



UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

**ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
PLANTEL ARAGON**

**ESTUDIO COMPARATIVO DE LOS PRINCIPALES SISTEMAS OPERATIVOS
PARA REDES DE COMPUTADORAS**

T E S I S

**QUE PARA OBTENER EL TITULO DE
INGENIERO EN COMPUTACION
P R E S E N T A**

**LUIS LOPEZ GONZALEZ
RAUL ESTRADA RAMIREZ**

DIRECTOR DE TESIS: M. En C. DAVID MOISES TERAN PEREZ



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

A DIOS

Gracias por tu bondad infinita, por darme la vida, y por darle fortaleza a mi espíritu para poder asimilar parte de tu infinita sabiduría gracias a la cual he alcanzado esta meta.

A mi Esposa: Alma

A ti, que desde el momento en que decidiste unir tu camino al mío, has reído y llorado a mi ritmo, a ti, que me acompañaste durante tantas madrugadas mientras construía este logro, no importando que tu jornada diaria hubiera sido más difícil que la mía, a ti que siempre has sido la fuerza de voluntad que abrazo cuando enfrente difíciles batallas y cuando he estado a punto de caer, siempre estas ahí para sostenerme, y por si fuera poco, me tomas del brazo y caminas a mi lado sufriendo las mismas adversidades, motivo por el cual este logro es de los dos, gracias por seguir en mi camino.

A mis Hijos: Aarón y Jessica

A ustedes que llegaron durante el transcurso de este proyecto, volviéndose a la vez el motivo principal para no detenerme.

Se que nunca comprendieron el porque me robe tantos momentos en los que debería de estar a su lado, hoy que termino, puedo decirles orgullosamente que este fue el pretexto.

Espero que este motivo el día de mañana me sea devuelto y porque no superado, se que encontrarán muchas adversidades y en esos momentos no duden que estaré con ustedes hasta que Dios me lo permita.

Gracias por llegar en el momento ideal.

A mi Mamá: Salome González

A ti, que desde la primera vez que me tuviste en tus brazos, me brindaste amor y cariño, hoy te doy el fruto de ese esfuerzo.

Gracias por ser mi guía en los momentos en que tomaba otra dirección, gracias por mantener en todo momento la confianza en mi, porque a pesar de mis decisiones siempre me apoyaste y supiste que lo lograría.

Gracias Mamá.

A mi Papá: Rodolfo López

A ti, que a pesar de que nunca has sido el padre cariñoso, sin embargo con un simple gesto me has demostrado cuanto me quieres. No con esto quiero decir que nunca me has apoyado, ya que gracias a ti he logrado llegar a esta etapa de mi vida.

Es difícil poder expresar en estas pocas líneas todo el agradecimiento que siento por todos los problemas que te he dado como hijo, este trabajo es un pequeño reconocimiento a tu labor como Padre, solo puedo decirte Gracias y que te quiero.

A mis hermanos: Valentín(†), Araceli, René, y Omar

A ustedes, que desde pequeños hemos tenido diferencias, pero no por eso hemos dejado de estar juntos apoyándonos en todo. Gracias por esos consejos valiosos en los momentos en que realmente necesitaba el apoyo que solo un hermano puede brindar, gracias.

A Raúl Estrada:

Chaparro creo eres como un hermano para mí, por que siempre me has ayudado en todo este largo camino, y has demostrado ser un verdadero amigo en las buenas y en las malas, Gracias.

M. en C. David Moisés Terán Pérez

En el momento en que estábamos sin saber que camino tomar para comenzar este trabajo, usted confió en nosotros y nos ha brindado un apoyo incondicional.

Gracias por la infinita paciencia durante la elaboración de este trabajo.

A DIOS

Gracias por tu bondad infinita, por darme la vida, y por darle fortaleza a mi espíritu para poder asimilar parte de tu infinita sabiduría gracias a la cual he alcanzado esta meta.

A mi Esposa: Sonia Zermeño

A ti, que desde el momento en que decidiste unir tu camino al mío, has reído y llorado a mi ritmo, a ti, que me acompañaste durante tantas madrugadas mientras construía este logro, no importando que tu jornada diaria hubiera sido más difícil que la mía, a ti que siempre has sido la fuerza de voluntad que abracé cuando enfrente difíciles batallas y cuando he estado a punto de caer, siempre estás ahí para sostenerme, y por si fuera poco, me tomas del brazo y caminas a mi lado sufriendo las mismas adversidades, motivo por el cual este logro es de los dos, gracias por seguir en mi camino.

A mis Hijos: Alejandra y Raúl

A ustedes que llegaron durante el transcurso de este proyecto, volviéndose a la vez el motivo principal para no detenerme.

Se que nunca comprendieron el porque me robe tantos momentos en los que debería de estar a su lado, hoy que termino, puedo decirles orgullosamente que este fue el pretexto.

Espero que este motivo el día de mañana me sea devuelto y porque no superado, se que encontrarán muchas adversidades y en esos momentos no duden que estaré con ustedes hasta que Dios me lo permita.

Gracias por llegar en el momento ideal.

A mi Mamá: Obdulia Ramirez

A ti, que desde la primera vez que me tuviste en tus brazos, me brindaste amor y cariño, hoy te doy el fruto de ese esfuerzo.

Gracias por ser mi guía en los momentos en que tomaba otra dirección, gracias por mantener en todo momento la confianza en mi, porque a pesar de mis decisiones siempre me apoyaste y supiste que lo lograría.

Gracias Mamá.

A mi Papá: Perfecto Estrada

A ti, que eres ejemplo de esfuerzo y responsabilidad; a ti, que durante muchos años has aguantado el dolor y cansancio en tus pies y has cargado todo un mundo de problemas y preocupaciones en tu espalda, sin embargo nunca te diste por vencido. Tu sabes lo difícil que ha sido este camino, en el cual siempre me has acompañado, ayudándome con el trabajo de tus manos para que yo siguiera adelante, Gracias por ser un gran ejemplo y un magnifico PADRE.

Donde quiera que estés, quiero que sientas este logro como parte tuya, porque tu fuiste uno de los pilares mas importantes para que yo terminara este trabajo.

Gracias por todo, te quiero papá.

A mis hermanos: Javier y Maria Guadalupe Estrada

A ustedes, que desde pequeños hemos tenido diferencias, pero no por eso hemos dejado de estar juntos apoyándonos en todo. Gracias por esos consejos valiosos en los momentos en que realmente necesitaba el apoyo que solo un hermano puede brindar, gracias.

A Luis López

Gracias por todo el apoyo que me has brindado y por estar conmigo en cualquier momento no importando cual fuera la circunstancia, nunca me has dado la espalda, siempre me has aconsejado y sobre todo me has aguantado, te has comportado como un hermano, gracias negro, muchas gracias.

M. en C. David Moisés Terán Pérez

En el momento en que estábamos sin saber que camino tomar para comenzar este trabajo, usted confió en nosotros y nos ha brindado un apoyo incondicional.

Gracias por la infinita paciencia durante la elaboración de este trabajo.

INTRODUCCION.....	7
OBJETIVO GENERAL	8
CAPITULO I.....	9
1. GENERALIDADES SOBRE REDES DE ORDENADORES	10
1.1 DEFINICIÓN.....	10
1.2 COMPONENTES DE UNA RED LOCAL.....	10
1.2.1 SERVIDOR.....	10
1.2.2 ESTACIONES DE TRABAJO.....	10
1.2.3 INTERFASE DE RED.....	10
1.2.4 CANAL DE COMUNICACIÓN.....	11
1.2.5 REPETIDORES.....	11
1.2.6 SISTEMA DE CABLEADO.....	11
1.2.7 SISTEMA OPERATIVO DE RED.....	11
1.2.8 SOFTWARE DE APLICACIÓN.....	12
1.3 TOPOLOGÍAS Y PROTOCOLOS.....	12
1.3.1 TOPOLOGÍA DE ESTRELLA.....	13
1.3.2 TOPOLOGÍA DE BUS.....	13
1.3.3 TOPOLOGÍA DE ANILLO.....	14
1.3.4 TOPOLOGÍA DE ÁRBOL.....	14
1.4 ARQUITECTURA DE REDES.....	15
1.4.1 REDES ARCNET.....	15
1.4.2 REDES ETHERNET.....	15
1.4.3 REDES "TOKEN" RING.....	16
1.4.4 FAST ETHERNET.....	16
1.4.5 FDDI.....	16
1.4.6 EL FRAME RELAY.....	16
1.4.7 <i>ATM</i>	17
1.5 MODELO DE REFERENCIA <i>ISO-OSI</i>	17
1.5.1 ESTRUCTURA GENERAL DEL MODELO.....	17
1.5.2 LOS SIETE NIVELES.....	18
1.6 SISTEMAS OPERATIVOS PARA RED.....	20
1.7 ARQUITECTURA DE SISTEMAS OPERATIVOS DE RED.....	20
1.7.1 SERVIDOR DE DISCOS.....	21
1.7.2 SERVIDOR DE ARCHIVOS.....	21
1.7.3 SERVIDOR DE BASE DE DATOS.....	22
1.7.4 ARQUITECTURA CLIENTE SERVIDOR.....	22
1.7.5 SERVIDORES PUNTO A PUNTO.....	22
CAPITULO II.....	23
2. INSTALACIÓN Y MANEJO DE REDES CON NETWARE® Y PRODUCTOS NOVELL®.	25
2.1 HISTORIA.....	25
2.2 CUMPLIMIENTO DE LOS REQUISITOS DEL SOFTWARE Y DEL SISTEMA.....	26
2.2.1 REQUISITOS DE SOFTWARE.....	27
2.3 PREPARACIÓN DEL ORDENADOR PARA LA INSTALACIÓN DE UN SERVIDOR.....	27
2.3.1 INSTALACIÓN DEL HARDWARE DE RED Y DEL ORDENADOR.....	27
2.3.2 CREAR Y INICIALIZAR UNA PARTICIÓN DE ARRANQUE.....	27
2.3.3 ACCESO A LOS ARCHIVOS DE INSTALACIÓN.....	28
2.4 INICIO DE LA INSTALACIÓN.....	28
2.4.1 SELECCIÓN DEL IDIOMA Y ACEPTACIÓN DEL ACUERDO DE LICENCIA.....	28
2.4.2 OPCIONES AVANZADAS.....	29
2.4.3 SELECCIÓN DEL RATÓN Y LA TARJETA DE VÍDEO.....	29
2.4.4 SELECCIÓN DE UN MÓDULO DE SOPORTE DE PLATAFORMA Y UN ADAPTADOR DE ALMACENAMIENTO.....	30

2.4.4.1 SELECCIÓN DE UN MÓDULO DE SOPORTE DE PLATAFORMA (EN SU CASO).	30
2.4.4.2 SELECCIÓN DE UN MÓDULO HOT PLUG PCI (EN SU CASO).....	31
2.4.4.3 SELECCIÓN DE UN ADAPTADOR DE ALMACENAMIENTO.....	31
2.4.5 SELECCIÓN DE UN DISPOSITIVO DE ALMACENAMIENTO Y UNA TARJETA DE RED.	31
2.4.5.1 SELECCIÓN DE UN DISPOSITIVO DE ALMACENAMIENTO.....	31
2.4.5.2 SELECCIÓN DE UNA TARJETA DE RED.....	31
2.4.6 CREACIÓN DE UNA PARTICIÓN DE NETWARE® Y UN VOLUMEN SYS.....	32
2.4.6.1 ELIMINACIÓN DE LOS VOLÚMENES SYS EXISTENTES (CONDICIÓN).....	32
2.4.6.2 CREACIÓN DE UNA PARTICIÓN NETWARE®.....	32
2.4.6.3 CREACIÓN DEL VOLUMEN SYS.....	33
2.4.7 ASIGNE UN NOMBRE AL SERVIDOR NETWARE® 5.....	34
2.4.8 INSTALACIÓN DEL SISTEMA DE ARCHIVOS DEL SERVIDOR NETWARE®.....	34
2.4.8.1 CREACIÓN DE VOLÚMENES.....	35
2.4.8.2 MODIFICACIÓN DE VOLÚMENES.....	36
2.4.8.3 ELIMINACIÓN DE VOLÚMENES.....	36
2.4.9 INSTALACIÓN DE PROTOCOLOS DE RED.....	36
2.4.10 AJUSTE DE LA ZONA HORARIA DEL SERVIDOR.....	37
2.4.11 CONFIGURACIÓN DE NDS, LA TECNOLOGÍA DE DIRECTORIOS DE NOVELL®.....	37
2.4.12 SELECCIÓN DEL TIPO DE NDS.....	37
2.4.12.1 INSTALACIÓN DEL SERVIDOR EN UN ÁRBOL NDS EXISTENTE.....	37
2.4.12.2 CREACIÓN DE UN NUEVO ÁRBOL NDS.....	38
2.4.13 ASIGNACIÓN DE LICENCIA AL SERVIDOR NETWARE®.....	39
2.4.14 INSTALACIÓN DE OTROS PRODUCTOS DE RED.....	39
2.4.15 INSTALACIÓN DE LA ESTACIÓN DE TRABAJO.....	40
2.4.15.1 INSTALACIÓN DEL CLIENTE NOVELL® PARA WINDOWS 95/98.....	40
2.5 CONSOLE ONE®.....	42
2.5.1 ¿POR QUÉ DEBERÍA UTILIZAR CONSOLEONE®?.....	42
2.5.2 INSTALACIÓN E INICIO DE CONSOLEONE®.....	43
2.5.3 REQUISITOS DEL SISTEMA PARA NETWARE®.....	43
2.5.4 INSTALACIÓN DE CONSOLEONE® EN NETWARE®.....	43
2.5.5 INICIACIÓN DE CONSOLEONE® EN NETWARE®.....	44
2.6 FUNDAMENTOS DE ADMINISTRACIÓN.....	44
2.6.1 ORGANIZACIÓN DE OBJETOS EN CONTENEDORES.....	44
2.6.2 CREACIÓN DE UN OBJETO ORGANIZACIÓN.....	45
2.6.3 CREACIÓN DEL OBJETO UNIDAD ADMINISTRATIVA.....	45
2.6.4 CREACIÓN DE UN OBJETO LOCALIDAD.....	45
2.6.5 CREACIÓN DE UN OBJETO PAÍS.....	45
2.6.6 CREACIÓN DE UN ALIAS PARA UN OBJETO.....	46
2.7 GESTIÓN DE CUENTAS DE USUARIO.....	46
2.7.1 CREACIÓN DE CUENTAS DE USUARIO.....	46
2.7.1.1 CREACIÓN DE UN OBJETO USUARIO.....	46
2.7.1.2 CREACIÓN DE UNA PLANTILLA DE USUARIO.....	47
2.7.2.1 CONFIGURACIÓN DE UN ENTORNO INFORMÁTICO DE RED DEL USUARIO.....	48
2.7.2.2 CONFIGURACIÓN DE SEGURIDAD DE ENTRADA ADICIONAL PARA UN USUARIO.	48
2.7.2.3 CONFIGURACIÓN DE UNA ESTIMACIÓN DEL USO DEL SERVIDOR NETWARE® DE UN USUARIO.....	48
2.7.3 CONFIGURACIÓN DE GUIONES DE ENTRADA.....	49
2.7.3.1 CREACIÓN DE UN GUIÓN DE ENTRADA.....	49
2.7.3.2 ASIGNACIÓN DE UN PERFIL A UN USUARIO.....	49
2.7.4 RESTRICCIONES DE HORA DE ENTRADA PARA USUARIOS REMOTOS.....	49
2.8 ADMINISTRACIÓN DE DERECHOS.....	50
2.8.1 ASIGNACIÓN EXPLÍCITA DE DERECHOS.....	50
2.8.1.1 CONTROL DEL ACCESO AL SISTEMA DE ARCHIVOS NETWARE®, POR RECURSO	51

2.8.1.2 CONTROL DEL ACCESO AL SISTEMA DE ARCHIVOS NETWARE®, POR TRUSTEE.	51
2.8.1.3 CONTROL DEL ACCESO A NDS, POR RECURSO.	52
2.8.1.4 CONTROL DEL ACCESO A NDS, POR TRUSTEE.	52
2.8.2 CÓMO OTORGAR EQUIVALENCIA.	53
2.8.2.1 CÓMO OTORGAR EQUIVALENCIA DE SEGURIDAD POR PERTENENCIA A GRUPO.	53
2.8.2.2 CÓMO OTORGAR EQUIVALENCIA DE SEGURIDAD EXPLÍCITAMENTE.	53
2.8.2.3 CONFIGURACIÓN DE UN ADMINISTRADOR MEDIANTE PROPIEDADES NDS ESPECÍFICAS.	53
2.8.3 VISUALIZACIÓN DE DERECHOS EFECTIVOS.	54
2.8.3.1 VISUALIZACIÓN DE DERECHOS EFECTIVOS PARA UN ARCHIVO O CARPETA DE UN VOLUMEN NETWARE®.	54
2.8.3.2 VISUALIZACIÓN DE DERECHOS EFECTIVOS SOBRE UN OBJETO O PROPIEDAD NDS.	54
2.8.4 ACERCA DE LOS DERECHOS NETWARE®.	55
2.8.4.1 DESCRIPCIONES DE DERECHOS.	55
2.8.4.2 ORÍGENES DE LOS DERECHOS.	55
2.8.4.3 CÓMO CALCULA NETWARE® LOS DERECHOS EFECTIVOS.	56
2.9 LA IMPRESIÓN EN LA RED.	57
2.9.1 LA IMPRESIÓN BASADA EN COLAS.	57
2.9.2 LA CONFIGURACIÓN RÁPIDA DE LOS SERVICIOS DE IMPRESIÓN.	58
2.9.3 ASIGNE USUARIOS A LAS COLAS DE IMPRESIÓN.	59
2.9.4 AGREGUE UNA IMPRESORA EN LA ESTACION DE TRABAJO.	60
2.9.5 SERVIDOR DE IMPRESIÓN NDPS.	61
2.9.5.1 ACERCA DE LOS SERVICIOS DISTRIBUIDOS DE IMPRESIÓN DE NOVELL®.	61
2.9.5.2 VENTAJAS DE LOS NDPS PARA LOS USUARIOS DE LA RED.	61
2.10 SERVICIO DE ACCESO REMOTO (RAS).	62
2.10.1 CONCEPTOS SOBRE RAS.	62
2.10.2 EL SERVICIO DE ACCESO REMOTO (RAS).	62
2.11 LAS COPIAS DE SEGURIDAD DEL SERVIDOR.	63
2.11.1 ELEGIR ENTRE COPIAS DE SEGURIDAD O COPIADO DE ARCHIVOS.	64
2.11.1.1 EL RESPALDO DIARIO DE LOS ARCHIVOS.	64
2.11.1.2 RESPALDO SEMANAL DEL SISTEMA COMPLETO.	65
2.11.1.3 LA COPIA MENSUAL DE LOS ARCHIVOS.	65
2.12 LA UTILIDAD SERVICIO DE GESTIÓN DE ALMACENAMIENTO DE NOVELL®.	65
2.13 REALIZAR UNA COPIA DE SEGURIDAD.	66
2.14 RESTAURAR UNA COPIA DE SEGURIDAD.	67
CAPITULO III.	67
3. INSTALACIÓN Y MANEJO DE LAS REDES CON UNÍX Y PRODUCTOS SCO.	70
3.1 HISTORIA DEL UNIX.	70
3.2 ESTRUCTURA DE UNÍS.	71
3.2.1 ESTRUCTURA DEL SISTEMA.	71
3.2.2 ARQUITECTURA DEL SISTEMA OPERATIVO UNÍX.	71
3.2.3 EL NÚCLEO O KERNEL DE UNIX.	73
3.3 INSTALACION DE SCO UNIX.	74
3.3.1 CUMPLIMIENTO DE LOS REQUISITOS DEL SISTEMA.	74
3.3.2 INTRODUCCIÓN A LA INSTALACIÓN.	74
3.3.3 PROCEDIMIENTO DE INSTALACIÓN.	75
3.3.3.1 CONFIGURACIÓN DEL DISCO DURO.	75
3.3.4 CONFIGURACIÓN DE LA ZONA GEOGRÁFICA.	77
3.3.5 INSTALACIÓN DE SOFTWARE ADICIONAL.	77
3.3.6 COLOCAR PASSWORD.	78
3.3.7 REINICIAR EL SISTEMA.	78
3.4. ESTRUCTURA DEL SISTEMA DE ARCHIVOS (FILE SYSTEM).	78

3.4.1 EL SISTEMA DE ARCHIVOS.....	78
3.4.2 CONCEPTOS BÁSICOS SOBRE ARCHIVOS.....	79
3.4.3 ESTRUCTURA INTERNA DEL SISTEMA DE ARCHIVOS.....	80
3.4.4 DESCRIPCIÓN DEL INODO.....	81
3.4.5 DIRECTORIOS.....	82
3.4.6 DISPOSITIVOS Y ARCHIVOS ESPECIALES.....	83
3.4.7 ACCESO A LOS ARCHIVOS.....	83
3.5 UNIX EN EL ÁMBITO DE USUARIO.....	84
3.5.1 TIPOS DE USUARIO.....	84
3.5.2 GRUPOS.....	85
3.5.3 CONEXIÓN AL SISTEMA.....	85
3.5.4 DESCONEXIÓN.....	86
3.6 EL "SHELL".....	86
3.6.1 EL "SHELL" BOURNE (sh).....	87
3.6.2 EL "SHELL" C (csh).....	87
3.6.3 EL "SHELL" KORN (ksh).....	88
3.6.4 EL "SHELL" C MEJORADO (tcsh).....	88
3.6.5 Procedimientos de "shell" o "shell" scripts.....	89
3.7 COMANDOS MÁS COMUNES.....	89
3.7.1 SINTAXIS DE LAS ÓRDENES.....	89
3.7.2 METACARACTERES.....	90
3.7.2.1 CARACTERES COMODINES.....	90
3.7.2.2 REDIRECCIONAMIENTO DE LA E/S.....	90
3.7.2.3 PIPE. PIPELINE.....	91
3.7.2.4 LÍNEAS MULTICOMANDO.....	91
3.7.3 ÓRDENES DE MANIPULACIÓN DE DIRECTORIOS.....	91
3.7.4 ÓRDENES DE MANIPULACIÓN DE ARCHIVOS.....	92
3.7.5 MODIFICACIÓN DE PERMISOS Y PROPIETARIOS.....	95
3.7.6 IMPRESIÓN.....	96
3.7.7 ÓRDENES DIVERSAS.....	96
3.8 ADMINISTRACIÓN DEL SISTEMA.....	97
3.8.1 EL SUPERUSUARIO Y SUS FUNCIONES.....	97
3.8.2 ARRANQUE Y PARADA DEL SISTEMA.....	98
3.8.2.1 ARRANQUE DEL SISTEMA.....	98
3.8.2.2 PARADA DEL SISTEMA.....	99
3.8.3 ADMINISTRACIÓN DE LOS SISTEMAS DE ARCHIVOS.....	100
3.8.3.1 MONTAR UN SISTEMA DE ARCHIVOS.....	100
3.8.3.2 CREAR UN SISTEMA DE ARCHIVOS.....	100
3.8.3.3 UTILIZACIÓN DEL DISCO.....	101
3.8.4 ADMINISTRACIÓN DE LAS CUENTAS DE USUARIO.....	102
3.8.4.1 ARCHIVOS ADMINISTRATIVOS.....	102
3.8.4.2 CREACIÓN / BORRADO / MODIFICACIÓN DE CUENTAS DE USUARIOS.....	103
3.8.4.3 CREACIÓN / BORRADO DE GRUPOS.....	104
3.8.4.4 LISTADO DE USUARIOS DEL SISTEMA.....	104
3.8.5 ADMINISTRACIÓN DE IMPRESORAS.....	105
3.8.5.1 CREAR UN PUERTO PARALELO.....	105
3.8.5.2 CREAR UNA IMPRESORA.....	106
3.8.6 COPIAS DE SEGURIDAD. RECUPERACIÓN.....	106
3.8.6.1 INTRODUCCIÓN.....	106
3.8.6.2 COPIAS INCREMENTALES CON BACKUP/RESTORE.....	107
3.8.6.3 COPIAS ESPECÍFICAS CON TAR Y CPIO.....	107
CAPITULO IV.....	106
4 INSTALACIÓN Y MANEJO DE REDES CON WINDOWS NT Y PRODUCTOS MICROSOFT.....	110
4.1 HISTORIA DE WINDOWS NT.....	110
4.2 INSTALACIÓN DE WINDOWS NT.....	110

4.2.1 REQUISITOS DEL SISTEMA PARA NT.....	110
4.2.2 ORGANIZACIÓN DE LOS SISTEMAS OPERATIVOS.....	111
4.2.3 PREPARACIÓN DE LA INSTALACIÓN.....	112
4.2.4 DETECCIÓN DEL HARDWARE.....	113
4.2.5 INSTALACIÓN.....	113
4.2.5.1 CONFIGURACIÓN DE UNIDADES DE ALMACENAMIENTO.....	114
4.2.5.2 SELECCIÓN DEL DIRECTORIO RAÍZ DE WINDOWS NT.....	116
4.2.5.3 SELECCIÓN DEL TIPO DE INSTALACIÓN.....	117
4.2.5.4 MODOS DE LICENCIA E INTRODUCCIÓN DE LOS DATOS PERSONALES.....	117
4.2.5.5 SELECCIÓN DEL TIPO DE SERVIDOR (SÓLO WINDOWS NT SERVER).....	119
4.2.5.6 CONTRASEÑA DEL ADMINISTRADOR.....	120
4.2.5.7 CREACIÓN DE UN DISQUETE DE EMERGENCIA.....	121
4.2.6 INSTALACIÓN EN RED DE WINDOWS NT.....	121
4.2.6.1 INSTALACIÓN DE INTERNET INFORMATION SERVER.....	122
4.2.6.2 INSTALACIÓN DE LA TARJETA DE RED.....	123
4.2.6.3 INSTALACIÓN DE LOS PROTOCOLOS DE RED.....	123
4.2.6.4 SELECCIÓN DEL GRUPO DE TRABAJO O DOMINIO.....	124
4.3 ADMINISTRACIÓN DE ARCHIVOS EN NT.....	125
4.3.1 SISTEMAS DE ARCHIVOS.....	125
4.3.1.1 FAT.....	126
4.3.1.2 HPFS.....	126
4.3.1.3 NTFS.....	126
4.3.2 MÉTODOS PARA GUARDAR LOS DATOS DE FORMA SEGURA.....	127
4.3.2.1 CONJUNTO DE UNIDADES DE ALMACENAMIENTO.....	127
4.3.2.2 RAID.....	128
4.3.2.3 DISCOS ESPEJO.....	128
4.3.2.4 CONJUNTOS DE BANDAS.....	128
4.3.2.5 EL SISTEMA DE ARCHIVOS NTFS.....	128
4.3.2.6 ADMINISTRACIÓN DE UNIDADES DE ALMACENAMIENTO EN WINDOWS NT.....	129
4.3.2.7 EL ADMINISTRADOR DE DISCOS.....	129
4.3.2.8 GUARDAR DATOS.....	130
4.3.2.9 DISCOS DUROS FRAGMENTADOS.....	134
4.3.2.10 SISTEMA DE ARCHIVOS DISTRIBUIDO.....	135
4.4.1 UN DOMINIO ÚNICO.....	137
4.4.2 DOMINIOS MAESTROS ÚNICOS.....	137
4.4.3 DOMINIOS MAESTROS MÚLTIPLES.....	137
4.4.3.1 ORGANIZACIÓN FLEXIBLE.....	138
4.5 RESOLUCIÓN DE LOS NOMBRES.....	138
4.5.1 LISTAS DE NOMBRES ESTÁTICAS.....	138
4.5.2 LISTAS DE NOMBRES DINÁMICAS.....	139
4.5.3 EXAMINADOR DE RED.....	139
4.5.4 SERVIDOR DE NOMBRES.....	139
4.6 LOS SERVICIOS WINS.....	139
4.7 SERVICIOS DNS.....	140
4.8 INSTALAR CLIENTES.....	140
4.9 ADMINISTRACIÓN DE USUARIOS.....	140
4.9.1 PANORÁMICA.....	141
4.9.2 EL ADMINISTRADOR DE USUARIOS.....	141
4.9.3 GRUPOS DE USUARIOS.....	143
4.9.3.1 GRUPOS DE USUARIOS GLOBALES Y LOCALES.....	143
4.9.3.2 GRUPOS DE USUARIOS PREDEFINIDOS.....	143
4.9.3.3 CREAR LOS PROPIOS GRUPOS DE USUARIOS.....	144
4.9.3.3 CREAR LOS PROPIOS GRUPOS GLOBALES DE USUARIOS.....	145
4.9.3.5 INCORPORAR GRUPOS GLOBALES DE USUARIOS A UN GRUPO LOCAL DE UN DOMINIO DE CONFIANZA.....	145
4.9.4 LA CUENTA DE USUARIO PASO A PASO.....	146
4.9.4.1 ADMINISTRAR CUENTAS DE USUARIO.....	150

4.9.5 DEFINIR LAS NORMAS DE SEGURIDAD.....	150
4.9.5.1 PROPIEDADES DE CUENTA.....	150
4.10 REDES RAS.....	151
4.10.1 CONFIGURAR RAS.....	152
4.11 IMPRESIÓN EN WINDOWS NT.....	155
4.11.1 IMPRESORAS.....	156
4.11.2 EL ADMINISTRADOR DE IMPRESIÓN.....	161
4.11.3 CONEXIÓN A UN SERVIDOR DE IMPRESIÓN.....	163
4.12 RESPALDOS EN NT.....	163
4.12.1 CREAR UNA COPIA DE SEGURIDAD.....	163
CAPITULO V.....	162
5. ANÁLISIS COMPARATIVO DE LAS TRES PLATAFORMAS (UNÍX, NETWARE®, WINDOWS NT).....	168
5.1 VENTAJAS Y DESVENTAJAS DE LOS SISTEMAS OPERATIVOS:.....	168
5.1.1 VENTAJAS DE NOVELL®.....	168
5.1.2 DESVENTAJAS DE NOVELL®.....	168
5.1.3 VENTAJAS DE WINDOWS NT.....	169
5.1.4 DESVENTAJAS DE WINDOWS NT.....	169
5.1.5 VENTAJAS DE UNÍX.....	170
5.1.6 DESVENTAJAS DE UNÍX.....	170
5.2 PARTICIPACIÓN EN EL MERCADO DE LOS SISTEMAS OPERATIVOS DE RED.....	171
5.3 ESTUDIO COMPARATIVO BASÁNDOSE EN UN MUESTREO EN PYMES DEL VALLE DE MÉXICO.....	173
5.4 UNA VISION A OTROS COMPARATIVOS.....	185
5.4.1 ESTUDIO COMPARATIVO ENTRE SISTEMAS OPERATIVOS (POR CENTENIAL NETWORKING LABS).....	185
5.4.1.1 SERVICIOS DE FICHEROS Y DE RED.....	186
5.4.1.2 GESTIÓN.....	188
5.4.1.3 MONITORIZACIÓN DE LOS SERVIDORES.....	190
5.4.1.4 ADMINISTRACIÓN DE LOS CLIENTES.....	190
5.4.1.5 FICHEROS E IMPRESIÓN.....	190
5.4.1.6 GESTIÓN DEL ALMACENAMIENTO.....	191
5.4.1.7 SEGURIDAD.....	191
5.4.1.8 ESTABILIDAD Y TOLERANCIA A FALLOS.....	192
5.4.1.9 DOCUMENTACIÓN.....	192
5.4.1.10 CONCLUSIONES.....	193
5.5 ESTUDIO COMPARATIVO POR COPYRIGHT DIGITAL EQUIPMENT.....	194
CONCLUSIONES.....	196
GLOSARIO DE TERMINOS.....	197
APÉNDICE I.....	200
REFERENCIAS Y BIBLIOGRAFÍA.....	202

INTRODUCCION

En los últimos años, la economía viene sufriendo una sustancial desaceleración, reduciendo los ingresos de las empresas y estrechando sus lucros. La reacción de las empresas está siendo buscar nuevas formas de maximizar los recursos de tecnología de la información (IT) que poseen y, al mismo tiempo, aprovechar nuevas tecnologías que les permitan abrir sus redes a empleados, clientes y socios, atender a las enormes demandas de almacenamiento, simplificar la administración de la red, y reducir los costos de administración y soporte.

La elección de un sistema operativo para servidor con el que vivirá por años una organización no se basa simplemente en la funcionalidad de la versión en particular de un producto. Se trata de una decisión estratégica de largo plazo, guiada por las necesidades de la organización en cuanto a una plataforma en que construir soluciones para sus problemas de negocios. Por otra parte, los requerimientos que las organizaciones exigen en los sistemas operativos para servidor se expanden rápidamente. De la necesidad básica de compartir archivos e impresoras, los requerimientos han crecido e incluyen las comunicaciones, Internet, administración y aplicaciones distribuidas de gran escala. Estos requerimientos tan diversos implican que el sistema operativo de servidor debe ser una plataforma de propósito múltiple, capaz de proporcionar un conjunto extenso e integrado de servicios, que sean excelentes en cada función individual.

La libertad de elegir es el mayor regalo que a las empresas dio la tecnología. En el ambiente de los sistemas operativos que se tratan en esta Tesis están Windows, Unix y Linux (en todas sus versiones), y NOVELL®. ¿Cuál conviene? La decisión no es cosa de juego, porque de ello dependerá la estabilidad de las operaciones de una empresa, la solidez de su base de datos, la confiabilidad de sus aplicaciones críticas y la logística interna. Se trata de ahorrar pesos y centavos, pero también angustias y problemáticas futuras.

Por los motivos anteriormente expuestos, es que se extiende este estudio, con la finalidad de proporcionar un punto de vista diferente, enfocado a la funcionalidad de los sistemas operativos con la perspectiva de la experiencia que tienen los administradores de redes. De tal manera que esta tesis pretende expresar de manera más real las experiencias que tienen los administradores de redes en nuestro país y sus puntos de vista sobre los Sistemas Operativos de Redes que se tratan en este documento, así como, un estudio detallado de los crecimientos que han tenido los Sistemas Operativos en el mercado mundial en los últimos años. Además se incluyen manuales de cada sistema Operativo sirviendo como marco de referencia para administradores de redes con o sin experiencia.

OBJETIVO GENERAL

El propósito de esta Tesis es proporcionar a los responsables de la administración de redes de ordenadores, las herramientas necesarias para la toma de decisiones en cuanto a Sistemas Operativos se refiere, esta información esta apoyada en la experiencia de profesionales y una encuesta realizada en 50 empresas en el Valle de México.

La intención es la de comparar y contrastar las implicaciones de escoger un sistema operativo en términos no técnicos, o al menos con la mínima jerga técnica posible, por este motivo, el trabajo se posicionó en el punto de vista de los administradores de redes de ordenadores basándose en su experiencia en el manejo de un determinado Sistema Operativo y no en la propia estructura interna.

OBJETIVOS PARTICULARES

CAPITULO I.-En este capítulo se muestra un panorama general del ámbito de las redes locales, se describen los conceptos básicos así como las distintas topologías existentes y modelo de referencia ISO/OSI, buscando de esta manera que el lector tenga las nociones necesarias para poder comprender los capítulos posteriores.

CAPITULO II.-Se pretende describir de manera general la historia, instalación y administración de Netware de Novell con la finalidad de que se pueda , comprender y evaluar este Sistema Operativo.

CAPITULO III.-Para poder tener un contexto adecuado de la administración de Unix el cual se basa en comandos se describe la estructura general del Sistema Operativo así como la de sus comando los cuales son indispensables para su correcta operación.

CAPITULO IV.-Para terminar con los Sistemas Operativos descritos en este trabajo de Tesis, se describe a continuación el Sistema Operativo Windows NT desde su historia hasta la administración, tomando en cuenta que este sistema es de origen gráfico, se pretendió que el contenido también así lo fuera para un mejor entendimiento del mismo.

CAPITULO V.- La parte fundamental de esta Tesis se basa en el desarrollo de este capítulo, ya que en él se muestra el resultado de un estudio de campo así como también los análisis de laboratorios que con equipo especializado realizaron mediciones más técnicas sobre el rendimiento interno de los Sistemas en cuestión, siendo el objetivo de este capítulo dar una vision que ayude a los involucrados en estas tecnologías a tomar la decision de que sistema elegir de acuerdo a las necesidades de su empresa.

CAPITULO I
GENERALIDADES SOBRE REDES DE COMPUTADORAS

1. GENERALIDADES SOBRE REDES DE ORDENADORES

1.1 DEFINICIÓN.

“¿Qué es una RED? : En el campo de la computación se puede decir que una red, es un conjunto de ordenadores enlazados entre sí y/o con otros equipos, cuya configuración permite que ésta sea un medio para transmitir, recibir, compartir y manejar información.

1.2 COMPONENTES DE UNA RED LOCAL.

Los componentes principales de una red son:

1.2.1 SERVIDOR.

Son aquellos ordenadores capaces de compartir sus recursos con otros. Los recursos compartidos pueden incluir impresoras, unidades de disco, CD-ROM, directorios en disco duro e incluso archivos individuales. Los tipos de servidores obtienen el nombre dependiendo del recurso que comparten. Algunos de ellos son: servidor de discos, servidor de archivos, servidor de archivos distribuido, servidor de terminales, servidor de impresoras, servidor de discos compactos, servidor web y servidor de correo.

El Servidor puede ser de dos tipos: Dedicado o no dedicado

- Dedicado, exclusivamente administra los recursos de la red
- No dedicado, además de administrar los recursos de la red, funciona como Estación de Trabajo

Las características y configuración del ordenador que sea posible definir como servidor, están en función de los requerimientos particulares del caso, generalmente se trata de un equipo robusto tanto en *hardware* como en *software*.

1.2.2 ESTACIONES DE TRABAJO.

Están representadas por cada una de los micro ordenadores conectados en red. Cada ordenador conectada a la red conserva la capacidad de funcionar de manera independiente, realizando sus propios procesos. Asimismo, los ordenadores se convierten en estaciones de trabajo en red, con acceso a la información y recursos contenidos en el servidor de archivos de la misma.

Esta puede ser desde una PC XT hasta una Pentium, equipada según las necesidades del usuario; o también de otra arquitectura diferente como *Macintosh*, *Silicon Graphics*, *Sun*, etcétera.

En la actualidad se fabrica *hardware* exprofeso para redes locales, como es el caso de los servidores y estaciones de trabajo de fábrica. En el mercado nacional podemos encontrar que la mayoría de los fabricantes de productos de marca como *IBM*, *HP*, *Compaq*, *DIGITAL*, *ACER*, etcétera., ofrecen productos de estas características.

1.2.3 INTERFASE DE RED.

Es un dispositivo que permite la interconexión de los nodos de la red. Para comunicarse con el resto de la red, cada ordenador debe tener instalada una tarjeta de interfase de red. Se les llama también adaptadores de red o sólo tarjetas de red. En la mayoría de los casos, la tarjeta se adapta en la ranura de expansión del ordenador. (figura I.1)

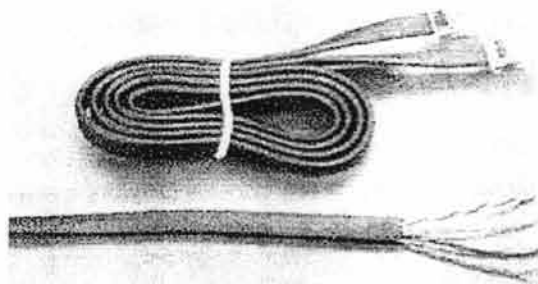


(figura I.1)

Según su especificación y normas, cada interfase de red determina los protocolos de comunicación y la forma de interconexión (topología) de cada red.

1.2.4 CANAL DE COMUNICACIÓN.

Es el medio físico por el cual se comunican los nodos de una red. Por lo general, es un cable dedicado a las comunicaciones, mismo que puede ser: (figura 1.2)



(figura 1.2)

- De tipo telefónico
- De par trenzado
- Coaxial
- Fibra óptica

Este canal de comunicación determina la velocidad máxima de transferencia de información que va desde los 2.5 Mbps hasta 1000 Mbps, dependiendo del tipo de cable que se utilice, sin embargo se están desarrollando nuevas tecnologías para incrementar estas velocidades.

También existen tecnologías para que el medio de comunicación sea inalámbrico, a partir de 1990 se comercializan interfases de red inalámbricas, con tecnologías de radio frecuencia, microondas, rayo láser, etcétera.

1.2.5 REPETIDORES.

Son dispositivos que permiten incrementar las distancias del medio de comunicación, reforzando su señal sin importar la topología; pueden ser tarjetas internas o cajas externas.

1.2.6 SISTEMA DE CABLEADO.

Este tipo de sistema se basa en la forma de conexión entre los equipos (topología), está en función de la interfase de red que se haya seleccionado.

1.2.7 SISTEMA OPERATIVO DE RED.

Es el *software* que se instala en el servidor de la red, permitiendo la compartición de los recursos, el control y la administración de la información de la red.

Los principales sistemas operativos de red en el mercado internacional, son:

- NETWARE® de NOVELL®. En diferentes versiones
- LAN MANAGER de Microsoft
- Windows NT y Windows para grupos de trabajo de Microsoft.
- Lantastic.
- Todos los NETBIOS compatibles.
- **IBM** LAN SERVER
- NETWORK

1.2.8 SOFTWARE DE APLICACIÓN.

Son las aplicaciones disponibles en la red, para los usuarios. Las más importantes son:

- Suites de Productividad Personal. (Procesadores de Texto, Hojas de Cálculo, Manejadores de Archivos, Presentaciones, etcétera.)
- Manejadores de Bases de Datos.
- Correo Electrónico.

1.3 TOPOLOGÍAS Y PROTOCOLOS.

Para protocolos, simplemente se adoptará la definición que por extensión se le da a este término, es decir, un conjunto de reglas aplicadas a las comunicaciones.

En redes locales, prácticamente existen tres tipos básicos de Topología, a saber:

- Estrella
- Bus
- Anillo

Se puede sumar a estos tipos básicos, la topología de árbol que es una conexión compuesta. Para el estudio de la Topología se deben de considerar dos tipos:

- Física
- Lógica

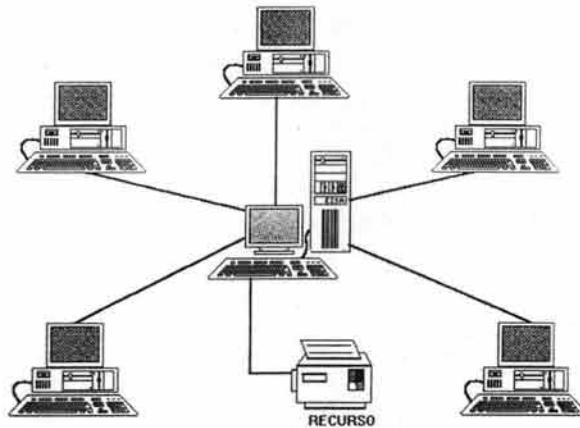
La topología física, es determinada por la disposición de los elementos conectados en la red, mientras que la Topología lógica, la determina el protocolo de comunicación que está operando en la red; no importando la disposición física de los elementos.

En el mercado actual existe una gran variedad de topologías físicas, para entender como funcionan todas estas, es importante conocer como funcionan tanto lógica como físicamente, los tipos básicos antes mencionados, y con base en esto, entender las características que cualquier topología en el mercado pueda ofrecer.

1.3.1 TOPOLOGÍA DE ESTRELLA.

En este tipo de conexión, el elemento central es el servidor con sus periféricos. Se mantiene preguntando constantemente a cada estación de trabajo mediante una comunicación exclusiva y por turno si desea transmitir información, en caso afirmativo, la atiende y al terminar prosigue su interrogatorio permanente.

En el despertar de las redes, esta topología fue la que se utilizó primero, pero resultaba una de las más caras. (figura 1.3)

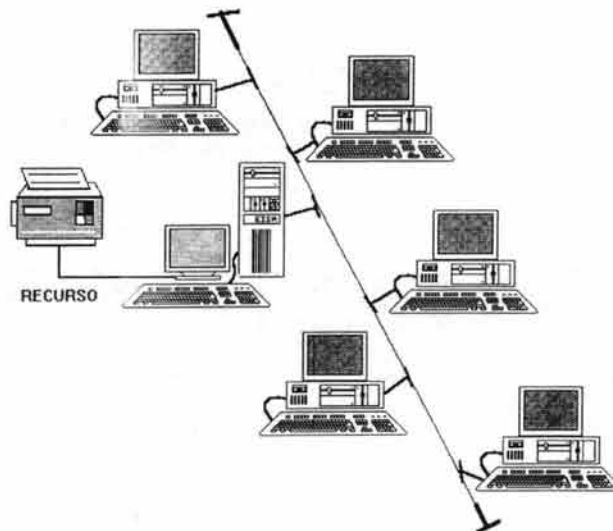


(figura 1.3)

1.3.2 TOPOLOGÍA DE BUS.

Esta conexión se considera que es la más sencilla de todas, donde las Estaciones de Trabajo y el Servidor, están enlazadas por un solo cable (coaxial o par trenzado), y la información viaja en ambos sentidos, por lo que es necesario prevenir las colisiones.

Por ello utiliza el Protocolo apropiado para tal caso, el CSMA/CD (Carrier Sense Multiple Access / Collision Detection). (figura 1.4)



(figura 1.4)

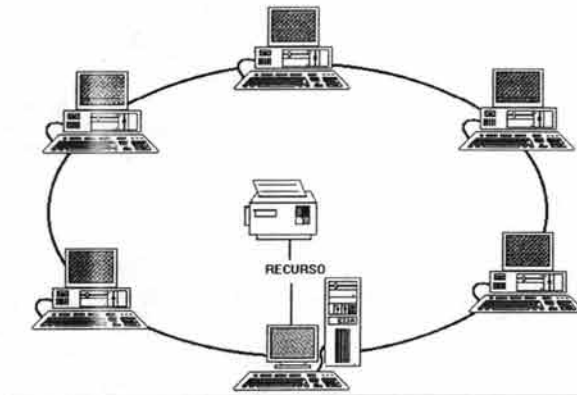
Con este protocolo, cualquier nodo transmite y espera a que se le confirme que la información fue recibida correctamente, de otra forma, se detecta la posible colisión, espera un tiempo a que el canal esté desocupado y la información se transmite nuevamente.

1.3.3 TOPOLOGÍA DE ANILLO.

En esta conexión, la información viaja ordenadamente en un solo sentido a través de un solo cable, describiendo un ángulo de 360° en cuyo anillo imaginario, están conectadas en serie las estaciones de trabajo y el servidor.

Una señal llamada "“TOKEN”" (Receptáculo, a modo de estafeta) va circulando por la red y pasando por cada estación, si la primera resultó ser la solicitante, previa identificación entrega la información, de lo contrario la deposita en "sobre cerrado" para que ésta a su vez la envíe a la siguiente, llevando la consigna de ser entregada hasta identificar a la estación solicitante.

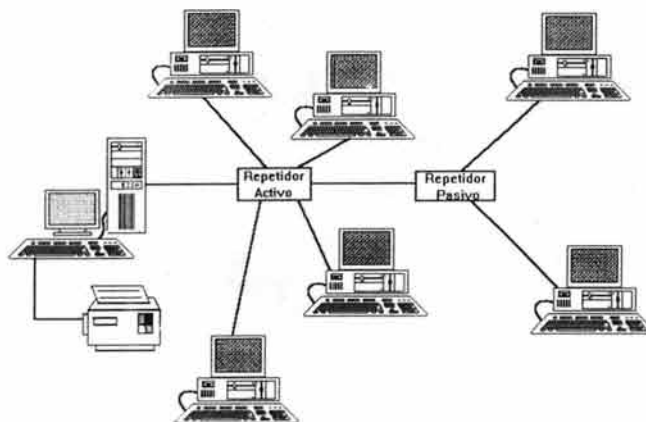
Cada estación de paso, colecta información adicional enviándola a la siguiente, y así se pasa la señal cerrando ciclos "circulares" por ello el protocolo apropiado para este caso se conoce como "TOKEN" PASSING. (figura 1.5)



(figura 1.5)

1.3.4 TOPOLOGÍA DE ÁRBOL.

Desde el punto de vista físico, esta conexión es combinada, como se mencionó anteriormente y es una opción más para implementar REDES, según las necesidades del usuario. (figura 1.6)



(figura 1.6)

1.4 ARQUITECTURA DE REDES.

Las redes están compuestas por muchos componentes diferentes que deben trabajar juntos para crear una red funcional. Los componentes que comprenden las partes de *hardware* de la red incluyen tarjetas adaptadoras de red, cables, conectores, concentradores y hasta el ordenador misma. Los componentes de red los fabrican, por lo general, varias compañías. Por lo tanto, es necesario que haya entendimiento y comunicación entre los fabricantes, en relación con la manera en que cada componente trabaja e interactúa con los demás componentes de la red. Afortunadamente, se han creado estándares que definen la forma de conectar componentes de *hardware* en las redes y el protocolo (o reglas) de uso cuando se establecen comunicaciones por red. Los tres estándares o arquitecturas más populares son: ARCnet, Ethernet y "Token" Ring. Ethernet y "Token" Ring son estándares respaldados por el organismo IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), mientras que ARCnet es un estándar de la industria que ha llegado a ser recientemente uno de los estándares del ANSI (Instituto Nacional de Estándares Americanos).

