSOFT WINDOWS 2000 SERVER EN 21 DIAS
EDITORIAL PRENTICE HALL

MARK MINASI , CRISTINA ANDERSON
MASTERING WINDOWS 2000 SERVER
EDITORIAL: MICRSOSOFT PRESS

MICROSOFT CORPORATION
MSCE TRAINING KIT MICROSOFT WINDOWS 2000 PROFESIONAL
MICROSOFT PRESS

KENNETH L. SPENCER
MICROSOFT WINDOWS 2000 SERVER , ADMINISTRACION Y CONTROL
EDITORIAL PRENTICE HALL

http://www.microsoft.com
http://www.microsoft.com/spanish