1.4.1 REDES ARCNET.

Producida en los años setenta por Datapoint Corporation, la red de cómputo de recursos conectados (ARCnet) es un estándar aceptado por la industria, aunque no lleva un número estándar de IEEE. ANSI reconoció a ARCnet como estándar formal, lo que la hizo parte de su estándar de LAN ANSI 878.1.

Como soporta una velocidad de transferencia de datos de 2.5 Mbps, ARCnet usa una topología lógica de bus y una ligera variación de la topología física de estrella. Cada nodo de la red está conectado a un concentrador pasivo o a uno activo. La tarjeta de red en cada ordenador está conectada a un cable que a su vez está conectado a un concentrador activo o pasivo. ARCnet se basa en un esquema de paso de señal ("token" passing) para administrar el flujo de datos entre los nodos de la red. Cuando un nodo está en posesión del "token" (señal), puede transmitir datos por la red. Todos los nodos, a excepción del receptor pretendido, pasan por alto los datos. Conforme se pasa el "token" a cada nodo, el nodo puede enviar datos.

Ya que cada nodo sólo puede enviar datos cuando tiene el "token", en ARCnet no suceden las colisiones que suelen darse en un esquema como el de CSMA/CD. Por lo tanto, ARCnet es menos susceptible a la saturación de la red que Ethernet. Durante algún tiempo ARCnet fue el estándar para LAN más popular; pero por causa en parte a su relativa baja velocidad (2.5 Mbps comparados con los 10 Mbps de Ethernet), casi no se usa para instalaciones nuevas.

1.4.2 REDES ETHERNET.

Ethernet, al que también se conoce como IEEE 802.3, es el estándar más popular para las LAN que se usa actualmente. El estándar 802.3 emplea una topología lógica de bus y una topología física de estrella o de bus. Ethernet permite datos a través de la red a una velocidad de 10 Mbps. Ethernet usa un método de transmisión de datos conocido como Acceso Múltiple con Detección de Portadora y Detección de Colisiones (CSMA/CD). Antes de que un nodo envíe algún dato a través de una red Ethernet, primero escucha y se da cuenta si algún otro nodo está transfiriendo información. De no ser así, el nodo transferirá la información a través de la red. Todos los otros nodos escucharán y el nodo seleccionado recibirá la información. En caso de que dos nodos traten de enviar datos por la red al mismo tiempo, cada nodo se dará cuenta de la colisión y esperará una cantidad de tiempo aleatoria antes de volver a hacer el envío. La topología lógica de bus de Ethernet permite que cada nodo tome su turno en la transmisión de información a través de la red. Así, la falla de un solo nodo no hace que falle la red completa. Aunque CSMA/CD es una forma rápida y eficiente para transmitir datos, una red muy cargada podría llegar al punto de saturación. Sin embargo, con una red diseñada adecuadamente, la saturación rara vez es preocupante. Existen tres estándares de Ethernet, 10BASE5, 10BASE2, y 10BASE-T, que definen el tipo de cable de red, las especificaciones de longitud y la topología física que debe utilizarse para conectar nodos en la red.

1.4.3 REDES "TOKEN" RING.

"Token" Ring, también llamado IEEE 802.5, fue ideado por *IBM* y algunos otros fabricantes. Con operación a una velocidad de 4 Mbps o 16 Mbps, "Token" Ring emplea una topología lógica de anillo y una topología física de estrella. La tarjeta de red de cada ordenador se conecta a un cable que, a su vez, se conecta a un concentrador central llamado unidad de acceso a multiestaciones (MAU). "Token" Ring se basa en un esquema de paso de señales ("token" passing), es decir que pasa un "token" (o señal) a todos los ordenadores de la red. El ordenador que esté en posesión del "token" tiene autorización para transmitir su información a otro ordenador de la red. Cuando termina, el "token" pasa al siguiente ordenador del anillo. Si el siguiente ordenador tiene que enviar información, acepta el "token" y procede a enviarla. En caso contrario, el "token" pasa al siguiente ordenador del anillo y el proceso continúa. La MAU se salta automáticamente un nodo de red que no esté encendido. Sin embargo, dado que cada nodo de una red "token" Ring examina y luego retransmite cada "token" (señal), un nodo con mal funcionamiento puede hacer que deje de trabajar toda la red. "Token" Ring tiende a ser menos eficiente que CSMA/CD (de Ethernet) en redes con poca actividad, pues requiere una sobrecarga adicional. Sin embargo, conforme aumenta la actividad de la red, "Token" Ring llega a ser más eficiente que CSMA/CD.

Existen varias tecnologías nuevas que satisfacen las necesidades de las redes actuales, incluyendo a Fast Ethernet, FDDI, Frame Relay y *ATM*.

1.4.4 FAST ETHERNET.

Para redes Ethernet que requieren altas velocidades de transmisión, fue establecido el estándar Fast Ethernet (IEEE 802.3u). Este estándar eleva el límite de velocidad de transmisión de 10 Mega bits por segundo (Mbps) a 100 Mbps con solo mínimos cambios en los cableados existentes.

Hay tres tipos de Fast Ethernet:

100BASE-TX: para el uso con cableados de par trenzado sin malla (Unshielded Twisted Pair o "UTP") nivel 5.

100BASE-FX: para el uso con cables de fibra óptica. 100BASE-T4: el cual utiliza un par extra de hilos para utilizar cableado existente tipo UTP nivel 3.

El estándar 100BASE-TX se ha vuelto el más popular debido a su gran compatibilidad con el estándar Ethernet 10BASE-T.

Ethernet de 1.0 Gigabit es una tecnología que promete una migración mas allá de Fast Ethernet de modo tal que las generaciones futuras de redes soportarán aún más altas velocidades de transferencia de datos.

1.4.5 FDDI.

La interfase de distribución de datos por fibra óptica (FDDI) es un estándar para la transferencia de datos por cable de fibra óptica. El estándar ANSI X3T9.5 para FDDI especifica una velocidad de 100 Mbps. Dado que el cable de fibra óptica no es susceptible a la interferencia eléctrica o tan susceptible a la degradación de la señal de red como sucede con los cables de red estándar. FDDI permite el empleo de cables mucho más largos que otros estándares de red.

1.4.6 EL FRAME RELAY.

Es un servicio orientado a la conexión, para mover datos de un nodo a otro a una velocidad razonable y bajo costo. El frame relay puede verse como una línea virtual rentada. El usuario renta un circuito virtual permanente entre dos puntos y entonces puede enviar tramas o frames (es decir, paquetes) de hasta 1600 bytes entre ellos. Además de competir con las líneas rentadas, el frame relay compete con los circuitos virtuales permanentes de X.25.

1.4.7 ATM.

ATM significa modo de transferencia asincrónica, es un conjunto de estándares internacionales para la transferencia de datos, voz y video por medio de una red a muy altas velocidades. Puesto que opera a velocidades que van desde 1.5 Mbps hasta 1.5 Gbps, *ATM* incorpora parte de los estándares Ethernet, "Token" Ring y FDDI para la transferencia de datos.

1.5 MODELO DE REFERENCIA ISO-OSI.

Las tecnologías que el hombre ha inventando, para comunicarse, siempre han seguido ciertas normas o reglas para su aceptación en un grupo social que puede ir desde una pequeña comunidad hasta toda una gran sociedad. En la época moderna las normas que rigen a las comunicaciones deben tener carácter universal. Hablando de comunicaciones digitales las normas o reglas universales están representadas por el modelo *ISO-OSI*.

El modelo OSI estructura en siete niveles o capas, el fenómeno global de la comunicación, es un marco hoy en día obligado y universalmente aceptado.

Las normalizaciones en redes locales tratan de encuadrarse dentro de este modelo. Además, las redes locales deberán acoplarse a las redes públicas de área extendida, actualmente existentes y en permanente expansión.

El modelo para la interconexión de sistemas abiertos, ISA u OSI se ha convertido en una referencia obligada para todo lo relacionado con la intercomunicación de ordenadores.

1.5.1 ESTRUCTURA GENERAL DEL MODELO.

Desde el punto de vista de ISO, un sistema abierto es el conjunto de uno o más ordenadores con su *software*, periféricos y terminales, capaces de procesar y transmitir información.

Es un modelo que está relacionado con las funciones que tienen que ser desarrolladas por el *hardware* y el software para obtener una comunicación fiable e independiente de las características específicas de la máquina. Es decir, está pensada para la interconexión de sistemas heterogéneos.

El sistema está compuesto por **siete niveles**, mediante los cuales dos sistemas informáticos se comunican entre sí. (figura I.7)



(figura I.7)

Con frecuencia, quienes inician el estudio del modelo se preguntan la razón de que sean siete niveles en la arquitectura y no un número mayor o menor.

El grupo de estudio que elaboró el modelo OSI pensó que la división en siete niveles era una buena propuesta, pero eso no significa que tenga que ser necesariamente así.

No obstante, este modelo ha sido plenamente aceptado tanto por fabricantes como por usuarios. Las características del modelo podrían resumirse de la siguiente forma:

- Cada nivel está representado por una entidad de nivel. Los niveles equivalentes en dos sistemas diferentes se comunican de acuerdo con unas reglas y convenios denominados protocolos de nivel o protocolos de pares.

- Cada nivel proporciona un conjunto definido de servicios al nivel superior y a su vez utiliza los servicios que le proporciona el nivel inmediatamente inferior.

- La comunicación se realiza a través de los niveles inferiores, siendo el protocolo de pares una abstracción lógica de relación entre las dos entidades comunicantes.

- Si un nivel N desea transmitir una unidad de datos a otro nivel N homólogo en otro sistema informático, se la pasará al nivel inmediatamente inferior, el cual le añadirá información delimitadora propia y a su vez pasará esta información a su nivel inmediatamente inferior.

En el sistema receptor cada nivel separará la parte del mensaje que le corresponde y pasará el resto a su nivel inmediatamente superior, que hará lo propio. Así el mensaje del nivel N es como si viajara horizontalmente hasta su nivel homólogo en recepción.

1.5.2 LOS SIETE NIVELES.

Los tres primeros niveles tratan los protocolos asociados con la red de conmutación de paquetes utilizada para la conexión y pueden agruparse dentro del llamado bloque de transmisión.

El nivel cuatro enmascara a los niveles superiores los detalles de trabajo de los niveles inferiores dependientes de la red, y junto con ellos forma el bloque de transporte.

Los tres niveles superiores, del quinto al séptimo, son los usuarios del bloque de transporte y aíslan la comunicación de las características específicas del sistema informático.

A continuación se analizan uno por uno los diferentes niveles, estudiando sus funciones y características.

El nivel siete: aplicación.

Este nivel se preocupa de proporcionar un conjunto de servicios distribuidos a los procesos de aplicación de los usuarios. El usuario se comunicará directamente con este nivel a través de la correspondiente interfase o agente de usuario.

Actualmente, se están desarrollando una serie de normas y recomendaciones tendientes a tipificar cada uno de estos servicios o aplicaciones distribuidas.

Entre los más conocidos podemos citar:

- Servicio de mensajería (correo electrónico)
- Servicio de almacenamiento y recuperación de documentos,
- Servicio de directorio, etcétera.

El nivel seis: Presentación.

Este nivel se ocupa de la representación de los datos usados por los procesos de aplicación del nivel siete. Por lo tanto, si es necesario, realizará la transformación de los datos que reciba de o para el nivel de aplicación. Esto en el caso de que el proceso originador y el receptor tuvieran versiones de datos sintácticamente diferentes, pero también puede darse el caso de que, para una determinada aplicación distribuida exista un conjunto de caracteres normalizados diferentes de los del originador y el receptor, en cuyo caso, los niveles de presentación respectivos deberían de hacer las transformaciones necesarias.

Otra función que se puede encargar al nivel seis, es la de velar por la seguridad de los datos, siendo responsable de la encriptación de mensajes confidenciales antes de su transmisión. La función inversa será realizada por el nivel de presentación del sistema receptor.

Nivel cinco: Sesión.

Su función es establecer y gestionar un camino de comunicación entre dos procesos del nivel de aplicación. Este nivel establece una sesión y se encarga de controlar la comunicación y sincronizar el diálogo.

La información que se envía se fracciona en pedazos y se generan unos puntos de sincronización. En caso de interrumpirse la sesión por alguna falla en la comunicación, los datos pueden ser recuperados y se conoce con precisión por ambos interlocutores hasta qué punto de sincronización la comunicación fue correcta.

Al reanudarse la sesión no será necesario transmitir de nuevo toda la información, sino solamente a partir del punto donde se quedó el último paquete de información válido.

En una sesión hay un diálogo entre máquinas, entre procesos y el protocolo debe regular quién "habla", cuándo y por cuánto tiempo.

Estas reglas necesitan ser acordadas cuando la sesión comienza. Este nivel también es responsable de dirigir el diálogo entre las entidades de nivel de presentación.

Para ello, cuando se establece una conexión de sesión, es necesario que ambos niveles cinco se pongan de acuerdo sobre el papel a desempeñar por cada uno de ellos en la comunicación.

Nivel cuatro: Transporte.

Este nivel es responsable de una transferencia de datos transparente entre dos entidades del nivel de sesión, liberando a dichas entidades de todo lo referente a la forma de llevar a cabo dicho transporte.

Los protocolos que manejan este nivel suelen llamarse protocolos "*end-to-end*", o protocolos entre puntos finales, debido a que este nivel se encarga de realizar una conexión lógica entre dos estaciones de transporte de los sistemas informáticos que quieren comunicarse, independientemente de donde se encuentren éstos.

Este nivel puede multiplexar varias conexiones de transporte dentro de una única conexión de red, o puede por el contrario, repartir una conexión de transporte entre varias conexiones de red.

Nivel tres: Red.

Este nivel enmascara todas las particularidades del medio real de transferencia. Es el responsable del encaminamiento de los paquetes de datos a través de la red. Cada vez que un paquete llega a un nodo, el nivel tres de ese nodo deberá seleccionar el mejor enlace de datos por el que envíe la información.

Las unidades de datos de este nivel son los paquetes de datos que deberán ir provistos de la dirección de destino. Por lo tanto, entre las funciones fundamentales del nivel de red se encuentran las de establecer, mantener y liberar las conexiones necesarias para la transferencia de los paquetes de datos.

Además, son funciones de este nivel la definición de la estructura de datos de los paquetes, las técnicas de corrección de errores, la entrega en secuencia correcta al nivel de transporte de los paquetes recibidos, así como otras de reiniciación y control de flujo.

Nivel dos: Enlace.

Un enlace de datos se establece siempre entre dos puntos físicos de conexión del sistema. En el caso de una red de datos de conmutación de paquetes, el nivel de enlace es responsable de la transferencia fiable de cada paquete al nivel de red.

Nivel uno: Físico.

Este nivel engloba los medios mecánicos, eléctricos, funcionales y de procedimiento para acceder al medio físico. Es el encargado de la activación y desactivación física de la conexión.

EL modelo *ISO-OSI*, proporciona un lenguaje universal entre los especialistas del medio de la interconexión de equipo de cómputo, para que hablen un "mismo idioma" y puedan comparar cualquier producto o tecnología respecto a dicho modelo.

También es saludable mencionar que los grandes centros de investigación de la industria están trabajando fuertemente para lograr una tecnología comercial que se apegue estrictamente al modelo, dicha tecnología es reconocida como *OSI*, pero en la actualidad no deja de ser un interesante proyecto, ya que la parte comercial tiene sus ojos puestos en tecnologías ya ampliamente probadas como *TCP-IP* y las nuevas tecnologías que manejan un gran ancho de banda como *ATM*, *Frame-Relay*, etcétera.

1.6 SISTEMAS OPERATIVOS PARA RED.

Se puede decir que el sistema operativo de una red, es el conjunto de programas que regulan el funcionamiento de ésta, proporciona los elementos para la interfase con el usuario, controla y define los niveles de seguridad, así como la manera en que se comparten los recursos.

Las funciones o tareas más importantes del sistema operativo son:

- Administrar y Compartir Recursos Físicos y Lógicos.
- Interfase con el Usuario.- Debe ser de la manera mas transparente posible. El éxito de una red depende de que el usuario final la utilice y explote.
- Seguridad e Integridad de la Información.- El sistema operativo debe ser el encargado de otorgar y/o limitar el uso de recursos en función de la jerarquía de los mismos, es decir, controlar los derechos y privilegios a usuarios autorizados.

Así mismo, debe prever mecanismos para asegurar la integridad de la información, entendiéndose por ésta, que la información se encuentre almacenada correctamente tanto física como lógicamente.

1.7 ARQUITECTURA DE SISTEMAS OPERATIVOS DE RED.

Para seleccionar adecuadamente un sistema operativo de red, antes de pensar en cual es el mejor producto por su fabricante (*NOVELL®*, *Microsoft*, *SCO*, etcétera.), Se tiene que analizar la arquitectura del sistema operativo de red que se requiere, según las necesidades particulares que se quieran resolver.

A continuación, se describen brevemente las principales arquitecturas de los sistemas operativos de red que existen en el mercado.

Las arquitecturas de sistema operativo de red son:

- Servidores de Disco.
- Servidores de Archivo
- Servidores de Base de Datos
- Cliente-Servidor
- Punto a Punto

1.7.1 SERVIDOR DE DISCOS.

Esta arquitectura fue el origen de los sistemas operativos de red, desde 1985 Apple con su Red Apple Talk, ya la soportaba.

Originalmente un servidor de discos, simplemente define secciones en el disco duro del Servidor y se las asigna a cada usuario, de forma que, cuando desde la estación se requiere acceder al disco duro de la red, solamente es necesario seleccionar una unidad lógica y en ese momento se tiene acceso a la partición del disco duro del Servidor correspondiente al usuario, cabe señalar que cada sección es independiente. Por ejemplo si dos usuarios requieren una misma aplicación, la aplicación debería estar cargada en las dos partes del disco duro correspondiente a cada usuario.

Esta arquitectura realmente no está orientada a compartir la información, sino compartir el disco duro.

Aparentemente esta tecnología está en desuso, pero en la actualidad tiene importantes aplicaciones sobre todo, en la definición de Servidores de Respaldo y Servidores de CDS.

1.7.2 SERVIDOR DE ARCHIVOS.

Un servidor de archivos, no comparte el disco duro del Servidor, sino que comparte o sirve los archivos que se almacenan en él, ya que resuelve el problema de la administración de archivos en la red, con un Software especializado.

Dicho Software tipo servidor de archivos, administra el acceso al disco compartido y a la información que contiene. El Software de referencia, está desarrollado específicamente para redes y construido a efecto de poder compartir archivos en un ambiente multiusuario, entendiéndose por multiusuario la utilización de un mismo archivo por más de un usuario a la vez.

El almacenamiento de datos compartido se controla por el Software del servidor de archivos. Las estaciones no manejan sus propias entradas y salidas, sino que envían requerimientos de alto nivel al Servidor y éste administra el acceso al disco. Debido a este control centralizado, los servidores de archivos, brindan a la red la integridad de datos como la que ofrecen los mini ordenadores y mainframes.

La mayoría de los sistemas operativos en la actualidad trabajan bajo el concepto de servidores de archivos, lo cual, es la evolución de los servidores de discos; el próximo paso, sobre el que ya se están dando los primeros avances comerciales son los servidores de bases de datos, mismos que se tratarán en su momento.

Este cambio de servidores de discos a servidores de archivos, se pudo dar gracias a la aparición de la versión 3.1 del MS-DOS, que a diferencia de las versiones anteriores ya estaba orientado a soportar tareas de tipo multiusuario, este paso fue de suma importancia porque abrió el camino y sentó las bases para la definición de los estándares de redes locales que actualmente existen.

1.7.3 SERVIDOR DE BASE DE DATOS.

Debido al gran éxito que tuvieron los servidores de archivos, cada vez más aplicaciones y necesidades robustas fueron migradas a redes LAN, entre ellas los manejadores de bases de datos. Debido a que en la arquitectura servidor de archivos se presenta un "cuello de botella" en el medio de comunicación, cuando varios usuarios concurrentemente quieren acceder a la misma base de datos.

Los servidores de bases de datos requieren de inversiones fuertes en **Hardware** y Software y están orientados solamente a usuarios corporativos, que por sus necesidades justifican estos costos.

1.7.4 ARQUITECTURA CLIENTE SERVIDOR.

La arquitectura Cliente Servidor, es una tecnología de punta, pero que, por aspectos comerciales, inclusive el termino ha caído en una especie de moda, donde todas las aplicaciones según sus fabricantes son Cliente Servidor.

Primero se establecerá de manera sencilla el concepto. Se debe de partir que en una LAN existe un proceso distribuido, donde el procesador del Servidor ejecuta las instrucciones del Sistema Operativo de red, generalmente de servicios de archivos, y el procesador de las Estaciones de Trabajo procesan los trabajos locales, pero las aplicaciones cada día requieren mayor poder en el procesador, lo que implicaría que las Estaciones de Trabajo tuvieran procesadores muy poderosos, con las respectivas consecuencias económicas, pero si se parte del hecho que los servidores cuentan con este tipo de procesadores, la Arquitectura Cliente-Servidor, implica aprovechar estos procesadores poderosos para hacer las tareas pesadas y los trabajos ligeros dejárselos al procesador de las Estaciones de Trabajo.

Sin duda, el modelo Cliente Servidor es el que le da a las redes locales la posibilidad de ir más allá de los servicios de impresión o de archivos y el que permite que el proceso de información sea verdaderamente distribuido. Continuamente surgen aplicaciones en este modelo para todos los sistemas operativos de red. Esto con seguridad ayudará a desarrollar eficientemente el proceso distribuido, que convierte a las Redes LAN de ordenadores en herramientas únicas dentro del mundo de la computación.

1.7.5 SERVIDORES PUNTO A PUNTO.

En los últimos años después del "auge de las redes LAN", la industria había olvidado a las pequeñas empresas que tenían necesidad de intercambio de información, pero no recursos para hacer grandes inversiones en redes de ordenadores, es entonces cuando surgen las Redes Punto a Punto.

Sus principales características son:

- Todos los nodos pueden ser servidores y estaciones de trabajo a la vez, compartiendo sus discos duros, CD-ROM e impresoras.
- El Sistema operativo de red debe instalarse en cada nodo, consume poca memoria y por lo tanto no se requiere de servidores dedicados.
- La Administración e instalación de la Red es muy sencilla, por lo que no se requiere de personal altamente calificado.
- Su sistema de seguridad es básico, pero puede ser suficiente para aplicaciones pequeñas.
- La principal ventaja de este tipo de redes es que son económicas, sencillas y fáciles de instalar, orientadas a cubrir el mercado de las pequeñas empresas.

Sus desventajas podrían estibar en su poca seguridad y lindantes de comunicaciones externas.

Las Redes Punto a Punto llenan una necesidad que otras arquitecturas no cubren, que todos los nodos de la Red compartieran sus recursos, y no solamente los servidores, hoy en día es común que coexistan en una misma Red un Sistema operativo servidor de archivos, un Cliente Servidor y un Sistema Punto a Punto para aprovechar todas las ventajas de estas diferentes arquitecturas.”¹

¹ Magaña, Saúl y Magaña, Adrian. (2000). Introducción a redes de microcomputadoras. Universidad Nacional Autónoma de México, Facultad de Ingeniería, División de Educación Continua, Diplomado de redes de Computadoras y Telecomunicaciones. México D.F.

CAPÍTULO II
INSTALACIÓN Y MANEJO DE REDES CON NETWARE® Y
PRODUCTOS NOVELL®.

2. INSTALACIÓN Y MANEJO DE REDES CON NETWARE® Y PRODUCTOS NOVELL®.

2.1 HISTORIA.

“NOVELL® NETWARE® está en el mercado desde 1983, el mismo año en que **IBM** introdujo el ordenador personal **IBM XT®** y el **DOS 2.0®** para **IBM PC®**. Cada uno de estos productos implantó estándares. El **IBM XT®** fue el primer ordenador de **IBM** que incorporaba un disco fijo, mientras que el **DOS 2.0®** para el **IBM PC®** fue el primer sistema operativo de disco que controlaba discos fijos sin complementos especiales. Ambos generaron un sistema de estándares para el crecimiento de los ordenadores hacia entornos y aplicaciones más complejas basadas en ellos. NETWARE® iba a convertirse en el sistema operativo en red a elegir para estos equipos.

NOVELL® desarrolló originalmente NETWARE® para ejecutarse en un servidor basado en el microprocesador Motorola MC68000 usando configuración de red NOVELL® S-Net. La presentación del XT de **IBM** y la versión 2 del **DOS** hizo ver a muchas empresas, entre ellas NOVELL®, la oportunidad de desarrollo del producto. Como el código de NETWARE® estaba escrito en “C”, que es un lenguaje de los denominados “portables”, NOVELL® pudo trasladar parte del código del NETWARE® existente al nuevo equipo.

Como es sabido, el entorno **DOS/Intel 8088** no es el mejor para ejecutar aplicaciones multiusuario, especialmente un sistema operativo multiusuario como NETWARE®. El **BIOS** (sistema básico de entradas / salidas), desarrollado para el ordenador original (y necesario con el **DOS**), está diseñado para monousuario. NOVELL® tomó la importante decisión de dejar de lado completamente este sistema de E/S y crear un sistema operativo que funcionase de forma más efectiva en modo multiusuario. Debido a esto, NETWARE® se escribió específicamente para el **hardware** de los sistemas basados en el 8088, sin tener en cuenta el **DOS** y su sistema de E/S. Esta estrategia fue la que marcó la buena estrella de NOVELL® desde entonces. Otras empresas que han desarrollado sus sistemas operativos de red para funcionar bajo **DOS** han sufrido sus limitaciones.

Las dificultades de NOVELL® estribaron en la necesidad de escribir y actualizar constantemente los controladores para ofrecer compatibilidad con el **DOS** a los usuarios. Estos problemas fueron solventados rápidamente usando un “shell” para **DOS** en las estaciones de trabajo. El “shell” es una interfase software que permite a los usuarios de las estaciones trabajar con el **DOS** de forma normal, ejecutando también órdenes NETWARE®. El “shell” intercepta las órdenes de la red y las dirige al servidor. Casi todas las aplicaciones del **DOS** se pueden ejecutar en el sistema operativo NETWARE®, gracias a su “shell” para **DOS**. Además, NETWARE® incluye programas para seguridad y tolerancia a fallos que son imposibles de preparar en la estructura de archivos del **DOS**, marcando un nivel claramente superior.

Mientras tanto, NOVELL® siguió mejorando NETWARE® al ritmo de los avances tecnológicos. NETWARE® 286 funciona en modo protegido del procesador 80286, el más eficiente. En 1989, NOVELL® presentó NETWARE® 386, el primer sistema operativo que aprovechaba al máximo las ventajas del microprocesador **Intel 80386**. El 80386 es especialmente adaptable a entornos multiusuario, como las redes.

La estrategia de NOVELL® ha sido siempre acelerar el crecimiento de las redes. Anteriormente, desarrollaba productos **hardware** para potenciar el crecimiento de aspectos importantes de las redes, dejando posteriormente la fabricación de estos productos en manos de otras empresas. Algunas de éstas se convirtieron pronto en proveedores importantes de productos en el mercado en expansión de las redes.

La estrategia de NOVELL® para los noventa giraba en torno a la computación en red. Esta sección explota la tecnología software, **hardware** y de gestión de redes a desarrollar por NOVELL® y otras empresas en los años venideros. Como NOVELL® representa uno de los puntales de la industria de las redes, su estrategia en el ámbito de empresa puede considerarse un indicador importante de la dirección que está tomando dicha industria en general. A principios de los noventa NETWARE® estaba siendo utilizado en un 60 % de las redes instaladas. El 40% restante estaba cubierto por productos de **3COM: 3+Open y 3+Share, Banyan Vines, PC LAN de IBM** y otros.

La fuerza motriz que impulsa la estrategia de computación en red de NOVELL® es una arquitectura llamada SISTEMAS ABIERTOS NETWARE®. Esta arquitectura tiene los siguientes objetivos:

- Permitir disponer de los servicios ofrecidos por NETWARE® en plataformas ampliables.
- Hacer que NETWARE® sea independiente del protocolo soportando los estándares importantes de la industria, como TCP/IP y los niveles de protocolo *OSI*.
- Ofrecer encaminamiento (*routing*) y redes de área amplia.
- Mantener abierta la arquitectura y ofrecer herramientas de desarrollo para crear aplicaciones que operen en un entorno distribuido de computación en red.

NOVELL® planea implementar esta estrategia ofreciendo o soportando plataformas de servidores, arquitectura abierta, una tecnología de protocolos abierta y servicios NETWARE®. Los servicios NETWARE® se refieren al propio sistema operativo NETWARE®.

El objetivo de la computación en red es ofrecer un acceso transparente a los datos y recursos de cualquier equipo informático desde cualquier otro. La clave consiste en utilizar la red existente como plataforma para construir estos nuevos servicios integrados. La transparencia resulta difícil por los distintos estándares *hardware* y software y las distintas normativas sobre protocolos y acceso al cable, así como por los distintos sistemas operativos. Como resulta poco probable que una red o sistema operativo se convierta en un único estándar, los únicos sistemas operativos que podrán ofrecer soluciones de computación en red serán los que permitan integrar múltiples estándares a los usuarios.

NOVELL® NETWARE® alcanzó parte de este objetivo en sus primeros desarrollos, ofreciendo independencia del medio y una estrategia denominada tecnología de protocolo abierto (*Open Protocol Technology, OPT*). La independencia del medio permite que NETWARE® funcione con unos 30 tipos distintos de redes utilizando más de 100 tarjetas de red diferentes. La tecnología de protocolo abierto hace que NETWARE® pueda trabajar con equipos *DOS*, *OS/2* y *Macintosh* en la misma red, teniendo en proyecto hacerlo con estaciones Unix. La OPT ofrece sin problemas una migración hacia protocolos estándares de la industria como *TCP/IP* y *OSI*.²

2.2 CUMPLIMIENTO DE LOS REQUISITOS DEL SOFTWARE Y DEL SISTEMA.

NETWARE® 5 requiere los requisitos mínimos del sistema que se indican a continuación:

- ordenador de tipo servidor con procesador Pentium o superior.
- Adaptador de vídeo con resolución VGA o superior (SVGA recomendado).
- 550 MB de espacio libre en disco (50 MB para una partición de arranque y 500 MB para una partición NETWARE®).
- 64 MB de memoria RAM (se recomiendan 128 MB para ejecutar aplicaciones basadas en Java).
- Una o varias tarjetas de red.
- Unidad de CD-ROM capaz de leer discos inicializados y homologados por la Norma ISO 9660.
- Se recomienda un ratón serie o PS/2, aunque no es obligatorio.

² García, J. Sistema Operativo de Netware® de Novell® V.5. En línea [URL], <http://www.monografias.com/trabajos6/sinov/sinov.shtml#histo>

2.2.1 REQUISITOS DE SOFTWARE.

Antes de proceder a la instalación, asegúrese de que dispone del software y la información siguientes:

- **DOS** 3.3 o superior. (**DOS** 7 está incluido en el disquete de la licencia de **NETWARE®** 5. No utilice la versión de **DOS** que se suministra con los sistemas operativos Windows 95, Windows 98 o Windows NT.)
- Controladores de CD-ROM para **DOS**.
- CD-ROM del sistema operativo **NETWARE®** 5.
- Disquete de licencia de **NETWARE®** 5.
- Cliente **NOVELL®** para **DOS** y Windows 3.1 x (opcional, para una instalación desde la red.)
- Una dirección IP (opcional, si se va a conectar el servidor a Internet.)
- Controladores del dispositivo de almacenamiento y tarjeta de red, como la dirección del puerto y la interrupción.

2.3 PREPARACIÓN DEL ORDENADOR PARA LA INSTALACIÓN DE UN SERVIDOR.

Para preparar su ordenador para un servidor **NETWARE®** 5, es necesario:

- Instalar el **hardware** de red y del ordenador.
- Crear e inicializar una partición de arranque **DOS**.
- Tener acceso a los archivos de instalación.

2.3.1 INSTALACIÓN DEL HARDWARE DE RED Y DEL ORDENADOR.

Siga las instrucciones del fabricante para instalar y conectar la tarjeta y el cableado de la red a su ordenador. Asegúrese de que todos los dispositivos de almacenamiento están correctamente interconectados a los adaptadores de almacenamiento.

2.3.2 CREAR Y INICIALIZAR UNA PARTICIÓN DE ARRANQUE.

NETWARE® requiere una partición de arranque de al menos 50 MB para iniciar el ordenador y cargar **NETWARE®**. La partición de arranque contiene los archivos del servidor y de inicio de **NETWARE®**.

Debe aumentar el tamaño de la partición de arranque para adaptarse a sus requisitos de configuración específicos.

Para crear y inicializar una partición de arranque, siga los pasos que se indican a continuación:

- Realice una copia de seguridad de los datos que desee en otro ordenador o mecanismo de almacenamiento fuera de línea.
- Si el ordenador ya tiene instalado un sistema operativo, Windows por ejemplo, debe eliminarlo completamente. Si desea conservar varios sistemas operativos en un ordenador, póngase en contacto con un proveedor de software de gestión de arranque.

- Arranque el ordenador con **DOS** 3.3 o superior. Puede también arrancar desde el disquete de la licencia de **NETWARE® 5**. **DOS 7** y todas las utilidades necesarias de **DOS** están incluidas en el disquete. No utilice la versión de **DOS** que se suministra con los sistemas operativos Windows 95, Windows 98 o Windows NT.

- Utilice **FDISK** para crear una partición activa **DOS** de 50MB introduciendo **FDISK**. (Cree una partición **DOS** primaria y configúrela como partición activa.) El ordenador se iniciará.

- Inicialice y transfiera a la partición los archivos del sistema **DOS** cambiando a A: e introduciendo **FORMAT C: /S**. El ordenador debe disponer ahora de una partición de arranque activa de al menos 50 MB. Continúe con la instalación mediante el acceso a los archivos de instalación.

2.3.3 ACCESO A LOS ARCHIVOS DE INSTALACIÓN.

Es posible instalar **NETWARE® 5** desde un CD-ROM local o desde los archivos de instalación ubicados en la red. Para tener acceso a los archivos de instalación de **NETWARE® 5**, siga los pasos que se indican a continuación:

- Instale el controlador de CD-ROM para su dispositivo de CD-ROM en la partición de arranque. El fabricante del CD-ROM suministra los controladores de CD-ROM de **DOS**. Asegúrese de que el nombre de archivo lógico de su unidad de CD-ROM (indicado en los archivos **config.sys** y **autoexec.bat**) no sea **CDROM** ni **CDINST**.

- Asegúrese de que el archivo **config.sys** contiene los siguientes comandos: **FILES=40** y **BUFFERS=30**.

- (Condición) Si realiza la instalación desde archivos ubicados en la red, instale el software Cliente **NOVELL®** (**NOVELL Client™**) para **DOS** y Windows 3.1 x que se encuentran en el CD-ROM de **Z.E.N.works™**. Una vez realizado el acceso a los archivos del programa de instalación, puede empezar el proceso de instalación.

2.4 INICIO DE LA INSTALACIÓN.

Para iniciar la instalación, siga los pasos que se indican a continuación:

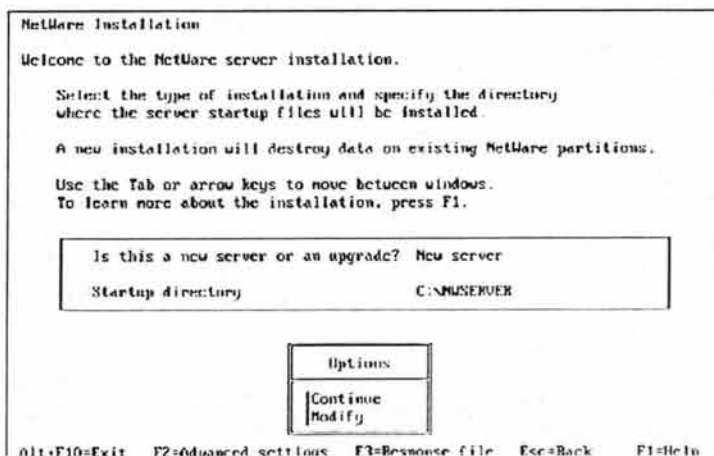
- Inserte el CD-ROM de **NETWARE® 5** o entre en la red para tener acceso a los archivos de instalación.

- En la unidad de CD-ROM o el indicador de red, introduzca **INSTALL**.

2.4.1 SELECCIÓN DEL IDIOMA Y ACEPTACIÓN DEL ACUERDO DE LICENCIA.

El programa de instalación está disponible en varios idiomas. Se pueden instalar posteriormente durante el programa de instalación otras opciones de idioma, como el idioma para el sistema operativo o para los usuarios. (figura II.1)

(figura II.1)



Aceptar el acuerdo de licencia implica leer y aceptar los términos y condiciones incluidos en el mismo.

- **Servidor nuevo** — Si realiza la instalación de un servidor nuevo, seleccione Servidor nuevo. Al instalar el servidor, no se eliminan las particiones del sistema ni las de tipo *DOS*, *UNIX** o *Windows*.

El programa de instalación de *NETWARE®* le indica los pasos necesarios para instalar fácilmente un servidor utilizando los valores por defecto. Puede asimismo personalizar la instalación del servidor para incluir opciones más avanzadas.

- **Actualizar** — Si realiza la actualización de un servidor existente a partir de una versión anterior de *NETWARE®*, seleccione Actualizar desde *NETWARE®* 3.1x ó 4.1x. La actualización conserva todos los datos del servidor: archivos, estructuras de directorios, particiones y volúmenes.
- **Directorio de inicio** — El Directorio de inicio se encuentra en la partición de arranque e incluye los archivos necesarios para lanzar el servidor *NETWARE®*.

Aunque los ajustes por defecto sirven para la mayoría de las configuraciones, se pueden especificar opciones avanzadas como el número de ID del servidor, opciones de reorganización y parámetros SET.

2.4.2 OPCIONES AVANZADAS.

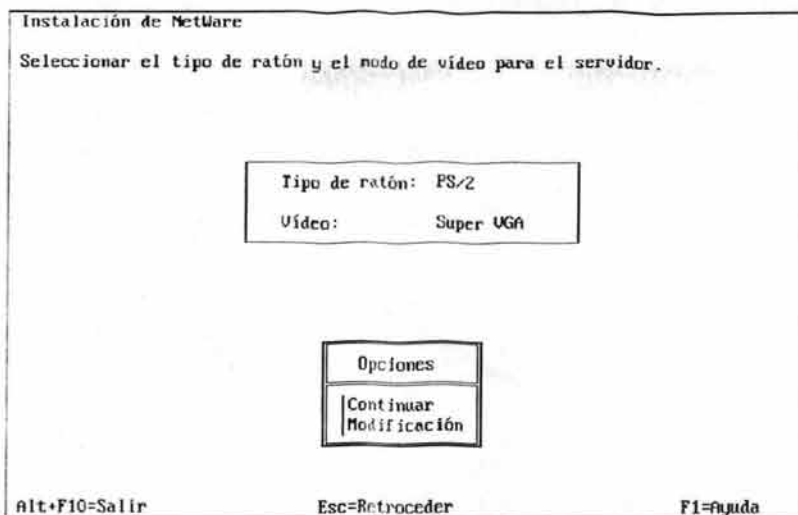
La pantalla Tipo de instalación le permite modificar las opciones por defecto por otras específicas para su entorno de red. Pueden modificarse las siguientes opciones:

- **Número de ID del servidor** — Un número único de identificación del servidor (ocho dígitos hexadecimales como máximo) identifica el servidor en la red.
- **Entorno filtrado** — Los “routers” entre segmentos de red se pueden configurar para enviar datos únicamente desde direcciones de ordenador específicas. Los datos que se envíen desde otras direcciones de ordenador no se reenviarán a otros segmentos.
- **Esquema de numeración** — Algunos administradores de red establecen un esquema de numeración predeterminado para identificar los servidores en ubicaciones u organizaciones particulares. Por ejemplo, todos los servidores del edificio A pueden empezar por 0101 y todos los servidores del edificio B por 0102.
- **Cargar el servidor al reorganizar** — Seleccione No si no desea que los archivos *autoexec.bat* y *config.sys* contengan los comandos que cargan automáticamente el sistema operativo del servidor cuando reorganiza el ordenador. Si se selecciona Sí, se renombran los archivos antiguos *autoexec.bat* y *config.sys* y se guardan con la extensión *.00x*.
- **Parámetros SET del servidor** — Puede que sea necesario modificar los parámetros SET para determinados controladores de dispositivo, como por ejemplo, las tarjetas de red y los dispositivos de almacenamiento, con objeto de poder completar la instalación. Los parámetros SET se guardan en el archivo *startup.ncf*.

2.4.3 SELECCIÓN DEL RATÓN Y LA TARJETA DE VÍDEO.

- **Tipo de ratón** — Seleccione un tipo de ratón si se encuentran disponibles en el ordenador. El programa de instalación admite los tipos de ratón serie y PS/2, aunque no son obligatorios.

- **Tipo de vídeo** — El programa de instalación de NETWARE® está optimizado para ofrecer una visualización con *hardware* de visualización de vídeo compatible con VESA 2. Seleccione Standard VGA únicamente si su tarjeta de vídeo no soporta 256 colores. (figura II.2)

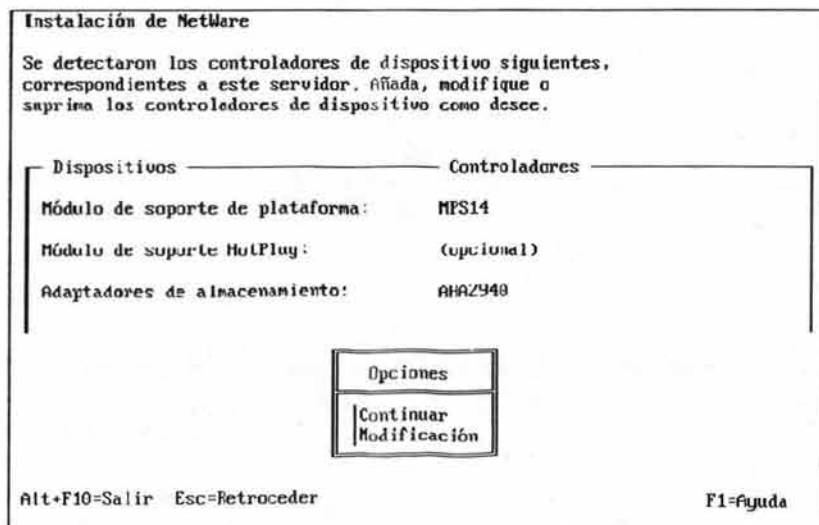


(figura II.2)

2.4.4 SELECCIÓN DE UN MÓDULO DE SOPORTE DE PLATAFORMA Y UN ADAPTADOR DE ALMACENAMIENTO.

Para seleccionar un módulo de soporte de plataforma y un adaptador de almacenamiento, es necesario:

- Seleccionar un módulo de soporte de plataforma (en su caso).
- Seleccionar un módulo *Hot Plug* PCI (en su caso).
- Seleccionar y configurar un adaptador de almacenamiento. (figura II.3)



(figura II.3)

2.4.4.1 SELECCIÓN DE UN MÓDULO DE SOPORTE DE PLATAFORMA (EN SU CASO).

Un módulo de soporte de plataforma (PSM) proporciona mayor rendimiento a los multiprocesadores y a determinadas configuraciones de *hardware*.

El programa de instalación puede detectar automáticamente un PSM. Si el programa no lo detecta, significa que su ordenador no necesita ninguno.

2.4.4.2 SELECCIÓN DE UN MÓDULO HOT PLUG PCI (EN SU CASO).

Los ordenadores que soportan la tecnología *Hot Plug* PCI permiten insertar y extraer adaptadores de almacenamiento y tarjetas de red mientras el ordenador está encendido.

Si el programa de instalación no detecta un módulo de soporte *Hot Plug* PCI, significa que su ordenador probablemente no soporta dicha tecnología.

2.4.4.3 SELECCIÓN DE UN ADAPTADOR DE ALMACENAMIENTO.

Un adaptador de almacenamiento se conecta al ordenador para proporcionar un enlace entre este último y uno o varios dispositivos de almacenamiento. El adaptador de almacenamiento requiere un controlador de software denominado módulo adaptador host (HAM) para comunicarse con el ordenador (host). Los dispositivos de almacenamiento requieren un controlador independiente denominado módulo de dispositivo personalizado (CDM).

Puesto que un único adaptador puede controlar varios dispositivos de almacenamiento, es posible que su ordenador sólo necesite un único HAM, aunque pueda contar con varios tipos de dispositivos – y por tanto con varios CDM.

El programa de instalación detecta automáticamente numerosos tipos de dispositivos de almacenamiento, como por ejemplo los adaptadores IDE y SCSI. Si su adaptador de almacenamiento no se detecta, seleccione el controlador adecuado en la lista de controladores disponibles de NETWARE® 5 o añada uno nuevo desde un disquete. Puede asimismo obtener los HAM del fabricante del adaptador de almacenamiento.

2.4.5 SELECCIÓN DE UN DISPOSITIVO DE ALMACENAMIENTO Y UNA TARJETA DE RED.

Para seleccionar un dispositivo de almacenamiento y una tarjeta de red, es necesario:

- Seleccionar y configurar el dispositivo de almacenamiento.
- Seleccionar y configurar la tarjeta de red.

2.4.5.1 SELECCIÓN DE UN DISPOSITIVO DE ALMACENAMIENTO.

Dispositivos de almacenamiento como discos duros, CD-ROM y cintas requieren un controlador de software para comunicarse con el adaptador de almacenamiento. El controlador de software para el dispositivo de almacenamiento se denomina módulo de dispositivo personalizado (CDM). Cada tipo de dispositivo de almacenamiento requiere un CDM.

El programa de instalación detecta automáticamente numerosos tipos de dispositivos de almacenamiento, como unidades IDE, SCSI, CD-ROM y cintas. Si su dispositivo de almacenamiento no se detecta, seleccione el controlador adecuado en la lista de controladores disponibles de NETWARE® 5 o añada uno nuevo desde un disquete. Los CDM se pueden obtener del fabricante del dispositivo de almacenamiento.

2.4.5.2 SELECCIÓN DE UNA TARJETA DE RED.

Las tarjetas de red, como la tarjeta NE3200™ de NOVELL®, requieren un controlador de software para poder comunicarse con la red. El controlador de software para la tarjeta de red se denomina controlador LAN.

El programa de instalación detecta automáticamente numerosos tipos de tarjetas de red. Si su tarjeta de red no se detecta, seleccione el controlador adecuado en la lista de NETWARE® 5 o añada uno nuevo desde un disquete. (figura II.4)



(figura II.4)

2.4.6 CREACIÓN DE UNA PARTICIÓN DE NETWARE® Y UN VOLUMEN SYS.

Las particiones normalmente se corresponden con los sistemas operativos, como NETWARE®, DOS o UNIX. Las particiones dividen una gran región de almacenamiento en secciones más pequeñas y manejables. Un dispositivo de almacenamiento puede incluir hasta cuatro particiones.

Puede utilizar los volúmenes para dividir las particiones de NETWARE® en secciones más pequeñas. Cada partición de NETWARE® puede tener hasta ocho volúmenes.

Para crear una partición de NETWARE® y un volumen Sys es necesario:

- Eliminar los volúmenes Sys existentes (condición).
- Crear una partición de NETWARE®.
- Crear un volumen Sys.

2.4.6.1 ELIMINACIÓN DE LOS VOLÚMENES SYS EXISTENTES (CONDICIÓN).

Si ya existe un volumen Sys en el servidor, debe sustituirlo al realizar una nueva instalación.

Al eliminar un volumen Sys durante la instalación de un nuevo servidor, debe seleccionar una de las siguientes opciones:

- Sustituir el volumen Sys y su partición NETWARE® — Esta opción eliminará el volumen Sys existente, así como toda la partición NETWARE® que lo incluye. Todos los volúmenes que forman parte de la partición de NETWARE® que contiene el volumen Sys también se eliminarán — aunque el volumen se expanda a otras particiones de NETWARE®.
- Eliminar todos los volúmenes de NETWARE® y las particiones de NETWARE®/NSS — Esta opción elimina todos los volúmenes NETWARE® y todas las particiones NETWARE®/NSS.

Cualquiera de las opciones elimina únicamente las particiones de NETWARE®. Otros tipos de partición, como las de DOS, UNIX o de utilidades / sistema, no se eliminarán.

2.4.6.2 CREACIÓN DE UNA PARTICIÓN NETWARE®

Durante las primeras etapas de la instalación, el programa le indicará los pasos necesarios para crear una única partición de NETWARE® que incluya el volumen Sys.

Tamaño de la partición de NETWARE® — Todo el espacio disponible del dispositivo de almacenamiento se asigna a la partición de NETWARE® a no ser que se modifique el tamaño.

Hot Fix™ es la característica de protección de datos de NETWARE® optimizada para su dispositivo de almacenamiento. Hot Fix mantiene una lista de áreas defectuosas en el dispositivo de almacenamiento y redirige los datos desde ubicaciones defectuosas a otras más seguras.

2.4.6.3 CREACIÓN DEL VOLUMEN SYS.

El sistema operativo NETWARE® 5 requiere un volumen de al menos 350 MB (figura II.5) denominado Sys. Aunque el sistema operativo sólo requiere 350 MB, el volumen Sys debe ser lo suficientemente amplio como para incluir todos los productos de NETWARE® que se van a instalar. (figura II.6)

Tamaño del volumen Sys

Productos de NetWare 5	Tamaño mínimo del volumen Sys
Sistema operativo NetWare 5	350 MB
NetWare 5 con los productos por defecto	450 MB
NetWare 5 con todos los productos	550 MB
NetWare 5 con todos los productos y la documentación	700 MB

(figura II.5)

Instalación de NetWare

Crear una partición NetWare y un volumen SYS.

Propiedades de la partición y del volumen SYS	
Dispositivo:	SEAGATE ST32171W rev:04R4 IU312-A0-D0:01
Tamaño de la partición de NetWare (MB):	1992.4
Tamaño de Hot Fix (MB):	4.0
Tamaño del volumen SYS (MB):	1988
NOTA: pulse F1 para ver las recomendaciones sobre el tamaño. Para las particiones NSS, deje en el disco espacio sin partición	

Opciones

Continuar
Modificación

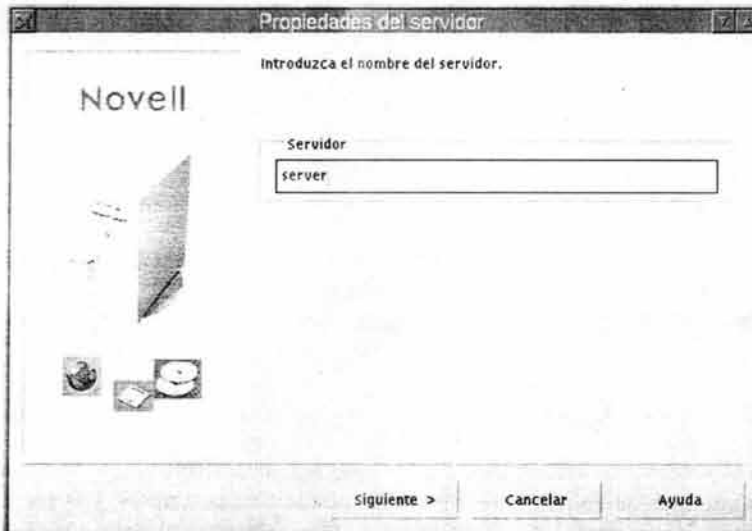
Alt+F10=Salir F1=Ayuda

(figura II.6)

2.4.7 ASIGNE UN NOMBRE AL SERVIDOR NETWARE® 5.

El nombre del servidor NETWARE® 5 debe ser distinto de todos los demás servidores del árbol NDS. El nombre puede contener entre 2 y 47 caracteres alfanuméricos e incluir guiones bajos y rayas, pero no espacios. El primer carácter no puede ser un punto.

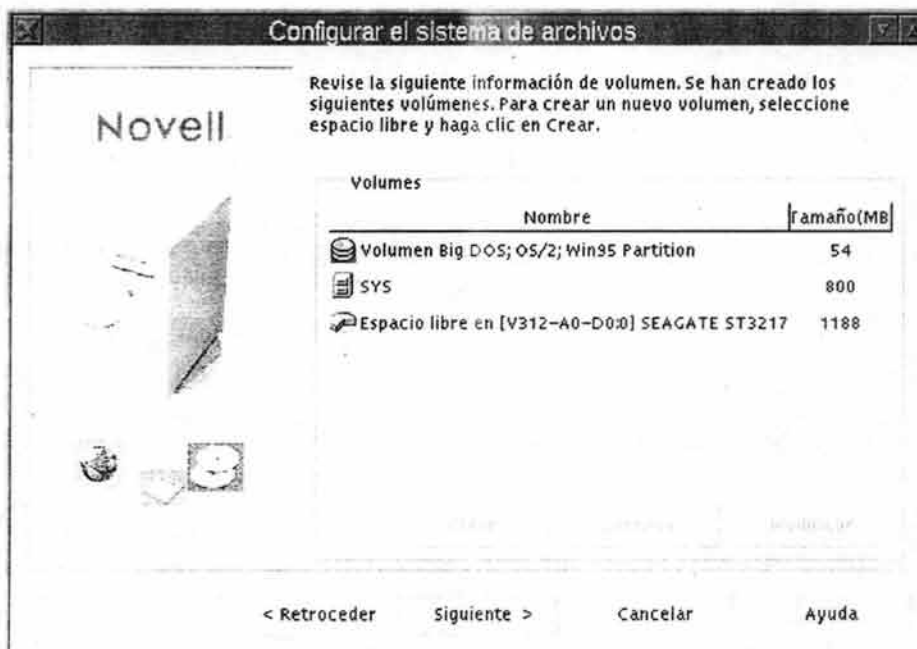
El nombre del servidor no puede ser igual que el nombre que vaya a utilizar para el árbol NDS. (figura II.7)



(figura II.7)

2.4.8 INSTALACIÓN DEL SISTEMA DE ARCHIVOS DEL SERVIDOR NETWARE®.

El servidor debe disponer ahora de una única partición NETWARE® y un único volumen denominado Sys. Si dispone de suficiente espacio para crear particiones y volúmenes adicionales, puede crearlos ahora. (figura II.8)



(figura II.8)

Al instalar el sistema de archivos NETWARE®, se puede:

- Crear volúmenes adicionales.
- Modificar volúmenes.
- Eliminar volúmenes.

Los volúmenes le permiten subdividir las particiones en secciones más manejables. Se pueden crear dos tipos de volúmenes – volúmenes tradicionales o volúmenes de los Servicios de almacenamiento de NOVELL® (NSS).

- Volumen tradicional de NETWARE® — El volumen de tipo tradicional de NETWARE® soporta todas las tecnologías de volúmenes de NETWARE®, incluida la subasignación, la compresión y el Sistema de seguimiento de transacciones (*Transaction Tracking System*™, TTS™).

- Volumen NSS — El NSS es una avanzada tecnología de sistema de archivos que mejora la gestión de los archivos y volúmenes extensos, los espacios de nombre y los dispositivos de almacenamiento. El tiempo necesario para montar volúmenes extensos se reduce significativamente gracias a los NSS.

2.4.8.1 CREACIÓN DE VOLÚMENES.

Se pueden crear volúmenes adicionales desde cualquier dispositivo de almacenamiento que tenga espacio disponible. Los nombres de volumen pueden tener entre 2 y 15 caracteres. Los caracteres válidos son de la A a la Z, del 0 al 9 y los caracteres _ ! - @ # \$ % & (). El nombre de volumen no puede empezar por un guión bajo ni tener dos o más guiones bajos consecutivos.

Es posible dividir un disco extenso en varios volúmenes durante la instalación. De forma inversa, un volumen se puede distribuir en varios discos.

Los volúmenes tradicionales pueden crearse a partir de espacio libre tradicional o sin particionar. Ambos tipos de espacio libre aparecen de la misma forma en la pantalla del Sistema de archivos de NETWARE®.

Para crear un volumen tradicional: Seleccione espacio libre y haga clic en Crear. Introduzca el nombre del volumen y haga clic en Aceptar. Para asignar sólo una parte del espacio libre al volumen, introduzca la cantidad que desea utilizar y haga clic en Aplicar al volumen.

Para que el volumen incluya espacio libre adicional, seleccione espacio libre adicional, introduzca la cantidad que desea utilizar y haga clic en Aplicar al volumen. Los volúmenes NSS pueden crearse a partir de espacio libre sin particionar.

Para crear un volumen NSS: Seleccione espacio libre y haga clic en Crear. (Si la opción Tipo de volumen no se encuentra disponible, el espacio libre seleccionado no está disponible para los NSS. Vuelva a la pantalla anterior y seleccione otro espacio libre.) Seleccione el tipo de volumen NSS. Introduzca el nombre del volumen y haga clic en Aceptar.

Para asignar sólo una parte del espacio libre al volumen, introduzca la cantidad que desea utilizar y haga clic en Aplicar al volumen. Para asignar más espacio libre a un volumen, seleccione espacio libre adicional, introduzca la cantidad que desea utilizar y haga clic en Aplicar al volumen. (figura II.9)



(figura II.9)

2.4.8.2 MODIFICACIÓN DE VOLÚMENES.

El tamaño de cualquier volumen existente puede aumentarse, pero no disminuirse. Para reducir el tamaño de un volumen existente, éste debe eliminarse y crearse de nuevo.

2.4.8.3 ELIMINACIÓN DE VOLÚMENES.

Puede eliminar cualquier volumen que haya creado excepto el volumen Sys. Cuando se elimina un volumen, todos los datos incluidos en el mismo se pierden.

2.4.9 INSTALACIÓN DE PROTOCOLOS DE RED.

NETWARE® 5 puede procesar paquetes de red IP y paquetes IPX tradicionales. Puede instalar protocolos de red de las siguientes formas:

- IP con el modo de compatibilidad IPX.
- Protocolo Internet (IP) exclusivamente.
- Internetwork Packet Exchange (IPX) exclusivamente.
- IP e IPX.

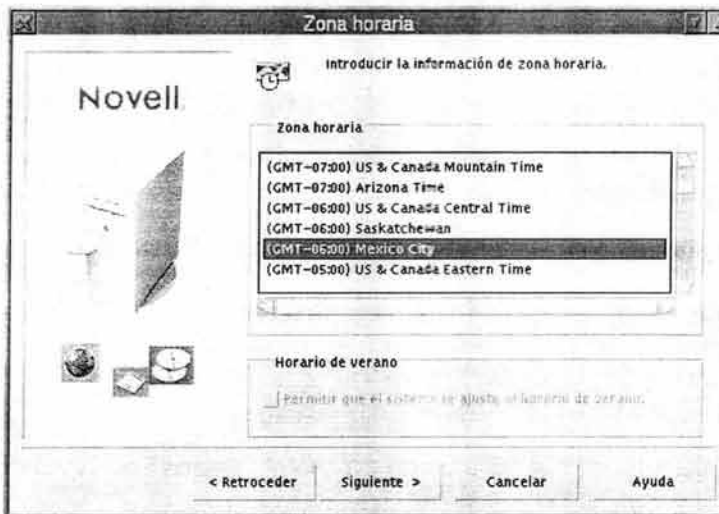
Los protocolos se asignan a las tarjetas de red. Ambos protocolos pueden asignarse a una única tarjeta de red, lo que permite al servidor comunicarse utilizando IP e IPX. (figura II.10)



(figura II.10)

2.4.10 AJUSTE DE LA ZONA HORARIA DEL SERVIDOR.

La hora y zona horaria del servidor son importantes para poder sincronizar las actividades de la red. Las opciones avanzadas de la sincronización horaria se encuentran disponibles durante la etapa de personalización de la instalación. (figura II.11)



(fig. II.11)

2.4.11 CONFIGURACIÓN DE NDS, LA TECNOLOGÍA DE DIRECTORIOS DE NOVELL®.

NDS, la tecnología del directorio de NOVELL®, proporciona un acceso global a todos los recursos de la red. Permite a los usuarios de la red que dispongan de los derechos adecuados como entrar en la red, visualizar y tener acceso a los recursos.

Los recursos de red tales como los servidores y las impresoras se presentan jerárquicamente en un árbol NDS. Los usuarios pueden entrar en el árbol NDS con un nombre de entrada y una contraseña únicos en lugar de entrar en servidores específicos.

2.4.12 SELECCIÓN DEL TIPO DE NDS.

Para configurar los NDS, debe escoger una de las opciones siguientes:

- Instalar el servidor en un árbol NDS existente.
- Crear un nuevo árbol NDS. (figura II.12)



(figura II.12)

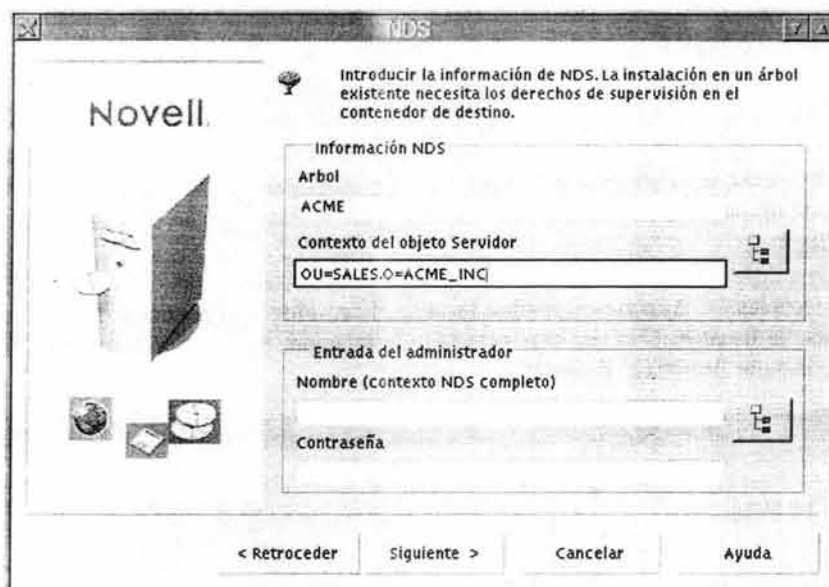
2.4.12.1 INSTALACIÓN DEL SERVIDOR EN UN ÁRBOL NDS EXISTENTE.

La instalación del servidor en un árbol NDS existente incorpora el servidor a la red.

El servidor puede instalarse en cualquier contenedor Organización (O) o Unidad administrativa (OU) del árbol NDS para el que disponga de derechos de supervisión. Se pueden crear contenedores durante la instalación. Se le solicitará que entre y proporcione el contexto, el nombre de usuario y la contraseña para el usuario con derechos de supervisión para el contenedor.

Si se trata del primer servidor NETWARE® 5 que se instala en un árbol NDS con servidores NETWARE® 4.1 x. se le solicitará que modifique el esquema. Cuando así se le solicite, deberá proporcionar el nombre del administrador y la contraseña para todo el árbol NDS. Para modificar el esquema NDS se necesitan derechos de supervisión en la raíz del árbol NDS existente.

Todos los servidores de archivos NETWARE® 4.1 x deben disponer de DS.NLM versión 5.99 o posterior. (figura II.13)



(fig. II.13)

2.4.12.2 CREACIÓN DE UN NUEVO ÁRBOL NDS.

Cree un nuevo árbol si está instalando una nueva red o si este servidor requiere un árbol NDS independiente. Los recursos del nuevo árbol sólo estarán disponibles para los usuarios que hayan entrado en él.

Cada árbol NDS debe tener un nombre distinto de los demás árboles NDS de la red. Se le solicitará asimismo que cree un usuario (cuyo nombre por defecto será ADMIN) con derechos de supervisión, que identifique un contexto NDS y que asigne una contraseña.

Ha creado un nuevo árbol NDS o instalado el servidor en un árbol NDS existente. El objeto Servidor NETWARE® y los objetos Volumen se instalarán en el contenedor que haya especificado.

Si ha creado un nuevo árbol NDS, se creará un usuario (cuyo nombre por defecto será ADMIN) con derechos de supervisión para el árbol NDS en el mismo contenedor que el objeto Servidor NETWARE®. (figura II.14)

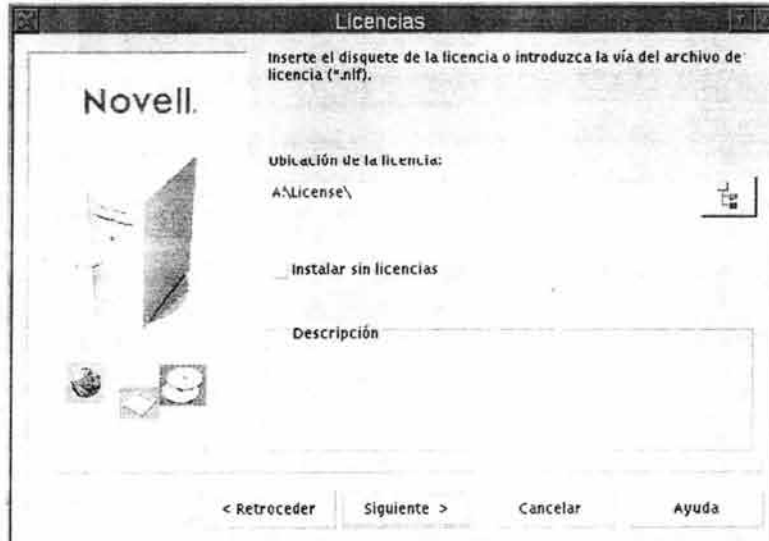


(fig. II.14)

2.4.13 ASIGNACIÓN DE LICENCIA AL SERVIDOR NETWARE®.

NETWARE® 5 debe contar con una licencia válida para poder funcionar como un servidor. Puede instalar la licencia desde el disquete de licencia de NETWARE® 5 o examinar un directorio que contenga las licencias de NETWARE® 5.

Instalar sin licencias — Aunque es posible instalar el servidor sin una licencia, éste sólo permitirá realizar dos conexiones de usuario. Una vez completada la instalación, puede usar la utilidad Administrador de NETWARE® para instalar licencias. (figura II.15)



(figura II.15)

2.4.14 INSTALACIÓN DE OTROS PRODUCTOS DE RED.

Una vez realizada la parte de instalación correspondiente al servidor NETWARE®, puede seleccionar otros productos de red para instalarlos. Dichos productos proporcionan funciones mejoradas a NETWARE® 5, como la gestión de la red y el acceso a Internet.

Para instalar un producto: Marque la casilla de verificación situada al lado del producto que desea instalar.

Aunque puede escoger los productos que desea instalar, si instala aquellos que están seleccionados por defecto tendrá la seguridad de que contará con las características recomendadas para NETWARE®. (figura II.16)



(figura II.16)

2.4.15 INSTALACIÓN DE LA ESTACIÓN DE TRABAJO.

Para la instalación de la estación de trabajo hay que tener en cuenta el sistema operativo disponible en cada una de ellas, ya que se pueden dar tres opciones:

- Cliente para Windows 95/98.
- Cliente para Windows NT.
- Cliente para *DOS* y Windows 3.x.

En esta caso se va a considerar que todas las estaciones tienen instalado Windows 95/98 y, por tanto, se va a utilizar dicho cliente.

2.4.15.1 INSTALACIÓN DEL CLIENTE NOVELL® PARA WINDOWS 95/98.

El cliente NOVELL® para Windows 95/98 es incompatible con los siguientes componentes de Microsoft.

- Cliente Microsoft para redes NETWARE®.
- Compartir impresoras y archivos para redes NETWARE®.
- Servicio para Servicios de directorio NOVELL®.
- NOVELL® NETWARE® (“shell” de estación de trabajo 3.x).
- NOVELL® NETWARE® (“shell” de estación de trabajo 4.0 o superior).
- Protocolo NOVELL® IPX ODI.

Estos componentes causan conflicto con el cliente NOVELL® para Windows 95/98. Si está instalado alguno de dichos componentes, el programa de instalación detectará el conflicto y lo eliminará.

El cliente NOVELL® para Windows 95/98 soporta IP e IPx/SPX y puede coexistir con NetBEUI

Por tanto, pueden instalarse los protocolos de tres maneras:

- IP sólo.
- IP + IPX.
- IPX sólo.

Antes de proceder a la instalación del cliente NOVELL® para Windows 95/98 en cada estación de trabajo, han de estar instaladas y funcionando correctamente las tarjetas de red (se puede ver desde el icono Sistema del Panel de control) y unidas por el cable correspondiente.

Para proceder a la instalación del cliente en la estación de trabajo, siga los pasos siguientes:

- Como se debe efectuar la instalación desde un CD-ROM, es necesario que la estación de trabajo cuente con uno (aunque sea portátil) perfectamente instalado o tener acceso a un CD-ROM compartido de otra estación de trabajo.
- Inserte el CD titulado NOVELL® Client Software de NETWARE® 5 en el lector de CD-ROM.
- Verá la pantalla inicial (en caso de instalarse desde una unidad CD-ROM remota, acceda desde Entorno de red al CD-ROM compartido, sitúese en el directorio raíz, vaya a la unidad correspondiente y ejecute el archivo WINSETUP.EXE).
- Seleccione el idioma en que va a realizar la instalación del cliente y aparecerá otra pantalla en donde deberá escoger Cliente Windows 95/98.
- Seleccione Instalación del Cliente NOVELL® y aparecerán los términos de la licencia.
- Cuando haya leído los términos de la licencia, marque en SI para aceptarlos y verá una pantalla para que escoja las opciones de instalación.
- Podrá escoger entre dos opciones para continuar la instalación:
 - Típica. Esta opción hace que el cliente se instale y configure con los valores por defecto (es válida para casi todos los ordenadores).
 - Personalizada. Esta opción permite seleccionar los componentes a instalar y su configuración (es válida para administradores de red y usuarios avanzados).
- Comenzará el proceso de instalación y se copiarán los archivos necesarios para el cliente NOVELL® para Windows 95/98.
- Si es la primera vez que lo instala en esa estación, le mostrará una pantalla indicándole que es aconsejable que defina un árbol preferente y un contexto de nombre o un servidor preferente que serán los datos correspondientes del servidor al que desea conectarse por defecto. Marque en SI para indicarlo.
- Indique el nombre del servidor y del árbol preferente y el contexto de nombre al que desea conectarse. Cuando haya finalizado, marque en Aceptar.
- Al finalizar la instalación, marque en Reiniciar para que se realicen los cambios y poder conectarse con el servidor.

Ahora, si ya está preparado el servidor, al arrancar la estación de trabajo, se iniciará automáticamente

la conexión mostrando una pantalla para que indique el nombre del usuario y su contraseña.

Si al realizar la instalación no indicó el nombre del servidor, del árbol y del contexto, marque en Avanzadas y podrá indicarlo.

Cuando haya finalizado, marque en Aceptar y se realizará la conexión con el servidor.”³

2. 5 CONSOLE ONE®.

“ConsoleOne® es una herramienta basada en Java para gestionar la red y sus recursos. Por defecto, permite gestionar:

- Objetos, esquemas, particiones y duplicados NDS.
- Recursos del servidor NETWARE®.

Si instala otros productos NOVELL®, se integrarán automáticamente funciones adicionales a ConsoleOne®. Por ejemplo, si instala NDS 8, la función para configurar la interfase LDAP a NDS se integrará automáticamente en ConsoleOne®.

2. 5.1 ¿POR QUÉ DEBERÍA UTILIZAR CONSOLEONE®?.

NOVELL® ha diseñado ConsoleOne® como una herramienta de gestión única y sigue trabajando para mejorar sus funciones y su rendimiento de modo que no sean necesarias las herramientas de legado como el Administrador de NETWARE®. A continuación encontrará algunas de las ventajas de ConsoleOne® sobre las herramientas de legado. Después de las ventajas, también se enumeran unas cuantas limitaciones.

Ventaja	Explicación
Utilización en un ordenador Windows o en un servidor NETWARE®	Como ConsoleOne® se basa en Java, se puede ejecutar en Windows, NETWARE®, Linux o Solaris. Las herramientas de legado Administrador de NETWARE®, Gestor de NDS™ y Gestor de esquemas sólo se ejecutan en Windows.
Gestión de los últimos productos NOVELL®	ConsoleOne® permite gestionar los últimos productos y mejoras de NOVELL®, mientras que el Administrador de NETWARE® y otras herramientas de legado no se han actualizado para ello. Por ejemplo, sólo ConsoleOne® puede administrar DirXML, <i>Single Sign-On</i> y Servidor de certificados.
Exploración de grandes árboles NDS	Si el árbol ejecuta NDS 8 y posee contenedores con miles de objetos, ConsoleOne® permite una exploración más rápida y más coherente. El Administrador de NETWARE® es más lento, ya que abre contenedores grandes y está limitado por la RAM disponible.
Acceso a recursos NDS mediante la federación DNS	Si un árbol ejecuta NDS 8.5 y se configura para federación DNS, ConsoleOne® permite acceder a contextos de dicho árbol tanto si entra en el mismo como sino. Esto permite tratar múltiples árboles NDS como un sólo sistema para asignar derechos y pertenencias a grupos. Ninguna herramienta de legado posee esta función.
Creación de duplicados NDS con filtro	Si el árbol ejecuta NDS 8.5, ConsoleOne® permite crear duplicados con filtro que sólo contienen los objetos y las propiedades necesarias para sincronizar con aplicaciones concretas, como por ejemplo PeopleSoft®. Ninguna herramienta de legado posee esta función.
Generar informes NDS	ConsoleOne® permite generar informes sobre objetos, usuarios, grupos y seguridad NDS. Ninguna herramienta de legado posee estas funciones.
Creación de todo tipo de objetos NDS	ConsoleOne® permite crear cualquier tipo de objeto definido en el esquema del árbol NDS, incluido los tipos personalizados que haya añadido. El Administrador de NETWARE® sólo puede crear tipos de objetos de los que posean módulos integrables.

³ Netware® 5.1. En línea [URL], <http://www.NOVELL.com/documentation/spanish/nw51/docui/index.html>

ConsoleOne también posee unas cuantas limitaciones en comparación con las herramientas delegado. La mayoría de ellas desaparecerán en las siguientes versiones.

Limitación	Explicación
No puede gestionar los servicios de impresión	Por ahora, deberá utilizar el Administrador de NETWARE® para gestionar los servicios de impresión de red.
No puede reparar NDS de forma remota ni comprobar la continuidad de partición	Por ahora, deberá utilizar la herramienta de legado Gestor de NDS para reparar NDS de forma remota en servidores específicos, para comprobar la continuidad de la partición o para cancelar una operación de partición iniciada por otro administrador.
No puede generar informes de esquema NDS	Por ahora, deberá utilizar la herramienta de legado Gestor de esquemas para generar informes del esquema del árbol NDS, a no ser que diseñe sus propios formatos de informe para generar informes de esquema en ConsoleOne®.
No puede crear ni ejecutar guiones de configuración de usuario nuevos.	ConsoleOne® permite crear todos los aspectos de las plantillas de usuario, excepto los guiones de configuración. Además, ConsoleOne® no puede ejecutar un guión de configuración al crear una cuenta de usuario nueva desde una plantilla. Deberá utilizar el Administrador de NETWARE® para realizar estas tareas.

2. 5.2 INSTALACIÓN E INICIO DE CONSOLEONE®.

Si instala ConsoleOne® en un servidor NETWARE®, puede ejecutarlo localmente en dicho servidor o remotamente en un ordenador Windows mediante una unidad asignada a dicho servidor.

Instalar ConsoleOne® en un servidor NETWARE® también permite a otros productos NOVELL®, como por ejemplo NDS, añadir los módulos integrables necesarios para la instalación.

2. 5.3 REQUISITOS DEL SISTEMA PARA NETWARE®.

Sistema operativo	NETWARE® 5 Support Pack 3 o posterior
Procesador	Recomendado: 200 MHz o más rápido
Espacio de disco	38 MB
Resolución de pantalla	Mínimo: 800 x 600 con 256 colores (necesarios sólo para ejecutar localmente en el servidor)

2.5.4 INSTALACIÓN DE CONSOLEONE® EN NETWARE®.

- Desactive Java y cualquier aplicación Java que se esté ejecutando en el servidor, incluida la GUI del servidor. Puede hacerlo escribiendo JAVA -EXIT en el indicador de la consola.
- Pida a todos los usuarios que actualmente estén ejecutando ConsoleOne® de forma remota mediante una conexión al servidor que salgan de sus sesiones de ConsoleOne®.
- En una estación de trabajo Windows, asigne una letra de unidad a la raíz del volumen SYS del servidor.

- En la misma estación de trabajo, inserte el CD que contiene ConsoleOne®.
- Explore el CD hasta que encuentre los paquetes ConsoleOne® disponibles > seleccione el paquete para Windows/NETWARE®
- Si está utilizando un CD que ejecuta un programa de instalación y observa una opción instalar sólo ConsoleOne®, seleccione dicha opción.
- Ejecute el archivo ejecutable de instalación (SETUP.EXE o CONSOLEONE.EXE).
- Siga las instrucciones de la pantalla para completar la instalación. Cuando solicite la ubicación donde instalarlo, seleccione la unidad asociada a la raíz del volumen SYS del servidor.

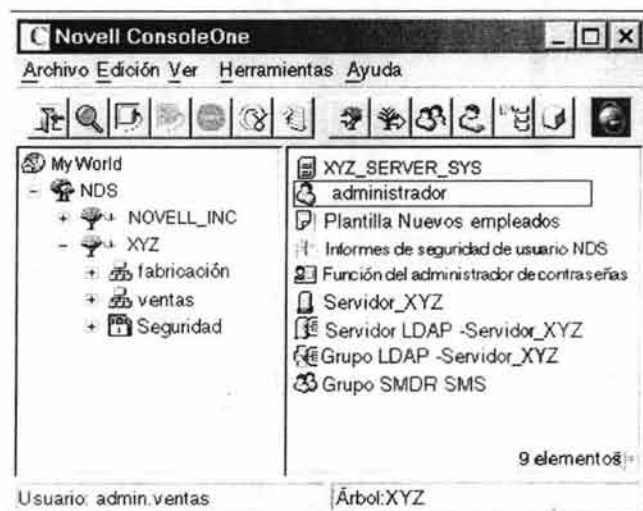
2. 5. 5 INICIACIÓN DE CONSOLEONE® EN NETWARE®.

Para iniciar ConsoleOne® localmente en un servidor NETWARE®, entre a C1START en el indicador de la consola.

2.6 FUNDAMENTOS DE ADMINISTRACIÓN.

En ConsoleOne®, se presenta la red y sus recursos como un conjunto de objetos que están organizados en varios contenedores, con Mi mundo en la parte superior. Utilice el panel izquierdo para expandir y comprimir contenedores. Utilice el panel derecho para trabajar con recursos específicos.

En general, las tareas de administración se efectúan examinando un objeto, haciendo clic en él con el botón derecho del ratón y seleccionando una acción. Las acciones disponibles dependen del tipo del objeto. Por ejemplo, la acción Objeto Nuevo sólo está disponible en contenedores. (figura II.17)



(figura II.17)

2.6.1 ORGANIZACIÓN DE OBJETOS EN CONTENEDORES.

Una vez que se encuentre en un árbol NDS, puede organizarlo creando varios tipos de contenedores y colocando objetos en los mismos. La seguridad de los objetos de un contenedor es automáticamente equivalente a la del contenedor; por tanto, asegúrese de gestionar los derechos al contenedor de acuerdo con esto. Puede crear alias para proporcionar acceso a un sólo objeto desde múltiples contenedores.

A continuación encontrará procedimientos para crear tipos de contenedores y alias comunes.

2.6.2 CREACIÓN DE UN OBJETO ORGANIZACIÓN.

- Haga clic con el botón derecho en el árbol o el Objeto País en que desea crear el objeto Organización > haga clic en Nuevo > Objeto.
- En Clase, seleccione Organización > haga clic en Aceptar.
- En Nombre, introduzca un nombre de hasta 64 caracteres. Asegúrese de que utiliza las convenciones de nombrado correctas.
- Si desea asignar valores de propiedades adicionales como parte del proceso de creación para el contenedor, seleccione Definir propiedades adicionales.
- Por ejemplo, puede crear un guión de entrada o configurar la detección de intrusos para el contenedor.
- Haga clic en Aceptar.

2.6.3 CREACIÓN DEL OBJETO UNIDAD ADMINISTRATIVA.

- Haga clic con el botón derecho del ratón en el objeto Organización o Unidad administrativa en el que desea crear el nuevo objeto Unidad administrativa > haga clic en Nuevo > Unidad administrativa.
- En Nombre, introduzca un nombre de hasta 64 caracteres. Asegúrese de que utiliza las convenciones de nombrado correctas.
- Si desea asignar valores de propiedades adicionales como parte del proceso de creación para el contenedor, seleccione Definir propiedades adicionales.
- Por ejemplo, puede crear un guión de entrada o configurar la detección de intrusos para el contenedor.
- Haga clic en Aceptar.

2.6.4 CREACIÓN DE UN OBJETO LOCALIDAD.

- Haga clic con el botón derecho del ratón en el objeto País, Organización o Unidad Administrativa en el que desea crear el objeto Localidad > haga clic en Nuevo > Objeto.
- En Clase, seleccione Localidad > haga clic en Aceptar.
- Rellene los campos Nombre y Nombrado por. Haga clic en Ayuda para obtener detalles.
- Haga clic en Aceptar.

2.6.5 CREACIÓN DE UN OBJETO PAÍS.

- Haga clic con el botón derecho del ratón en el objeto de árbol > haga clic en Nuevo > Objeto.
- En Clase, seleccione País > haga clic en Aceptar.
- En Nombre, introduzca el código de país ISO de dos letras. Haga clic en Ayuda para obtener detalles.

- Ejemplo: FR para Francia
- Si desea asignar valores de propiedades adicionales como parte del proceso de creación para el contenedor, seleccione Definir propiedades adicionales.
- Por ejemplo, puede proporcionar un nombre más descriptivo para el país.
- Haga clic en Aceptar.

2.6.6 CREACIÓN DE UN ALIAS PARA UN OBJETO.

- Haga clic con el botón derecho del ratón en el contenedor en que desea crear el alias > haga clic en Nuevo > Objeto.
- En Clase, seleccione Alias > haga clic en Aceptar.
- En Nombre, introduzca un nombre de hasta 64 caracteres. Asegúrese de que utiliza las convenciones de nombrado correctas.
- Haga clic en el botón Examinar situado al lado del campo Objeto > seleccione el objeto al que desea que represente el alias > haga clic en Aceptar.
- Si desea asignar valores de propiedades adicionales como parte del proceso de creación para el alias, seleccione Definir propiedades adicionales.
- Haga clic en Aceptar.

2.7 GESTIÓN DE CUENTAS DE USUARIO.

Configurar una cuenta de usuario NDS conlleva la creación de un objeto Usuario y la configuración de propiedades para controlar la entrada y el entorno informático de la red del usuario. Puede utilizar un objeto Plantilla para facilitar estas tareas.

Puede crear guiones de entrada para que los usuarios se conecten automáticamente a los archivos, impresoras y otros recursos de red necesarios para entrar. Si varios usuarios utilizan los mismos recursos, puede situar los comandos del guión de entrada en un contenedor y los guiones de entrada de perfil.

2.7.1 CREACIÓN DE CUENTAS DE USUARIO.

Una cuenta de usuario es un objeto Usuario del árbol NDS. Un objeto Usuario especifica el nombre de entrada de un usuario y proporciona información adicional utilizada por NDS y NETWARE® para controlar el acceso del usuario a los recursos de la red. Si lo desea, puede definir propiedades de usuario por adelantado en una plantilla, antes de crear realmente el objeto Usuario.

2.7.1.1 CREACIÓN DE UN OBJETO USUARIO.

- Haga clic con el botón derecho del ratón en el contenedor en que desea crear el objeto Usuario > haga clic en Nuevo > Usuario. (figura II.18)



- Rellene el recuadro de diálogo Usuario nuevo. Haga clic en Ayuda para obtener detalles.
 - Para aplicar una plantilla durante la creación del objeto Usuario, seleccione Utilizar plantilla.
 - Para definir propiedades de usuario adicionales durante la creación del objeto Usuario, seleccione Definir propiedades adicionales.
- Haga clic en Aceptar.
- Si aparece el recuadro de diálogo Definir contraseña, defina la contraseña de entrada del usuario > haga clic en Aceptar.

2.7.1.2 CREACIÓN DE UNA PLANTILLA DE USUARIO.

- Haga clic con el botón derecho del ratón en el contenedor en que desea crear el objeto Plantilla > haga clic en Nuevo > Objeto.
- En Clase, seleccione Plantilla > haga clic en Aceptar.
- Rellene el recuadro de diálogo Plantilla nueva. Haga clic en Ayuda para obtener detalles.
 - Para clonar un objeto Usuario o plantilla existente, seleccione Utilizar plantilla o usuario.
 - Para definir las propiedades de la plantilla inmediatamente después de crear el objeto Plantilla, seleccione Definir propiedades adicionales. Después de pulsar Aceptar, verá páginas de propiedades con un aspecto similar al de las de un objeto Usuario. Hay ayuda disponible en todas las páginas de propiedades.
- Haga clic en Aceptar.

2.7.2 CONFIGURACIÓN DE CARACTERÍSTICAS DE CUENTAS OPCIONALES.

Después de crear un objeto Usuario, tiene la opción de configurar el entorno informático de red del usuario, implementar características de seguridad de entrada adicionales y configurar una estimación sobre el uso del servidor NETWARE® del usuario.

2.7.2.1 CONFIGURACIÓN DE UN ENTORNO INFORMÁTICO DE RED DEL USUARIO.

- Haga clic en el objeto Usuario o Plantilla para el cual desee configurar el entorno informático de red > haga clic en Propiedades. (Utilice un objeto Plantilla si aún no ha creado el objeto Usuario.)
- En la pestaña General, seleccione la página Entorno.
- Complete la página de propiedades. Haga clic en Ayuda para obtener detalles.
- Haga clic en Aceptar.

2.7.2.2 CONFIGURACIÓN DE SEGURIDAD DE ENTRADA ADICIONAL PARA UN USUARIO.

- Haga clic con el botón derecho en el objeto Usuario o plantilla para el que desea configurar la seguridad de entrada > haga clic en Propiedades. (Utilice un objeto Plantilla si aún no ha creado el objeto Usuario.)
- En la pestaña Restricciones, rellene las páginas de propiedades que desee. Haga clic en Ayuda para obtener detalles sobre cualquier página.
- Haga clic en Aceptar.
- Para configurar la detección de intrusos para todos los objetos usuario de un contenedor:
 - Haga clic con el botón derecho del ratón en el contenedor > haga clic en Propiedades.
 - En la pestaña General, seleccione la página Detección de intrusos.
 - Rellene la página de propiedades. Haga clic en Ayuda para obtener detalles.
 - Haga clic en Aceptar.

2.7.2.3 CONFIGURACIÓN DE UNA ESTIMACIÓN DEL USO DEL SERVIDOR NETWARE® DE UN USUARIO.

- Haga clic con el botón derecho en el objeto Usuario o Plantilla para el que desea configurar la contabilidad > haga clic en Propiedades. (Utilice un objeto Plantilla si aún no ha creado el objeto Usuario.)
- En la pestaña Restricciones, seleccione la página Saldo de la cuenta.
- Rellene la página de propiedades. Haga clic en Ayuda para obtener detalles.
- Haga clic en Aceptar.
- Utilice el Administrador de NETWARE® para configurar uno o más servidores NETWARE® en los que se puedan cargar los servicios de la red. Consulte la ayuda en línea del Administrador de NETWARE® para obtener detalles.

2.7.3 CONFIGURACIÓN DE GUIONES DE ENTRADA.

Un guión de entrada es una lista de comandos que se ejecuta cuando un usuario se conecta. Se utiliza habitualmente para conectar al usuario con recursos de red, como archivos e impresoras. Los guiones de entrada se ejecutan en la estación de trabajo del usuario con el siguiente orden:

- Guión de entrada de contenedor.
- Guión de entrada de perfil.
- Guión de entrada de usuario.

Durante la entrada, si el sistema no encuentra ninguno de estos guiones de entrada, pasa al siguiente de la lista. Si no se encuentra ninguno, el sistema ejecuta un guión por defecto que asocia una unidad de búsqueda a la carpeta SYS:PUBLIC del servidor por defecto del usuario. El servidor por defecto se establece en la página de propiedades Entorno del objeto Usuario.

2.7.3.1 CREACIÓN DE UN GUIÓN DE ENTRADA.

- Haga clic con el botón derecho del ratón en el objeto en el que desee crear el guión de entrada > haga clic en Propiedades.
- En la página Guión de entrada, entre los comandos de guión de entrada que desee.
- Haga clic en Aceptar.
- Si ha creado el guión de entrada en un objeto Perfil, asigne el perfil a los usuarios que desee tal como se explica a continuación.

2.7.3.2 ASIGNACIÓN DE UN PERFIL A UN USUARIO.

- Haga clic con el botón derecho en el objeto Usuario o Plantilla para el que desea asignar el perfil > haga clic en Propiedades. (Utilice un objeto Plantilla si aún no ha creado el objeto Usuario.)
- En la página Guión de entrada, haga clic en el botón Examinar situado al lado del campo Perfil > seleccione el objeto Perfil > haga clic en Aceptar.
- Haga clic en Aceptar.
- Asegúrese de que el usuario tenga en efecto el derecho de Examinación para el objeto Perfil y el derecho de Lectura para la propiedad Guión de entrada del objeto Perfil.

2.7.4 RESTRICCIONES DE HORA DE ENTRADA PARA USUARIOS REMOTOS.

En la página de propiedades Restricciones de hora de un objeto Usuario, puede limitar el horario de acceso a NDS del usuario. (Por defecto, no existen limitaciones horarias de entrada.) Si configura una restricción horaria de entrada y el usuario se ha conectado llegada la hora, el sistema emitirá una advertencia para salir en cinco minutos. Si al cabo de cinco minutos el usuario aún está conectado, se desconectará automáticamente y perderá todo el trabajo no guardado.

Si un usuario entra de forma remota desde una zona horaria distinta a la del servidor que procesa la petición de entrada, cualquier restricción horaria de entrada establecida para el usuario no se ajustará a la diferencia horaria. Por ejemplo, si restringe la entrada a un usuario los lunes de 1:00 a.m. a 6:00 a.m. y el usuario entra remotamente desde una zona horaria con una diferencia de una hora más que la del servidor, la restricción se hará efectiva de 2:00 a.m. a 7:00 a.m. para dicho usuario.

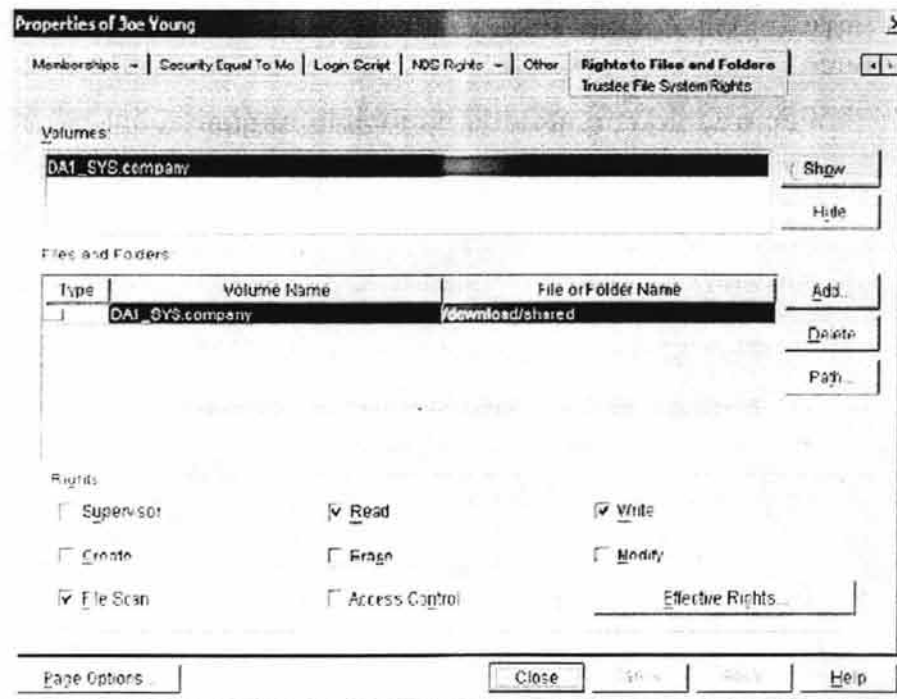
2.8 ADMINISTRACIÓN DE DERECHOS.

Los derechos son indicadores del sistema que puede definir en recursos de red individuales para controlar el acceso a dichos recursos. Cuando asigne derechos, enlázelos siempre con un objeto Usuario, Grupo u otro NDS® que sea el *Trustee* (poseedor) de los derechos. En ConsoleOne®, puede otorgar derechos de *Trustee* a dos tipos distintos de recursos:

- Propiedades y objetos NDS.
- Archivos y carpetas en volúmenes NETWARE®.
- El sistema de archivos NETWARE® almacena y aplica los derechos a estos recursos. Cuando un usuario intenta acceder a un recurso, el sistema (NDS o NETWARE®) calcula los derechos efectivos de usuario sobre dicho recurso. Al hacerlo, el sistema comprueba no sólo las asignaciones de derechos explícitos del usuario, sino también las equivalencias de seguridad del usuario y los filtros que bloquean la herencia de asignaciones de derechos explícitas.

2.8.1 ASIGNACIÓN EXPLÍCITA DE DERECHOS.

Cuando la asignación de derechos por defecto del árbol NDS proporciona a los usuarios demasiado acceso, o por el contrario, un acceso insuficiente a los recursos, puede crear o modificar asignaciones explícitas de derechos. Cuando cree o modifique una asignación de derechos, empiece seleccionando el recurso que está controlando el acceso o el *Trustee* (el objeto NDS que tiene o tendrá los derechos). (figura II.19)



(figura II.19)

2.8.1.1 CONTROL DEL ACCESO AL SISTEMA DE ARCHIVOS NETWARE®, POR RECURSO

- Haga clic con el botón derecho en el recurso (archivo, carpeta o volumen) cuyo acceso desea controlar > haga clic en Propiedades.
- **SUGERENCIA:** Seleccione un volumen o una carpeta cuyo acceso a todos sus recursos desea controlar.
- En la página *Trustees*, edite la lista de *Trustees* y sus asignaciones de derechos según sea necesario.
 - Para añadir un objeto como *Trustee*, haga clic en Añadir *Trustee* > seleccione el objeto > haga clic en Aceptar > bajo Derechos de acceso, asigne los derechos del *Trustee*.
 - Para modificar las asignaciones de derechos de un *Trustee*, seleccione el *Trustee* > bajo Derechos de acceso, modifique la asignación de derechos según sea necesario.
 - Para eliminar un objeto como *Trustee*, seleccione el objeto > haga clic en Suprimir *Trustee* > Sí. El *Trustee* suprimido ya no tendrá derechos explícitos para el archivo o la carpeta, pero puede que todavía tenga derechos efectivos mediante la herencia o equivalencia de seguridad.
- Haga clic en Aceptar.

2.8.1.2 CONTROL DEL ACCESO AL SISTEMA DE ARCHIVOS NETWARE®, POR TRUSTEE.

- Haga clic con el botón derecho en el *Trustee* (el objeto que posee o poseerá los derechos) > seleccione Propiedades.
- En la página Derechos para archivos y carpetas, haga clic en Mostrar > seleccione el volumen NETWARE® que contiene el sistema de archivos cuyo acceso desea controlar > haga clic en Aceptar.
- La lista Archivos y Carpetas se rellenará con los archivos y carpetas para los que el *Trustee* tenga asignaciones de derechos en el volumen seleccionado.
- Edite las asignaciones de derechos según sea necesario.
 - Para añadir una asignación de derechos, haga clic en Añadir > seleccione el archivo o la carpeta cuyo acceso desea controlar > haga clic en Aceptar > bajo Derechos, asigne los derechos de *Trustee*.
 - Para modificar una asignación de derechos, seleccione el archivo o la carpeta cuyo acceso desea controlar > bajo Derechos, modifique los derechos de *Trustee* según sea necesario.
 - Para eliminar una asignación de derechos, seleccione el archivo o la carpeta a la que desee controlar el acceso > haga clic en Suprimir > Sí. El *Trustee* ya no tendrá derechos explícitos para el archivo o la carpeta, pero puede que todavía tenga derechos efectivos mediante la herencia o equivalencia de seguridad.
- Repita los pasos 2 y 3 según sea necesario para editar las asignaciones de derechos de *Trustee* en otros volúmenes NETWARE®.
- Haga clic en Aceptar.

2.8.1.3 CONTROL DEL ACCESO A NDS, POR RECURSO.

- Haga clic con el botón derecho del ratón en el recurso NDS (objeto) para el que desea controlar el acceso > haga clic en *Trustees* de este objeto.
- **SUGERENCIA:** Seleccione un contenedor cuyo acceso a todos sus objetos desea controlar.
- Edite la lista de *Trustees* y sus asignaciones de derechos según sea necesario. Haga clic en Ayuda para obtener detalles.
 - Para añadir un objeto como *Trustee*, haga clic en Añadir *Trustee* > seleccione el objeto > haga clic en Aceptar > asigne los derechos del *Trustee* > haga clic en Aceptar.
 - Para modificar las asignaciones de derechos de un *Trustee*, seleccione el *Trustee* > haga clic en Derechos asignados, modifique la asignación de derechos según sea necesario > haga clic en Aceptar.
 - Para eliminar un objeto como *Trustee*, seleccione el objeto > haga clic en Suprimir *Trustee* > Sí. Los *Trustees* suprimidos ya no tendrán derechos explícitos a este objeto ni a sus propiedades, pero podrían tener derechos efectivos a través de la herencia o la equivalencia de seguridad.
 - Haga clic en Aceptar.

2.8.1.4 CONTROL DEL ACCESO A NDS, POR TRUSTEE.

- Haga clic con el botón derecho en el *Trustee* (el objeto que posee o poseerá los derechos) > seleccione Derechos para otros objetos.
- En el recuadro de diálogo de búsqueda, especifique la parte del árbol NDS en la que deben buscarse los objetos NDS para los cuales el *Trustee* tenga actualmente asignaciones de derechos. Haga clic en Ayuda para obtener detalles.
- Haga clic en Aceptar en el recuadro de diálogo.
- Aparecerá un recuadro de diálogo que muestra el progreso de la búsqueda. Una vez efectuada la búsqueda, aparecerá la página Derechos para otros objetos con los resultados de la búsqueda rellenos.
- Edite las asignaciones de derechos NDS del *Trustee* según sea necesario. Haga clic en Ayuda para obtener detalles.
 - Para añadir una asignación de derechos, haga clic en Añadir objeto > seleccione el objeto cuyo acceso desea > haga clic en Aceptar > asigne los derechos de *Trustee* > haga clic en Aceptar.
 - Para modificar una asignación de derechos, seleccione el objeto cuyo acceso desea controlar > haga clic en Derechos asignados > modifique la asignación de derechos del *Trustee* > haga clic en Aceptar.
 - Para eliminar una asignación de derechos, seleccione el objeto al que desee controlar el acceso > haga clic en Suprimir objeto > Sí. El *Trustee* ya no tendrá derechos explícitos a este objeto ni a sus propiedades, pero podría tener derechos efectivos a través de la herencia o la equivalencia de seguridad.
 - Haga clic en Aceptar.

2.8.2 CÓMO OTORGAR EQUIVALENCIA.

Un usuario que sea equivalente en seguridad a otro objeto NDS efectivo posee todos los derechos de dicho objeto, tanto en el sistema de archivos NDS como en NETWARE®. Un usuario es automáticamente equivalente en seguridad a los grupos y funciones a los que pertenece.

Todos los usuarios son, implícitamente, equivalentes en seguridad al *Trustee* [Público] y a cada contenedor por encima de sus objetos usuario del árbol NDS, incluido el objeto árbol. También puede otorgar explícitamente equivalencia de seguridad de un usuario a cualquier objeto NDS.

2.8.2.1 CÓMO OTORGAR EQUIVALENCIA DE SEGURIDAD POR PERTENENCIA A GRUPO.

- Si aún no lo ha hecho, cree el objeto Grupo o Función con el que desee que los usuarios tengan equivalencia de seguridad.
- Otorgue al grupo o función los derechos NDS o NETWARE® que desee que tengan los usuarios.
- Edite la pertenencia a grupo del grupo o función para incluir a los usuarios que necesiten derechos del grupo o función.
 - Para un objeto Grupo, utilice la página de propiedades Miembros.
 - Para un objeto Función administrativa, utilice el campo Ocupante de la página de propiedades Identificación.
 - Para un objeto de función RBS, utilice la página de propiedades Miembros de la función.
- Haga clic en Aceptar.

2.8.2.2 CÓMO OTORGAR EQUIVALENCIA DE SEGURIDAD EXPLÍCITAMENTE.

- Haga clic con el botón derecho en el usuario o en el objeto con el que desea que el usuario tenga equivalencia de seguridad > haga clic en Propiedades.
- Otorgue la equivalencia de seguridad de la siguiente forma:
 - Si selecciona el usuario, en la pestaña Pertenencia a grupo seleccione la página Seguridad igual a > haga clic en Añadir > seleccione el objeto con el que desee que el usuario tenga equivalencia de seguridad > haga clic en Aceptar.
 - Si selecciona el objeto para el que desea que el usuario tenga equivalencia de seguridad, haga clic en Seguridad igual a mí, haga clic en Añadir > seleccione el usuario > haga clic en Aceptar.
- Haga clic en Aceptar.

2.8.2.3 CONFIGURACIÓN DE UN ADMINISTRADOR MEDIANTE PROPIEDADES NDS ESPECÍFICAS.

- Si todavía no lo ha hecho, cree el objeto Usuario, Grupo, Función o Contenedor que desea configurar como un *Trustee* para las propiedades específicas.
- Si crea un contenedor como *Trustee*, todos los objetos debajo de ese contenedor tendrán los derechos que le conceda.

- Haga clic con el botón derecho en el contenedor del nivel superior que desea que gestione el administrador > haga clic en *Trustee* de este objeto.
- En la página de propiedades, haga clic en Añadir *Trustee* > seleccione el objeto que represente al administrador > haga clic en Aceptar.
- En el recuadro de diálogo Derechos asignados a:
 - Deseleccione la casilla de verificación Mostrar sólo las propiedades de esta clase de objeto.
 - Para cada propiedad que el administrador vaya a gestionar, asigne los derechos necesarios. Asegúrese de que selecciona la casilla de verificación Heredable de cada asignación de derechos. Haga clic en Ayuda para obtener detalles.
 - Haga clic en Aceptar.
- Haga clic en Aceptar en el recuadro de diálogo Propiedades.

2.8.3 VISUALIZACIÓN DE DERECHOS EFECTIVOS.

Los derechos efectivos son los derechos reales que los usuarios pueden ejercer en recursos de red específicos. Los calcula el sistema (NDS o NETWARE®) en función de las asignaciones de derechos explícitas, la herencia y la equivalencia de seguridad. Puede consultar al sistema para determinar los derechos efectivos de un usuario en cualquier recurso.

2.8.3.1 VISUALIZACIÓN DE DERECHOS EFECTIVOS PARA UN ARCHIVO O CARPETA DE UN VOLUMEN NETWARE®.

- Haga clic con el botón derecho del ratón en el archivo, carpeta o volumen > haga clic en Propiedades. (Seleccione un volumen para ver los derechos efectivos en la raíz del sistema de archivos.)
- En la página *Trustee*, haga clic en Derechos efectivos.
- Si el objeto cuyos derechos efectivos desea ver no aparece en el campo *Trustee*, haga clic en el botón Examinar situado al lado del campo > seleccione el *Trustee* deseado > haga clic en Aceptar.
- Visualizar los derechos efectivos.
- Haga clic en Aceptar.

2.8.3.2 VISUALIZACIÓN DE DERECHOS EFECTIVOS SOBRE UN OBJETO O PROPIEDAD NDS.

- Haga clic con el botón derecho del ratón en el objeto NDS > haga clic en *Trustees* de este objeto.
- Seleccione la página Derechos efectivos en la pestaña Derechos de NDS.
- Si el objeto cuyos derechos efectivos desea ver no aparece en el campo Para *Trustee*, haga clic en el botón Examinar situado al lado del campo > seleccione el *Trustee* deseado > haga clic en Aceptar.
- Visualice los derechos efectivos que desee.

- Puede ver derechos efectivos del objeto de forma global, de todas las propiedades del objeto y de propiedades individuales. Haga clic en Ayuda para obtener detalles.
- Haga clic en Aceptar.

2.8.4 ACERCA DE LOS DERECHOS NETWARE®.

Esta sección describe los derechos específicos que los usuarios pueden tener sobre los archivos y carpetas de volúmenes NETWARE®, los posibles orígenes de dichos derechos y el método que usa el sistema de archivos NETWARE® para calcular los derechos efectivos de usuarios relativos a archivos y carpetas.

2.8.4.1 DESCRIPCIONES DE DERECHOS.

La tabla siguiente describe los derechos individuales que un *Trustee* puede tener para un archivo o carpeta de un volumen NETWARE®.

Derecho	Otorga al <i>Trustee</i>
Supervisión	Todos los derechos sobre el archivo o la carpeta y cualquier elemento subordinado. Este derecho no se puede filtrar (bloquear) en el archivo o carpeta actual o en los elementos subordinados, ni tampoco se puede revocar en elementos subordinados individuales.
Lectura	La capacidad de abrir y leer el archivo o carpeta y cualquier elemento subordinado. Incluye la capacidad de ejecutar archivos de programa.
Escritura	La capacidad de abrir y escribir (modificar) el archivo o carpeta y cualquier elemento subordinado.
Creación	La capacidad para crear elementos nuevos y recuperar elementos suprimidos en la carpeta y cualquier subcarpeta.
Borrado	La capacidad para suprimir el archivo o la carpeta y cualquier elemento subordinado.
Modificación	La capacidad de cambiar el nombre y atributos del archivo o carpeta y de cualquier elemento subordinado. El <i>Trustee</i> no puede ver o modificar el contenido real de los archivos.
Exploración de archivos	La capacidad de ver (en un listado o navegador) el archivo o carpeta y cualquier elemento subordinado, incluida su vía hasta la raíz del volumen.
Control de acceso	La capacidad para cambiar las asignaciones (derechos) de <i>Trustee</i> y el filtro de los derechos heredados del archivo o carpeta.

2.8.4.2 ORÍGENES DE LOS DERECHOS.

Un archivo o carpeta determinada puede tener múltiples asociaciones de derechos asignadas, cada una enlazada con un *Trustee* (poseedor) distinto de los derechos. El *Trustee* hereda los derechos de una carpeta para los elementos que se hallan dentro, así el *Trustee* puede ejercer los derechos en elementos subordinados sin tener una asignación explícita para dichos elementos. Sin embargo, puede colocar un filtro

en los elementos subordinados individuales para evitar que se hereden derechos específicos. Dichos filtros se aplican globalmente a todos los *Trustees* que poseen los derechos especificados.

A parte de tener derechos explícitos y heredados para un archivo o carpeta, un usuario también puede tener derechos para un archivo o carpeta mediante la equivalencia de seguridad con otro objeto NDS. Por ejemplo, si un usuario es miembro de un grupo o función NDS y a dicho grupo o función se le han otorgado ciertos derechos, el usuario posee, de forma efectiva, dichos derechos adicionales mediante la equivalencia de seguridad.

2.8.4.3 CÓMO CALCULA NETWARE® LOS DERECHOS EFECTIVOS.

NETWARE® calcula los derechos efectivos de un usuario cada vez que dicho usuario intenta acceder a un archivo o carpeta de un volumen NETWARE®

- Comprueba si el usuario posee el derecho de Supervisión sobre el servidor NETWARE® donde reside el archivo o la carpeta de destino. (NDS proporciona esta información a NETWARE®.)
 - En caso afirmativo, el usuario posee efectivamente todos los derechos del sistema de archivos del servidor y se omite el resto del proceso.
 - En caso negativo, continúa con el próximo paso.
- Determina los objetos NDS con los que el usuario posee una equivalencia de seguridad. (NDS proporciona esta información a NETWARE®.)
- Desciende al siguiente nivel del sistema de archivos por la vía de acceso hacia el archivo o la carpeta de destino.
- Comprueba si al usuario, o a cualquier objeto con el que el usuario tenga una equivalencia de seguridad, se le ha asignado el derecho de Supervisión en el nivel actual.
 - En caso afirmativo, el usuario posee efectivamente todos los derechos del sistema de archivos a partir de este nivel y se omite el resto del proceso.
 - En caso negativo, continúa con el próximo paso.
- Ejecuta lo siguiente para el usuario y para cada objeto con el que el usuario posee una equivalencia de seguridad:
 - Comprueba si al usuario (u objeto) se le han asignado derechos de no Supervisión en el nivel actual. En caso afirmativo, define los derechos efectivos del usuario (u objeto) en los derechos especificados en la asignación y omite el paso 6. En caso negativo, continúa con el subpaso siguiente.
 - Elimina, de los derechos efectivos actuales, cualquier derecho bloqueado por un filtro de herencia en el nivel actual.
- Si el nivel actual del sistema de archivos es el archivo o la carpeta de destino, los derechos efectivos finales del usuario son la suma de sus derechos efectivos actuales más los derechos efectivos actuales de cada objeto con el que el usuario posea una equivalencia de seguridad. Si aún no se ha llegado al archivo o carpeta de destino, vuelve al paso 3.”⁴

⁴ ConsoleOne 1.3. En línea [URL], <http://www.novell.com/documentation/spanish/consol13/index.html>

2.9 LA IMPRESIÓN EN LA RED.

“Cuando se imprime desde un ordenador aislado con una impresora conectada a él, el trabajo de impresión es dirigido directamente desde el ordenador al dispositivo impresor.

En un entorno de red se puede enviar la impresión requerida a la impresora local (si la hay); o bien encaminarse a una impresora de la red.

El trabajo de impresión enviado a una impresora de la red debe estar coordinado con los trabajos originados en otras estaciones de trabajo.

Para ello, NETWARE® incorpora dos métodos de organización de la impresión en la red:

- Utilizando la impresión basada en colas.
- Utilizando los Servicios de impresión distribuidos (NDPS).

2.9.1 LA IMPRESIÓN BASADA EN COLAS.

Este método es el utilizado por NETWARE® desde sus primeras versiones y se mantiene por compatibilidad con ellas.

Cuando un usuario inicia la impresión de un trabajo en la red, el trabajo no se envía directamente a la impresora de la red, sino a una cola de impresión del servidor correspondiente.

Allí se almacena hasta que la impresora está disponible para la impresión requerida. Un servidor de impresora controla la disponibilidad de dicha impresora y envía la impresión requerida en un orden establecido.

En cada servidor NETWARE® puede haber un servidor de impresión con un número máximo de 255 impresoras y cada impresora puede tener varias colas de impresión.

Lo primero que debe hacer el administrador es asignar, al menos, una cola de impresión a cada impresora de la red, configurar cada impresora, asignarlas al servidor de impresora y asignar los usuarios o grupos que van a utilizar cada cola de impresión.

Es posible que haya usuarios, además del administrador, que tengan prioridad de acceso a la impresora.

De ese modo, dichos usuarios podrán cambiar el orden de los trabajos de impresión según sea necesario. Ellos serán los operadores de cola.

Antes de nada, es necesario que las impresoras estén conectadas físicamente a la red (a un servidor y/o a una estación de trabajo).

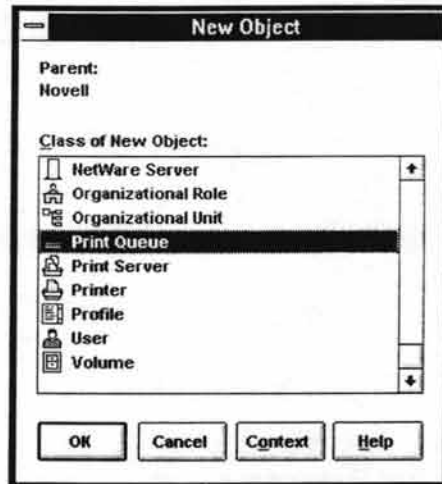
Puede establecer la configuración de la impresión de dos formas:

- De forma rápida (creando los objetos Servidores de impresión, impresoras y colas de impresión automáticamente).
- Creando los objetos Servidores de impresión, impresoras y colas de impresión de forma manual y luego relacionándolos.

2.9.2 LA CONFIGURACIÓN RÁPIDA DE LOS SERVICIOS DE IMPRESIÓN.

Para la configuración rápida de la impresión basada en colas, siga los pasos siguientes:

- Ejecute el Administrador de NETWARE®.
- Sitúese en el contenedor que desee (en el ejemplo VENTAS), abra el menú Herramientas, seleccione Configuración rápida de los Servicios de impresión (No NDPS) y aparecerá una pantalla. (figura II.20)



(figura II.20)

En ella podrá configurar las impresoras de la red y las colas que pueden compartir los usuarios del contenedor seleccionado incluyendo la creación de los objetos Servidor de impresión, Impresora y Cola de impresión, y la carga del software del controlador y del servidor adecuado.

Se encuentran los siguientes apartados:

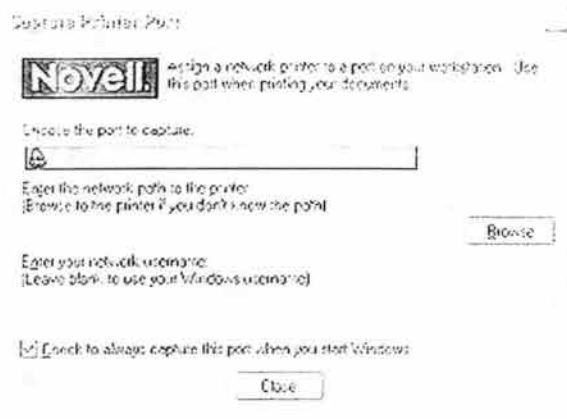
- Servidor de impresión. Indica un nombre para designar a este objeto (si pulsa el botón que hay a la derecha del campo podrá seleccionar un servidor de impresión que ya estuviera creado anteriormente).

En el bloque Impresora se encuentran los siguientes campos:

- Nombre. Indica un nombre para el objeto Impresora.
- Tipo. Indica el tipo de comunicación que utiliza la impresora. Si marca en el triángulo que hay a la derecha del campo podrá seleccionar el que desea.

Si marca en Comunicación (también es posible que aparezca al seleccionar un tipo) verá una pantalla donde:

- Puerto. Indica el puerto paralelo que utiliza la impresora (puede elegir entre LPT1, LPT2 o LPT3). (figura II.21)



(figura II.21)

- Interrupciones. Indica la interrupción que utiliza la impresora. Hay dos opciones:

En ella se encuentran los siguientes campos:

- Usar interrupciones. Indica la interrupción específica que desea utilizar (si selecciona esta opción, debe indicar en Interrupción el número correspondiente).
- Sondeo. Indica que el ordenador utiliza la interrupción del temporizador en lugar de un número de interrupción específico para enviar señales a la impresora (la mayoría de las veces este método proporciona un rendimiento satisfactorio y evita la posibilidad de conflictos de interrupción).
- Tipo de conexión. Indica el tipo de conexión para la impresora. Puede ser de dos maneras:
 - Carga manual. Indica que el controlador se carga manualmente (esta opción se ha de seleccionar para una impresora que esté conectada mediante un cable a cualquier ordenador de la red).
 - Auto-Carga. Indica que el controlador se carga automáticamente (esta opción se ha de seleccionar para las impresoras que están conectadas mediante Un cable a Un servidor NETWARE®).

Cuando haya finalizado, marque en Aceptar y volverá a la pantalla anterior.

- Tipo de portada. Indica el tipo de portada que desea utilizar (texto o *postscript*).

En el bloque Cola de impresión se encuentran los siguientes campos:

- Nombre. Indica un nombre para el objeto Cola de impresión.
- Volumen. Indica el nombre completo del volumen en el que debe crearse la cola física (si pulsa el botón que hay a la derecha del campo podrá seleccionar Un volumen).

Puede aceptar los valores que da por defecto o indicar los que desee (en el ejemplo se aceptan los nombres de los objetos que da por defecto). Cuando haya finalizado, marque en Crear.

- Verá que se han creado los tres objetos y que se encuentran en el árbol del directorio.

2.9.3 ASIGNE USUARIOS A LAS COLAS DE IMPRESIÓN.

Tanto si se han creado los objetos de impresión de forma automática como manual, es necesario indicar que usuarios y/o grupos pueden utilizar las colas de impresión.

Para ello, siga los pasos siguientes:

- Ejecute el Administrador de NETWARE®.
- Sitúese en una cola de impresión y pulse [Entrar].
- Marque en Usuarios y verá una nueva pantalla:

Observe que se ven las asignaciones que acaba de realizar y que muestran que los tres objetos están relacionados.

En ella se ve la lista de usuarios que pueden emitir tareas de impresión a esta cola (para editar la lista, debe ser un operador de la cola). Como en la lista aparece un contenedor (VENTAS), todos los usuarios del mismo también pueden emitir tareas de impresión a esta cola.

Si marca en Añadir podrá ampliar la lista con nuevos usuarios, grupos o contenedores.

Si se sitúa en algún usuario, grupo o contenedor de la lista y marca en Suprimir, se quitará

- Cuando haya finalizado, marque en Aceptar.

2.9.4 AGREGUE UNA IMPRESORA EN LA ESTACION DE TRABAJO.

Es necesario agregar una impresora en Windows 95/98 por cada impresora que haya conectado en la estación de trabajo.

Para ello, siga los pasos siguientes:

- Desde el escritorio de Windows 95, abra Mi PC y pulse dos veces el botón izquierdo del ratón sobre Impresoras.
- Pulse dos veces el botón izquierdo del ratón sobre **Agregar impresora** y entrará en el asistente. Marque en Siguiente.
- Seleccione **Impresora en red**, marque en Siguiente y verá una nueva pantalla:
- Marque en Examinar, aparecerá otra pantalla:

Marque en el signo + que hay a la izquierda del nombre del servidor (en el ejemplo, PRINCIPAL) y le mostrará las colas de impresión que hay creadas.

- Seleccione una de las que creó para su utilización de forma remota y marque en Aceptar

- Le habrá pasado a la pantalla anterior en el campo **Ruta de acceso nombre de cola**.

Indique si desea imprimir desde programas basados en MS-DOS, marque en Siguiente y verá otra pantalla

- Marque en **Capturar puerto de impresora** para poder imprimir desde algunos programas basados en MS-DOS y verá una nueva pantalla:

Marque en Aceptar para asociar la cola de impresión a LPT1 y volverá a la pantalla anterior para que marque en Siguiente.

- Verá una pantalla dividida en dos partes. En la parte izquierda, llamada **Fabricantes**, deberá seleccionar el correspondiente a la impresora (en el ejemplo HP) y en la parte derecha, llamada **Impresoras**, deberá seleccionar la correspondiente a la que está agregando (en el ejemplo HP LaserJet5L PCL).

- Cuando haya finalizado, marque en Siguiente y verá otra pantalla:
Confirme el nombre de la impresora (o modifíquelo), indique si esta impresora es la que se va a utilizar como predeterminada (en el ejemplo, Sí) y marque en Siguiente.

- Indique si desea imprimir una página de prueba para ver el funcionamiento de la impresora y marque en Finalizar.

- Empezará a copiar los archivos del controlador de la impresora (necesitará el CD de Windows 95/98) y, cuando finalice, se agregará un icono en la carpeta Impresoras.

2.9.5 SERVIDOR DE IMPRESIÓN NDPS.

Los Servicios distribuidos de impresión de NOVELL® (NDPS™) constituyen el sistema de impresión preferente y por defecto de NETWARE® 5. Los NDPS™ admiten impresión basada tanto en IP como en IPX. El sistema de impresión exclusivo de NOVELL®, basado en cola de espera, también está totalmente soportado en NETWARE® 5, lo que permitirá a los usuarios continuar imprimiendo como hasta ahora, en espera de que Ud. complete su transición a los NDPS.

2.9.5.1 ACERCA DE LOS SERVICIOS DISTRIBUIDOS DE IMPRESIÓN DE NOVELL®.

Los NDPS se han concebido con el fin de gestionar modernas impresoras interconectadas y gestionar las nuevas funciones que ofrecen. Como resultado de ello, los NDPS reducirán en gran medida los costes de la gestión de impresión de red mediante:

- Una administración centralizada, simplificada y desde un solo punto a todos los recursos de impresión de la red.
- Una comunicación bidireccional y en tiempo real entre los administradores o usuarios y la impresora correspondiente al estado de la tarea o impresión.
- Notificación de eventos configurables.
- Una estrecha integración con los NDS.
- Una estrecha integración con las características de gestión del *hardware* de impresora.
- Descarga e instalación automáticas del controlador de impresora.
- Soporte a impresoras existentes y otros dispositivos de salida.
- Compatibilidad con clientes y plataformas ajenos a NOVELL®.

2.9.5.2 VENTAJAS DE LOS NDPS PARA LOS USUARIOS DE LA RED

Con los NDPS, cuando un usuario instala una impresora, el controlador se descarga y se configura automáticamente. Los NDPS también permiten a los administradores de la red determinar aquellas impresoras que han de instalarse automáticamente cuando los usuarios entran en la red.

Los NDPS ofrecen una comunicación bidireccional con impresoras de red desde estaciones de trabajo clientes. Los usuarios pueden:

- Interrogar acerca del estado de una tarea de impresión en tiempo real, la disponibilidad de una impresora o las capacidades y configuración actual de la impresora.

- Dar instrucciones especiales respecto a las tareas de impresión enviadas.
- Solicitar que la impresora notifique la presencia de determinados eventos.⁵

2.10 SERVICIO DE ACCESO REMOTO (RAS).

“El Servicio de Acceso Remoto (RAS) proporciona acceso remoto a la red a administradores que se encuentran en una ubicación ajena a donde se encuentra la red.

2.10.1 CONCEPTOS SOBRE RAS.

El Servicio de Acceso Remoto (RAS) utiliza distintos métodos de comunicación.

Los métodos de comunicación usados por RAS son:

- **MÓDEM analógico.** RAS soporta una gran variedad de módems que pueden ser configurados para soportar llamadas entrantes y salientes a través de la red telefónica conmutada.
- **RDSI.** La Red Digital de Servicios Integrados es lo más avanzado actualmente en comunicaciones digitales. Utiliza dos “*routers*” (uno en cada extremo) y una línea telefónica digital para enviar los datos a 128 Kilobits por segundo.
- **X25.** Este método, antiguo y lento pero eficaz, permite conectarse a una red utilizando dos “*routers*” (uno en cada extremo) y un sistema basado en paquetes que viaja a través de la red telefónica. Su utilización es recomendable para distancias cortas y poco volumen de datos.

2.10.2 EL SERVICIO DE ACCESO REMOTO (RAS).

El Servicio de Acceso Remoto se puede instalar cuando se hace la instalación servidor NETWARE® 5 (es el producto llamado Servidor de acceso a Internet) o anteriormente desde el módulo NWCONFIG o desde la opción Instalación del menú de la consola gráfica del servidor.

Para configurar el Servicio de Acceso remoto siga los pasos siguientes:

- Cargue el módulo NIASCFG.NLM desde la consola del servidor (la primera vez que lo haga le mostrará una pantalla indicándole que debe migrar todas las líneas LOAD y BIND), pulse [Intro] y verá otra pantalla:
- Si selecciona Configure NIAS, le mostrará la otra pantalla:
- Si selecciona Protocols and *Routing*, verá la pantalla principal del módulo INETCFG.
- Si selecciona Remote Access, le pedirá que indique el nombre del administrador y su contraseña para extender el esquema de NDS incluyendo propiedades del objeto CONNECT. Cuando lo haya hecho, pulse [Intro] y le preguntará si desea ver las instrucciones.
- Seleccione SÍ y le mostrará las instrucciones de configuración del acceso remoto. Cuando lo haya leído, pulse [Esc] y confirme que desea salir.
- Le mostrará una pantalla de aviso indicándole que puede pulsar [VS] para ver el proceso de configuración. Pulse [Intro] para empezar el proceso de configuración.

⁵ Raya Cabrera, J. y Raya Pérez E. (2000). Netware® 5 Instalación, Configuración y Administración. México: Alfaomega. 286-340pp

- Le preguntará si dispone de adaptadores sincronicos (X25 o RDSI). Si tiene adaptadores asincronicos (módem), conteste NO.
- Le indicará que pulse [Intro] para seleccionar el adaptador serie que desee instalar. Cuando lo haya hecho, pulse [Intro].
- Le indicará que ha sido instalado. Pulse [Intro] e indique Si desea cargar más dispositivos.
- Le mostrará una pantalla de aviso advirtiéndole de que tenga conectado el MÓDEM, ya que va a intentar detectarlo. Pulse [Intro] y empezará la detección.
- Cuando lo haya encontrado le mostrará la otra pantalla.
- Seleccione Continue With Automated Setup para continuar con el proceso y le preguntará Si desea que detecte el tipo de MODEM.
- Seleccione Si y empezará el proceso. Cuando lo haya encontrado, le mostrará la pantalla siguiente.
- Si es el MÓDEM correcto, seleccione Si (en caso contrario seleccione No y elíjalo de la lista).
- En ambos casos le mostrará otra pantalla. Indique los servicios que desea cargar.
- Si selecciona PPRNS deberá indicar el protocolo que desea utilizar para el servicio:
 - IP. En este caso deberá indicar la dirección IP, la mascara de subred Si desea usar compresión de cabeceras, y un rango de direcciones para los clientes PPP.
 - IPX. En este caso deberá indicar la dirección de red IPX.
- Repita el proceso con los demás servicios que desee cargar y cuando haya finalizado, pulse [Esc].
- Le mostrara una pantalla indicándole que ha completado la instalación. Pulse [Intro] y pasará a otra pantalla.
- Puede salir del modulo pulsando [Esc].⁶

2.11 LAS COPIAS DE SEGURIDAD DEL SERVIDOR.

“¿Qué ocurriría si por error, distracción, etcétera se produce una pérdida de datos importante? Pues no pasaría nada Si se cuenta con un buen sistema de copias de seguridad de dichos datos que permita restaurar la información prácticamente al mismo nivel que se encontraba antes de su pérdida.

Antes de empezar con la explicación sobre las posibles técnicas de copias de seguridad, es necesario determinar quién va a ser el responsable de su realización.

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.

⁶ Raya Cabrera, J. y Raya Pérez E. (2000). Netware® 5 Instalación, Configuración y Administración. México: Alfaomega, 659-672pp

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 el administrador de la red, como responsable de mantener el funcionamiento y mantenimiento del sistema, el que se encargue de las tareas de copias de seguridad o delegue en alguien que tenga equivalencia de administrador.

2.11.1 ELEGIR ENTRE COPIAS DE SEGURIDAD O COPIADO DE ARCHIVOS.

Hay dos tipos diferentes de protección de los datos:

- Las copias de seguridad.
- El copiado de archivos.

La diferencia básica entre ambos sistemas está en el motivo de su realización.

Normalmente se realiza una copia de seguridad del sistema para proteger los datos de los errores mecánicos y humanos. Las copias de seguridad protegen de los problemas de *hardware* como, por ejemplo, fallos en algún disco duro. También son útiles cuando se borran, sin darse cuenta, los archivos de datos o los programas.

El copiado de los archivos se realiza, sin embargo, para guardar ciertos archivos a lo largo del tiempo, de la misma forma que se guardan copias en papel.

Un buen procedimiento de copiado es una gran ayuda para gestionar el espacio en el disco duro, ya que hay archivos que no se necesitan de forma continuada y, sin embargo, están ocupando espacio en el disco.

Hay algunas normas que es aconsejable seguir:

- Respalde diariamente los archivos modificados.
- Respalde semanalmente el sistema entero.
- Copie mensualmente los archivos.

2.11.1.1 EL RESPALDO DIARIO DE LOS ARCHIVOS.

El proceso del respaldo de los archivos casi siempre necesita bastante tiempo para su realización. Por tanto, es conveniente que sólo realice el respaldo diario de los archivos que hayan sido modificados.

Primero, deberá determinar cuales son los archivos que deben respaldarse. Por lo general, los programas de aplicaciones y del sistema operativo no suelen sufrir variaciones y, por tanto, no necesitan respaldarse diariamente.

En cambio, los archivos de datos y de configuración de los programas o del sistema operativo son los que sufren variaciones, por tanto deberá respaldarlos diariamente.

Para ello, podría seguir dos métodos de respaldo:

- Respaldo diferencial. Se realiza con los archivos cuyo BIT de archivación se puso a uno en el último respaldo, completo, pero no se restaura a cero (dicho BIT de archivación) para que los archivos vuelvan a respaldarse al día siguiente.
- Respaldo incremental. Se realiza con los archivos cuyo BIT de archivación se puso a uno en el último respaldo completo, pero se restaura a cero (dicho BIT de archivación) para que los archivos no se vuelvan a respaldar al día siguiente (a no ser que se hayan vuelto a modificar).

Para poder localizar fácilmente el respaldo realizado en último lugar, es muy recomendable poner en cada uno la fecha y la hora en que se hizo.

2.11.1.2 RESPALDO SEMANAL DEL SISTEMA COMPLETO.

Este método consiste en realizar un respaldo completo de todo el contenido ordenador y, al igual que el método diario, es recomendable que se realice en unidades de cinta.

De este modo, en caso de tener que restaurar el contenido del ordenador se realizará de forma fácil y rápida.

Es el método más adecuado, porque permite tener pocas copias y, de esa forma, poder encontrar fácilmente la adecuada.

2.11.1.3 LA COPIA MENSUAL DE LOS ARCHIVOS.

Por lo general, la copia de los archivos es suficiente que se realice una vez al mes. Asegúrese de que tiene copiados los archivos en un medio o soporte diferente (cinta, disco, disquete) que las copias de seguridad, para que en caso de pérdida o deterioro de la cinta pueda recuperar la información.

El objetivo del copiado es distinto al del respaldo de los archivos, por lo que tendrá que seguir diferentes procedimientos, entre los cuales se encuentran:

- Determine que directorios y archivos son los que van a copiarse.
- Determine si los archivos van a ser borrados después de ser copiados.
- Es recomendable que comprima los archivos antes de copiarlos, ya que reducirá el espacio de almacenamiento y el tiempo que tardará en realizarse el proceso.
- Saque un listado de los archivos que se han copiado.
- Guarde en lugar seguro las copias de los archivos

2.12 LA UTILIDAD SERVICIO DE GESTIÓN DE ALMACENAMIENTO DE NOVELL®.

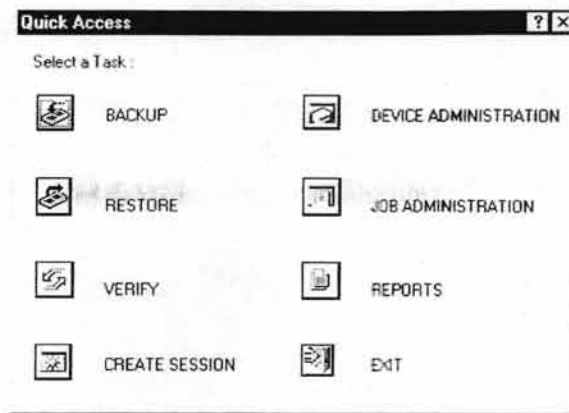
La utilidad Servicio de gestión de almacenamiento de NOVELL® le permite realizar copias de seguridad (o restaurarlas) desde una estación de trabajo. (funciona con unidades de cinta de formato DC-6000 y cartuchos de 4 y 8 mm.)

Para poder trabajar con ella, siga los pasos siguientes:

- Ejecute el archivo NWBACK32.EXE que se encuentra en el directorio IPUBLIC del volumen SYS del servidor (si lo desea puede crear un directo desde el escritorio) y verá una nueva pantalla.

En ella debe indicar el *Tree Name* (es el nombre del árbol NDS), el SMDR Context (es el contexto SMDR). Lo indicó cuando cargó el módulo SMDR la primera vez y el *SMDR Group Context* es el contexto del grupo SMDR. Lo indicó cuando cargó el modulo SMDR la primera vez.

- Cuando haya finalizado, marque OK (estos valores los puede modificar desde la opción Configurar SMDR del menú Archivo) y vera la siguiente pantalla: (figura II.22)



(figura II.22)

- Copia de seguridad. Permite realizar una copia de seguridad.
- Restaurar. Permite recuperar los datos de una copia de seguridad.
- Verificar. Permite seleccionar la cola, el servidor y el dispositivo que debe verificarse una vez realizada una copia de seguridad de los datos.
- Crear sesión. Permite seleccionar la cola, el servidor y el dispositivo para los que se debe crear una sesión.
- Administración de tareas. Permite seleccionar la cola, el servidor, el dispositivo y la tarea que debe cambiarse para una sesión de copia de seguridad o de restauración.
- Administración de dispositivos. Permite seleccionar la cola, el servidor y el medio que debe cambiarse para una sesión de copia de seguridad o de restauración.
- Informes. Muestra los archivos de registro de la sesión y de errores para una sesión de copia de seguridad y de restauración.
- Salir. Abandona a utilidad.

2.13 REALIZAR UNA COPIA DE SEGURIDAD.

Para realizar una copia de seguridad, siga los pasos siguientes:

- Desde el menú de Acceso rápido o desde Sesión nueva del menú del Archivo, seleccione Copia de seguridad y verá una nueva pantalla:

La parte central de la pantalla se encuentra dividida en dos partes:

- **COPIA DE SEGURIDAD DE.** Permite seleccionar NDS, un servidor, una estación de trabajo, una partición *DOS* o la base de datos de GroupWise. Para poder realizar una copia de seguridad, seleccionar, por lo menos, uno de dichos elementos (para despliegue las opciones pulsando dos veces el botón izquierdo ratón sobre cada una de ella y marque en el cuadrado que hay a la izquierda de la entrada (archivo, directorio, volumen...) que desee algunos casos, deberá indicar el nombre del usuario y su contraseña para poder desplegarlo).
- **COPIA DE SEGURIDAD.** Permite seleccionar la cola, el ser dispositivo y el medio en el que residirá la copia de seguridad. Para poder realizar una copia de seguridad, debe seleccionar uno de elementos (tal y como se indicó en el punto anterior).

- Marque en el ícono Ejecutar (es el quinto empezando por la derecha) y verá una nueva pantalla:
- Seleccione el tipo de copia de seguridad que desea hacer. marque en *siguiente* y cambiará a otra pantalla.
- Seleccione el subconjunto de lo que desee hacer la copia de seguridad (o acepte los valores por defecto). Para seleccionar un subconjunto, pulse dos veces el botón izquierdo del ratón sobre una de las entradas de Opciones del filtro disponibles y especifique los archivos y directorios que desee incluir o excluir del conjunto de copia de seguridad seleccionado. Cuando haya finalizado, marque en *Siguiente* y verá otra pantalla:
- Excluya los datos que desee utilizando las Opciones de filtrado, marque en *Siguiente* pasará a otra pantalla.
- Indique la hora y fecha en la que desea que se haga la copia de seguridad. Cuando haya finalizado, marque en *Siguiente* y pasará a otra pantalla.
- Indique el intervalo para volver a ejecutarla, marque en *Siguiente* y pasará a otra pantalla.
- En ella se encuentran los siguientes apartados:
 - Desea reprogramar. Si activa la casilla, podrá volver a programar la tarea.
 - Anexar a las sesiones previas en los medios. Si no activa la casilla, sobrescribirá las sesiones existentes en el medio.
 - Descripción de la tarea a emitir. Le permite indicar un nombre descriptivo de la tarea para su identificación.
 - Mantener la tarea finalizada. Si activa la casilla, mantendrá el trabajo en la cola después de la ejecución (10 que permite volver a emitirla posteriormente).
 - Cuando haya acabado, marque Finalizar.
- Marque Aceptar para confirmar la emisión de la tarea.
- Le mostrará una pantalla de confirmación. Marque de nuevo Aceptar.
- Una vez emitida la tarea, puede hacer un seguimiento del proceso si selecciona Sesión nueva del menú Archivo y elige Administración de tareas.

En la ventana izquierda seleccione la cola en la que se está realizando la tarea y aparecerá la lista de tareas (la tarea activa en ese momento estará con un ícono de color verde). Marque sobre dicha tarea, seleccione Propiedades dinámicas del menú Administración de tareas y aparecerá una pantalla con los resultados de la tarea.

2.14 RESTAURAR UNA COPIA DE SEGURIDAD.

Para restaurar una copia de seguridad, siga los pasos siguientes:

- Desde el menú de Acceso rápido o desde Sesión nueva del menú Archivo, seleccione Restaurar y verá una nueva pantalla:

La parte central de la pantalla se encuentra dividida en dos partes:

○ RESTAURAR. Permite seleccionar la cola, el servidor, el dispositivo y el medio en el que reside la copia de seguridad (si el contexto actual ya no contiene la cola donde reside la copia, seleccione Cambiar contexto del menú Archivo y elija el nombre del árbol).

○ ¿DÓNDE RESTAURAR?. Permite seleccionar el lugar donde desea restaurar la copia de seguridad.

- Marque en el icono Ejecutar (es el quinto empezando por la derecha).
- Seleccione la sesión de dicho medio que desee restaurar y marque Siguiente.
- Seleccione los subconjuntos de lo que desee restaurar utilizando los filtros disponibles para excluir o incluir lo que desee restaurar. Cuando haya finalizado, marque Siguiente.
- Controle los datos que desee restaurar utilizando las Opciones de filtrado. Cuando haya finalizado, marque Siguiente y verá otra pantalla:
- Si desea restaurar los datos en una ubicación distinta, active la casilla Restaurar en otra ubicación e indique el lugar.
- Verifique las opciones de sobre escritura de los datos durante la restauración y marque Siguiente.
- Seleccione la hora y la fecha que desee para iniciar la restauración y marque Siguiente.
- Indique el intervalo y el número de reejecución. Cuando haya finalizado, marque Siguiente.
- Introduzca la información solicitada en esta pantalla (reprogramación, descripción de la tarea, etcétera.) y marque Finalizar.
- Marque Aceptar para confirmar la emisión de la tarea.
- Le mostrará una pantalla de confirmación. Marque de nuevo Aceptar
- Una vez emitida la tarea, puede hacer un seguimiento del proceso si selecciona sesión nueva del menú Archivo y elige Administración de tareas.

En la ventana izquierda seleccione la cola en la que se está realizando la tarea y aparecerá la lista de tareas (la tarea activa en ese momento estará con un ícono de color verde). Marque sobre dicha tarea, seleccione Propiedades dinámicas del menú Administración de tareas y aparecerá una pantalla con los resultados de la tarea.⁷

⁷ Raya Cabrera, J. y Raya Pérez E. (2000). Netware® 5 Instalación, Configuración y Administración. México: Alfaomega, 659-672pp

CAPÍTULO III
INSTALACIÓN Y MANEJO DE LAS REDES CON UNIX Y
PRODUCTOS SCO

3. INSTALACIÓN Y MANEJO DE LAS REDES CON UNIX Y PRODUCTOS SCO.

3.1 HISTORIA DEL UNIX.

“En la década de los sesenta, en la cual se vivía un ambiente de computación en el cual no se soportaba sino un usuario y un programa ejecutándose, además de que el procesamiento de los datos era por lotes y la interacción con los usuarios era escasa, parecía ambicioso pensar en un ambiente de multiprogramación y multitarea, pero a finales de la década se concibió la idea y se trató de implementar en un sistema llamado *MULTICS*, desarrollado por Bell Laboratories junto con el MIT y General Electric; pero no funcionó y el grupo de investigadores que se encontraba desarrollando este proyecto se dispersó.

Este sistema Multics no prosperó, pero a partir de él, Ken Thompson, uno de los investigadores del proyecto *MULTICS*, y sus colegas construyeron el sistema operativo UNIX. La primera versión de UNIX fue escrita en 1969. Esta versión de UNIX se ejecutaba en un ordenador PDP-7. En 1970, Thompson, junto con Dennis Ritchie, lo transportó a un PDP-11/20. Ritchie diseñó y escribió además el primer compilador de “C” con objeto de ofrecer un lenguaje que pudiera usarse para escribir una versión transportable del sistema. En 1973, Ritchie y Thompson reescribieron en “C” el kernel de UNIX, el corazón del sistema operativo.

Las primeras licencias de UNIX se entregaron en 1974 a las universidades, con fines educativos, en una versión conocida como quinta edición. La sexta edición, también conocida como V6, fue liberada en 1976 y su distribución fue mucho más extensa que la quinta. La séptima edición, liberada por Bell Laboratories en 1978, fue la primera que tenía como principal objetivo la transportabilidad. Esta edición, implantada en los ordenadores DEC PDP-11, Interdata 8/32 y VAX, ha servido como punto de partida común para todo el mundo UNIX. Si hay una versión que defina al UNIX “clásico”, es la séptima edición.

La liberación de la sexta y la séptima ediciones dio lugar a varios caminos independientes, pero no aislados, del desarrollo de UNIX. Los tres vástagos más influyentes de la séptima edición fueron las desarrolladas por AT&T Informational System como versiones de System V (no confundir con la quinta edición); los sistemas de investigación que Bell Laboratories siguió desarrollando, y los diversos sistemas BSD (Berkeley Software Distribution).

Entre los descendientes de System V están Xenix, de Microsoft; HP-UX, de Hewlett Packard; UTS, de Amdahl; AIX, de *IBM*; System V/386, de Interactive; e IRIX, de Silicon Graphics. Actualmente, SCO (Santa Cruz Operation) vende tanto Xenix como UNIX; SCO Xenix se distribuye por licencia de Microsoft y está basado en la primera versión de System V, mientras que SCO UNIX incluye las últimas novedades de desarrollo. SCO será la versión de UNIX con la que se trabajará.

Los descendientes principales de BSD UNIX son SunOS, de Sun Microsystems, y Ultrix, de Digital Equipment Corporation. Berkeley no ofrece mantenimiento para los sistemas que desarrolla. Mt. Xinu ofrece mantenimiento comercial de BSD UNIX además de su propia versión de BSD UNIX.

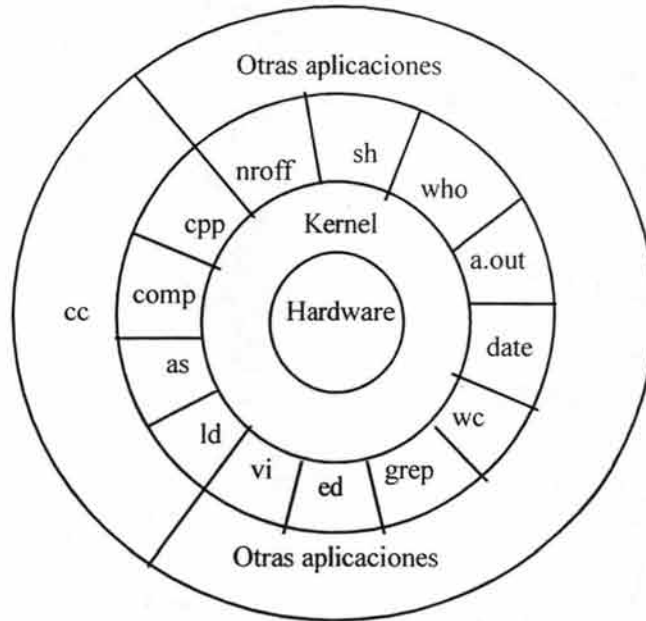
A finales de los años ochenta se presentó un cambio de gran magnitud en el mundo UNIX, al incorporarse el sistema X-Windows al entorno UNIX. Este sistema, conocido en forma abreviada como X, ocasionó un cambio de los entornos de trabajo basados en caracteres a interfases gráficas con el usuario.

Hoy día, UNIX es un sistema muy diferente de lo que fue a principios de los años setenta. En aquella época, el sistema representativo era un solo procesador que servía a un conjunto de terminales de teletipo conectadas al procesador a través de líneas telefónicas directas o conmutadas. El sistema representativo actual es una estación de trabajo con una pantalla de alta definición de mapa de bits que opera con un sistema de ventanas y participa activamente en una extensa red de ordenadores. En aquella época, UNIX era pequeño, sencillo y no comercial, destinado a un público reducido y selecto. Ahora, UNIX es un producto comercial importante, grande, complicado, que se utiliza en una amplia gama de aplicaciones, muchas veces por personas que no tienen experiencia de programación.

3.2 ESTRUCTURA DE UNIX.

3.2.1 ESTRUCTURA DEL SISTEMA.

En la figura III.1 se describe la arquitectura a alto nivel del sistema UNIX. El *hardware* en el centro del diagrama provee al sistema operativo con servicios básicos tales como interrupciones y excepciones, niveles de ejecución (prioridades), administración de memoria, etcétera. El sistema operativo interactúa directamente con el *hardware*, suministrando servicios a los programas y librándoles de la idiosincrasia del *hardware*. El sistema operativo es denominado normalmente como sistema kernel, o simplemente kernel. Como los programas son independientes del *hardware* que hay por debajo, es fácil moverlos entre sistemas UNIX que corren en diferentes máquinas si los programas no hacen referencia al *hardware* subyacente.



(figura III.1)

Programas como el "shell" y editores mostrados en niveles exteriores interactúan con el kernel por medio de un bien definido conjunto de llamadas al sistema. Las llamadas al sistema instruyen al kernel para hacer varias operaciones para el programa llamador e intercambiar datos entre el kernel y el programa. Muchos de los programas mostrados en la figura están disponibles en las configuraciones estándar del sistema y son conocidos como comandos, pero los programas de usuario pueden existir también en este nivel, indicado por el programa `a.out`, el nombre estándar para los archivos ejecutables producidos por el compilador de "C". Otros programas de aplicación pueden construirse en el nivel más alto. Por ejemplo, el compilador de "C", `cc`, está en el nivel más exterior de la figura: invoca al preprocesador de "C", al compilador de dos pasos, al ensamblador y al enlazador, todos ellos programas de nivel inferior.

3.2.2 ARQUITECTURA DEL SISTEMA OPERATIVO UNIX.

Los dos conceptos centrales en el modelo del sistema UNIX son los archivos y los procesos. La figura III.2 muestra un diagrama de bloques del kernel, mostrando varios módulos y las relaciones entre ellos. En particular, se muestra el subsistema de archivos en la parte izquierda y el subsistema de control de procesos en la parte derecha, los dos mayores componentes del kernel.

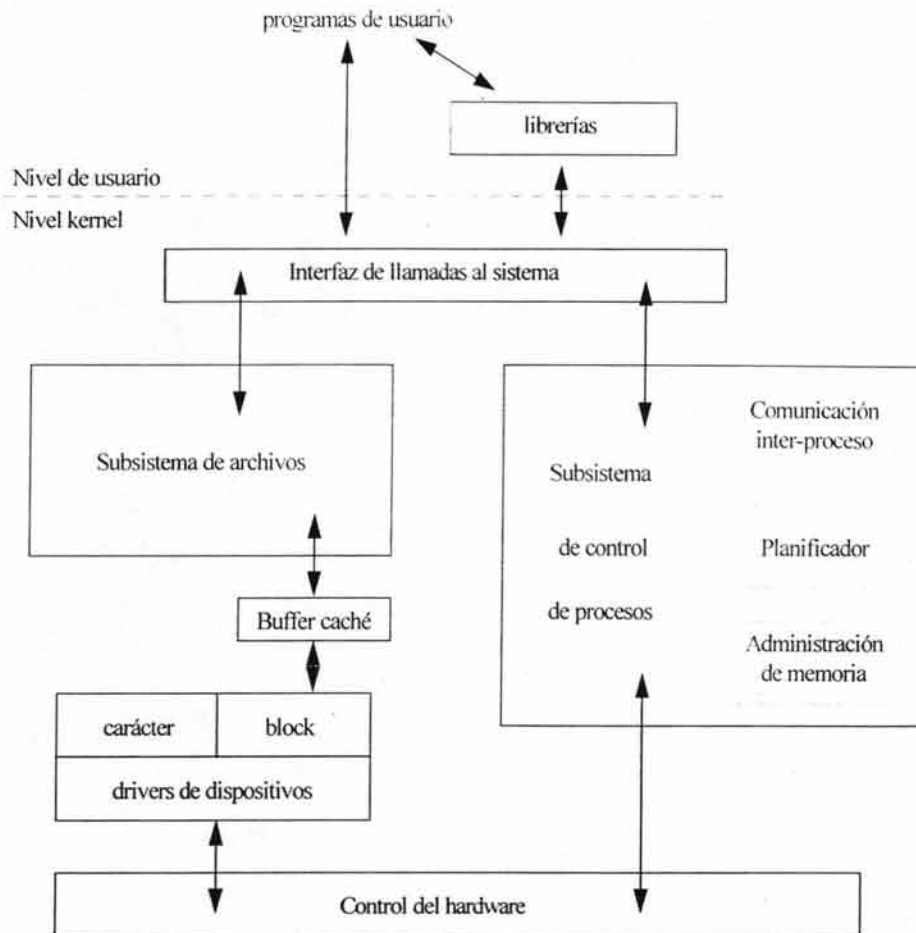


figura III.2

La figura III.2 muestra tres niveles: usuario, kernel y *hardware*. Las llamadas al sistema y las librerías representan el borde entre los programas de usuario y el kernel. Las llamadas al sistema son parecidas a las funciones en los programas en "C" y las librerías transforman estas funciones a las primitivas necesarias para entrar en el sistema operativo. Los programas en lenguaje ensamblador deben invocar a las llamadas al sistema directamente sin las librerías de las llamadas al sistema.

Las llamadas interactúan con el subsistema de archivos y con el subsistema de control de procesos. El subsistema de archivos controla los archivos, asigna espacio a los archivos, administra el espacio libre, controla el acceso a los archivos, etcétera. Los procesos interactúan con el subsistema de archivos mediante un específico conjunto de llamadas al sistema.

El subsistema de archivos accede a los archivos de datos usando un mecanismo de buffer que regula el flujo de datos entre el kernel y los dispositivos de almacenamiento secundario. El mecanismo de buffer interactúa con los controladores de dispositivos de E/S de tipo bloque para iniciar la transferencia de datos desde y hacia el kernel. Los controladores de dispositivos (device drivers) son los módulos del kernel que controlan las operaciones con los dispositivos periféricos. El subsistema de archivos además interactúa directamente con los controladores de dispositivos de E S de tipo carácter sin la intervención de un mecanismo de buffer.

El subsistema de control de procesos es el responsable de la sincronización de los procesos, la comunicación entre procesos, administración de memoria principal y la planificación de procesos. El subsistema de archivos y el subsistema de control de procesos interactúan cuando se carga un archivo en memoria para su ejecución.

El módulo de administración de memoria controla la asignación de memoria. Si en algún momento no hay suficiente memoria física para todos los procesos, el kernel los mueve entre la memoria principal y la secundaria.

El módulo del planificador o *scheduler* asigna la CPU a los procesos. Planifica los procesos para ser ejecutados por turno hasta que voluntariamente liberen la CPU mientras esperan un recurso o hasta que el kernel los saca cuando su tiempo de ejecución supera el tiempo de quantum.

Finalmente, el control del *hardware* es el responsable de las interrupciones y de las comunicaciones con la máquina. Los dispositivos como los discos o terminales pueden interrumpir a la CPU mientras un proceso se está ejecutando. Así, el kernel debe restablecer la ejecución del proceso interrumpido después de servir a la interrupción.

3.2.3 EL NÚCLEO O KERNEL DE UNIX.

El kernel de UNIX es el corazón del sistema operativo. Controla el acceso al ordenador y a sus archivos, asigna recursos a las distintas actividades que se llevan a cabo en el ordenador, mantiene el sistema de archivos y administra la memoria del ordenador. Aunque los usuarios comunes rara vez tienen una interacción explícita con el kernel, éste es un aspecto medular de UNIX.

La figura III.1 nos muestra la capa del kernel inmediatamente por debajo de la capa de las aplicaciones de usuario. El kernel suministra varias operaciones primitivas que ayudan a los procesos del usuario a soportar la interfase de usuario. Entre los servicios suministrados por el kernel están:

- Controlar la ejecución de procesos permitiendo su creación, finalización o suspensión y comunicación.
- Planificar los procesos para su ejecución en la CPU. El sistema es de tiempo compartido: la CPU ejecuta un proceso, el kernel lo suspende cuando termina su quantum de tiempo y el kernel planifica otro proceso para su ejecución. El kernel después replanifica el proceso suspendido.
- Asignar memoria principal a los procesos en ejecución. El kernel permite a los procesos compartir porciones de su espacio de direcciones bajo ciertas condiciones, pero protege el espacio de direcciones privado de un proceso de accesos exteriores. Si el sistema se encuentra bajo memoria libre, el kernel puede liberar memoria escribiendo un proceso temporalmente en memoria secundaria, llamado área de swap. Si el kernel escribe el proceso completo en el área de swap, la implementación de UNIX se denomina sistema de *swapping*; si escribe páginas de memoria al área de swap, se denomina sistema paginado.
- Asignar memoria secundaria para un almacenamiento eficiente y reutilización de datos de usuario. Este servicio constituye el sistema de archivos o *filesystem*. El kernel asigna almacenamiento secundario a los archivos de usuario, controla zonas de memoria no usadas, estructura el sistema de archivos de forma fácil de comprender y protege los archivos de usuario de accesos ilegales.
- Permitir accesos controlados de los procesos a los dispositivos periféricos como terminales, unidades de cinta o disco y dispositivos de red.

Un administrador del sistema puede ajustar las características operativas del sistema mediante la configuración del kernel. La configuración del kernel es la acción de decirle a éste, de que tamaño deben ser las tablas que utiliza el UNIX para el manejo de sus recursos; dicho proceso se hace mediante la modificación de un archivo de parámetros. Después se toma el kernel y se enlaza con ciertas subrutinas y se genera un nuevo kernel con las nuevas entradas. Este proceso no queda operativo hasta que no se inicie de nuevo el equipo. Esta configuración solamente la puede realizar el administrador del sistema.

Por ejemplo, cuando se configura el kernel es el momento donde se determina el número de archivos que se pueden encontrar abiertos, el número de procesos que se pueden estar ejecutando a un mismo tiempo, y el tamaño de los buffers; todos estos recursos los maneja UNIX por medio de tablas y listas. El tamaño de estas tablas es definido por el administrador del sistema, por consiguiente este tamaño no se puede modificar en medio de la ejecución.

Cuando no se configura bien el kernel con una debida estructuración y se deja exceso de espacio para tablas se está desperdiciando la memoria, quitándole espacio a los procesos, debido a que tiene un kernel muy grande.⁸

3.3 INSTALACION DE SCO UNIX.

3.3.1 CUMPLIMIENTO DE LOS REQUISITOS DEL SISTEMA.

SCO Unix requiere los requisitos minimos del sistema que se indican a continuación:

- ordenador de tipo servidor con procesador Pentium o superior.
- Adaptador de video con resolución VGA o superior (SVGA recomendado).
- 700 MB de espacio libre en disco.
- 32 MB de memoria RAM
- Una o varias tarjetas de red.
- Unidad de CD-ROM capaz de leer discos inicializados homologados por la Norma ISO 9660.
- Se recomienda un ratón serie o PS/2, aunque no es obligatorio.

3.3.2 INTRODUCCIÓN A LA INSTALACIÓN.

El SO está conformado por un conjunto de paquetes de software los cuales controlan las acciones de su sistema de ordenador, este hace que las tareas que podrían ser muy complejas para el usuario se conviertan en tareas fáciles. SCO UNIX es un sistema operativo de red el cual es considerado como un sistema multitarea, ya que se pueden realizar varias tareas al mismo tiempo; y multiusuario, porque varios usuarios pueden hacer uso del sistema en un mismo tiempo.

La distribución de SCO UNIX 3.2 v. 4.2, puede adquirirse en Discos, Cinta CD.

Distribución en discos debe contener lo siguiente:

- Dos disquetes etiquetados con N1 (Boot) y N2 (*filesystems* de root).
- Un disquete etiquetado con M1 (Master Installation Floppy).
- Utilerías básicas, los cuales son un conjunto de disquetes etiquetados con la letra B.

⁸ Rey de Perea Campos J. Escuela de Administración de Negocios, E . A . N . ; Taller práctico sobre el sistema operativo unix; diplomado en informática; Universidad de Almería España. En línea [URL], <http://www.ual.es/~jperea/documentacion/unix/Taller.exe>

- Utilerías extendidas, un conjunto de disquetes etiquetados con la letra X.

3.3.3 PROCEDIMIENTO DE INSTALACIÓN.

Insertar el disco con la etiqueta N1 y prender el equipo, después de un momento aparecerá un prompt como el siguiente:

Boot:

Si el Disco necesita controladora Presione Aquí, de lo contrario solo presione la tecla [ENTER].

El sistema pedirá ahora el disco con la etiqueta N2 lo que inicializará el ambiente de instalación interactivo, la primera pregunta que se presenta es la siguiente:

- Fresh installation.
- Update installation.
- Salir (Exit).

Se debe elegir la opción 1, para realizar una nueva instalación.

A continuación se pide seleccionar el tipo de teclado:

- American.
- British.
- French.
- German.
- Italian.
- Spanish.

Seleccione el número que corresponda a su tipo de teclado, preferentemente elija la opción 1
Seleccionar la clase de instalación:

- Instalación completa, configurable.
- Instalación automática.
- Salir.

Elegir la opción 1. Esta opción es utilizada para sistemas con requerimientos especiales. Permite especificar los tamaños de las particiones del sistema UNIX, así como preservar *filesystem* existentes, espacios para el área de swap y preservar las particiones que no sean de Unix.

Activar particiones o crearlas

3.3.3.1 CONFIGURACIÓN DEL DISCO DURO.

- Desplegar los parámetros actuales.
- Modificar parámetros.
- Seleccionar parámetros default.

Seleccionar la Opción: q
fdisk de UNIX SCO

- Despliega la partición del disco.
- Usar el disco completo para UNIX.
- Usar el resto del disco para UNIX.
- Crear partición UNIX
- Activar partición.
- Borrar partición.

Opción: ?

? Dependiendo de la actividad a realizar, elegir el número correspondiente.

? = 2 En el caso de que todo el disco sea para UNIX.

Verificar el disco.

- Verificar partición de UNIX.
- Verificar un rango específico de pistas.
- Verificar un *filesystem* específico.

Elegir opción 1

- Scan rápido
- Scan profundo

Elegir opción 1

¿Deseas que el scan sea destructivo (Y/N)?

Elegir : Y

¿Deseas continuar (Y/N)? "se destruirán todos los datos"

Elegir : Y

Después de que se haya verificado, elegir la opción: q, para continuar con la instalación.

Preservar los *filesystems*.

Y. En caso que el disco ya tenga instalado UNIX puede preservarse los *filesystems*, y se elige la opción:

En caso de que no se quieran preservar o de que no se tengan los *filesystems* se elige la opción: N
Se cuenta con la opción de hacer ajustes manuales (utilería divvy), esto nos permite particionar nuestros *filesystems* y áreas de acuerdo a los requerimientos del usuario.

Nota. El *filesystem* de root debe de encontrarse en los primeros 1024 cilindros.

n- nombre.

t- tipo de *filesystem*.

s- inicio de bloque.

e- fin de bloque.

r- restaura la tabla original.

NOTAS:

El área de **swap** debe ser el doble del área de RAM.

El *filesystem* **u** se crea y se le da el nombre.

El área de **ope** solo se le asigna un nombre.

Para salir elegir: q

Para que tome las particiones que se le dieron elegir la siguiente opción:

i[install]

En caso de que se requiera hacer alguna modificación elegir la siguiente opción;

r[regresar]

Si se eligió la opción **i** eso hará que se empiecen a crear los *filesystem*.

NOTA:

El disco N2 debe estar dentro del drive.

El sistema pedirá que se inserten los siguientes discos:

N1 (Boot)

M1

B1

B2

B3

Número de serie (Serial Number): 2BC000888

Llave (KEY): qocljvyl

3.3.4 CONFIGURACIÓN DE LA ZONA GEOGRÁFICA.

Te encuentras en Norteamérica (Y/N)

Elegir la opción N

Escribe tu localización con 1-9 caracteres: Toluca

A cuántas horas del meridiano de greenwich te encuentras: -6

Deseas horario de verano (Y/N)

Elegir la opción N

Introduce la fecha y hora con el siguiente formato ([yymmdd] hhmm)

3.3.5 INSTALACIÓN DE SOFTWARE ADICIONAL.

1. - Instalar software adicional (utilerías)

2. - Proceder con la configuración.

Elegir opción 1

Al elegir la opción uno nos muestra el siguiente menú:

INSTALL	REMOVE	LIST	QUIT
---------	--------	------	------

Elegir la opción INSTALL.

Elegir nuevo producto

Producto completo

Insertar los discos conforme te los pida, del X1 al X7

Salir del menú.

Posteriormente te pedirá los siguientes datos:

Nombre del equipo.

Especificar el nivel de seguridad.

1. -Alta seguridad.

2. -Seguridad mejorada.

3. -Seguridad tradicional.

4. -Baja seguridad.

Elegir opción 3

1. -Correr el sistema administrador.

2. -Continuar.

Elegir opción 2

3.3.6 COLOCAR PASSWORD.

- 1.- Pick a password.
2. - Pronunciable password.

Elegir opción 1

3.3.7 REINICIAR EL SISTEMA

Con esto finaliza la instalación del SCO Unix ⁹

3.4. ESTRUCTURA DEL SISTEMA DE ARCHIVOS (FILE SYSTEM).

3.4.1 EL SISTEMA DE ARCHIVOS

“El sistema de archivos o file system es la forma en el que UNIX gestiona los archivos existentes en el sistema. El sistema de archivos está caracterizado por:

- Una estructura jerárquica.
- Un tratamiento consistente de los archivos de datos.
- Habilidad para crear y borrar archivos.
- Crecimiento dinámico de los archivos.
- Protección de los archivos de datos.
- Tratamiento de los dispositivos periféricos como archivos.

El sistema de archivos está organizado como un árbol con un único nodo raíz llamado root (se representa con “/”); cada nodo que no es hoja de la estructura del sistema de archivos es un directorio de archivos. Cada archivo está identificado por un nombre de archivo. El nombre de archivo viene dado por un nombre de camino o ruta (*path name*) que describe como localizarlo en la jerarquía del sistema de archivos. Un nombre de camino es una secuencia de nombres de componentes separados por caracteres “/”; una componente es una secuencia de caracteres que identifica un archivo que está contenido en el componente precedente (directorio).

Un camino completo comienza con un carácter “/” y especifica un archivo que puede ser encontrado empezando en el nodo raíz del sistema de archivos. Así, “/etc/passwd”, “/bin/who” y “/usr/src/cmd/who.c” son caminos completos que identifican archivos en el árbol mostrado en la figura III.3, pero “/bin/who” y “/usr/src/date.c” no. Un camino no tiene porqué empezar desde el root ya que pueden ser identificados de forma relativa al directorio actual o de trabajo de un proceso en ejecución, omitiendo el carácter “/” inicial en la ruta.

⁹ Correa García I. Instalación del Sistema Operativo SCO Unix. En línea [URL], <http://software.uaemex.mx/documentos/SCO/indice.html>

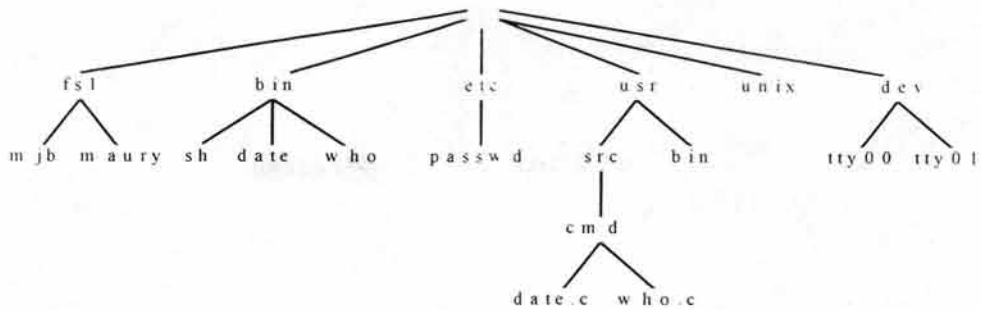


figura III.3

Por ejemplo, si nos encontramos en el directorio src, la ruta cmd/date.c identifica un archivo existente en el árbol.

3.4.2 CONCEPTOS BÁSICOS SOBRE ARCHIVOS.

El sistema de archivos de UNIX consiste en un conjunto de archivos. En UNIX, un archivo es una secuencia de bytes. El sistema no impone estructura alguna a los archivos, ni asigna significado a su contenido; el significado de los bytes depende únicamente de los programas que interpretan el archivo. Además, como veremos más adelante, esto es cierto no sólo para archivos en disco sino también para dispositivos periféricos. Cintas magnéticas, mensajes de correo, caracteres tecleados, salida para impresora, datos que fluyen en interconexiones, cada uno de estos archivos no son más que una secuencia de bytes desde el punto de vista del sistema y sus programas.

Hay tres tipos de archivos:

- Archivos ordinarios, que contienen datos.
- Archivos especiales, que permiten el acceso a dispositivos como terminales e impresoras y que también tienen otros propósitos.
- Directorios, que contienen información sobre un conjunto de archivos y que se emplean para localizar un archivo por su nombre.

La representación interna de un archivo viene dado por un nodo, el cual contiene una descripción del almacenamiento físico del archivo e información acerca del propietario del archivo, permisos de acceso y tiempos de acceso. Será descrito más adelante. Todos los archivos tienen un inodo, pero puede tener varios nombres, todos ellos accederían al mismo inodo. Cada nombre se denomina enlace. Cuando un proceso referencia un archivo por su nombre, el kernel analiza el nombre de archivo de cada componente, comprueba que el proceso tiene permiso para buscar los directorios en la ruta y recupera el inodo correspondiente al archivo. Por ejemplo, si un proceso realiza la llamada

```
Open ("/fs2/mjb/rje/sourcefile",1);
```

El kernel busca el inodo de "/fs2/mjb/rje/sourcefile". Cuando un proceso crea un nuevo archivo, el kernel le asigna un inodo libre. Los inodos se almacenan en el sistema de archivos, tan pronto como sea posible, pero el kernel los lee desde una tabla de inodos en memoria principal cuando manipula archivos.

En el UNIX tradicional un nombre de archivo es de máximo 14 caracteres. En el BSD y el System V Release 4 pueden ser hasta de 256 caracteres. Las extensiones no son separadas necesariamente por punto. Existen caracteres que pueden causar conflictos en el intérprete de comandos. Por lo tanto deben evitarse en un nombre de archivo. Estos son:

., S. & ! () , ; < > , @ , ^ , { , } , [, . , * , ? , \ , <Space> , <Tab> , <Backspace>

No se deben usar tampoco caracteres invisibles (caracteres de control) ni caracteres de opción de comando (+, -).

Un archivo está almacenado en bloques. Existen dos tipos de bloques:

- Bloque lógico: Se define como la unidad mínima de asignación de espacio de almacenamiento.
- Bloque físico: Se define como la mínima unidad de lectura y escritura de un disco. También se conoce como el sector de un disco. El tamaño estándar es de 512 bytes.

El bloque lógico es siempre igual o mayor que el bloque físico. Lo mínimo que el sistema operativo UNIX asigna a un archivo es un bloque lógico, así se tenga un archivo con un tamaño real menor al tamaño del bloque lógico.

Por ejemplo: si se define un bloque lógico de 1K, y se tiene un archivo que ocupa 1200 bytes, entonces a este archivo le corresponderían dos bloques lógicos, pero si nos damos cuenta siempre se va a tener una pérdida o desperdicio de memoria, al menos que el tamaño real del archivo sea múltiplo del bloque lógico que se le asigne.

3.4.3 ESTRUCTURA INTERNA DEL SISTEMA DE ARCHIVOS.

Los distintos sistemas de archivos tienen básicamente la misma estructura, que se muestra en la figura III.4, la cual está formada por cuatro partes fundamentales:

- Bloque de arranque (*boot block*): Es el bloque 0 de todo sistema de archivos. Está reservado al programa de carga inicial (*bootstrap*) y contiene la información necesaria para arrancar el sistema. Aunque solo es necesario un bloque de arranque, todos los sistemas de archivos del sistema tienen un bloque de arranque (posiblemente vacío).
- Superbloque (*super block*): Es el bloque 1. Contiene la información más importante del sistema de archivos y contiene los siguientes campos:
 - El tamaño del sistema de archivos.
 - El número de bloques libres.
 - Una lista de los bloques libres disponibles.
 - El índice del siguiente bloque libre en la lista de bloques libres.
 - El tamaño de la lista de inodos.
 - El número de inodos libres.
 - Una lista de inodos libres.
 - El índice del siguiente inodo libre en la lista de inodos libres.
 - Un flag indicando que el súper bloque ha sido modificado.
 - Campos de bloqueo para las listas de bloques libres e inodos libres.

- Lista de inodos (*inode list*): Esta lista está formada por un número de bloques que contiene el número de inodos especificado en el superbloque, que varía dependiendo del número total de bloques que tenga el sistema de archivos. La longitud de la lista de inodos se determina en el momento de creación del sistema de archivos.

- Bloques de datos (*data block*): El resto del dispositivo lógico está formado por los bloques de datos. Son matrices unidimensionales y contienen los datos realmente almacenados en directorios, archivos y bloques de punteros a bloques de datos y a bloques de la lista libre.



figura III.4

3.4.4 DESCRIPCIÓN DEL INODO.

Como hemos visto anteriormente, los sistemas de archivos en UNIX utilizan una estructura en disco, denominado inodo, para almacenar información sobre cada archivo. El contenido de un inodo, mostrado en la figura III.5, es el siguiente:

- Modo: Su tamaño es de 2 bytes. Incluye el tipo de archivo y permisos de acceso. Se dedica 4 bits al tipo de archivo, 9 a los permisos de acceso y 3 a los permisos especiales.
- Cuenta de enlaces: Representa el número de nombres que tiene el archivo en la jerarquía de directorios.
- Identificador del usuario propietario (valor decimal).
- Identificador del grupo del propietario (valor decimal).
- Tamaño del archivo (en bytes).
- Direcciones de bloque: Su tamaño es de 40 bytes. Su utilización depende del tipo de archivo:
 - Ordinarios y directorios: Contiene 13 punteros (10 punteros directos, un indirecto simple, un indirecto doble y un indirecto triple) como se describe en la figura III.6.
 - Especiales: Sólo se utilizan 4 bytes y en lugar de contener los punteros a bloques contienen el número principal (*major*) y secundario (*minor*) del dispositivo.
- Fecha de acceso: Fecha y hora en que fue accedido por última vez (lectura / escritura).
- Fecha de modificación: Fecha y hora de la última vez que fue modificado.
- Fecha de cambio de inodo: Fecha y hora en que el inodo del archivo fue modificado (por ejemplo, cambio en los permisos de acceso).

Modo
Cuenta de enlace
ID. de usuario
ID. de grupo
Tamaño del archivo
Direcciones de bloque
Fecha de acceso
Fecha de modificación
Fecha de cambio de inodo

figura III.5

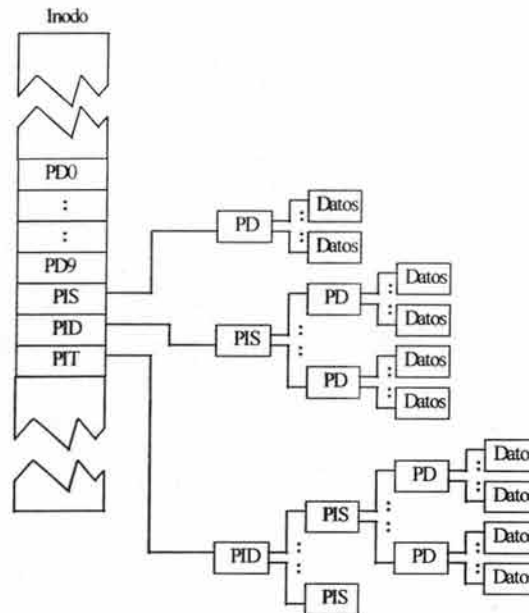


figura III.6

3.4.5 DIRECTORIOS.

Como hemos visto, los directorios son los archivos que proporcionan al sistema de archivos su estructura jerárquica; ellos juegan un importante papel en la conversión de un nombre de archivo a un número de inodo. Un directorio es un archivo cuyos datos son una secuencia de entradas, cada una de ellas constituida por un número de inodo y el nombre de un archivo contenido en el directorio. Los bloques de almacenamiento de los directorios en los primeros sistemas de archivos que se diseñaron tienen el formato mostrado en la figura III.7.

Inodo	Nobre del archivo
20	.
2	..
45	datos
53	fich
:	:
:	:

figura III.7

Cada entrada en el directorio ocupa 16 bytes; de los cuales, dos corresponden al número de inodo y 14 al nombre del archivo. Como se puede observar, todo directorio comienza con dos entradas como mínimo: un identifica al directorio actual ('.') y la otra al directorio padre ('..').

Existen otros sistemas de archivos que permiten nombres de archivos de hasta 255 caracteres, como es el caso de los sistemas de archivos *ufs*.

3.4.6 DISPOSITIVOS Y ARCHIVOS ESPECIALES.

Cuando un programa accede a un determinado dispositivo mediante una llamada al sistema, establece una comunicación con el driver correspondiente al dispositivo usado. Esta comunicación no es directa, existe un punto de unión entre el programa y el driver correspondiente. En la figura III.8 se representa esta relación.



figura III.8

Todos los dispositivos en UNIX son tratados como archivos. Estos archivos especiales (*device special file*), conocidos también como nodos de dispositivos (*device nodes*) constituyen el medio de acceso a los dispositivos. Entre los dispositivos que aparecen se encuentran los dispositivos de cinta, impresoras, particiones de disco y terminales. Básicamente existen dos tipos de archivos especiales:

- Archivos especiales tipo bloque: Se emplean para manejar dispositivos cuya unidad mínima de tratamiento de información es el bloque.
- Archivos especiales tipo carácter: Se emplean para dispositivos cuya unidad mínima de tratamiento de información es el carácter. También se engloban dispositivos que utilizan un tamaño distinto del bloque.

Estos archivos en realidad están vacíos. El sistema emplea dos números enteros, denominados número principal o mayor (14 bits) y un número secundario o menor (18 bits) y almacenados en el inodo del archivo, para acceder al dispositivo asociado.

El número principal identifica una clase de dispositivo (en realidad identifica al driver de dicha clase como pueden ser terminales, impresoras, discos, etcétera.) y el número secundario identifica a un elemento de dicha clase (un terminal específico, un disco concreto,...).

3.4.7 ACCESO A LOS ARCHIVOS.

Desde el punto de vista del acceso a un archivo, existen tres tipos de usuarios a los que se les pueden dar o denegar permisos sobre un archivo:

- | | | |
|-----|--------|---|
| (u) | user | Propietario del archivo. |
| (g) | group | Usuarios pertenecientes al grupo del propietario. |
| (o) | others | Resto de usuarios que no pertenecen al grupo. |

La capacidad de un usuario para trabajar con archivos depende del tipo de acceso que tenga a dicho archivo. Los accesos disponibles en UNIX son:

Para un archivo:

- Permiso de lectura (r): Permite ver el contenido del archivo.
- Permiso de escritura (w): Permite cambiar el contenido del archivo.
- Permiso de ejecución (x): Permite ejecutar un archivo (como cualquier orden de UNIX).

Para un directorio:

- Permiso de lectura (r): Permite ver los nombres de los archivos de un directorio. Si se quiere información detallada sobre dichos archivos el directorio tiene que tener el permiso de ejecución para dicho usuario.
- Permiso de escritura (w): Permite cambiar el contenido de dicho directorio; crear nuevos archivos, suprimir los existentes (este último caso depende de los permisos de escritura de los propios archivos).
- Permiso de ejecución (x): Se debe hablar más bien de permiso de búsqueda ya que permite situarse en dicho directorio y según el resto de los permisos, permitirá crear, borrar, modificar o copiar archivos.

Además de los permisos de acceso rwx para el propietario del archivo, el grupo al que pertenece el propietario y resto de usuarios, existen tres permisos especiales que afectan cuando se emplea el archivo como programa ejecutable. Estos modos sólo se aplican a archivos ejecutables y sólo el súper usuario puede fijarlos. Estos son:

- set-uid Permite fijar el identificador de usuario (valor octal 4000), e indica que cuando el programa se ejecuta, el identificador de usuario pasa a ser el del propietario del archivo.
- set-gid Permite fijar el identificador de grupo (valor octal 2000), e indica que cuando el programa se ejecuta, el identificador de grupo pasa a ser el del grupo propietario del archivo.
- sticky BIT Se denomina "BIT de adherencia"(valor octal 1000) y se aplica a programas que son compartibles por muchos usuarios. Con el BIT de adherencia se consigue que el programa no abandone el espacio de intercambio (swap) aunque nadie lo esté utilizando. Se suele aplicar a programas de uso intensivo para mejorar sus tiempos de respuesta.

Los dos primero permisos son de utilidad para programas, como mail, que deben crear archivos en directorios no necesariamente poseídos por la persona que ejecuta el programa.

3.5 UNIX EN EL ÁMBITO DE USUARIO.

3.5.1 TIPOS DE USUARIO.

Para usar un sistema UNIX es necesario estar registrado como uno de sus usuarios. Cada usuario tiene un nombre de ingreso al sistema, una contraseña y un área del sistema de archivos reservada para almacenar sus archivos.

Básicamente, existen dos tipos de cuentas de usuarios:

- Cuentas de usuarios ordinarios: Son las más comunes. Contienen la siguiente información:

- Un nombre de usuario (login).
- Una clave de acceso o palabra de paso (password).
- Un identificador de grupo.
- Un directorio personal (home directory, \$HOME).
- Un "shell" de conexión o de ingreso (login "shell").

- Cuenta de súper usuario: Cualquier sistema UNIX debe tener un superusuario. Es la persona encargada de administrar el sistema; por ejemplo se encarga de crear nuevos usuarios, configurar dispositivos,... El súper usuario tiene el nombre "root" como nombre de usuario. Se identifica porque en pantalla aparece un prompt diferente al de un usuario normal (normalmente el carácter "#"). El súper usuario tiene acceso a todos los archivos y directorios del sistema.

El archivo /etc/passwd tiene información acerca de las cuentas de usuarios existentes en el sistema. Este archivo sólo puede ser modificado por el súper usuario.

3.5.2 GRUPOS.

El sistema UNIX proporciona un entorno particularmente bueno para grupos de personas (usuarios) que trabajen conjuntamente en el mismo proyecto o proyectos relacionados. Cada usuario pertenece a un grupo. Algunos sistemas permiten que un usuario pertenezca a más de un grupo, y no es necesario que un grupo tenga más de un usuario. El grupo tendrá asignado un nombre de grupo e identificador de grupo. El grupo se establece al crear la cuenta de un usuario.

Cada usuario es conocido en el sistema de forma individual o como miembro de un grupo. Como miembro de un grupo, un usuario puede tener permiso para acceder a archivos y directorios a los que no tendría de forma personal.

El archivo /etc/group tiene información acerca de los grupos existentes en el sistema. Este archivo sólo puede ser modificado por el súper usuario.

Estos archivos, el /etc/passwd y el /etc/group,

3.5.3 CONEXIÓN AL SISTEMA.

Para poder entrar en una cuenta aparece el llamado system login prompt:

```
eancol
```

```
Welcome to SCO UNIX System V/386 Release 3.2
```

```
eancol!login:
```

Donde "eancol" es el nombre del host o hostname. Se introduce el nombre de usuario (también conocido como *login name, user id o account*). A continuación se nos pedirá la palabra de paso o clave de acceso:

```
Password:
```

y aparecerá información sobre la última conexión al sistema y revisión de SCO:

```
Last successful login for <user>: <fecha> <hora> on <terminal>
```

```
Last unsuccessful login for <user>: <fecha> <hora> on <terminal>
```

```
SCO UNIX System V/386 Release 3.2
```

```
Copyright © 1976-1990 UNIX System Laboratories, Inc.
```

Welcome to SCO UNIX System V/386 Release 3.2
From
The Santa Cruz Operation, Inc.
Terminal type is ANSI

Después se ejecutaría un archivo de configuración existente en el home directory del usuario. Cada "shell" tiene sus propios archivos de configuración.

El "shell" **Bourne**: El archivo de configuración que utiliza es:

- .profile Órdenes que se ejecutan antes del "shell".

El "shell" **C**: Los archivos de configuración que utiliza son los siguientes:

- .cshrc Se ejecuta inicialmente. Contiene órdenes.
- .login Se ejecuta después que el archivo anterior y contiene órdenes para especificar el tipo de terminal y las variables de entorno.
- .logout Órdenes que se ejecutan cuando se desea abandonar el "shell".

Después se ejecutaría el "shell" de ingreso y aparecerá el prompt correspondiente.

3.5.4 DESCONEJIÓN.

Se utiliza cuando se termina el trabajo con UNIX. Se conoce como "logout" o "log off". Se realiza escribiendo logout o exit. En otros sistemas UNIX, también se puede mediante <Ctrl>-d (fin de archivo).

3.6 EL "SHELL".

Un "shell" o intérprete de comandos es un programa que interpreta y ejecuta los mandatos conforme se proporcionan desde la terminal. No se requiere ningún privilegio especial para ejecutar un "shell"; para el kernel de UNIX, un "shell" es como cualquier otro programa. Entre las características más comunes de un "shell" están la interpretación de procedimientos de "shell", la expansión de caracteres comodines en nombres de archivos, la combinación de mandatos para formar interconexiones, la recuperación de mandatos previos, las construcciones condicionales y los ciclos, y las variables para crear abreviaturas.

El "shell" que se invoca cuando se ingresa al sistema se denomina "shell" de ingreso. El "shell" de ingreso de cada usuario se especifica en el campo correspondiente en el archivo /etc/passwd. El administrador del sistema que establece la cuenta de un usuario define su "shell" de ingreso y es el único que puede cambiarlo. Sin embargo, un usuario puede cambiar su "shell" de ingreso si coloca el mandato:

```
exec "shell"
```

al final de su archivo de iniciación de ingreso. Este mandato transfiere el control de su terminal específicamente al "shell". También se puede cambiar de "shell" durante una sesión, introduciendo el nombre del "shell". Por ejemplo: csh, ksh, etcétera.

A continuación se comentan algunas características de los "shells" más utilizados.

3.6.1 EL "SHELL" BOURNE (sh).

El "shell" Bourne, sh, escrito por Steve Bourne en 1979, es parte de la séptima edición de UNIX y el primero de los "shells" principales. Los "shells" más nuevos son más sencillos de usar porque ofrecen recursos de los que carecía el "shell" Bourne, como la edición de líneas de mandatos, la recuperación de mandatos emitidos previamente y los alias para los mandatos de uso común. No obstante, muchos usuarios de UNIX prefieren el "shell" Bourne para uso interactivo. Casi todos los procedimientos de "shell" siguen los convencionalismos del "shell" Bourne.

Entre los recursos importantes que ofrece "shell" están los siguientes:

- Operadores para la ejecución en segundo plano, o ejecución condicional de mandatos.
- Enunciados para repetir la ejecución de mandatos, incluida la iteración a lo largo de una secuencia de valores que pueden asignarse a una variable de iteración.
- Variables sustituibles, tanto nombradas como numeradas. Las variables numeradas, también conocidas como parámetros o parámetros de posición, contienen los argumentos de un mandato.
- Exportación de variables específicas a un proceso hijo.
- Tres formas de entrecomillado.
- Ejecución de mandatos en subshells.
- Notificación automática de la llegada de correo.
- Inclusión de datos de entrada para un mandato en un procedimiento de "shell" como parte del procedimiento.
- Atrapado de señales y ejecución de mandatos específicos cuando ocurre una señal determinada.
- Ejecución de mandatos en archivos de iniciación antes de leer cualquier entrada. Estos archivos de iniciación pueden servir para adecuar sh a las necesidades propias.

3.6.2 EL "SHELL" C (csh).

El "shell" C, disponible a través del mandato *csh*, se desarrolló como parte de BSD UNIX. A pesar de su nombre, el "shell" C no es mucho más parecido a "C" que el "shell" Bourne. Algunas de las características del "shell" C que no se incluyen en el "shell" Bourne son:

- La posibilidad de recuperar mandatos previos mediante un mecanismo de "historia".
- La capacidad de conmutar entre procesos y controlar su avance ("control de trabajos").
- Formas más flexibles de sustitución de variables.
- Operadores adicionales, como aparecen en "C".
- Alias para mandatos de uso frecuente. sin tener que usar procedimientos de "shell".

Varios de los mandatos en *csh* se comportan igual que sus contrapartes de *sh*.

3.6.3 EL "SHELL" KORN (*ksh*).

El "shell" Korn, *ksh*, ofrece una síntesis de las características de los "shell" Bourne y "C", además de otras propias. Fue desarrollado por David Korn, de AT&T Bell Laboratories, en 1982, presentando versiones mejoradas en 1986 y 1988. Se incluye como característica estándar de la versión 4 de System V y otros sistemas; También se puede obtener por separado.

El "shell" Korn sigue de cerca los convencionalismos del "shell" Bourne, y casi todos los procedimientos de "shell" escritos para el primero funcionan con el segundo. Las características principales que se adoptaron del "shell" C son:

- Listas históricas para la recuperación de mandatos previos.
- Control de trabajos, con la capacidad para pasar trabajos específicos al primer plano o al segundo.
- Alias para los nombres de mandatos.
- Empleo de '~' para representar el directorio base del usuario o, al combinarse con un nombre de usuario, el de otro usuario.
- Capacidad para calcular expresiones numéricas generales y asignar el resultado a una variable.

Algunas de las características nuevas de *ksh* son:

- Edición interactiva de la línea de mandatos, incluida la complementación de nombres de archivo con las mismas características de *csh* y la posibilidad de editar la lista histórica.
- Mejores definiciones de funciones, que ofrecen variables locales y permiten escribir funciones recursivas.
- Comparación extendida de patrones para nombres de archivos y otras construcciones, parecidas a la de *egrep*.
- Capacidad para extraer la porción de una cadena especificada por un patrón.
- Capacidad para cambiar fácilmente de un directorio a otro.

3.6.4 EL "SHELL" C MEJORADO (*tcsh*).

El "shell" *tcsh* es una versión mejorada del "shell" C que ha adquirido mucha popularidad. Algunos de los recursos adicionales que ofrece son:

- Capacidad para editar la línea de mandatos interactivamente.
- Llamada sencilla de mandatos ejecutados con anterioridad, los cuales se pueden editar.
- Complementación interactiva de nombres de archivos y mandatos.
- Consulta de la documentación de un mandato al momento de teclearlo.
- Capacidad para programar la ejecución periódica de un mandato.

- Marcas de la hora en la lista histórica.

3.6.5 PROCEDIMIENTOS DE "SHELL" O "SHELL" SCRIPTS.

Un procedimiento de "shell" es un archivo que contiene secuencias de mandatos de "shell", igual que si se hubieran tecleado. Los procedimientos de "shell", también llamados "shell" scripts, permiten adecuar el entorno añadiendo mandatos propios. Aunque la escritura de un script requiere un poco de programación, es mucho más fácil que escribir un programa en "C".

Cuando un "shell" detecta un mandato que no es intrínseco, es decir, uno que el "shell" no reconoce y ejecuta directamente, llama al kernel para que lo ejecute. El mandato puede ser un programa compilado o un "shell" script. En el segundo caso, el kernel tiene que seleccionar un "shell" para ejecutar el script. Este "shell" hijo se denomina subshell.

La manera como el kernel hace su elección depende del sistema. El caso por omisión es siempre una versión del "shell" Bourne o, en algunas ocasiones, el "shell" Korn (que es casi compatible con aquél). La compatibilidad con el "shell" Bourne es esencial porque, históricamente, éste era el único disponible en la séptima edición; varios procedimientos de "shell" de uso común suponen, sin indicación explícita, que son interpretados por el "shell" Bourne.

La mayoría de los sistemas se adhieren al convencionalismo de BSD UNIX que especifica que la primera línea de un procedimiento de "shell" tiene la forma

```
#! shell
```

Donde "shell" es el nombre de la ruta completa del "shell" que se usa para interpretar el script. El espacio en blanco después de "#!" es opcional. Por ejemplo, si se escribe un guión usando el conjunto de mandatos del "shell" C, deberá comenzar con

```
#! /bin/csh
```

Algunos sistemas que no respetan el convencionalismo "#!" ofrecen otra manera de etiquetar los procedimientos de "shell": si el primer carácter es ".", se considera como un script del "shell" Bourne; si el primer carácter es "#", se considera como un script del "shell" C.

3.7 COMANDOS MÁS COMUNES.

3.7.1 SINTAXIS DE LAS ÓRDENES.

Una orden o comando es una secuencia de palabras por uno o más espacios en blanco. Formato:

```
NombreOrden Opción(es) Expresión NombreArchivo(s)
```

La primera palabra es la propia orden. El resto de las palabras son argumentos de la orden. Estos son los argumentos de las órdenes:

- Opción(es): Es una literal, normalmente precedida por el signo menos. Por ejemplo: -al. Una opción modifica la acción de la orden de alguna manera o da detalles de cómo tiene que funcionar exactamente.
- Expresión: Describe una cadena de caracteres que se va a utilizar como entrada para la orden.
- NombreArchivo(s): Nombre de uno o más archivos que la orden va a manipular de alguna manera.

Ejemplos:

rm -fi datos.txt fich.pas	Borra dos archivos con las opciones "f" e "i".
grep "Hola" saludo	Busca patrones en un archivo donde el primer argumento es una expresión y el segundo argumento es un nombre de archivo.

Si por alguna razón tiene que utilizar un argumento que contiene un espacio o bien tiene que limitarlo, el argumento entero debería colocarse entre comillas dobles ("") o entre comillas simples o apóstrofes.

3.7.2 METACARACTERES.

El "shell" reconoce como especiales una serie de caracteres, a los que se les denomina como meta caracteres. Tienen varias aplicaciones, que a continuación se describen.

3.7.2.1 CARACTERES COMODINES.

Estos caracteres se utilizan para sustituir una secuencia de caracteres. Entre los más importantes están:

?	Identifica a un único carácter.
*	Identifica a una cadena de caracteres.
~	Abreviatura del home directory.
.	Abreviatura del directorio de trabajo actual.
..	Abreviatura del directorio padre del actual.
[..]	Proporciona un sólo carácter de los que aparecen entre los corchetes.
[x-y]	Proporciona algún carácter dentro del rango x, y. Se pueden especificar varios rangos o combinar rangos con caracteres. No hace falta ningún carácter separador.

3.7.2.2 REDIRECCIONAMIENTO DE LA E/S.

Estos caracteres se usan para cambiar la entrada estándar (que es el teclado) o la salida estándar (que es el monitor). Son los siguientes:

>	Redirecciona la salida hacia un archivo o dispositivo. Si el archivo existe, dará error.
>>	Añade la salida a un archivo.
<	Redirecciona la entrada de un archivo. Hay comandos que no aceptan el redireccionamiento de entrada.
cmd << word.	Indica que un comando o un programa, cmd, normalmente interactivo, acepta sus órdenes desde el mismo archivo o dispositivo (usualmente un "shell" script). Word se interpreta literalmente como la marca de fin de entrada para el comando.
>&	Salida de errores: Cuando se produce un error, se usa un canal diferente (que el de salida) para informar del error. Se puede enviar los errores a otro archivo o dispositivo.
" "	Comillas simples: Es otra forma de redireccionar la salida. Se ejecuta primero lo que se encuentra entre las comillas, y el resultado puede servir como argumento para otro comando.

Por ejemplo:

rm *	No elimina los archivos ocultos.
rm 'ls -a'	Elimina todos los archivos.

3.7.3.3 PIPE. PIPELINE.

Un pipe consiste en usar la salida de una orden como entrada a otra orden. Se representa con el carácter "|". Un pipeline o interconexión es un conjunto de órdenes unidas por pipes. Por ejemplo:

```
ls /etc | wc
```

Muestra el número de líneas, palabras y caracteres del listado del directorio /etc.

3.7.2.4 LÍNEAS MULTICOMANDO.

;
\
(
(Date;who) | wc

Separa órdenes en una línea de entrada, ejecutando una detrás de otra.
Al final de una línea, permite continuar la orden en la siguiente línea de entrada. En otro caso, antecede a un carácter con significado especial.
Se utilizan para agrupar comandos. Por ejemplo:
Ejecuta el comando date y después el who. La salida de ambos sirve como entrada al comando wc.

3.7.3 ÓRDENES DE MANIPULACIÓN DE DIRECTORIOS.

- Cambiar de directorio (cd - Change Directory).

Sintaxis:

```
cd [<dir>]
```

casos especiales:

```
cd ..  
cd $HOME  
cd $home  
cd
```

El primer caso especial permite situarse en el directorio padre del directorio actual. Los otros tres casos nos permiten situarnos automáticamente en nuestro directorio de trabajo (home directory).

Mostrar el directorio actual (pwd - Path Work Directory).

Sintaxis:

```
pwd
```

Crear un directorio (mkdir - MaKe DIRectory).

Sintaxis:

```
mkdir <dir>
```

Borrar un directorio (rmdir - ReMove DIRectory).

Sintaxis:

```
rmdir <dir>
```

Renombrar un directorio (mv - MoVe).

Sintaxis:

```
mv <dir-antiguo> <dir-nuevo>
```

Esta orden no cambia el contenido del directorio.

Copiar directorios (cp - COPY)

Sintaxis:

```
cp -R <dir-origen> <dir-destino>
```

Copia recursivamente los archivos y directorios que contenga (subdirectorios).

Mostrar el contenido de un directorio (ls - LiSt)

Sintaxis:

```
ls [aFRxt] [<dir>]
```

El comando "l" es equivalente a "ls -l". Significado de la descripción detallada de "ls -l":

```
...
drwxr-x---2      julio group 224          Jul 19 11:19  bin
drwxr-x---      2 julio group 336      Jul 17 17:14  fuentes
-rw-r-----    1 julio group 24        Jul 25 15:57  cx
-rwxr-x--x     1 julio group 35        Jul 19 11:44  whiet
```

- El primer campo es el modo del archivo. La primera columna nos indica el tipo de archivo (- ordinario, d directorio, b archivo especial de bloque, c archivo especial de carácter, l archivo simbólico, p archivo especial FIFO). El resto del campo nos dice cuáles son los permisos del archivo.

- Número de enlaces. Para archivos es normalmente 1. Si es mayor de 1 indica que existen entradas en otros directorios apuntando a ese archivo. Para directorios, indica el número de entradas de subdirectorios que contiene.

- Nombre del propietario. Muestra el nombre del propietario del directorio o archivo.
- Nombre del grupo del propietario.
- Tamaño del archivo, en bytes. Para archivos de texto es el número de caracteres.
- Fecha y hora de la última modificación.
- Nombre del archivo.

Otras opciones de la orden *ls* son:

ls -x Lista los archivos por columnas.

ls -F Marca los directorios con '/', los archivos ejecutables con '*' y los enlaces simbólicos con '@'.

ls -t Lista ordenada según el tiempo de la última modificación.

ls -R Visualiza los contenidos de cada subdirectorio a partir del indicado (opción recursiva).

ls -g Igual que la opción '-l', excepto que el propietario no es mostrado.

ls -a Muestra los archivos ocultos. Los archivos ocultos son los que empiezan con el carácter '.'. Por ejemplo: .profile, cshrc

3.7.4 ÓRDENES DE MANIPULACIÓN DE ARCHIVOS.

Mostrar el tipo de un archivo.(file)

Sintaxis:

```
file <filename>
```

Determina el tipo de un archivo examinando su contenido. Algunas de los posibles resultados son:

<filename> : ASCII text
<filename> : empty
<filename> : directory
<filename> : symbolic link to filename
<filename> : "shell" script text
<filename> : commands text

Crear o inicializar un archivo (touch)

Sintaxis:

touch <filename>

Crea o inicializa un archivo. Su tamaño será de 0 bytes.

Mostrar el contenido de un archivo (more, cat, tail, head)

more

Sintaxis:

more [<filename>]

Visualiza un archivo de texto pantalla a pantalla. Una vez que se está ejecutando se puede hacer lo siguiente:

- pulsar el espaciador para visualizar otra pantalla.
- pulsar <Return> para avanzar línea a línea.
- escribir /patrón para avanzar hasta la 1ª línea que contenga dicho patrón.
- pulsar el carácter 'q', para salir.

Ejemplo:

```
% more /etc/passwd
```

cat

Sintaxis:

```
cat [<filename>...]
```

Permite visualizar el contenido de uno o más archivos sin paradas a través del dispositivo de salida estándar. Se puede detener la imagen pulsando <Ctrl>-S, y para continuar <Ctrl>-Q. Ejemplo:

```
% cat profile exrc
```

pg

Sintaxis:

```
pg [- + <número>] [+/<patrón>] <filename> ...
```

Permite paginar la salida. Si el fichero a ver tiene más de 24 líneas, 'pg' visualizará las 23 primeras y presentará en la línea 24 un carácter ':' de petición de orden:

- si pulsa <Return> verá la siguiente página.

- si desea abandonar deberá pulsar 'q'.

Otras opciones de pg:

% pg -20 archivo Fija el tamaño de pantalla en 20 líneas en lugar de las 24 que hay por defecto.

% pg +13 archivo Comienza a visualizar a partir de la línea 13.

% pg +patrón/ archivo Comienza a listar a partir de la 1ª línea que contenga 'patrón'.

tail

Sintaxis:

```
tail [ +1 - <número>] <filename>
```

Permite examinar el final de un archivo. Por defecto visualizará las diez últimas líneas, pero es posible modificar dicho número. Ejemplos:

```
% tail -3 /etc/passwd
```

Visualiza las tres últimas líneas del archivo /etc/passwd.

```
% tail +10 /etc/group
```

Visualiza el archivo a partir de la línea 10. Si se utiliza la opción

'+nº líneas', y el archivo no tiene tantas líneas, no se visualizará nada.

head

Sintaxis:

```
head [ - <número>] <filename>
```

Permite visualizar las diez primeras líneas de un archivo, aunque como en el caso de tail se puede modificar su valor. Ejemplo:

```
% head -20 /etc/tempcap Muestra las primeras 20 líneas.
```

-Mover o renombrar un archivo (mv - MoVe)

Sintaxis:

```
mv <filename1> <filename2>
```

o

```
mv <filename>... <directory>
```

Ejemplos:

```
mv mensaje01 mesj.01 Cambia el nombre del archivo mensaje01; Y en el caso de que existiese mesj.01 éste cambiará su contenido por el de mensaje01.
```

```
mv user10/mbox user11 Movemos el archivo 'mbox' del directorio user10 al directorio user11.
```

Copiar archivos (cp - COPY).

Sintaxis:

```
cp <filename1> <filename2>
```

o

```
cp <filename>... <directory>
```

Ejemplo:

```
cp /etc/motd mensaje Copia el directorio de trabajo el archivo 'motd' y renombra el archivo.
```

Después de haber realizado la copia de un archivo, el modo del archivo es el mismo que tenía el original.

Borrar archivos (rm - ReMove).

Sintaxis:

```
rm <filename> ...
```

Permite borrar o suprime uno o más archivos de un directorio (sólo puede borrarlos el propietario o el súper usuario). En el caso de que uno de los archivos a suprimir estuviese protegido contra escritura, 'rm' le informaría del modo real del archivo, y esperaría una respuesta: si pulsa 'y' procede a borrarlo y si pulsa cualquier otra tecla no lo borrará. Opciones:

-I: (Interactiva). 'rm' pide confirmación de cada uno de los archivos que va a borrar, independientemente de que esté o no protegido.

-F: Si se quiere forzar la supresión de archivos estén o no protegidos.

-R: Si se quiere borrar el contenido del directorio actual, y de los posibles subdirectorios que existan a partir de él (recursivamente).

3.7.5 MODIFICACIÓN DE PERMISOS Y PROPIETARIOS.

Definir los permisos de creación de un archivo o directorio (umask)

Sintaxis:

```
umask [<valor>]
```

Donde <valor> es un valor en octal indicando los permisos del propietario, grupo y otros. Que se van inhabilitar cuando se cree un archivo. Normalmente es 022. El primer dígito indica los permisos del propietario, el segundo los permisos del grupo y el tercero los permisos de otros. El permiso de ejecución se indica con 1, el de escritura con 2 y el de lectura con 4. Para una combinación de estos permisos, se suman esos valores. Ejemplo:

```
% umask 037
```

Los archivos que se creen tendrán inicialmente los permisos de rwx para el propietario, r-- para el grupo y --- para el resto.

Cambio del propietario de un archivo (chown).

Sintaxis:

```
chown <username> <filename> ...
```

Cambia el propietario de un archivo o de un directorio. <username> pueden ser también el UID. Sólo el propietario y el súper usuario pueden cambiar al propietario de un archivo.

Cambio del grupo de un archivo (chgrp).

Sintaxis:

```
chgrp <groupname> <filename> ...
```

Permite cambiar la propiedad de grupo de directorios y archivos a otro grupo del sistema.

Cambio de los permisos de un archivo (chmod).

Sintaxis:

```
chmod modo archivo ...
```

chmod cambia los permisos de un archivo o directorio donde el modo es [ugoa+-rwx]. Siendo:

u	usuario/propietario
g	grupo
o	otros usuarios
a	todos los usuarios (equivale a ugo)
+	da el permiso
-	quita el permiso
rwx	permisos de lectura, escritura y ejecución

Sólo puede ser cambiado por el propietario del archivo o por el súper usuario. El modo se puede especificar también en octal. Ejemplos:

```
chmod ug+x programa      Da permiso de ejecución al propietario y grupo del archivo
                           "programa".
chmod 777 publico        Da todos los permisos a todos los usuarios para el archivo
                           "público"
```

3.7.6 IMPRESIÓN.

Impresión de archivos (lp).

Sintaxis:

```
lp <filename>
```

El archivo se imprime en la impresora por defecto del sistema. Tras ejecutar la orden el sistema nos indicará el número de solicitud de impresión o 'id-request'.

Cancelación de una petición de impresión (cancel).

Sintaxis:

```
cancel [<id-request>]
```

Tan sólo se puede cancelar las peticiones de impresión que haya efectuado un determinado usuario.
Ejemplo:

```
% cancel 65
```

Estado del servicio de impresión (lpstat).

Visualiza el estado de las solicitudes de impresión efectuadas. Opciones:

- o Permite ver el estado de las peticiones de todos los usuarios.
- p Permite ver el estado de todas las impresoras.

3.7.7 ÓRDENES DIVERSAS

Cambio de password (passwd)

Sintaxis:

```
passwd
```

Cambia la clave de acceso (palabra de paso) a una cuenta de usuario. Sólo el propietario de la cuenta o el súper usuario pueden cambiar un password.

¿Quién está en el sistema? (who / who am i)

Sintaxis:

```
who
ó
who am i
```

Informa quién está conectado al sistema o quién soy yo. Aparece la siguiente información:

```
UserName Terminal FechaConexión (DireccInternet)
```

Limpiar la pantalla del terminal (clear)

Sintaxis:
clear

Enlaces a archivos (ln)

Sintaxis:
ln [-s] <filename>

Permite enlaces fijos (hard) o simbólicos (symbolic) a archivos o directorios.

- Enlace fijo: Es una entrada en un directorio estándar. Sólo se hacen a archivos existentes y dentro del mismo file system al que pertenezca el archivo. Para eliminar un archivo, se tiene que eliminar todos los enlaces fijos (incluyendo el primer nombre que se le dio al archivo).
- Enlace simbólico: Se realiza con la opción -s. Es una entrada de directorio especial que apunta a otro archivo existente. El archivo puede estar en otro file system. Si se elimina el archivo al que apunta, no eliminan todos sus enlaces simbólicos.

3.8 ADMINISTRACIÓN DEL SISTEMA.

3.8.1 EL SUPERUSUARIO Y SUS FUNCIONES.

El súper usuario, cuyo nombre de usuario (login) es "root", el que tiene poderes olímpicos sobre la ejecución (y posible destrucción) del sistema. El súper usuario no está restringido por ninguna de las protecciones de que dispone el sistema: puede obtener cualquier fichero, puede cancelar cualquier proceso. Hay algunas operaciones del sistema que sólo el súper usuario puede realizar.

Existen varias formas para pasar a súper usuario. Una forma de entrar es arrancar el sistema en modo monousuario. Otra forma es entrar en la cuenta de súper usuario como si de un usuario normal se tratase, introduciendo el nombre de usuario root cuando aparece el mensaje login; después se introduce su clave. Una última forma de entrar es estando en una cuenta de usuario normal, introducir el comando *su* y después introducir la clave.

La principal tarea del súper usuario es la administración del sistema UNIX.

La administración del sistema consiste básicamente en gestionar los recursos del sistema para que se puedan utilizar de la forma más eficiente posible así como llevar control de los usuarios potenciales del sistema. Entrando más en detalle, las tareas de administración del sistema más comunes son las siguientes:

- Añadir usuarios.
- Instalar software (como aplicaciones y actualizaciones del sistema operativo).
- Instalar *hardware* (como tarjetas, impresoras, terminales y módems).
- Mantener la seguridad e integridad del sistema y de la red.
- Diagnosticar y arreglar problemas software y *hardware* cuando ocurran.
- Comprobar el uso de los sistemas de archivos para asegurarse de que no estén llenos y además controlar el uso indiscriminado de los mismos.
- Mantener impresoras, módems y terminales remotos.
- Realizar copias de seguridad de los sistemas de archivos.
- Mantener servicios de red, correo y otros servicios de comunicaciones.

3.8.2 ARRANQUE Y PARADA DEL SISTEMA.

3.8.2.1 ARRANQUE DEL SISTEMA.

La carga inicial (booting) es el proceso que hay que realizar para echar a andar el sistema cuando se conecta el ordenador inicialmente o cuando lo reinicializa después de una detención.

El programa de carga inicial, llamado bootstrap, que se encuentra almacenado en el bloque de arranque del sistema de archivos raíz. Este programa se encarga de traer a memoria un programa más complejo, el cual se encarga de cargar, configurar e iniciar el sistema UNIX.

El proceso de arranque consta de tres pasos fundamentales:

- Cargar el sistema operativo.
- Verificar los sistemas de archivos (si el sistema se paró anormalmente).
- Elegir el modo de funcionamiento.

A continuación se describen estos tres pasos:

Cargar el sistema operativo:

El primer paso en el arranque del sistema es cargar el sistema operativo desde el disco duro del ordenador.

Se enciende el ordenador y ésta carga el bootstrap y muestra el siguiente mensaje:

```
SCO System V/386
```

```
Boot
```

```
:
```

Se pulsa <Return> y el bootstrap carga el sistema operativo. Cuando el sistema está cargado, muestra información sobre sí mismo y verifica que el sistema de archivos raíz está correcto y no tiene errores. Si no hay errores se pasa al paso tercero donde se elige el modo de funcionamiento. Si hay errores en el sistema de archivos, se pasará al punto donde se reparará el sistema de archivos.

Reparando el sistema de archivos:

Es necesario reparar el sistema de archivos si aparece el siguiente mensaje:

```
fsstat: root filesystem needs checking  
OK to check the root filesystem (/dev/root) (y/n)?
```

Cada sistema de archivos que se quiera cargar y tenga errores, mostrará un mensaje similar. Para trabajar sin problemas, el sistema operativo necesita reparar el sistema de archivos.

Para reparar el sistema de archivos, introduzca 'y'. La utilidad *fsck* (que será explicada más adelante) limpiará el sistema de archivos, reparando los archivos dañados o borrando los archivos que no se hayan reparado.

Cuando la reparación se haya completado, el sistema preguntará por el modo de funcionamiento.

Eligiendo el modo de funcionamiento:

Se debe elegir el modo de funcionamiento tan pronto como salga el siguiente mensaje:

INIT: SINGLE USER MODE
Type CONTROL-d to continue with normal startup.
(or given the root password for system maintenance):

El sistema tiene dos modos de funcionamiento: funcionamiento normal y mantenimiento del sistema. El funcionamiento normal es la forma ordinaria de trabajar con el sistema. Este es el modo multiusuario, o sea, que permite la entrada de los usuarios. El modo de mantenimiento del sistema está reservado para trabajar siendo el súper usuario y no permite la entrada de múltiples usuarios: se trabaja en modo monousuario.

Para elegir el modo multiusuario pulse <Ctrl>-d. El sistema mostrará un mensaje de comienzo, y se le pedirá que introduzca el tiempo del sistema. Entonces el sistema ejecuta los comandos encontrados en los directorios /etc/rc, generando mensajes de comienzo para varios servicios del sistema, como los servicios de impresora o de red. Después el sistema mostrará el mensaje "login:". A partir de aquí, cualquier usuario puede iniciar su sesión.

Para elegir el modo de mantenimiento de sistema se introduce la clave de acceso del súper usuario. Se muestra el prompt del súper usuario ("#"). Los comandos de los directorios /etc/rc no se ejecutan.

3.8.2.2 PARADA DEL SISTEMA.

Parar un sistema UNIX requiere algo más que apagar el ordenador ya que hay que realizar una serie de pasos para preparar al sistema para la parada. El procedimiento exacto varía dependiendo de la configuración. Un procedimiento típico podría ser parecido al siguiente.

- Enviar mensajes de aviso a todos los usuarios presentes informando que el sistema va a ser desconectado próximamente.
- Cancelar (kill) todos los procesos en ejecución excepto el proceso de la consola.
- Desmontar los sistemas de archivos.
- Utilizar la orden sync para asegurar que toda la actividad de entrada-salida con el sistema de archivos se ha terminado.
- Apagar el ordenador si es necesario.

Existen dos comandos para parar el sistema: el comando shutdown o (bajo ciertas condiciones) el comando haltsys.

Usando el comando shutdown:

El comando shutdown es la forma normal de parar el sistema y debe ser usado cuando el sistema se encuentra en modo multiusuario. El mismo avisa automáticamente a los usuarios mediante el siguiente mensaje:

```
Broadcast Message from root (<terminal>) on eancol <Fecha>  
THE SYSTEM IS BEING SHUT DOWN NOW ! ! !  
Log off now or risk your files being damaged.
```

Esperará unos segundos, para dar tiempo a los usuarios a desconectarse, y pedirá confirmación para la parada del sistema. Después cerrará todas las cuentas y cancelará todos los servicios del sistema. Sólo se podrá apagar el sistema cuando aparezca el siguiente mensaje:

```
** Safe to Power Off **  
- or -  
** Press Any Key to Reboot **
```

Usando el comando shutdown con la opción -gn, el proceso de parada comenzará después de n minutos.

Usando el comando haltsys:

El comando *haltsys* para el sistema inmediatamente. El comando debe usarse sólo cuando se está trabajando en modo monousuario. Si hay usuarios conectados cuando se ejecuta *haltsys*, se terminará su sesión y perderán los trabajos que estaban haciendo. Además, los servidores de red así como otros programas son terminados anormalmente y pueden crear problemas cuando re arranquen.

Al igual que el comando shutdown, no se debe desconectar la máquina hasta que no aparezca el mensaje:

```
** Safe to Power Off **  
- or -  
** Press Any Key to Reboot **
```

3.8.3 ADMINISTRACIÓN DE LOS SISTEMAS DE ARCHIVOS.

3.8.3.1 MONTAR UN SISTEMA DE ARCHIVOS.

Para poder utilizar un sistema de archivos hay que montarlo, o sea, enlazarlo a la estructura de directorios ya existente para que el sistema tenga noticia de su existencia. Para montarlo se necesita un punto de montaje (mount point), que generalmente es un directorio vacío.

Para montar un sistema de archivos se usa la orden mount. Su sintaxis es la siguiente:

```
mount [- r] [- t tipo] dispositivo directorio
```

Donde dispositivo indica el archivo especial asociado con el sistema de archivos que se va a montar y directorio es el punto de montaje. Con la opción -r se indica que el sistema de archivos será de sólo lectura. Con la opción -f se especifica el tipo de sistema de archivos que se va a instalar. Si se omite esta opción, se toma por defecto el mismo tipo que el del sistema de archivos raíz. Esto son los sistemas de archivos disponibles:

AFS	Acer Fast Filesystem.
DOS	DOS <i>filesystem</i> .
EAFS	Extended Acer Fast Filesystem.
HS	High Sierra CD-ROM <i>filesystem</i> .
S51K	AT&T UNIX System V 1 Kbyte <i>filesystem</i> .
XENIX	XENIX 286/386 <i>filesystem</i> .

Para desmontar un sistema de archivos se usa el comando umount cuya sintaxis es la siguiente:

```
umount dispositivo
```

Donde dispositivo es el archivo especial asociado al sistema de archivos. Un sistema de archivos no se puede desmontar si está en uso: tiene algún archivo abierto o hay algún usuario en alguno de sus directorios.

3.8.3.2 CREAR UN SISTEMA DE ARCHIVOS.

La orden mkfs crea un sistema de archivos nuevo. La forma básica de la orden mkfs es la siguiente:

```
mkfs dispositivo tamaño
```

Al construir un sistema de archivos nuevo, hay que especificar el número de bloques que contiene. El comando `mkfs` utiliza ese número para determinar el número de bloques que reservará para inodos. Por ejemplo, supongamos que se tiene un dispositivo sobre disco flexible llamado `/dev/fd0`. Supóngase además que ese disco flexible puede contener un máximo de 2000 bloques. Se construirá un sistema de ficheros sobre este dispositivo así:

```
# mkfs /dev/fd0 2000
```

A continuación, sólo queda montar el sistema de archivos creado con la orden `mount`.

3.8.3.3 UTILIZACIÓN DEL DISCO.

Se verá a continuación las órdenes `df`, que permite determinar el grado de ocupación de los sistemas de archivos; `du`, que determina el tamaño de los archivos y directorios; y `quot`, que muestra el número de bloques utilizado por cada usuario.

La orden `df`:

La orden `df` muestra la cantidad de espacio de disco asignado a los sistemas de archivos montados, la cantidad de espacio usado y disponible, y el porcentaje total que ha sido usado por los sistemas de archivos montados. Su sintaxis básica es:

```
df [-vi] [<filesystem>]
```

Ejemplo:

```
/          (/dev/root   ):  323304 blocks 45192 i-nodes
/home     (/dev/u       ):  157358 blocks 19951 i-nodes
```

Muestra los siguientes campos: punto de montaje, dispositivo asociado, bloques (de 1024 bytes) libres, inodos libres. Un sistema de archivos no podrá llenarse completamente. Esto es así porque el sistema reserva una fracción del espacio en el sistema de archivos para permitir trabajar bien a las rutinas de asignación en el sistema de archivos. La cantidad reservada es normalmente un 10%. Cuando todo el espacio disponible está usado (excepto el área de reserva), sólo el súper usuario podrá crear nuevos archivos y/o asignar bloques de datos a los archivos existentes.

La opción `-i` informa del número de inodos totales, usados y libres. La opción `-v` muestra los bloques totales, los usados, los libres y el porcentaje de bloques usados.

La orden `du`:

`du` muestra el número de kbytes de todos los archivos (recursivamente) de un directorio especificado o del archivo dado como `<filename>`. Por defecto sólo aparecen los directorios y subdirectorios. Si un archivo tiene varios enlaces, sólo se cuenta uno. Su sintaxis es la siguiente:

```
du [-s] [-a] [<filename> ... ]
```

Las opciones realizan las siguientes modificaciones a la orden `du`:

```
-s      Muestra una única entrada correspondiente al <filename> especificado.
-a      Genera una entrada para cada archivo del directorio nombrado.
```

La orden `quot`:

`quot` muestra el número de bloques (de 1024 bytes) que pertenece a cada usuario del sistema de archivos especificado. Si no se especifica ninguno, se revisan todos los sistemas de archivos montados. Su sintaxis es como sigue:

quot [-f] [<filesystem>]

Con la opción -f se nos muestra el número de archivos y el espacio que ocupan para cada usuario. Este comando sólo lo puede usar el súper usuario.

3.8.4 ADMINISTRACIÓN DE LAS CUENTAS DE USUARIO.

3.8.4.1 ARCHIVOS ADMINISTRATIVOS.

Cada usuario que accede al sistema debe tener una cuenta de usuario (user account). El archivo que contiene información sobre cada cuenta del sistema y de los usuarios que pueden conectarse localmente a la máquina es el /etc/passwd. Las claves de acceso se almacenan en el archivo /etc/shadow. Si este archivo no existe, se almacenarán en el /etc/passwd. El archivo /etc/group almacena información acerca de los grupos de usuario existentes en el sistema.

El archivo /etc/passwd:

Contiene información sobre cada cuenta de usuario. En este archivo se tendrá una entrada por cada cuenta que exista en el sistema conteniendo información de la siguiente forma:

```
username:password:uid:gid:comentario:directorio:"shell"
```

El significado de cada campo es el siguiente:

Username, Nombre de conexión de la cuenta (nombre de usuario). Es una combinación de números y letras.

Password, Palabra de paso (palabra clave) encriptada de la cuenta. Si este campo es nulo, la cuenta no se demanda password. Si existe el archivo /etc/shadow, entonces aparece el carácter 'x' y la clave encriptada junto con información adicional aparece en el /etc/passwd.

Uid, identificador de usuario de la cuenta. Es un identificador único para el sistema. Es un número entre 10 y 60000. Los identificadores del 0 al 9 se reservan para las cuentas del sistema. El uid del root es normalmente.

Gid, Identificador del grupo al que pertenece la cuenta. Es un identificador numérico del grupo por defecto para ese usuario. Su valor puede estar entre 0 y 60000.

Comentario, Nombre real del usuario y otra información que aparecerá en las cabeceras de mensaje del correo del usuario.

Directorio, Nombre completo del home directory de la cuenta.

"shell", "shell" de ingreso de la cuenta.

El archivo /etc/shadow:

Contiene información sobre el password de cada cuenta de usuario. En este archivo se tendrá una entrada por cada cuenta que exista en el sistema conteniendo información de la siguiente forma:

```
username:password:ultcambio:minimo:maximo
```

El significado de cada campo es el siguiente:

Username Nombre de usuario.

Password Clave encriptada de la cuenta. Tendrá como prefijo la cadena "*"LK*" cuando la cuenta está bloqueada, o la cadena "*RETIRED*" cuando la cuenta está siendo retirada. Estará vacío este campo cuando la cuenta no posea password.

Ultcambio, El número de días desde el 1 de Enero de 1970, y la fecha del último cambio en el password.

Mínimo, El número mínimo de días requerido entre cambios de password.

Máximo, El número máximo de días en los cuales el password es válido.

El archivo /etc/group:

La base de datos que almacena información sobre todos los grupos del sistema es el archivo etc/group.

Cada entrada en este archivo tiene la sintaxis siguiente:

```
groupname:password:gid:listausuarios
```

siendo:

groupname, Nombre del grupo.

Password, Clave encriptada del grupo (sin usar).

Gid, Identificador de grupo. Debe ser único en la máquina local.

Lista usuarios, Lista de usuarios que pertenecen al grupo.

3.8.4.2 CREACIÓN / BORRADO / MODIFICACIÓN DE CUENTAS DE USUARIOS.

Con la utilidad administrativa sysadmsh se pueden realizar estas operaciones siguiendo una serie de menús. Sin embargo, vamos a ver como crear cuentas de usuario, como borrarlas o modificarlas de forma "manual".

Para crear una cuenta de usuario se deben seguir esta serie de pasos:

- Crear una entrada con el nuevo usuario en el archivo /etc/passwd, asignándole un nombre de usuario (login name), un identificador de usuario no usado, un identificador de grupo, un directorio de trabajo (home directory) y un "shell" de conexión.
- Añadir el usuario a su grupo en el archivo /etc/group.
- Crear el directorio de trabajo.
- Copiar los archivos de arranque correspondientes al "shell" de ingreso que se le haya asignado al usuario. Estos archivos se encuentran en los directorios ubicados en /usr/lib/mkuser.
- Cambiar el propietario y el grupo del directorio de trabajo y de los archivos creados en él y asignárselo al usuario nuevo.
- Crear password para la nueva cuenta.

Como ejemplo, vamos a crear la cuenta pepe:

- Añadir la siguiente entrada al archivo /etc/passwd:
pepe::507:50:Cuenta de ejemplo:/home/pepe:/bin/csh
- Añadir el usuario a la entrada correspondiente en el archivo /etc/group:
group::50:julio,german,pepe

- Crear el directorio de trabajo:
mkdir /home/pepe
- Copiar los archivos de arranque:
cp /usr/lib/mkuser/csh/cshrc /home/pepe/.cshrc
cp /usr/lib/mkuser/csh/login /home/pepe/.login
- Cambiar el propietario y el grupo de los archivos creados:
chown pepe /home/pepe
chown pepe /home/pepe/.cshrc
chown pepe /home/pepe/.login
chgrp group /home/pepe
chgrp group /home/pepe/.cshrc
chgrp group /home/pepe/.login
- Crear el passwd de la cuenta nueva:
passwd pepe

A partir de aquí, el nuevo usuario puede conectarse ya.

Para borrar un usuario, se siguen dos pasos:

- Usar el comando `rmuser usuario` para borrar al usuario de las bases de datos.
- Borrar el directorio de trabajo del antiguo usuario y todos los archivos creados por él.

Para modificar alguna característica de un usuario, se pueden editar los archivos correspondientes y hacer las modificaciones a mano.

3.8.4.3 CREACIÓN / BORRADO DE GRUPOS.

La forma de crear / borrar usuarios es editando el archivo `/etc/group` y hacer los cambios pertinentes.

La creación de grupos de usuarios perfectamente definidos, proporciona al sistema un grado de seguridad adicional permitiendo controlar el acceso a archivos y directorios de una forma más organizada.

3.8.4.4 LISTADO DE USUARIOS DEL SISTEMA.

La orden `finger`, sin especificar un nombre de usuario, muestra información sobre cada usuario que está conectado. Su sintaxis es:

```
finger [opciones] [<username> ...]
```

La información que muestra es la siguiente:

- Nombre de conexión (login name).
- Nombre completo (full name).
- Nombre de terminal (terminal name).
- Tiempo de inactividad (idle time).
- Tiempo de conexión (login time).

- Posición (location). Comentario en el /etc/ttytab si se conecta localmente y hostname si se conecta remotamente.

Si se especifica un nombre de usuario aparecerá además la siguiente información.

- Directorio de trabajo y "shell" de conexión del usuario.
- Tiempo de la última conexión de usuario (si en ese instante no están conectados) o tiempo que llevan conectados (si están conectados).
- Terminal (e información del terminal obtenido en el /etc/ttytab) o host del que está conectado remotamente.
- La última vez que el usuario recibió y leyó el correo.
- Plan de trabajo contenido en el archivo .plan que puede encontrarse en el home directory del usuario.
- Proyecto en el que esté trabajando el usuario descrito en el project del home directory si existe.

Opciones:

- l Fuerza el formato de salida largo.
- s Fuerza el formato de salida corto.

3.8.5 ADMINISTRACIÓN DE IMPRESORAS.

3.8.5.1 CREAR UN PUERTO PARALELO.

Para instalar una impresora es necesario tener creado un puerto paralelo. A continuación vamos a ver como crear este dispositivo. Para crear un puerto paralelo se usa el comando:

```
mkdev parallel
```

Aparecerá el siguiente menú:

- Add a parallel port.
- Remove a parallel port.
- Show configuration.
- Help.

Tenemos las opciones de añadir un puerto paralelo, eliminar un puerto paralelo, mostrar información sobre configuración y pedir ayuda. Elegiremos la opción 1 y entonces aparecerá otro menú, preguntando por el tipo de puerto paralelo que queremos crear:

- Serial/Parallel adapter #1: address=378-37f
- Parallel/Monochrome adapter : address=3bc-3be
- Serial/Parallel adapter #2 : address=278-27a

Elegimos el puerto que queremos y nos preguntará a continuación por el IRQ con el siguiente mensaje:

Should this port use interrupt (default 5):

A continuación, el sistema asignará un archivo de dispositivo al puerto, por ejemplo el /dev/lp0. Por último nos informará de que el kernel ha sido modificado y nos preguntará si queremos recompilarlo para almacenar los cambios.

3.8.5.2 CREAR UNA IMPRESORA.

Para crear y configurar una impresora usamos el comando siguiente:

```
mkdev lp
```

Nos aparecerá un “shell” parecido al sysadmsh: un sistema de menús y ventanas. Elegiremos la opción Configure y después la opción Add se introducirán los siguientes datos acerca de la impresora:

Nombre, Nombre que queremos que tenga la impresora dentro del sistema.

Comentario, Nombre completo de la impresora o cualquier comentario que se quiera hacer sobre la misma.

Nombre de clase, Nombre del grupo al que se quiere añadir la impresora. Las impresoras que se vayan configurando se pueden agrupar siguiendo cualquier criterio.

Usar interfase de impresora, Se especifica el nombre de la interfase que va a usar la impresora.
Conexión, Tipo de conexión de la impresora. Puede ser directa (local) o de llamada (en red).

Dispositivo, El archivo del dispositivo que va a utilizar la impresora (por ejemplo /dev/lp0).

Banner, Se pregunta si se desea el servicio de banner en la impresora.

Si se quiere colocar esta impresora como la impresora por defecto, se elige la opción Configure, después la opción Default y por último se especifica el nombre de la impresora.

Para terminar de configurar la impresora hay que realizar las siguientes acciones, dentro del menú Schedule de la opción Configure:

- Se elige la opción Begin.
- Se elige la opción Accept y se indica el nombre de la impresora.
- Se elige la opción Enable y se indica el nombre de la impresora.

Con todo esto queda ya creada una impresora. Los usuarios pueden usarla mediante el comando lp.

3.8.6 COPIAS DE SEGURIDAD. RECUPERACIÓN.

3.8.6.1 INTRODUCCIÓN.

Las copias de seguridad son una de las tareas más usuales y necesarias a realizar en el mantenimiento de todo el sistema. El objetivo de toda copia de seguridad es poder recuperar toda la información en caso de que ésta se pierda, por ello, es aconsejable que se realicen con una cierta periodicidad y planificación. Por ejemplo, sería deseable que se hicieran copias diarias de aquellos directorios que contienen los datos de los usuarios.

3.8.6.2 COPIAS INCREMENTALES CON BACKUP/RESTORE.

La orden backup:

La orden backup realiza copias de seguridad incrementales, de los archivos del home directory de un usuario especificado, o de un conjunto de archivos y directorios determinados. Las copias son restauradas con la orden restore. Su sintaxis es la siguiente:

```
backup [-h] [-t] [-p] [-c] [-f archivos] [-u usuarios] [-d dispositivo]
```

Sus opciones son:

- h Produce una historia de ls Backups realizados.
- c Realiza un backup completo. Todos los archivos modificados desde la instalación del sistema son copiados.
- p Realiza un backup incremental. Copia sólo los archivos modificados desde la fecha del último backup.
- f Copia los archivos especificados en el argumento archivos.
- u Copia el home directory del usuario especificado.
- d Se usa para especificar el dispositivo de destino que se va a utilizar.
- t Se usa cuando el dispositivo especificado es una cinta.

La orden restore:

Restaura los archivos copiados con la orden *backup*. Su sintaxis es la siguiente:

```
restore [-c] [-i] [-o] [-t] [-d dispositivo]
```

Sus opciones son:

- c Realiza una completa restauración. Todos los archivos de la copia son restaurados.
- i Obtiene una lista de los archivos existentes en la copia. Ningún archivo es restaurado.
- o Sobrescribe los archivos existentes. Si esta opción no se especifica, los archivos de la copia que ya existan no son restaurados.
- t Indica que el dispositivo donde está la copia es una cinta.
- d Especifica el dispositivo donde se encuentra la copia de seguridad.

3.8.6.3 COPIAS ESPECÍFICAS CON TAR Y CPIO.

La orden tar:

La orden tar crea archivos de cinta (tarfile) y añade o extrae archivos. Un tarfile es habitualmente una cinta magnética pero puede ser un archivo.

Su sintaxis básica es:

```
tar c|t|u|x[opciones] [tarfile] archivos
```

Letras de función:

- c Crea un nuevo tarfile y escribe los archivos en él.
- t Lista la tabla de contenidos de tarfile.
- u Los archivos especificados son añadidos al tarfile si éstos no están aún o si han sido modificados desde la copia en este tarfile.
- x Extrae los archivos nombrados desde el tarfile. Si no se especifican archivos, se extraerán todos los archivos.

Si un archivo especificado es un directorio, se copiará o se recuperará recursivamente, es decir, se tratarán todos los archivos y subdirectorios que existan en él.

Opciones:

- v Normalmente tar trabaja silenciosamente. Con esta opción, tar mostrará el nombre de cada archivo.
- f Usa el próximo argumento como nombre del tarfile.

La orden cpio:

cpio realiza copias de archivos a un archivo de copia de cpio. Los archivos de copia de cpio contienen rutas de archivos e información de estado, junto con el contenido de los archivos almacenados. Su sintaxis es la siguiente:

```
cpio -i | -o [opciones]
```

Sus comandos son:

- o Copia archivos a la salida estándar. Normalmente se redirecciona a un dispositivo de copia de seguridad. Los archivos a copiar los obtiene de la entrada estándar.
- i Extrae archivos de la entrada estándar. Los archivos extraídos son copiados en el directorio actual. Se pueden especificar los archivos que se quieren recuperar. Cada etiqueta de archivo debe ir entre comillas dobles.

Las opciones de “cpio -o” más importantes son:

- a Actualiza las fechas de acceso de los archivos cuando se completa la copia.
- c Escribe una cabecera en ASCII.
- v Informa de los archivos que se están copiando.

Las opciones de “cpio -i” más importantes son:

- d Crea los directorios necesarios.
- r Renombra archivos interactivamente. Si da el carácter '.', se copiará el nombre original. Si el usuario de una línea vacía, se salta el archivo.
- t Muestra los archivos existentes del archivo de entrada especificado. No se recupera ningún archivo.
- u Copia incondicional. Normalmente no se recuperan los archivos cuya fecha de modificación en disco sea más nueva que en el medio de recuperación. Con esta opción, se recupera sin tener en cuenta la fecha de modificación.”¹⁰

¹⁰ Rey de Perea Campos J. Escuela de Administración de Negocios, E . A . N . : Taller práctico sobre el sistema operativo uníx; diplomado en informática; Universidad de Almería España. En línea [URL], <http://www.ual.es/~jperea/documentacion/unix/Taller.exe>

CAPÍTULO IV
INSTALACIÓN Y MANEJO DE REDES CON WINDOWS NT
Y PRODUCTOS MICROSOFT

4 INSTALACIÓN Y MANEJO DE REDES CON WINDOWS NT Y PRODUCTOS MICROSOFT

4.1 HISTORIA DE WINDOWS NT.

WINDOWS NT (WINDOWS NEW TECHNOLOGY, NT).

El sistema operativo de 32 bits desarrollado originalmente para que sea *OS/2* 3.0 antes que Microsoft e *IBM* discontinuaran su trabajo con *OS/2*. NT se diseñó para estaciones de trabajo avanzadas (Windows NT 3.1) y para servidores (Windows NT 3.1 Advanced Server).

El primer lanzamiento fue Windows NT 3.1 en Septiembre de 1993.

A diferencia de Windows 3.1, que era una interfase gráfica que corría sobre MS-DOS, Windows NT es un sistema operativo por sí solo. El usuario lo ve como Windows 3.1. pero tiene multi-procesos real, seguridad y protección de memoria.

Está basado en un microkernel, con un direccionamiento de hasta 4GB de RAM, soporte para sistemas de archivos FAT,NTFS y HPFS, soporte de red incorporado, soporte multiprocesador, y seguridad C2.

NT está diseñado para ser independiente del *hardware*. Una vez que la parte específica de la máquina - la capa HAL (Capa de Abstracción de *Hardware*)- ha sido llevada a una máquina particular, el resto del sistema operativo debería compilar teóricamente sin alteración. Se lanzó una versión de NT para correr en máquinas Alpha de DEC.

NT necesitaba un 386, con al menos 12MB de RAM (preferible 16MB), y al menos 75MB de disco duro libre.

WINDOWS NT 3.1

Primera versión de Windows NT (WNT). Existe una leyenda popular que dice que la persona responsable del desarrollo de VMS en VAX de DEC fue también responsable de Windows NT, y si cada letra de VMS es avanzada a la siguiente letra del abecedario se llega a WNT.

WINDOWS NT 3.5

Una versión más mejorada de NT 3.1. Desde esta versión Windows NT se vende como "Windows NT 3.5 Workstation" y "Windows NT 3.5 Server".

WINDOWS NT 4

La nueva versión de Windows NT, denominada "Cairo" en su etapa de desarrollo. Presenta las mismas características de la interfase de Windows 95. Tiene algunas modificaciones en su diseño con respecto a las porciones GDI y USER del sistema operativo.

4.2 INSTALACIÓN DE WINDOWS NT.

4.2.1 REQUISITOS DEL SISTEMA PARA NT.

Windows NT 4.0 ha sido creado como un sistema operativo para ordenadores de alto rendimiento y ofrece a los usuarios profesionales un rendimiento de sistema suficiente. Por lo tanto, los requisitos de NT en cuanto al ordenador en el que se van a instalar son claramente superiores a los que precisan otros sistemas operativos como Windows 95 o Dos / Windows 3.x. A continuación se describirá qué configuraciones son necesarias para poder utilizar Windows NT con un rendimiento mínimo, recomendable y para aplicaciones profesionales.

	Windows NT Workstation	Windows NT Server (configuración mínima)	Windows NT Server (configuración recomendada)
Procesador	Intel 486 DX, mejor Pentium 90 o mejor aún; Alpha, MIPS, PowerPC	Pentium 90	Pentium PRO o Dual Pentium
Memoria RAM	A partir de 12 MB(Intel) o 16 MB (RISC)	A partir de 12 MB(Intel) ó 16 MB (RISC)	64 MB o más
Memoria de duro	A partir de 117 MB (Intel) o 124 MB (RISC) mínimo temporalmente	A partir de 148 MB (Intel) ó 158 MB (RISC) temporalmente 50 MB 50 MB	Dos discos duros disco espejo de 4 GB reflejados
Controlador	E-IDE o SCSI	E-IDE o SCSI	SCSI
Tarjeta gráfica	Tarjeta aceleradora VGA con al menos 2 MB de memoria	Sólo administración del sistema en el servidor: tarjeta S-VGA básica, sino superior	Sólo administración del sistema en el servidor: tarjeta S-VGA básica, sino superior
Unidad de CD	ATAPI, mejor SCSI	ATAPI, mejor SCSI	ATAPI, mejor SCSI

4.2.2 ORGANIZACIÓN DE LOS SISTEMAS OPERATIVOS.

Es posible que se quiera trabajar con más de un sistema operativo sin tener que disponer de un ordenador para cada uno de los sistemas. En este caso, es preciso llegar a una solución de compromiso e instalar en un solo ordenador varios sistemas operativos que se puedan activar durante el inicio a través de un administrador de inicio.

Si se desea montar un ordenador con distintos sistemas operativos, vale la pena planificar bien la partición adecuada para el disco duro. Algunos sistemas operativos requieren una partición primaria para su inicio; otros, tienen bastante con una partición extendida. Finalmente, las particiones pueden recibir formato de diversos sistemas de archivos, los cuales dificultan un intercambio de datos mutuo.

Estos sistemas operativos se pueden instalar de forma paralela:

- Windows NT 4(versión Workstation o Server) y versiones anteriores de NT.
- DOS.
- Windows 95.
- NeXT.
- Unixware.
- NETWARE®.
- OS/2.
- Linux.

Los administradores de inicio de que disponen son:

- Administrador de inicio de NT.
- Administrador de inicio de OS/2

- Administrador de inicio como LILO de Linux

Además, es posible utilizar la configuración de inicio dual de Windows 95.

En primer lugar, debería planificar, qué sistema de archivos quiere asignar a cada partición de su disco duro. Cuando existen varias particiones primarias sólo se puede acceder a los datos de la partición activa. Por lo tanto, primarias solamente deben contener los elementos esenciales del sistema operativo correspondiente. El resto de los datos están mejor guardados en unidades lógicas. Una vez que se haya decidido por una combinación de sistemas de archivos, el segundo paso consiste en seleccionar el administrador de inicio adecuado.

Con Windows NT se puede conmutar entre varias versiones de NT y una versión de *DOS* o de Windows 95. Por consiguiente si sólo deben estar instalados en su ordenador estos sistemas operativos no necesitará ningún administrador de inicio aparte.

Si, junto con Windows NT, debe utilizarse otro sistema operativo que requiera una partición primaria propia (*OS/2* o Linux), es mejor emplear el administrador de inicio de *OS/2* o productos adicionales (como el administrador de inicio LILO). En estos casos, será precisa una partición primaria propia en el primer disco duro (C:).

4.2.3 PREPARACIÓN DE LA INSTALACIÓN.

Windows NT 4.0 se suministra en un CD o en un CD y tres disquetes. En la versión que sólo incluye el CD, estos tres disquetes se crean, opcionalmente, con el programa de instalación. Con dichos disquetes se llevan a cabo los primeros pasos de la instalación y se ejecuta Windows NT. A continuación se trasladan todos los archivos de sistema desde el CD o desde una unidad de disco duro temporal en la que se han copiado previamente los datos.

La opción que decida dependerá de si Windows NT 4.0 detecta directamente la unidad de CD-ROM de su ordenador o no.

Para instalar Windows NT 4.0 en un ordenador Intel, utilice el programa WINNT.EXE que se encuentra en el directorio *i386* de CD de instalación.

Puede activar dicho programa

- En Windows NT para actualizar una versión ya existente del programa, o
- Desde el símbolo de sistema de *DOS*.

En ambos casos, se crearán los tres disquetes de inicio y, eventualmente, se copiarán los archivos en un directorio temporal del disco duro. Con el comando WINNT.EXE/B es posible instalar directamente Windows NT desde la unidad de CD-ROM sin los disquetes de inicio.

Si se instala Windows NT en un ordenador sin sistema operativo, es mejor crear los disquetes de inicio en otro ordenador. Una vez iniciada la instalación, Windows NT tratará de detectar la unidad de CD-ROM y ejecutar la instalación. Si durante la instalación desde los disquetes de inicio no se detectara dicha unidad, sería preciso instalar Windows NT a través de una red o bien crear una partición *DOS* en el ordenador e instalar el controlador de CD-ROM. Luego se inicia el ordenador y se inicia la instalación. Dependiendo de si desea instalar Windows NT desde el CD-ROM, desde un directorio temporal o de si sólo quiere crear los disquetes de inicio, deberá activar el programa de instalación WINNT.EXE con distintos parámetros.

La siguiente tabla ofrece un resumen de ellos.

Parámetro	Efecto
/S[:] Nombre de la ruta	Indica la ruta de origen de los archivos de Windows NT; también puede tratarse de una unidad de red.
/T[:] Nombre del directorio	Indica el directorio temporal en el que se guardan archivos para la instalación; también puede tratarse de una unidad de red.
/I[:] Archivo Inf	Indica el nombre del archivo de información de instalación. La opción predeterminada es el archivo DOSNET.INF.
/O	Sólo crea los disquetes de inicio.
/OX	Crea los disquetes de inicio para una instalación desde el CD-ROM (o desde disquetes).
/X	Ejecuta el programa de instalación sin disquetes de inicio.
/F	Desactiva la comprobación de los archivos para la copia en disquetes de inicio.
/C	Pasa por alto los controles de espacio disponible en los disquetes de inicio.
/B	Instalación sin disquetes; en este caso es necesario indicar mediante los datos de los archivos de instalación.
/U	Permite una instalación automática si se indica mediante la ruta de origen de los archivos de instalación.

4.2.4 DETECCIÓN DEL *HARDWARE*.

Cada vez más, los sistemas operativos van equipados con una detección de *hardware* que reconoce e instala por su cuenta cada uno de los elementos del ordenador y dispositivos periféricos. En sistemas operativos como Windows NT, Windows 95 u OS/2, es imposible que se realicen errores graves en las indicaciones y se provoquen daños en el *hardware*.

La instalación de un dispositivo resulta particularmente fácil si el sistema operativo suministra e instala todos los controladores necesarios. Para describir esta característica se creó la expresión Plug&Play (que traducido sería algo así como "conectar y funcionar"). Lamentablemente, aún no funciona de forma totalmente satisfactoria con Windows NT.

Windows NT soporta durante la instalación la característica Plug&Play para muchos dispositivos, desde tarjetas gráficas pasando por unidades de CD-ROM hasta unidades de cinta para copias de seguridad.

4.2.5 INSTALACIÓN.

Se mostrará el proceso de instalación después de crear los disquetes de inicio.

En cualquier momento de la instalación se puede solicitar ayuda con la tecla <F1>.

El programa de instalación presenta un mensaje de bienvenida y pregunta si se desea instalar Windows NT ahora, reanudar una instalación interrumpida o cancelar el trabajo.

Si instala Windows NT en el ordenador por primera vez, basta con que pulse la tecla <Enter>. (figura IV.1)



(figura IV.1)

4.2.5.1 CONFIGURACIÓN DE UNIDADES DE ALMACENAMIENTO.

El primer paso de la instalación consiste en que Windows NT detecte las unidades de almacenamiento (CD-ROM, unidades de copia de seguridad, adaptadores SCSI) del ordenador. (figura IV.2)



(figura IV.2)

Es posible instalar posteriormente unidades de almacenamiento si no han sido detectadas automáticamente. Los discos duros IDE y EIDE se detectan automáticamente en la posterior instalación de

Windows NT (basta con activar el administrador de discos duros y registrar y dar formato al o a los discos en NT). Pero los discos SCSI deben ser instalados manualmente con el ícono SCSI en el Panel de control de Windows NT.

El programa de instalación le muestra finalmente la configuración de las unidades de almacenamiento de todos los dispositivos detectados. (figura IV.3)



(figura IV.3)

La instalación de Windows NT realiza entonces particiones, si fuera necesario, en los discos duros. Dichas particiones reciben formato con el sistema de archivos que haya indicado. (figura IV.4)



(figura IV.4)

4.2.5.2 SELECCIÓN DEL DIRECTORIO RAÍZ DE WINDOWS NT.

Una vez que los discos duros tengan particiones y formato, se debe indicar un directorio raíz para los archivos de sistema de Windows NT. Si anteriormente no había instalado en el ordenador ninguno de los sistemas operativos Windows NT, Windows 95, Windows 98 o Windows para trabajo en grupo, puede elegir el directorio libremente, darle un nombre y establecer la partición de destino en el disco duro. (figura IV.5)



(figura IV.5)

Sin embargo, si ya había instalado alguno de los sistemas operativos anteriormente mencionados, puede sobrescribir el existente con Windows NT o bien instalar Windows NT en otro directorio (a través de la instalación personalizada).

Si elige la primera opción, las aplicaciones existentes se instalarán rápidamente si son compatibles con Windows NT, y las configuraciones personales que haya realizado se incorporarán a Windows NT. En cambio si instala el nuevo sistema operativo en otro directorio se conserva el anterior y, al iniciar, podrá elegir entre ambos sistemas con el administrador de inicio de Windows NT.

Sugerencia:

En ocasiones puede ser conveniente instalar dos veces NT 4 en el disco duro. Cuando, por ejemplo, en una versión de NT debe iniciar demasiados servicios, que quizá sean incompatibles entre sí, la velocidad de ejecución de NT en parte se reduce drásticamente.

De este modo concluyen las configuraciones de instalación basadas en **DOS** y el programa de instalación intentará reiniciar su equipo. Para ello deberá retirar el disquete de inicio de su unidad. Por último, se cargará automáticamente el asistente de instalación, el cual le indicará los pasos necesarios. (figura IV.6)



(figura IV.6)

4.2.5.3 SELECCIÓN DEL TIPO DE INSTALACIÓN.

En el primer paso del asistente de instalación puede elegir que tipo de instalación desea ejecutar:

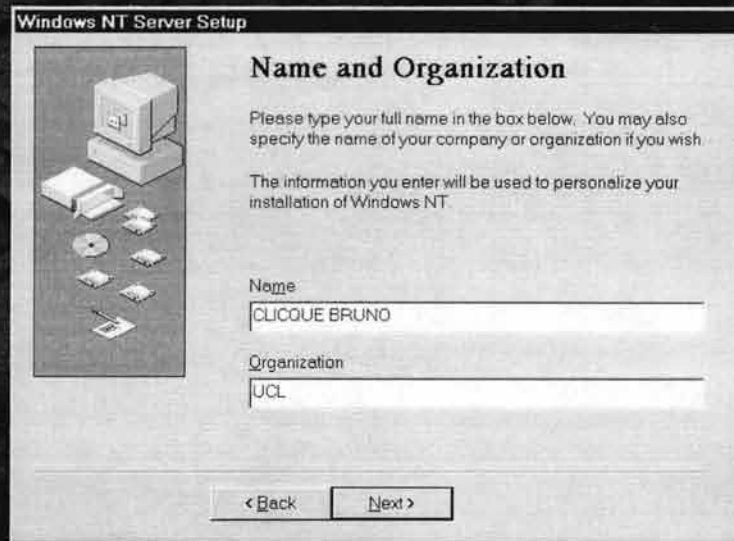
- Instalación típica: es el tipo más sencillo. El asistente de instalación se encarga de tomar la mayoría de decisiones instalando todas las opciones predeterminadas. Windows NT se instala con todos los componentes adicionales (como HyperTerminal y MS Exchange).
- Instalación portátil: esta opción se ha incorporado especialmente para la instalación de Windows NT en ordenadores portátiles. Sólo se instala una versión reducida.
- Compacta: aquí sólo se instalan los archivos de sistema más importantes de Windows NT, a fin de ahorrar espacio en el disco duro.
- Personalizada: con esta variante puede confirmar y modificar todas las configuraciones de la instalación. También deberá elegir los componentes del sistema que desea instalar.

4.2.5.4 MODOS DE LICENCIA E INTRODUCCIÓN DE LOS DATOS PERSONALES.

En esta parte de la instalación debe introducir sus datos personales y un nombre para el ordenador, así como elegir el modo de licencia. Son necesarias las siguientes configuraciones:

- Un nombre de usuario y una empresa a través de los cuales Windows NT le pueda identificar. Sin estos datos no puede proseguir con la instalación. (figura IV.7)

Windows NT Setup

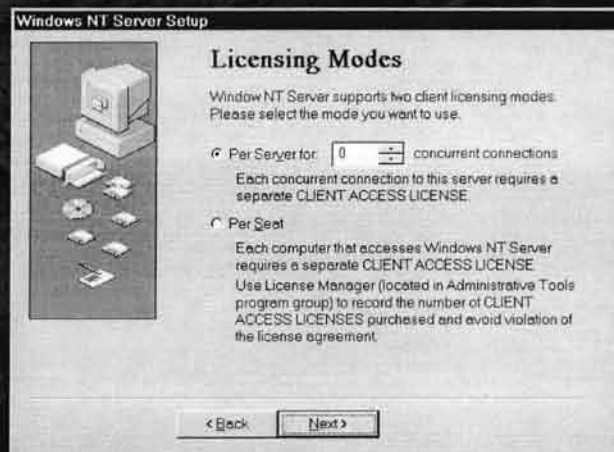


The screenshot shows the 'Name and Organization' step of the Windows NT Server Setup. On the left, there is an illustration of a computer system with a monitor, keyboard, mouse, and floppy disks. The main area contains the following text: 'Please type your full name in the box below. You may also specify the name of your company or organization if you wish.' Below this, it says 'The information you enter will be used to personalize your installation of Windows NT.' There are two input fields: 'Name' with the text 'CLIQUE BRUNO' and 'Organization' with the text 'UCL'. At the bottom, there are two buttons: '< Back' and 'Next >'.

(figura IV.7)

- Como modo de licencia se elige entre *Por puesto* o *Por servidor*. (figura IV.8)

Windows NT Setup



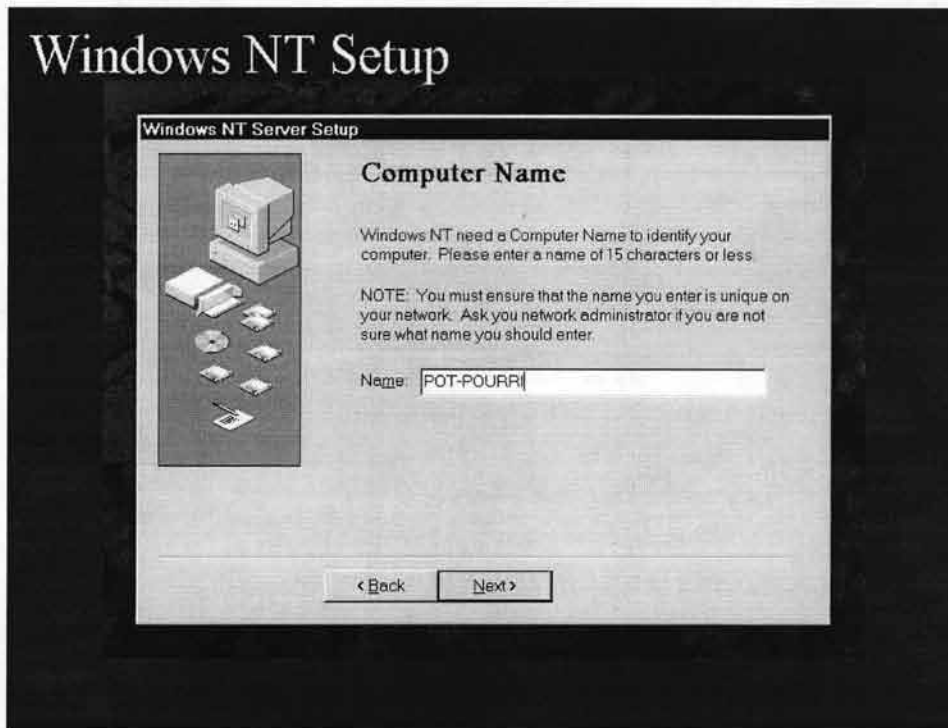
The screenshot shows the 'Licensing Modes' step of the Windows NT Server Setup. On the left, there is an illustration of a computer system with a monitor, keyboard, mouse, and floppy disks. The main area contains the following text: 'Windows NT Server supports two client licensing modes. Please select the mode you want to use.' There are two radio button options: 'Per Server for: 0 concurrent connections' (which is selected) and 'Per Seat'. Below the 'Per Server' option, it says 'Each concurrent connection to this server requires a separate CLIENT ACCESS LICENSE.' Below the 'Per Seat' option, it says 'Each computer that accesses Windows NT Server requires a separate CLIENT ACCESS LICENSE. Use License Manager (located in Administrative Tools program group) to record the number of CLIENT ACCESS LICENSES purchased and avoid violation of the license agreement.' At the bottom, there are two buttons: '< Back' and 'Next >'.

(figura IV.8)

Información:

Si elige la opción *Por puesto*, no podrá cambiarla posteriormente. En cambio, si elige la licencia *por servidor*, luego podrá cambiarla por *licencia por puesto*.

- Indique el nombre con el que se da de alta el ordenador en la red. Este nombre no puede coincidir con el de ningún otro ordenador de la red, con el nombre del dominio ni con ningún nombre de usuario. Los nombres de los ordenadores en Windows NT pueden tener hasta 15 caracteres de longitud y no pueden contener ningún carácter especial ni acentos. El nombre de un ordenador se puede modificar en cualquier momento desde el Panel de control. (figura IV.9)

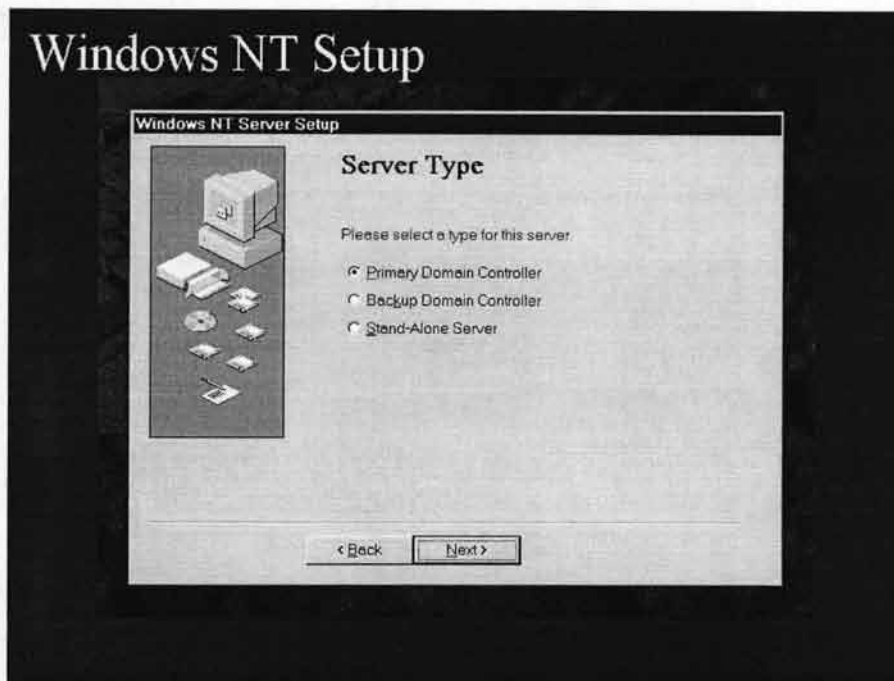


(figura IV.9)

En la instalación personalizada se preguntarán los componentes que deben instalarse, impresoras locales incluidas.

4.2.5.5 SELECCIÓN DEL TIPO DE SERVIDOR (SÓLO WINDOWS NT SERVER).

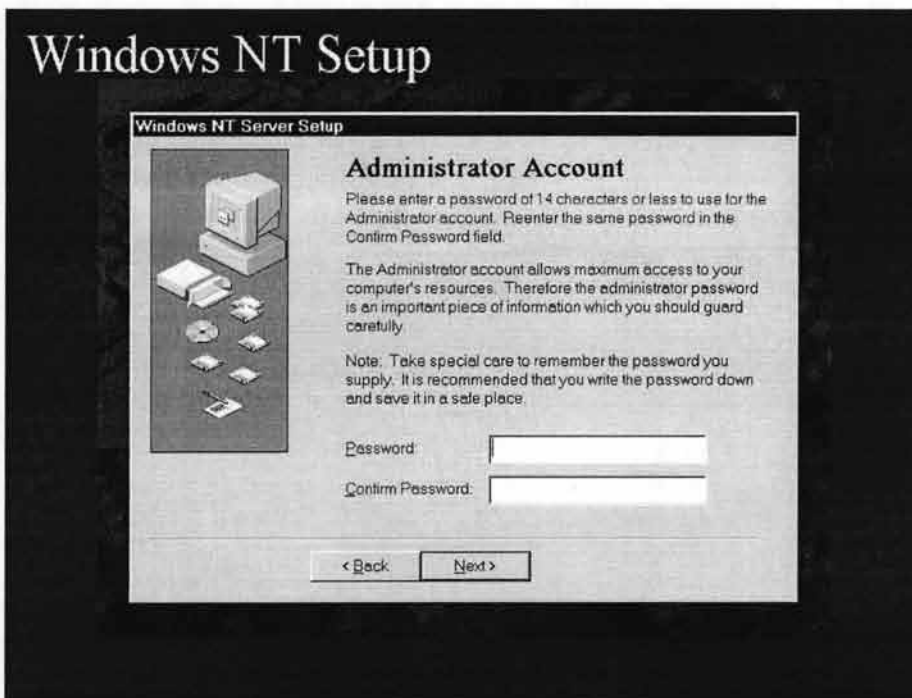
- Los dominios de Windows NT son administrados por un controlador principal de dominio, el cual gestiona la base de datos de seguridad con todos los datos de los usuarios. Cada dominio de Windows NT debe tener exactamente un controlador principal de dominio y uno o varios controladores de dominio de reserva (también llamados controladores de seguridad). Los controladores de dominio de reserva sólo pueden instalarse si ya funciona en la red el controlador principal de dominio. (figura IV.10)



• (figura IV.10)

4.2.5.6 CONTRASEÑA DEL ADMINISTRADOR.

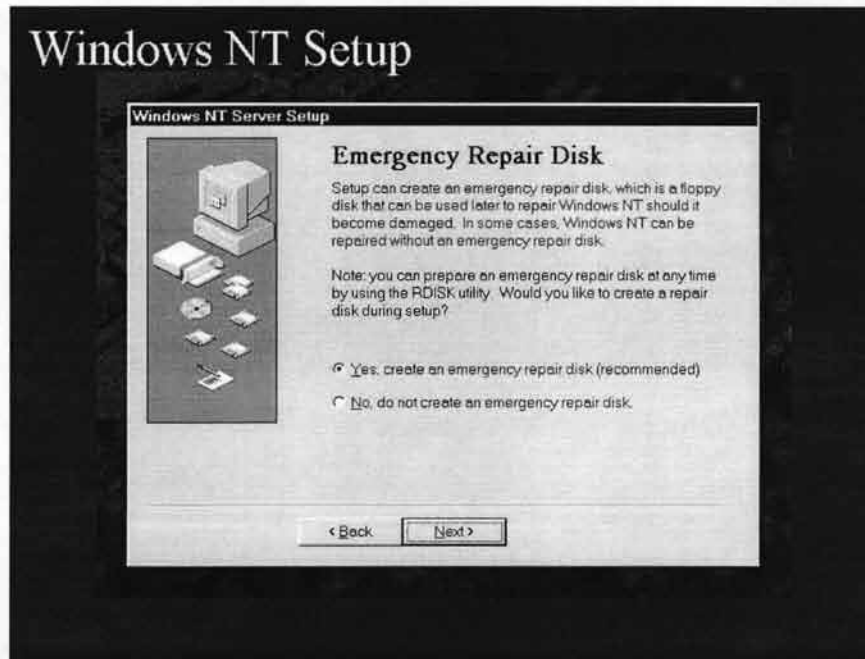
• El programa de instalación configura en su sistema Windows NT un acceso con el nombre de Administrador. Únicamente este usuario (siempre y cuando no asigne derechos de administrador a otros usuarios) puede realizar todas las configuraciones en el sistema local y dentro de los dominios. En este punto del programa de instalación se establece la contraseña para este acceso. (figura IV.11)



(figura IV.11)

4.2.5.7 CREACIÓN DE UN DISQUETE DE EMERGENCIA

Tras un bloqueo del sistema que haya dañado la totalidad de la base de datos de seguridad incluyendo las copias de seguridad, Windows NT puede restablecerse con la ayuda de un disquete. Este disquete de emergencia contiene todos los componentes del sistema que el usuario ha introducido o que Windows NT ha detectado hasta ahora. (figura IV.12)

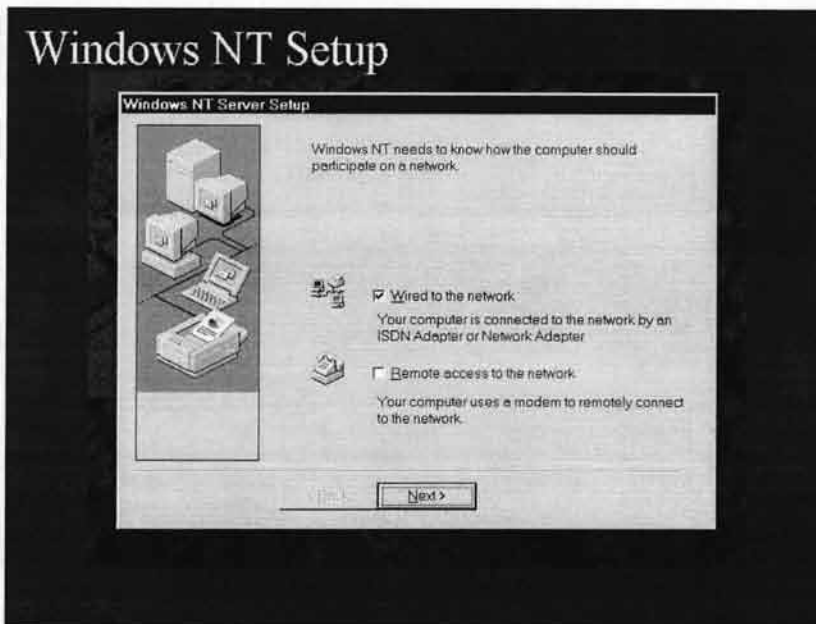


(figura IV.12)

4.2.6 INSTALACIÓN EN RED DE WINDOWS NT.

Windows NT se utiliza, en la mayoría de aplicaciones, dentro de una red, ya sea como servidor de una red Windows NT, como estación de trabajo en una red Windows o como parte de una red heterogénea.

Con el programa de instalación también se instala la funcionalidad de red de Windows NT. Debe decidir si su ordenador estará conectado en una red local o si establecerá la conexión con esa red a través de una conexión RAS. Obviamente también se pueden elegir ambas opciones a la vez. (figura IV.13)



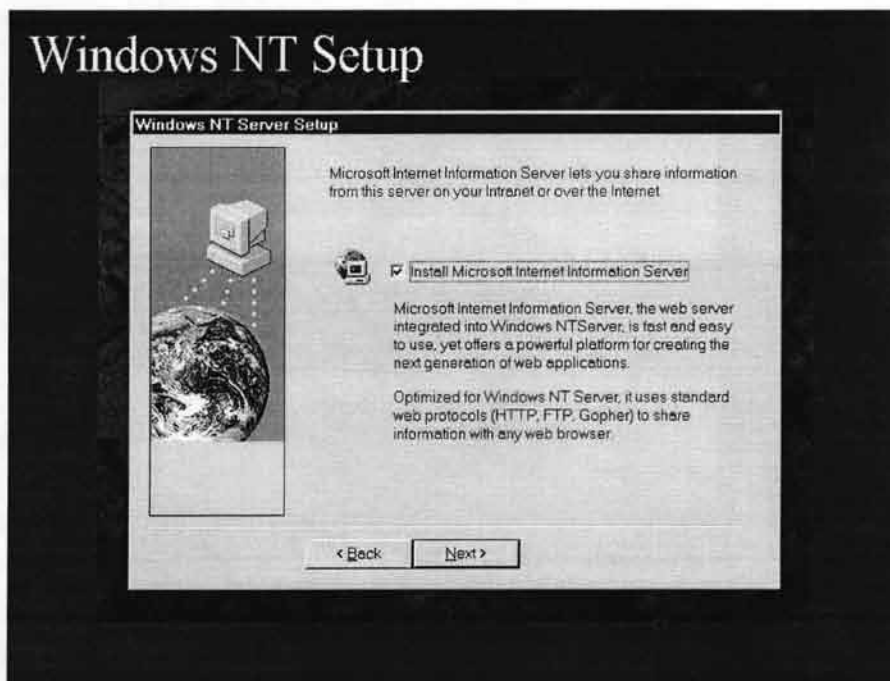
(figura IV.13)

A continuación se detallan los pasos más importantes de la instalación en red.

4.2.6.1 INSTALACIÓN DE INTERNET INFORMATION SERVER.

Windows NT en su versión 4.0 se suministra con Internet Information Server. Si está conectado a Internet a través de un proveedor de Internet, puede ofrecer servicios WWW y FTP.

Windows NT Server y Windows NT Workstation utilizan distintas versiones de Internet Information Server. La versión que se suministra con Windows NT Workstation está pensada para la utilización en intranets, mientras que la versión para Windows NT Server puede funcionar como un "auténtico" servidor WWW y FTP en Internet. (figura IV.14)



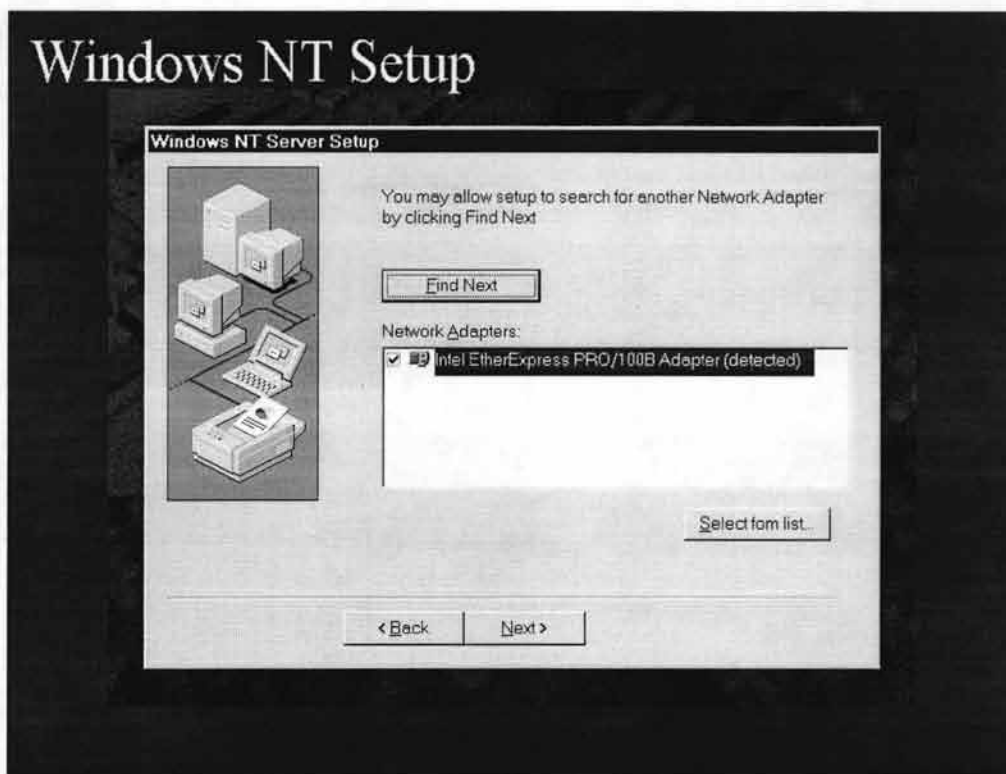
(figura IV.14)

4.2.6.2 INSTALACIÓN DE LA TARJETA DE RED.

La parte más importante de la instalación de una conexión en red es la instalación del adaptador de red. En el caso de una LAN, se trata de la tarjeta de red, y en el caso de una WAN suele tratarse de un módem o de una tarjeta RDSI.

El programa de instalación puede detectar automáticamente la tarjeta de red instalada en su sistema si Windows NT es compatible con el adaptador de red.

Si deja que Windows NT detecte la tarjeta de red, el programa de instalación examinará el ordenador en busca de adaptadores compatibles. En caso de utilizar más de un adaptador de red, pulse el botón *Buscar siguiente* en cuanto el programa de instalación haya encontrado un adaptador.(figura IV.15)



(figura IV.15)

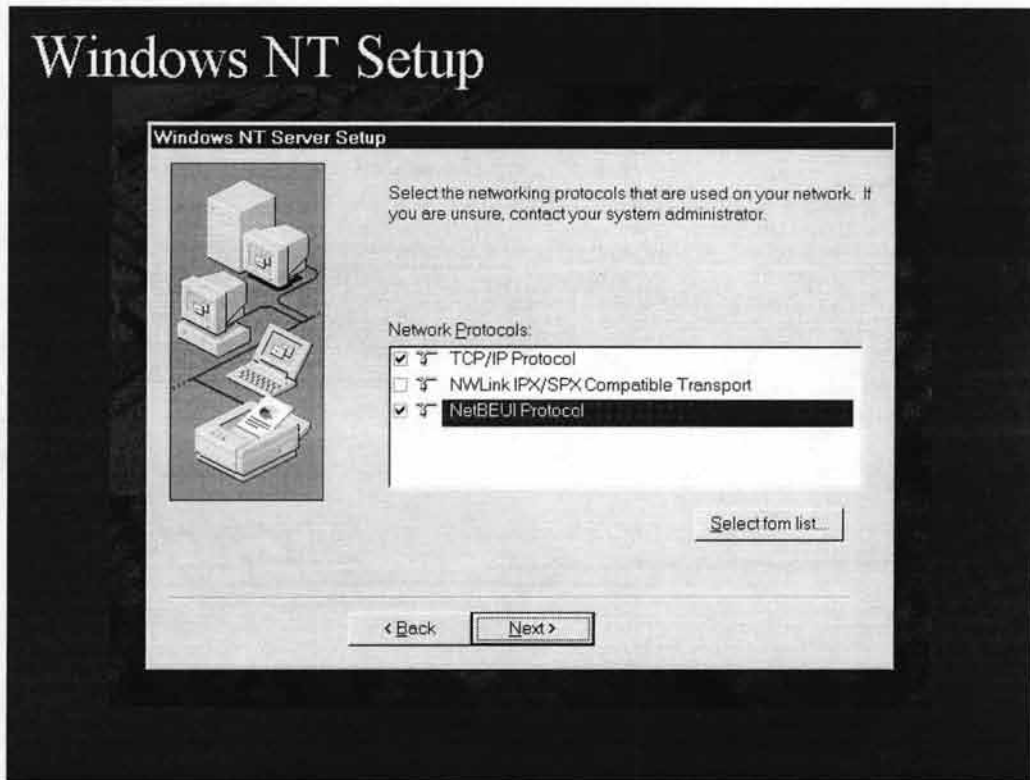
4.2.6.3 INSTALACIÓN DE LOS PROTOCOLOS DE RED.

Después de haber instalado el adaptador de red, deberá determinar que protocolos de red serán transmitidos a través del mismo. Windows NT establece entonces una conexión entre el protocolo y los controladores para la tarjeta correspondiente (denominada “*binding*” o enlace).

Windows NT es compatible con los siguientes protocolos de red:

- **NetBEUI:** NetBEUI es el protocolo estándar en las redes Microsoft Windows en Windows NT a partir de la versión 3.1, Windows para Trabajo en grupo o Windows 95. En la mayoría de los casos se utiliza en redes pequeñas, con menos de 200 clientes. NetBEUI sólo soporta un encaminamiento simple a través de funciones de “Token” Ring.
- **NWLink:** Este protocolo compatible con IPX/SPX y, por lo tanto, con NOVELL® NETWARE®, se utiliza en la mayoría de redes LAN grandes. Tiene capacidades de encaminamiento y trabaja junto con aplicaciones cliente-servidor de NETWARE®.

TCP/IP: Es el protocolo estándar en redes de área extensa y en Internet. Como TCP/IP es compatible con todas las plataformas de sistemas es el protocolo estándar en redes heterogéneas. TCP/IP tiene plena capacidad de encaminamiento. (figura IV.16)



(figura IV.16)

El programa de instalación establece los enlaces de los distintos protocolos con las tarjetas de red. Los controladores de redes RAS son tratados como tarjetas de red. En primer lugar, acepte las configuraciones predeterminadas de Windows NT. La edición de los enlaces sólo merece la pena si utiliza en su ordenador varias tarjetas de red que utilizan distintos protocolos. Si eliminamos los enlaces innecesarios, la velocidad de Windows NT se incrementará.

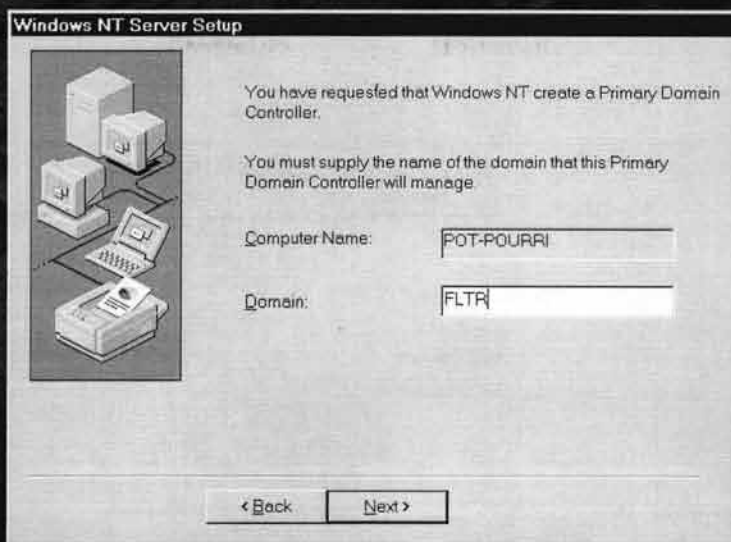
4.2.6.4 SELECCIÓN DEL GRUPO DE TRABAJO O DOMINIO.

Windows NT soporta vinculaciones de red a través del grupo de trabajo de una red punto a punto o del dominio de una red Windows NT.

En este punto tiene que decidir si sólo desea darse de alta en un grupo de trabajo o si el ordenador debe formar parte de una red Windows NT, en cuyo dominio tendrá que darse de alta.

El primer inicio de sesión en el sistema es el del administrador, ya que aún no se ha creado ningún usuario. Además, por lo general se deberán efectuar otras configuraciones adicionales que sólo puede llevar a cabo el administrador. (figura IV.17)

Windows NT Setup



(figura IV.17)

Con esto concluimos la instalación propiamente dicha, ahora lo que se podría instalar son componentes opcionales como por ejemplo el módem, un CD-ROM o una tarjeta RDSI.

4.3 ADMINISTRACIÓN DE ARCHIVOS EN NT.

Los discos duros contienen el bien más preciado: los datos. Si los datos no se guardan periódicamente, la pérdida de datos puede ser catastrófica para la empresa.

Existen varias posibilidades para protegerse de incidentes y sus consecuencias. El riesgo de pérdida de datos se reduce a través de:

- La selección de discos duros de mayor calidad.
- La elección de un sistema de archivos estable (es NT: NTFS).
- La organización de datos segura y compatible con el sistema de archivos o el controlador de disco duro.
- La copia de los datos realizando copias de seguridad regulares (mejor diarias) y reflejando el disco duro o utilizando sistemas RAID 5.

4.3.1 SISTEMAS DE ARCHIVOS.

Los sistemas de archivos organizan los datos en los discos duros distribuyéndolos en áreas físicamente accesibles del disco. Algunos sistemas de archivos aceleran los procesos de lectura y escritura con memorias caché propias.

Los sistemas operativos de ordenadores utilizan principalmente los siguientes sistemas de archivos:

- FAT
- HPFS
- NTFS

Estos sistemas de archivos se diferencian por su seguridad y rendimiento:

4.3.1.1 FAT.

Tabla de asignación de archivos (FAT) es el sistema de archivos más sencillo.

En un archivo aparte (FAT), consta en qué sectores del disco duro (o del disquete) se encuentra cada parte de un archivo. Para ello, FAT divide el disco duro en bloques. El número de bloques es limitado y todos los bloques de un disco duro deben tener siempre el mismo tamaño. En discos duros grandes con sólo una partición FAT se pierde mucho espacio. Además, los bloques FAT grandes provocan errores de disco duro con facilidad. Los sistemas de archivos FAT hasta ahora imponían al usuario la limitación 8+3 para el nombre de archivos y directorios.

Desde la aparición de Windows 95 con su sistema de archivos FAT ampliado (V-FAT), esta limitación ya no existe. Sin embargo, V-FAT no ha podido mejorar la seguridad y la estabilidad del sistema de archivos.

Además, pronto se produce una fragmentación del disco duro, ya que la información se escribe en los bloques FAT de todo el disco.

4.3.1.2 HPFS.

Sistemas de archivos de alto rendimiento (HPFS) pertenecen a los sistemas de archivos instalables (IFS). Se encuentra principalmente en ordenadores OS/2, aunque originalmente fue desarrollado por Microsoft. Los sistemas de archivos HPFS son mucho más seguros, estables y rápidos que los sistemas FAT. HPFS accede a los datos del disco duro a través de un búfer de alta velocidad (caché) y soporta varias particiones activas al mismo tiempo. En los sistemas de archivos HPFS, los nombres de archivo pueden tener hasta 254 caracteres de longitud.

4.3.1.3 NTFS.

El sistema de archivos de NT (NTFS) ha sido desarrollado especialmente para Windows NT. NTFS es aun más seguro y estable que HPFS, aunque necesita algo más de tiempo para acceder a los archivos. Si desea crear discos duros espejo o dividirlos en bandas con paridad, deberá utilizar una partición NTFS. Estas funciones especiales del Administrador de discos de Windows NT no son compatibles con otros sistemas de archivos.

Windows NT ofrece, junto con el sistema de archivos NTFS, medidas de seguridad ampliadas para el acceso a archivos y directorios. De forma similar a los sistemas de archivos UNIX, se pueden definir derechos sobre archivos y directorios de forma individual para cada grupo. Windows NT no ofrece ningún mecanismo de seguridad en el sistema de archivos FAT.

El sistema de archivos de Windows NT considera cada sector del soporte de datos como archivo o parte de un archivo al que se le asignan determinados atributos y derechos de usuario. De modo similar a los sistemas de archivos FAT, en un archivo especial se define qué sectores pertenecen a cada archivo y dónde se encuentran los mismos. NTFS denomina a ese archivo MFT (Tabla maestra de archivos). La MFT también contiene una entrada de registro, que se encarga de restablecer archivos en Windows NT.

En la MFT se comparte para cada archivo un determinado espacio, que luego puede incorporar la información sobre donde está guardado del archivo.

Los archivos pequeños también pueden incorporarse directamente en este espacio, mientras que los archivos grandes se guardan en forma de un Btree. NT compara en este árbol el valor buscado con dos entradas existentes y luego reanuda la búsqueda en una u otra rama. Es este árbol de búsqueda jerárquico se establece qué partes del archivo se encuentran en cada sector del disco duro. Así pues, dado que la MFT no es, a diferencia de la FAT, una tabla lineal, durante la búsqueda de un archivo el sistema tampoco debe examinar obligatoriamente toda la estructura. Esto explica el acceso más rápido a archivos de los sistemas NTFS frente a los sistemas de archivos FAT.

La siguiente tabla resume las propiedades de los sistemas de archivos FAT, HPFS y NTFS.

	FAT	HPFS	NTFS
Nombres de archivo	8+3 caracteres	254 caracteres	256 caracteres
Atributos de archivo	Sin derechos de acceso	Derechos de acceso	Derechos de acceso
Directorios	Sin clasificar	Btree	Btree
Distribución de unidades en varios discos duros	no	no	Sí
Discos espejo	no	Sólo con HPFS 386	Sí
Registro de eventos	no	-	Sí

La tabla siguiente resume con que sistemas de archivos trabajan algunos de los sistemas operativos comentados anteriormente y si éstos pueden leer o escribir datos en ellos.

	FAT	HPFS	NTFS
Windows NT 4.0	Leer y escribir	No compatible	Leer y escribir
Windows NT 3.x	Leer y escribir	Leer y escribir	Leer y escribir
DOS/Windows 3.x	Leer y escribir	-	-
Windows 95	Leer y escribir	Leer con programas	Leer a través de redes adicionales
OS/2	Leer y escribir	Leer y escribir	-
Linux	Leer y escribir	-	-

4.3.2 MÉTODOS PARA GUARDAR LOS DATOS DE FORMA SEGURA.

4.3.2.1 CONJUNTO DE UNIDADES DE ALMACENAMIENTO.

Con un conjunto de unidades de almacenamiento se puede reunir espacio disponible en distintos discos físicos (hasta 32), a fin de obtener un único gran volumen con una letra de unidad común. Dicho volumen puede ser dividido en particiones y unidades lógicas, al igual que un disco físico. Los conjuntos de unidades de almacenamiento pueden ampliarse en cualquier momento con más espacio disponible de otros discos duros, sin poner en peligro los datos existentes del conjunto de unidades de almacenamiento. Sin embargo, no es posible reducir el conjunto de unidades sin eliminar los datos que contiene.

Si bien los conjuntos de unidades de almacenamiento permiten un uso eficaz de los discos pequeños o de los espacios disponibles "restantes" de distintos discos duros, por otro lado, ponen en peligro la seguridad de los datos de todo el sistema. Los defectos de un disco duro físico impiden el acceso a los archivos restantes del conjunto de almacenamiento de datos en cuestión, incluso en otros discos que estén intactos.

4.3.2.2 RAID.

El sistema RAID (Redundant Array of Inexpensive Drives, sistema redundante de discos duros económicos) también reúne, en Windows NT, distintas estrategias para dividir el espacio disponible en diversos discos duros. De los seis grados de RAID (de 0 a 5), algunos protegen los datos de posibles pérdidas por daños en el equipo, mientras que otros aumentan la velocidad de lectura y escritura.

Los procedimientos RAID más conocidos son el RAID 1 y el RAID 5. El RAID 1 duplica los datos en los discos duros idénticos (discos espejo). El RAID 5 forma paridades de conjuntos de bandas, que se distribuyen de forma redundante por todos los discos duros (ver un poco más abajo, en conjunto de bandas). El RAID 5 aumenta el rendimiento en la lectura de datos, pero, en cambio, es más lento que el RAID 1 para escribir. El RAID 5 de Windows NT se controla a través de programa y carga notablemente la memoria principal. Es más efectivo y seguro el RAID 5 del equipo, a través de controladores de discos duros RAID junto con discos intercambiables durante el funcionamiento.

4.3.2.3 DISCOS ESPEJO.

Con los discos espejo se reproducen los datos de una partición o de una unidad de un disco en un área libre de otro disco duro. Esta área del segundo disco duro deja entonces de estar visible en el administrador de archivos y en la interfase de comandos, puesto que sólo refleja datos. Los discos espejo son un medio muy eficaz para protegerse contra una posible pérdida de datos debida a un error del disco duro. Sin embargo, de este modo no es posible evitar los defectos de control, los virus y otros problemas, ya que también hacen mella en el conjunto de almacenamiento de datos.

4.3.2.4 CONJUNTOS DE BANDAS.

En un conjunto de bandas, los datos no se escriben como una totalidad en el disco duro, sino en pequeñas partes denominadas bandas. Los conjuntos de bandas pueden extenderse por distintas áreas de una unidad física (o incluso de distintas). Es posible crear conjuntos de bandas con o sin paridad. Para una banda con paridad es preciso un número impar de partes de espacio disponible (tres o más), mientras que para un conjunto de bandas sin paridad siempre hará falta un número par (dos o más).

Los conjuntos de bandas sin paridad ofrecen ventajas en cuanto a velocidad, porque los datos pueden escribirse al mismo tiempo en distintos discos (quizá utilizando para ello distintos controladores). Si se produce un error en una unidad de almacenamiento de un conjunto de bandas, se pierden todos los datos del conjunto, ya que el resto de bandas, generalmente, no pueden recuperar datos sin la información del defectuoso.

Muy distinto es con bandas con paridad. Aunque con ellas se pierde la ventaja de la velocidad que ofrecen las bandas sin paridad, a partir de la información de paridad se pueden recuperar datos de una banda defectuosa.

4.3.2.5 EL SISTEMA DE ARCHIVOS NTFS.

Windows NT, como sistema operativo de nueva tecnología tenía que incorporar un sistema de archivos de nueva tecnología y despedirse definitivamente del sistema de archivos FAT. Aunque el sistema de archivos FAT, gracias a su ampliación a VFAT, domine los nombres de archivo largos en Windows 95 / *DOS* 7, apenas cumple los criterios de un sistema de archivos profesional que pueda utilizarse en servidores.

Las características principales son:

- Los sistemas de archivos para sistemas operativos multiusuario y servidor precisan derechos de acceso avanzados para usuarios individuales y para grupos de usuarios.
- NTFS permite particiones de disco duro mucho más grandes y archivos como (V)FAT (máximo 4 GB), por lo que está preparado para ser utilizado en servidores. Además, NTFS

es compatible con los métodos RAID 1 a 5, que sirven para aumentar la velocidad de acceso y para hacer copias de los datos mediante los discos duros espejo (ver arriba).

- NTFS distingue mayúsculas de minúsculas en los nombres de archivos y directorios y permite caracteres especiales como los acentos. Con ello cumple las directivas del estándar UNICODE.

- Las particiones NTFS pueden recuperarse de forma más fácil que las particiones (V)FAT después de un fallo del sistema.

- NTFS es menos propenso que (V)FAT a la fragmentación de los discos duros.

NTFS hace patentes sus ventajas en cuanto a velocidad frente a FAT especialmente en cooperación con los controladores SCSI. Gracias al acceso asincrónico a los datos pueden desplazarse procesos de lectura y escritura a las colas de espera, librando así al procesador de una carga. Durante la edición de un proceso pueden aceptarse y editarse entonces otros procesos. Especialmente en servidores Windows NT, que tienen que afrontar numerosos procesos de lectura y escritura debido a los accesos simultáneos de los usuarios, es donde NTFS experimenta un aumento de velocidad más evidente en controladores SCSI de 32 bits.

Hasta la versión 3.51, Windows NT era compatible con el sistema de archivos HPFS. Este sistema de archivos desarrollado originalmente por Microsoft se sigue suministrando actualmente con OS/2. HPFS es tan seguro como NTFS y en su ampliación para WARP Server muestra las mismas propiedades en cuanto a compatibilidad con RAID y derechos de acceso. Lamentablemente, desde la versión 4.0 Windows NT sólo puede leer particiones HPFS y convertirlas en otras particiones, pero no puede crear particiones HPFS propias o escribir en ellas.

4.3.2.6 ADMINISTRACIÓN DE UNIDADES DE ALMACENAMIENTO EN WINDOWS NT.

La administración de discos duros es especialmente interesante para servidores. Los servidores disponen de varios discos duros, generalmente mucho más grandes que los ordenadores de escritorio. Los datos de esos discos duros no sólo deben ponerse a disposición de los clientes, sino que también deben de estar guardados en los discos duros de forma segura.

Tamaño de los discos duros: el tamaño de los discos duros no es asunto del sistema operativo instalado. Sin el controlador Enhanced IDE o LBA *BIOS* pueden surgir problemas con los discos IDE, ya que sólo son iniciables las particiones por debajo de 540 MB. En los discos SCSI no hay este tipo de problemas.

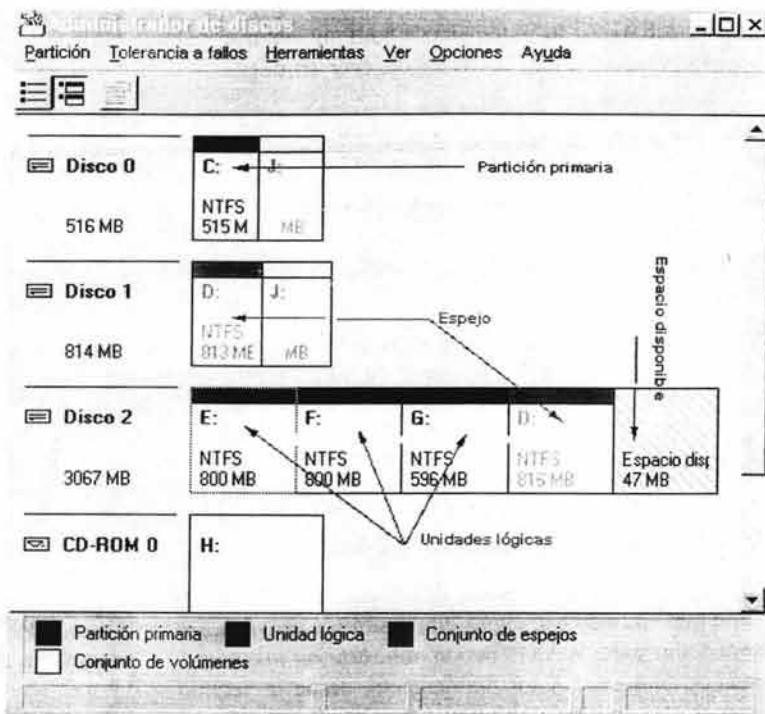
Seguridad: de la seguridad de los datos de un disco duro se encarga, esencialmente, junto con la calidad del disco duro en sí, el sistema de archivos. La seguridad de los datos comprende, además de lo mencionado, un buen plan de seguridad y una copia de seguridad.

Velocidad de acceso: es necesario procurar una velocidad de acceso suficiente, a fin de que el trabajo con unidades de red no ponga a prueba la paciencia del usuario. La velocidad de acceso no sólo es cuestión del disco en sí y del controlador de disco duro, sino también del sistema de archivos y particiones.

Windows NT ofrece un programa adicional propio para la administración de discos duros, el Administrador de discos.

4.3.2.7 EL ADMINISTRADOR DE DISCOS.

El administrador de disco es la herramienta gráfica que emplea NT para la gestión de discos duros, con dicha herramienta podemos: (figura IV.18)



(figura IV.18)

- Gestionar particiones de disco y unidades lógicas.
- Dar formato a volúmenes y asignarles nombres.
- Leer la información del estado de los discos.
- Leer la información del estado de los volúmenes, la etiqueta y la letra del volumen, el sistema de archivos y su tamaño.
- Crear y modificar las asignaciones de letras.
- Ampliar un volumen o un conjunto de volúmenes.
- Crear y eliminar conjuntos de volúmenes.
- Crear o eliminar conjuntos de bandas con o sin paridad.
- Regenerar un miembro no encontrado de un conjunto de bandas.
- Establecer o romper conjuntos de espejos.

Antes de comenzar un par de advertencias: el administrador de discos no permite trabajar sobre la partición de sistema (normalmente C:), ya que contiene los archivos necesarios para que NT se ejecute, el resto de las particiones son totalmente moldeables pero tendrá que tener cuidado con lo que hace en aquellas que contengan datos, ya que podría perderlos.

4.3.2.8 GUARDAR DATOS.

En los apartados anteriores se ha presentado distintas posibilidades de proteger los datos de forma activa. En este caso, se habla de protección activa porque estas medidas evitan las pérdidas de datos. Ahora se tratarán las medidas de seguridad pasivas con las cuales se reducen al mínimo las consecuencias de una

pérdida de datos. Una de las medidas de seguridad pasiva consiste en guardar periódicamente los datos en otros soportes de datos.

Aquí se hará referencia a “verdaderas” unidades de copia de seguridad.

Elegir el medio:

Una de las primeras cuestiones a considerar para guardar datos es la elección del medio de almacenamiento correcto. Se dispone de los medios siguientes, entre otros, con distintas capacidades de almacenamiento:

- Cintas de copia de seguridad de hasta 500 MB.
 - Cintas DAT (DDS1, DDS2) de hasta 2 ó 4 GB, comprimidas hasta 4 u 8 GB (en función del medio: cinta DAT de 90 o 120 metros).
- Cintas DLT de hasta 20 ó 40 GB.
- Unidades magnetoópticas hasta 900 MB.
- CD-ROM con hasta 600 MB.
- Discos intercambiables mínimo 1 GB.

El tamaño de los datos reduce la selección de las posibles unidades de almacenamiento. En cualquier caso, también se debe tener en cuenta la durabilidad y el manejo de los medios. Los CD-ROM grabados por uno mismo duran mucho menos que los editados por los fabricantes. La capa del CD en la que se escribe es muy delicada y puede quedar inutilizable con sólo algunos rasguños. Además, actualmente algunos críticos de estos medios predicen unos pocos años de durabilidad incluso tratándolos con cuidado ya que los CD de plástico se descomponen.

Los CD-ROM gozan de la decisiva ventaja de que sólo con introducirlos en una unidad de CD-ROM se puede trabajar con los datos. Por lo tanto, se puede prescindir de la reproducción de los datos tal y como sucede con una unidad de cinta.

Las unidades MLO son muy seguras, puesto que los datos se escriben en el medio bajo un determinado aumento de temperatura. En cuanto el medio se enfría, no puede dañarse, por ejemplo, con un imán.

Las cintas son un medio de almacenamiento de gran durabilidad. Para almacenar datos en una cinta, lo que se denomina copia de seguridad se debe escribir en ella con un programa especial y para leer los datos se debe utilizar el mismo programa.

Precisamente sobre esta cuestión, las empresas no deben elegir cualquier programa ni cualquier unidad para realizar copias de seguridad sino utilizar estándares que sean soportados durante las dos décadas siguientes. Si opta por una unidad SCSI-DAT utilizando el programa para copias de seguridad de Windows NT, hasta cierto punto puede estar seguro de que estas copias podrán leerse con versiones posteriores de NT. Lo mismo se puede aplicar para proveedores conocidos, que vendan programas de este tipo desde hace años.

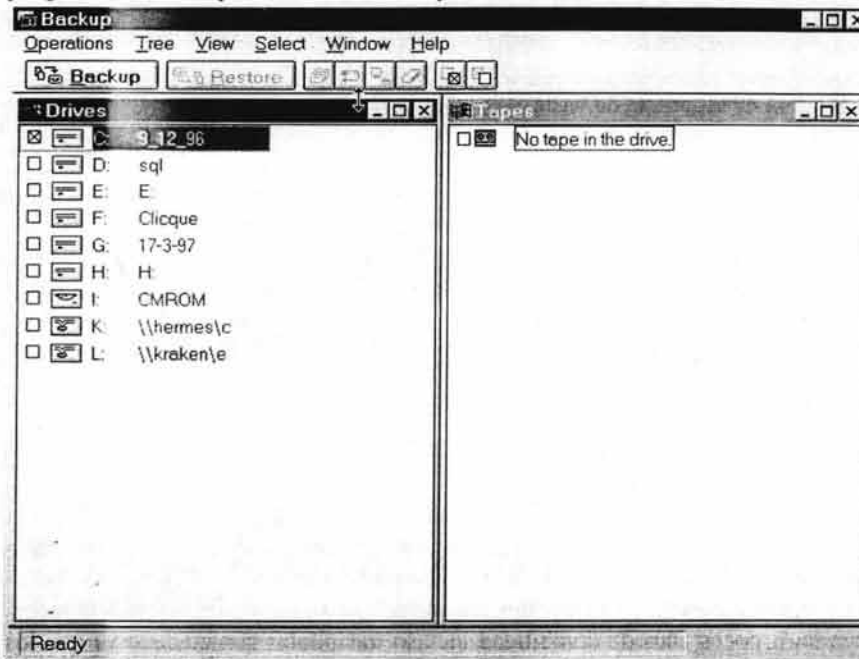
Copias de seguridad de Windows NT:

Windows NT contiene, en su versión estándar, un sencillo programa de copias de seguridad de la casa Seagate, el fabricante de Arcada Backup para NT. Con el mismo se pueden guardar datos en unidades de cintas compatibles con Windows NT y previamente instaladas en Windows NT.

En Windows NT también se pueden iniciar copias de seguridad con el comando backup de la interfase de comandos. De esta forma, es posible iniciar copias de seguridad fácilmente, a través de conexiones remotas con el ordenador Windows NT.

Almacenamiento de datos con el programa de copias de seguridad de NT

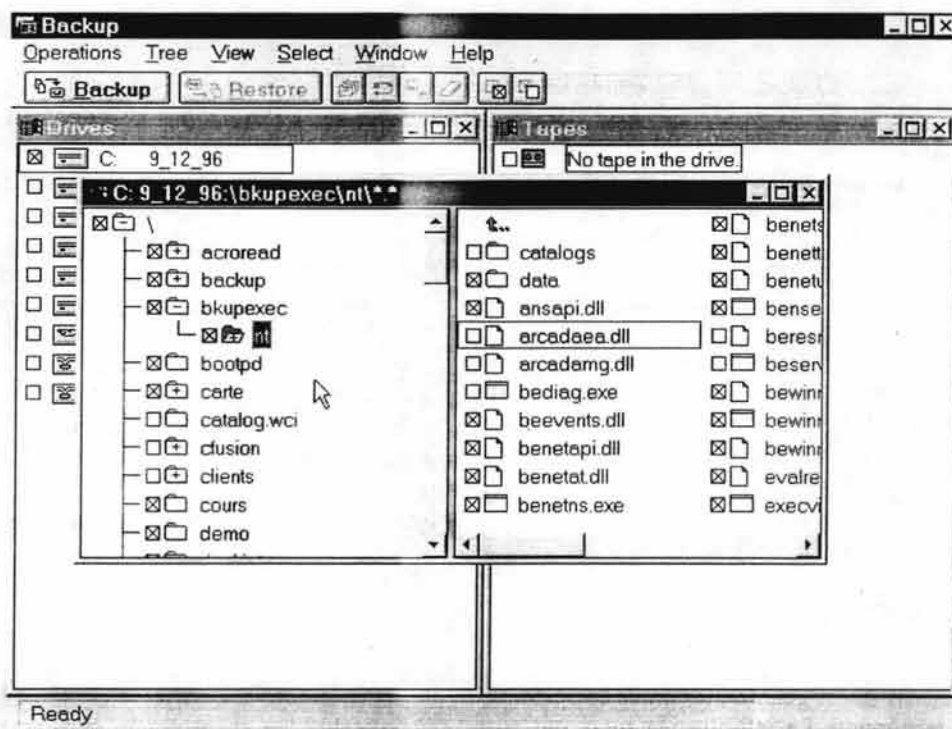
Inicie el programa **Copia de seguridad** en el menú **Herramientas administrativas**. Durante el inicio el programa intenta rápidamente detectare y mostrar las unidades de cinta instalada.(figura IV.19)



(figura IV.19)

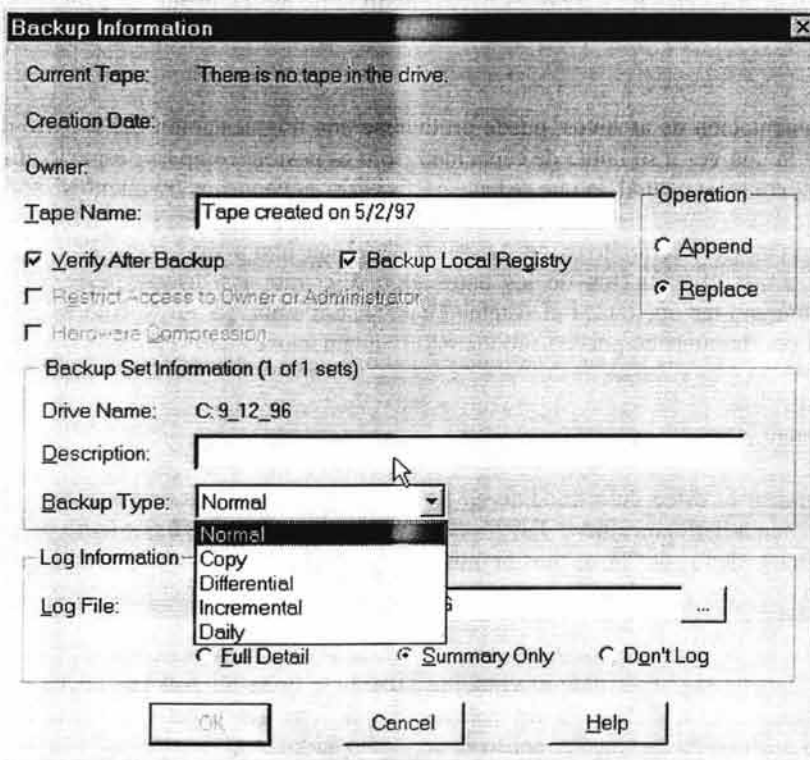
En la ventana **Unidades** obtendrá una relación de las carpetas y archivos del ordenador y de las unidades de red vinculadas.

Pulsando dos veces el ícono de la unidad se muestran las carpetas de la misma en una nueva ventana. En ella puede seleccionar los directorios que quiera copiar. Si ya ha seleccionado previamente la unidad, estarán seleccionados todos los directorios. Para anular esta selección deberá pulsar la casilla que se encuentra en la esquina superior izquierda.(figura IV.20)



(figura IV.20)

Luego, pulse el botón **Copia de seguridad** e indique el nombre y otros particulares para la copia de seguridad.(figura IV.21)



(figura IV.21)

Programas para copias de seguridad:

A título de ejemplo de un buen programa para copias de seguridad, describiré aquí el ARCserve y Arcada Backup Exec para Windows NT. Con ARCserve de la casa Cheyenne se pueden administrar varios servidores de forma centralizada. A través de acceso remoto (RAS) es posible modificar la configuración de ARCserve he iniciar tareas de copias de seguridad. De este modo, ARCserve funciona como servicio del sistema y, por lo tanto, no precisa ningún usuario conectado. Gracias a la división del proceso de tareas, proceso de cinta y proceso de base de datos, se garantiza una alta estabilidad y velocidad. Para incrementar la velocidad de la copia se puede acceder, de forma paralela a distintos dispositivos de copia de seguridad. Un detector de virus hace posible la integridad de los datos antes de la copia. Además, se puede consultar información sobre destinatarios de llamadas, correo electrónico, colas de impresión, SNMP o mensajes de red.

Arcada Backup Exec es un producto de la firma Seagate. En Arcada Backup se instalan y planifican las tareas a través del programa Backup Exec. A través de RAS puede iniciar de modo remoto trabajos de copia de seguridad con Backup Exec View y comprobar si las copias se han realizado correctamente.

Arcada Backup se luce por su integración en Windows NT. Por ejemplo: todos los eventos importantes del sistema se escriben directamente en el registro de aplicaciones de NT.

4.3.2.9 DISCOS DUROS FRAGMENTADOS.

Los discos duros guardan los datos en sectores, de forma consecutiva. El disco duro se va llenando con datos de este modo. La información sobre qué partes de un archivo se encuentra en que sectores está guardada en la tabla de asignación de archivos. En el sistema de archivos NTFS este archivo se denomina *Master File Table* (MFT).

Cuando se eliminan archivos se comparten las áreas correspondientes, aunque éstas no pueden ser sobrescritas realmente hasta que se agota el espacio al final del disco duro. En este preciso momento surge el problema de la fragmentación de archivos. Si las áreas disponibles son más pequeñas que el archivo a guardar, es preciso dividir el archivo en varias áreas, es decir, subdividirlo en fragmentos. Cuanto mayor es la frecuencia con que se eliminan, reducen y amplían archivos, más fragmentos se van formando en el disco duro.

Además de la fragmentación de archivos, puede producirse una fragmentación del soporte de datos. Si el disco duro ya ha llegado una vez a su límite de capacidad, sólo es posible compartir espacio eliminando o reduciendo archivos. Pero, como es natural, lo que se hace es dividirlo en pequeños fragmentos.

En NTFS, la fragmentación de archivos no juega un papel tan importante como en el sistema de archivos (V)FAT. Debido a una organización de los datos algo diferente, los discos duros NTFS no se fragmentan tan rápidamente como los que tienen el sistema (V)FAT. Sin embargo, en servidores cuyos datos se escriben y se modifican con frecuencia, pueden producirse fragmentaciones que retardan notablemente el acceso a los datos.

Programas defragmentadores:

Para volver a organizar el disco duro dividido en fragmentos y escribir los archivos seguidos en lo posible es necesario un programa defragmentador. Este tipo de programas pueden trabajar fuera de línea y en línea. Las defragmentaciones fuera de línea no permiten ningún acceso a los archivos durante la reorganización del disco duro. Así, por ejemplo, en una estación de trabajo pueden ejecutarse durante un funcionamiento en vacío o al apagar o encender el ordenador.

Para un servidor, estos programas defragmentadores fuera de línea no son tan adecuados. Todo administrador de sistema causará la irritación de sus compañeros si tiene que parar el sistema con mucha frecuencia, y trabajar por la noche o en domingo tampoco es un medio adecuado.

En estos casos, es preciso recurrir a los defragmentadores en línea, que permiten acceder a los datos mientras se están escribiendo y, a pesar de ello, trabajan de forma fiable. Es fácil imaginarse que un programa de este tipo no es fácil de crear y que con un programa que funciona de forma imperfecta es muy fácil dañar todos los datos de un disco duro.

Microsoft no ofrece un programa defragmentador para NTFS, como ocurre con el sistema de archivos (V)FAT. En este caso hay que recurrir a la ayuda de otros fabricantes. Ya existen defragmentadores sencillos como el shareware o freeware. Para uso empresarial es mejor recurrir a las versiones comerciales ampliadas de estos programas, puesto que la mayoría de ellas permiten la terminación de la defragmentación y también son adecuadas para la administración remota.

Como ejemplo de estos programas citamos Diskeeper de Executive Software.

4.3.2.10 SISTEMA DE ARCHIVOS DISTRIBUIDO.

Con el Sistema de archivos distribuido (DFS), es posible administrar y utilizar recursos en redes grandes de modo más fácil y claro. Con DFS pueden activarse los recursos compartidos de muchos ordenadores distintos en una red a través de una estructura unitaria. Con DFS ya no es preciso pelearse con largos árboles con dominios, ordenadores y recursos compartidos, sino que se utiliza una jerarquía unitaria para acceder a dichos recursos.

Así trabaja DFS:

Hasta ahora se utilizaba en Windows NT, al igual que en otros sistemas operativos Windows, el *Universal Convention System* (UNC) a fin de nombrar los servidores y los recursos. En general, la dirección de un archivo en la red tiene entonces este aspecto:

En general...

\\Servidor\Recurso\Ruta de acceso al directorio\Nombre de archivo

o con un ejemplo...

\\SERVIDOR NT \USUARIO\LUIS\PRIVADO\LIBRO.XLS

Se puede asignar a los recursos una determinada letra de unidad en el cliente de la red. Windows lo denomina entonces *Vincular una unidad de red*. El aspecto es el siguiente:

En general...

X:\Ruta de acceso al directorio\Nombre de archivo

o en nuestro ejemplo

X:\LUIS\PRIVADO\LIBRO.XLS

Algunos programas no pueden trabajar con un sistema puramente UNC, por lo que es necesario vincular siempre una unidad con un determinado recurso.

En redes grandes con numerosos servidores y estaciones de trabajo que dan a compartir muchos recursos distintos, el sistema UNC resulta poco claro. Para encontrar un determinado recurso es preciso

- Conocer el servidor que lo contiene.
- Descubrir en él el recurso y,
- Localizar el archivo correcto dentro del árbol de directorios de ese recurso.

Para vincular todos los recursos necesarios con una unidad no hay suficiente con las letras del abecedario. Además, estas unidades de red vinculadas de forma fija consumen unos valiosos recursos del sistema, por lo menos en Windows 3.11 y Windows 95.

DFS presenta los distintos recursos de los servidores de una red con una estructura jerárquica unitaria. En ella es posible clasificar los archivos y directorios por contenido y no es preciso tener en cuenta el espacio físico.

DFS se comporta un poco como el sistema de archivos de un soporte de datos. No es preciso que uno mismo compruebe los distintos bloques en los que se guarda un archivo –tal vez fragmentado –, sino que únicamente se selecciona el archivo. El sistema de archivos busca entonces los datos en sí en los bloques del soporte de datos.

Con DFS, el usuario tampoco tiene que buscar mucho rato un archivo determinado si el mismo se ha trasladado a otro directorio o a otro servidor por razones de organización. Dado que la entrada del DFS para ese archivo sigue siendo la misma, se sigue presentando con la misma dirección para los usuarios (independientemente del ordenador y el directorio en los que se encuentre realmente).

Como es natural, DFS no sólo ofrece ventajas para los usuarios. Los administradores del sistema también se aprovechan del hecho de que DFS amplía las configuraciones de seguridad del servidor Windows NT a todos los recursos compartidos. Por lo tanto, ya no es preciso pensar en unidades FAT compartidas sin protección. En entornos heterogéneos, DFS permite observar de forma unitaria las unidades y los directorios de los ordenadores compatibles (FAT, HPFS, NTFS) y estaciones de trabajo Unix (NFS y otros sistemas de archivos Unix). Así pues, los usuarios ya no necesitan clientes NFS adicionales ni tendrán que administrarlos.

Finalmente, DFS puede acelerar notablemente el acceso a los recursos mediante el almacenamiento temporal de los recursos de red activados una vez.

4.4 LOS DOMINIOS EN WINDOWS NT.

Los dominios articulan las redes extensas en redes parciales más claras, y con ello reducen el trabajo de administración. Windows NT soporta hasta 26.000 usuarios y unos 250 grupos de dominio. Sin embargo, no es posible administrar tales cantidades de forma cómoda.

El número de dominios en que se divide una organización depende de:

- El número de usuarios
- La organización empresarial y
- Las necesidades en cuanto a seguridad de cada uno de los departamentos.

A continuación se presentan distintos modelos y sus posibilidades de aplicación.

Los límites del sistema

En primer lugar, el número de usuarios, de ordenadores y de grupos de usuarios influye en la división de una red Windows NT. Para su administración, Windows NT crea una base de datos denominada *Directory Database*. Ésta puede alcanzar como máximo 40 Mbyte y se encuentra tanto en el controlador principal de dominio como en el controlador de dominio de reserva.

Windows NT necesita espacio disponible para cada elemento:

- 1 Kbyte para cada usuario
- 0,5 Kbytes para cada ordenador de la red y,

En estos casos, es preciso recurrir a los defragmentadores en línea, que permiten acceder a los datos mientras se están escribiendo y, a pesar de ello, trabajan de forma fiable. Es fácil imaginarse que un programa de este tipo no es fácil de crear y que con un programa que funciona de forma imperfecta es muy fácil dañar todos los datos de un disco duro.

Microsoft no ofrece un programa defragmentador para NTFS, como ocurre con el sistema de archivos (V)FAT. En este caso hay que recurrir a la ayuda de otros fabricantes. Ya existen defragmentadores sencillos como el shareware o freeware. Para uso empresarial es mejor recurrir a las versiones comerciales ampliadas de estos programas, puesto que la mayoría de ellas permiten la terminación de la defragmentación y también son adecuadas para la administración remota.

Como ejemplo de estos programas citamos Diskeeper de Executive Software.

4.3.2.10 SISTEMA DE ARCHIVOS DISTRIBUIDO.

Con el Sistema de archivos distribuido (DFS), es posible administrar y utilizar recursos en redes grandes de modo más fácil y claro. Con DFS pueden activarse los recursos compartidos de muchos ordenadores distintos en una red a través de una estructura unitaria. Con DFS ya no es preciso pelearse con largos árboles con dominios, ordenadores y recursos compartidos, sino que se utiliza una jerarquía unitaria para acceder a dichos recursos.

Así trabaja DFS:

Hasta ahora se utilizaba en Windows NT, al igual que en otros sistemas operativos Windows, el *Universal Convention System* (UNC) a fin de nombrar los servidores y los recursos. En general, la dirección de un archivo en la red tiene entonces este aspecto:

En general...

`\\Servidor\Recurso\Ruta de acceso al directorio\Nombre de archivo`

o con un ejemplo...

`\\SERVIDOR NT \USUARIO\LUIS\PRIVADO\LIBRO.XLS`

Se puede asignar a los recursos una determinada letra de unidad en el cliente de la red. Windows lo denomina entonces *Vincular una unidad de red*. El aspecto es el siguiente:

En general...

`X:\Ruta de acceso al directorio\Nombre de archivo`

o en nuestro ejemplo

`X:\LUIS\PRIVADO\LIBRO.XLS`

Algunos programas no pueden trabajar con un sistema puramente UNC, por lo que es necesario vincular siempre una unidad con un determinado recurso.

En redes grandes con numerosos servidores y estaciones de trabajo que dan a compartir muchos recursos distintos, el sistema UNC resulta poco claro. Para encontrar un determinado recurso es preciso

- Conocer el servidor que lo contiene.
- Descubrir en él el recurso y,
- Localizar el archivo correcto dentro del árbol de directorios de ese recurso.

Para vincular todos los recursos necesarios con una unidad no hay suficiente con las letras del abecedario. Además, estas unidades de red vinculadas de forma fija consumen unos valiosos recursos del sistema, por lo menos en Windows 3.11 y Windows 95.

DFS presenta los distintos recursos de los servidores de una red con una estructura jerárquica unitaria. En ella es posible clasificar los archivos y directorios por contenido y no es preciso tener en cuenta el espacio físico.

DFS se comporta un poco como el sistema de archivos de un soporte de datos. No es preciso que uno mismo compruebe los distintos bloques en los que se guarda un archivo –tal vez fragmentado–, sino que únicamente se selecciona el archivo. El sistema de archivos busca entonces los datos en sí en los bloques del soporte de datos.

Con DFS, el usuario tampoco tiene que buscar mucho rato un archivo determinado si el mismo se ha trasladado a otro directorio o a otro servidor por razones de organización. Dado que la entrada del DFS para ese archivo sigue siendo la misma, se sigue presentando con la misma dirección para los usuarios (independientemente del ordenador y el directorio en los que se encuentre realmente).

Como es natural, DFS no sólo ofrece ventajas para los usuarios. Los administradores del sistema también se aprovechan del hecho de que DFS amplía las configuraciones de seguridad del servidor Windows NT a todos los recursos compartidos. Por lo tanto, ya no es preciso pensar en unidades FAT compartidas sin protección. En entornos heterogéneos, DFS permite observar de forma unitaria las unidades y los directorios de los ordenadores compatibles (FAT, HPFS, NTFS) y estaciones de trabajo Unix (NFS y otros sistemas de archivos Unix). Así pues, los usuarios ya no necesitan clientes NFS adicionales ni tendrán que administrarlos.

Finalmente, DFS puede acelerar notablemente el acceso a los recursos mediante el almacenamiento temporal de los recursos de red activados una vez.

4.4 LOS DOMINIOS EN WINDOWS NT.

Los dominios articulan las redes extensas en redes parciales más claras, y con ello reducen el trabajo de administración. Windows NT soporta hasta 26.000 usuarios y unos 250 grupos de dominio. Sin embargo, no es posible administrar tales cantidades de forma cómoda.

El número de dominios en que se divide una organización depende de:

- El número de usuarios
- La organización empresarial y
- Las necesidades en cuanto a seguridad de cada uno de los departamentos.

A continuación se presentan distintos modelos y sus posibilidades de aplicación.

Los límites del sistema

En primer lugar, el número de usuarios, de ordenadores y de grupos de usuarios influye en la división de una red Windows NT. Para su administración, Windows NT crea una base de datos denominada *Directory Database*. Ésta puede alcanzar como máximo 40 Mbyte y se encuentra tanto en el controlador principal de dominio como en el controlador de dominio de reserva.

Windows NT necesita espacio disponible para cada elemento:

- 1 Kbyte para cada usuario
- 0,5 Kbytes para cada ordenador de la red y,

- 4 Kbytes para un grupo de unos 300 usuarios.

Mediante estos números se pueden plantear situaciones sobre cuándo y con qué configuración una red traspasará los límites de Windows NT.

4.4.1 UN DOMINIO ÚNICO.

La forma de organización más sencilla de una red NT es un dominio único. Los accesos de los usuarios y los recursos del dominio son controlados por un controlador principal de dominio (PDC) y uno o varios controladores de dominio de reserva (BDC). Cada controlador de dominio puede administrar hasta 5.000 usuarios si está equipado con la memoria RAM suficiente.

En un dominio único, los administradores del PDC (controlador principal de dominio) pueden gestionar todos los usuarios, todos los ordenadores (clientes y servidor) y todos los recursos del dominio. Esto requiere una administración eficaz. Si se divide la red, también se dividen las tareas administrativas en varias posiciones.

4.4.2 DOMINIOS MAESTROS ÚNICOS.

Si una red es lo suficientemente pequeña para administrarse en un dominio único pero, por razones de organización, dentro de la empresa se necesitan distintos dominios, la opción apropiada es el concepto de dominios maestros únicos. En el mismo, todos los usuarios y grupos de usuarios globales se crean y administran en el dominio maestro. Los ordenadores de cada una de las distintas unidades organizativas de la empresa se sitúan en distintos dominios, los cuales ponen su confianza en el dominio maestro.

En este modelo, los usuarios se registran en el dominio maestro. Este dominio en sí no ofrece ningún otro recurso, sino que únicamente regula las configuraciones de seguridad de los usuarios y grupos de usuarios. Los recursos propiamente dichos son ofrecidos por los otros dominios. Gracias a la posición de confianza unilateral del resto de dominios hacia el dominio maestro, éste puede servir de mediador entre los recursos de cada uno de los dominios.

Un dominio maestro se administra de forma centralizada. Esta tarea se puede realizar por un centro de cálculo o un departamento especial de informática. En este caso, los administradores se benefician de la administración centralizada: deben cuidarse en un único dominio de los usuarios y grupos de usuarios, así como de sus configuraciones de seguridad y, por lo tanto, pueden administrar una red de muchos dominios distintos.

En cambio, los recursos de cada uno de los dominios de una red de este tipo pueden administrarse en el dominio maestro o en el dominio respectivo. Los datos delicados como la administración de usuarios se deja en unas manos, mientras que los datos menos delicados, como la administración de recursos, se delegan a cada una de las unidades organizativas que gestionan dominios propios. Cada uno de los dominios se puede dividir para adaptarse a la organización de la empresa.

En una organización de este tipo, los controladores de dominio de reserva de cada uno de los dominios trabajan como controladores de dominio de reserva del dominio maestro y aseguran la red múltiples veces contra fallos de los controladores de dominio.

4.4.3 DOMINIOS MAESTROS MÚLTIPLES.

En el caso de los dominios maestros múltiples, se vinculan entre sí dos o más dominios maestros. Todos los dominios de los dominios maestros tienen una posición de confianza unilateral hacia todos los dominios maestros. Los dominios maestros, por su parte, tienen una posición de confianza bilateral entre sí. Al igual que en el concepto de dominios maestros únicos, los accesos de usuarios sólo se gestionan en los dominios maestros, mientras que el resto de dominios ponen a disposición sus recursos.

En un dominio maestro múltiple (dividido), cada usuario de cualquier dominio de recursos puede registrarse en cualquier dominio maestro, ya que los dominios maestros tienen posiciones de confianza bilaterales en ambas direcciones. En este modelo, a cada usuario del dominio maestro se le asigna exactamente una cuenta de ordenador, de forma que en cada dominio maestro se pueden administrar hasta 26.000 usuarios.

4.4.3.1 ORGANIZACIÓN FLEXIBLE.

Los dominios maestros múltiples ofrecen las siguientes ventajas:

- Es posible administrar organizaciones con más de 40.000 usuarios dividiéndolas en distintos dominios maestros. En principio, el concepto de los dominios múltiples no tiene número máximo de usuarios, puesto que se pueden instalar tantos dominios maestros como se desee.
- Los usuarios móviles, como colaboradores en el exterior, pueden conectarse desde cualquier lugar del mundo y desde cualquier dominio de recursos de la red.
- La red se puede administrar de forma centralizada (dentro del marco de los dominios maestros) o descentralizada (también a nivel de los dominios de recursos).
- En el modelo de dominios maestros múltiples también se pueden reproducir estructuras organizativas complejas. Las empresas con filiales por todo el mundo, las unen en una sola red a través de dominios maestros divididos. Dicha red se puede administrar, a pesar de todo, de forma centralizada dentro de cada una de las filiales.
- Los controladores de dominio de reserva pueden estar distribuidos a través de LANs y WANs para protegerlas especialmente contra pérdidas de datos debidas a incendio o catástrofe similar.

4.5 RESOLUCIÓN DE LOS NOMBRES.

Con la red cliente-servidor y el concepto de dominios, podría estar solucionado el riesgo de seguridad de este concepto de red tan simple. Pero ahora queda por resolver la cuestión de los nombres: ¿cómo pueden saber los usuarios de una red, ya sea cliente-servidor o punto a punto, qué ordenador ha compartido qué recursos y con qué nombre?

Este problema lo solucionan distintos conceptos.

4.5.1 LISTAS DE NOMBRES ESTÁTICAS.

La solución más simple es un archivo con los nombres y los recursos compartidos de todos los clientes y servidores de la red. Consultando este archivo se pueden observar los recursos disponibles.

Un archivo de este tipo debe estar ubicado de forma centralizada en el servidor de registro de la red, a fin de que los clientes lo puedan consultar. El concepto es sencillo y suficiente, siempre y cuando no se modifique mucho la estructura de la red. Sobre todo no se debe modificar el nombre del servidor, ya que en tal caso los clientes ya no sabrían dónde se tienen que registrar y, por lo tanto, tampoco podrían consultar las listas de recursos. Además, no se conocen todos los recursos compartidos hasta que no se reinician los clientes y el servidor.

Estas listas de nombres estáticas también existen actualmente en Windows NT. Con ellas es posible administrar:

- Los nombres para el NetBIOS en el archivo Lmhosts.
- Los nombres de redes TCP/IP en el archivo Hosts.

Ambos archivos se encuentran en el subdirectorio System32Drivers\etc del directorio raíz de Windows NT.

4.5.2 LISTAS DE NOMBRES DINÁMICAS.

Una ampliación sencilla del concepto son las listas dinámicas. Aquí, el servidor consulta los recursos compartidos en todos los ordenadores de la red, a intervalos regulares. De esta forma, los clientes también conocen, a intervalos regulares, los nuevos recursos compartidos del servidor. Este concepto representado en redes NOVELL® 3.1x se denomina Service Advertising Protocol (SAP). El inconveniente decisivo de esta solución se presenta en redes grandes con numerosos recursos compartidos: en estos casos, la actualización de las listas sobrecarga la red.

4.5.3 EXAMINADOR DE RED.

La primera respuesta de Microsoft a la problemática de los nombres consistió en los examinadores de red. Estos programas pueden examinar la red para buscar ordenadores disponibles y, dentro de cada uno de estos ordenadores, recursos compartidos. Como esta lista se crea de nuevo cada vez que se consulte, el concepto es particularmente aconsejable para redes punto a punto, en las cuales se pueden modificar a corto plazo los recursos disponibles. Como esta búsqueda en la red también debe ser organizada, en las redes Windows NT existe un examinador maestro, que suele ser el controlador principal de dominio, aunque no es necesario. Cada cliente, al darse de alta en el servidor también se da de alta en el examinador maestro con el mensaje de incluirse en la lista.

Pero también el concepto del examinador llega a sus límites en redes grandes. Si las listas de recursos disponibles son demasiado extensas, la consulta dura mucho tiempo. Es por ello que la consulta de recursos se ha restringido al grupo de trabajo o dominio en el que se ha dado de alta al cliente. Del resto de grupos de trabajo y dominios sólo se indican los nombres. En caso de que, incluso así, en redes grandes surjan problemas, es posible separar los dominios mediante tipologías de red bridge o router. Para ello, los dominios deben comportarse como subredes en un entorno TCP/IP.

4.5.4 SERVIDOR DE NOMBRES.

En redes realmente grandes, la relación de los nombres no puede realizarse mediante examinadores. En estos casos, cada ordenador debe tener una dirección única, a través de la cual se pueda consultar. De la asignación de los nombres de los ordenadores se encarga entonces el servidor de nombre. Estas máquinas contienen una base de datos sencilla que asigne nombres a las direcciones de los ordenadores. Si existen varios servidores de nombre, deben estar sincronizados entre sí. La dirección de un ordenador debe ser única en toda la red.

Esta vía es la que se aplica en Internet basada en TCP/IP. Desde el Service Pack 3 de la versión 3.51 de Windows NT, este programa puede actuar también como servidor de nombre. Antes de dicha versión únicamente había servidores WINS, que convertían los nombres y direcciones de redes Windows al sistema DNS y viceversa. Si dentro de una red Windows NT también se utiliza el protocolo TCP/IP, el servidor de nombre de Windows NT Server puede relacionar todos los nombres de esa red.

4.6 LOS SERVICIOS WINS

La relación de nombres en Windows NT puede realizarse a través de dos vías distintas:

- NetBIOS a través de TCP/IP (NetBT), el servicio WINS que se describe en este apartado, y
- DNS (Domain Name System), que presentamos en el apartado siguiente.

El servicio WINS forma parte de las capas de protocolo de la red Windows NT y convierte los nombres de los ordenadores de la red Windows en direcciones IP. Para ello, este servicio trabaja junto con el examinador de red, el cual relaciona los ordenadores registrados en la red.

4.7 SERVICIOS DNS.

El sistema jerárquico DNS (Domain Name System, Sistema de Nombres de Dominio) con una base de datos dividida, asigna nombres a los ordenadores en Internet. En principio, DNS trabaja como WINS: en una base de datos se asignan los nombres DNS a las direcciones únicas de cada ordenador. No obstante, a diferencia de WINS, DNS trabaja con una base de datos estática que tiene preparada esa información.

4.8 INSTALAR CLIENTES.

En redes basadas en el servidor, una de las principales tareas (que por cierto suele llevar bastante tiempo) del administrador del sistema es la instalación de clientes. En esta cuestión Windows NT puede prestar mucha ayuda. Con el administrador de clientes de red pueden crear disquetes de inicio y de instalación para clientes.

Con esta opción se crea un disquete de inicio que arranca el cliente y puede conectarlo inmediatamente con la red NT. Tras establecer la conexión se instala automáticamente el sistema seleccionado (Windows para trabajo en grupo o Windows NT Workstation) en el cliente. Para la instalación de Windows para trabajo en grupo es preciso que previamente se haya instalado un *DOS* en el cliente.

De esta forma, se pueden instalar clientes de todas las versiones de Windows y clientes de *MS-DOS*.

Para crear el disquete de inicio de cliente debe saber si el mismo arranca desde una unidad de 3 ½ ó de 5 ¼ pulgadas (hoy en día sería raro el segundo caso) y qué tarjeta de red está instalada en ese ordenador. Evidentemente, debe tratarse de una tarjeta compatible con Windows NT.

Si el cliente no debe ser instalado a través de la red, cree un juego de disquetes para instalar el cliente en el servidor. También puede utilizar la rutina de instalación de Windows para trabajo en grupo del CD-ROM del servidor NT.

De esa forma se crean disquetes de instalación para:

- Redes MS-DOS.
- LAN-Manager para MS-DOS y OS/2.
- Redes RAS para MS-DOS, y
- TCP/IP para Windows 3.11.

No siempre el administrador del sistema puede trabajar directamente en el servidor NT para instalar un nuevo usuario u ordenador. Es por ello que se pueden compartir para determinados clientes, programas básicos de administración de redes en el servidor, en un directorio aparte. Las configuraciones deseadas se pueden realizar entonces a través de la red. Este procedimiento, no obstante, sólo se puede aplicar en Windows NT Workstation o en ordenadores Windows 95.

4.9 ADMINISTRACIÓN DE USUARIOS.

Windows NT es un auténtico sistema operativo de red multiusuario. Por eso, a diferencia de Windows 95 y de Windows 3.x, es necesaria una administración de los usuarios. Los administradores del sistema son los que definen quién está autorizado a utilizar los dominios del servidor NT y con qué derechos. A los usuarios locales de NT Workstation se les ofrece la posibilidad de personalizar la pantalla de presentación del entorno Windows NT.

La administración de los usuarios tiene tareas fundamentales:

- Posibilitar la personalización y optimización de la pantalla de presentación y el funcionamiento del sistema operativo para el mayor número de usuarios posible, de acuerdo con las necesidades de cada uno de ellos. Eso significa que, para proteger los datos, a veces es conveniente no permitir el libre acceso de todos los usuarios a todos los archivos de NT Server.

- La segunda tarea fundamental es garantizar la seguridad del sistema. Los derechos limitados de todo usuario normal no permitan modificar los archivos más importantes del sistema (como son los archivos de registro) ni, por lo tanto, causar daños graves. Por esa razón, no siempre es conveniente hacerse administrador de NT Workstation cuando se es el único usuario de la misma. Los administradores de red de un dominio NT sólo deberían entrar en la red como administradores para trabajos de mantenimiento: para reconocer rápidamente el mal uso de los derechos de acceso a la red de los usuarios "normales".

- La tercera tarea también está relacionada con la seguridad del sistema. Se trata, esta vez, de protegerse contra el acceso indebido de terceros. Si todos los usuarios aseguran sus derechos de acceso con contraseñas seguras, el acceso indebido de terceros a NT Server, una red Windows NT, o a Windows NT Workstation resulta mucho más difícil. La seguridad de Windows NT está sujeta a normas estrictas dictadas por el departamento de defensa de EUA. Si bien en Windows NT se puede configurar un nivel de seguridad Class C2, en la práctica no tiene mucho sentido trabajar con este sistema debido a los constantes controles de seguridad y los protocolos de eventos. Windows NT Server debería quedar cerrado de manera mecánica, pues quien puede acceder físicamente a Windows NT Server, también puede manipular los datos guardados en él.

4.9.1 PANORÁMICA.

En Windows NT, la administración de usuarios se realiza a través del Administrador de usuarios y otros programas del sistema.

Utilice:

- El Administrador de usuarios para dominios para crear nuevos usuarios, grupos locales y globales, definir directivas generales y crear un perfil y un script de conexión para cada uno de ellos.

- El Administrador de servidores para definir las propiedades y derechos de acceso de los directorios libres del servidor, separar los usuarios del servidor NT o configurar la duplicación de directorios, y

- El Explorador de Windows NT para realizar las configuraciones de seguridad de directorios y archivos o compartir recursos.

Con estas tres utilidades gráficas, se pueden crear y mantener usuarios y administrar los derechos de acceso y recursos del sistema.

4.9.2 EL ADMINISTRADOR DE USUARIOS.

Las personas administradoras de sistemas operativos gráficos como Windows NT necesitan una administración de usuarios que sea clara y economice trabajo. Y eso es precisamente lo que les ofrece el programa Administrador de usuarios para dominios. En las redes NT, los dominios son grupos de ordenadores regidos por las mismas directivas de seguridad y de información de cuentas (de los usuarios).

Estos datos están administrados y controlados por los Controladores de dominio: el controlador principal de dominio y el controlador secundario de dominio. La base de datos de usuarios NT se encuentra en el Controlador principal de dominio (PDC) y existe un duplicado de la misma en los restantes controladores de seguridad de dominio (BDC). Cuando falta el Controlador principal de dominio, el control de la inscripción de usuarios lo realiza el siguiente controlador de seguridad de dominio disponible.

El administrador de usuarios permite:

- Crear usuarios, crear perfiles de usuario y llevar el mantenimiento de ambos.
- Configurar información de cuentas para los usuarios.
- Crear las propias cuentas.
- Crear grupos.
- Crear configuraciones de acceso (Logon).
- Realizar configuraciones de seguridad, y
- Definir las relaciones de confianza para otros dominios.

Naturalmente, el Administrador de usuarios también posee sus propios derechos de acceso. Los administradores son los únicos autorizados a configurar todos los parámetros. Otras cuentas de usuario, como son el operador de cuentas o los administradores de dominio sólo están autorizados a configurar determinados parámetros del Administrador de usuarios. (figura IV.22)



(figura IV.22)

4.9.3 GRUPOS DE USUARIOS.

Los grupos de usuarios reúnen varios usuarios en una unidad. Windows NT predetermina los grupos cuyas propiedades no se pueden modificar. Los grupos de usuarios se pueden crear en un solo dominio o bien en varios dominios enlazados entre sí por relaciones de confianza.

Con los grupos de usuario se pueden incorporar usuarios de un dominio a otro, siempre que los dominios hayan establecido una relación de confianza entre sí. De ese modo, los usuarios de los otros dominios no sólo pueden acceder a los recursos del otro servidor, sino incluso ser administrados por éste.

4.9.3.1 GRUPOS DE USUARIOS GLOBALES Y LOCALES.

La creación de grupos de usuarios facilita enormemente la tarea de los administradores de la red. En lugar de definir detalladamente los derechos de acceso a la red para cada uno de los usuarios, los grupos permiten asignar los derechos en bloque a todo un grupo, ya sea predefinido o de creación propia. De ese modo, se otorgan diferentes derechos en una sola asignación.

Microsoft distingue entre grupos locales y grupos globales.

- Los grupos globales están formados por diferentes usuarios del mismo dominio, agrupados con un solo nombre común. Los grupos de usuarios globales se crean dentro de un dominio y no pueden incluir usuarios de otros dominios. En compensación, a los grupos de usuarios globales, sí se les pueden asignar derechos en otros dominios. Por eso reciben estos grupos el calificativo de "globales".

- Los grupos locales están formados por usuarios y grupos globales. Estos grupos y usuarios pueden pertenecer indistintamente al dominio en que se ha creado el grupo local o a cualquier otro dominio de confianza.

4.9.3.2 GRUPOS DE USUARIOS PREDEFINIDOS.

Para que se haga una idea clara de cómo y porqué Windows NT crea grupos de usuarios, se ha elaborado la siguiente lista con todas las propiedades de los grupos de usuarios predefinidos.

Administradores.

Los administradores son, naturalmente quienes poseen la mayoría de los derechos para configurar los parámetros del servidor y de los dominios. La cuenta de administrador, como tal, no se puede borrar. Sólo se pueden borrar los administradores de dominio. Si bien los administradores poseen derechos plenos, su cuenta puede caducar. Por eso es aconsejable crear otras cuentas de administrador, como medida de seguridad, para poder recurrir a ellas en caso necesario (imagínese, por ejemplo, qué pasaría si cambia la palabra clave de la cuenta de administrador y al cabo de unos días no se acuerda ya de ella). Determinados archivos pueden estar bloqueados también para los administradores. Cada administrador puede conseguir acceso a todos los archivos, pero para esta acción debe seguir un protocolo; el auténtico usuario pierde así el acceso al archivo, lo cual le informa, indirectamente, de que el administrador ha tomado ese derecho.

Operadores de servidores:

Este grupo posee todos los derechos para administrar un servidor de dominio. Puede liberar y bloquear recursos, realizar copias de seguridad y administrar usuarios. Los operadores de servidor pueden reiniciar el servidor de una red. Pero el operador no puede modificar el sistema del servidor. Los operadores del sistema son un grupo local.

Operadores de cuentas.

Los operadores de cuentas pueden administrar a los usuarios de un dominio y crear y mantener las cuentas de usuario. Sin embargo, hay determinadas cuentas especiales, como las de administradores y otros operadores, a las cuales no pueden acceder. De otro modo, los administradores de cuentas podrían convertirse por cuenta propia en administradores.

Operadores de impresión:

Como su nombre indica, estos operadores se encargan única y exclusivamente de administrar los trabajos de impresión, sin poseer otros derechos especiales de acceso.

Operadores de copia:

Los operadores de copias de seguridad pueden realizar copias de seguridad de los archivos del servidor, y de las unidades de libre acceso de los clientes de la red NT, con la utilidad Backup de Windows NT u otro tipo de programa apropiado. No están autorizados a reproducir las copias de seguridad.

Duplicadores:

Windows NT Server puede sincronizar sus directorios con otro equipo Windows NT Server o Workstation de la red. Al hacerlo, Windows NT Server está operando como servidor de exportación, los otros ordenadores de Windows NT son quienes importan los datos. De ese modo, se pueden hacer copias de seguridad de datos importantes en varios ordenadores a la vez, y administrar de manera central los directorios utilizados y modificados con mayor frecuencia, al mismo tiempo que se mantienen de manera local en los ordenadores. Para administrar esta función existe un grupo especial de usuarios: los Duplicadores. Por motivos de seguridad, ningún usuario estándar debería formar parte del grupo de los duplicadores. Si desea utilizar la duplicación de directorios debe crear, por ejemplo, un usuario que sea miembro del grupo de los duplicadores. El servicio de duplicación de directorios se inicia entonces con ayuda del usuario creado.

Usuarios:

En Windows NT Server, los usuarios sólo disponen, en realidad, del derecho de acceso. Los derechos para modificar el sistema permanecen exclusivamente al cliente, a través del cual acceden los usuarios al servidor. Los usuarios obtienen, de manera predeterminada, el derecho de acceso a determinados directorios de Windows NT Server.

Invitados:

La categoría predefinida de Invitados se ha creado para todos aquellos que sólo quieren acceder temporalmente a la red. Los invitados poseen derechos mínimos en el servidor y sólo pueden realizar cambios insignificantes en las estaciones de trabajo.

Todos:

Todos no es en realidad ningún grupo de usuarios, al menos no aparece como tal en el Administrador de usuarios. Pero si asigna derechos de acceso en el Explorador, siempre se encontrará con el grupo Todos. Este grupo engloba a todos los usuarios que pueden acceder a los dominios. A través del grupo Todos se pueden asignar derechos de acceso a archivos y directorios, siempre que sean válidos para todos los usuarios del dominio NT, en lugar de hacerlo a través de usuarios individuales o grupos de usuarios.

4.9.3.3 CREAR LOS PROPIOS GRUPOS DE USUARIOS.

Además de los grupos predefinidos, es posible crear grupos propios con un perfil de derechos muy concreto. Para ello, se puede recurrir a los perfiles predefinidos de esos grupos, o bien crear las propiedades de los nuevos grupos. También aquí se puede distinguir entre grupos locales y globales.

Se va a crear, a continuación, un nuevo grupo de usuarios para los integrantes del departamento Tecnología de la Información. Este grupo de usuarios está formado por administradores que entre otras tareas, deben realizar también pequeños trabajos de administración en los dominios de otros departamentos.

En primer lugar, hay que decidir si va a tratarse de un grupo local o global. En el ejemplo se pretende que los integrantes del grupo de usuarios se puedan incluir en otros dominios y viceversa, que los grupos de usuarios de otros dominios se puedan incluir a su vez en este grupo para realizar allí tareas de administración. Por lo tanto, hay que crear un grupo global.

El paso siguiente consiste en darle al grupo sus usuarios. Para que el grupo de usuarios pueda trabajar también en otros dominios de confianza (y, por lo tanto, disfrutar de determinados derechos dentro de ellos), hay que incluirlos dentro de esos dominios como grupos locales de usuarios. Todas estas configuraciones se realizan con el Administrador de usuarios para dominios.

4.9.3.3 CREAR LOS PROPIOS GRUPOS GLOBALES DE USUARIOS.

- Inicie el Administrador de usuarios de dominio.
- Seleccione la opción Usuario, Grupo global nuevo, defina un nombre para el nuevo grupo de usuarios y escriba una descripción del grupo.
- Complete el cuadro de lista Miembros, seleccionando los miembros que desee para el grupo en el cuadro No son Miembros; a continuación, incorpórelos en el nuevo grupo de usuarios pulsando la casilla Agregar.

La tecla <Ctrl> le permite seleccionar varios miembros a la vez e incorporarlos juntos en el nuevo grupo.

- Revise sus selecciones y confirme.

Con los pasos anteriores ha creado usted el nuevo grupo de usuarios que deseaba. El grupo aparece a partir de ahora en el Administrador de usuarios en el que se ha creado el grupo de usuarios, y en la lista de grupos de usuarios que se muestra en la parte inferior del Administrador de usuarios.

Dentro del dominio, el nuevo grupo de usuarios sólo responde a fines clasificatorios. Los integrantes de un grupo de usuarios de caracterizan normalmente por determinadas propiedades comunes a todos ellos. En nuestro ejemplo se va a utilizar el grupo de usuarios para asignar a todos sus integrantes determinados derechos en los dominios de confianza.

Para ello hay que incorporar todo el grupo global de usuarios en un grupo local de usuarios del dominio de confianza que posean derechos específicos (por ejemplo, en el grupo local de usuarios Administradores de Impresión).

4.9.3.5 INCORPORAR GRUPOS GLOBALES DE USUARIOS A UN GRUPO LOCAL DE UN DOMINIO DE CONFIANZA.

- Cree una relación de confianza entre el dominio al que haya que incorporar el grupo global de usuarios y el dominio al que pertenezca actualmente ese mismo grupo de usuarios. Para crear la relación de confianza, utilice la opción Directivas, Relaciones de confianza del Administrador de usuarios e incorpore los dominios a través del botón Agregar.
- Active, en el Administrador de usuarios, las propiedades del grupo local de usuarios en el que quiera incorporar el grupo de usuarios del otro dominio.

- Pulse el botón Agregar. En el cuadro de diálogo Insertar usuarios y grupos, seleccione en primer lugar el dominio desde el cual quiere insertar los usuarios o el grupo. La lista de usuarios y grupos disponibles incluye, ahora, en sus líneas a los usuarios y los grupos globales del dominio seleccionado.
- Seleccione aquí el grupo de usuarios que se acaba de crear. Incorpórelo a continuación en el grupo de usuarios del dominio actual utilizando para ello la casilla Insertar.
- Confirme y cierre sus ajustes.

Con estos pasos ha asignado a todos los integrantes de un grupo global, determinados derechos dentro de un dominio de confianza. Si no hubiera incluido en un grupo a todos esos usuarios, habría tenido que incorporarlos uno a uno al dominio de confianza.

Si se incorporan nuevos integrantes al dominio, a los que haya que asignar los mismos derechos, sólo tendrá que incluirlos en el grupo global de usuarios. De ese modo, obtendrán también las propiedades y derechos de todo el grupo en ese dominio. Sin los grupos de usuarios, cada nuevo usuario se tendría que dar de alta por separado en cada dominio de confianza y asignarle individualmente los correspondientes derechos.

4.9.4 LA CUENTA DE USUARIO PASO A PASO.

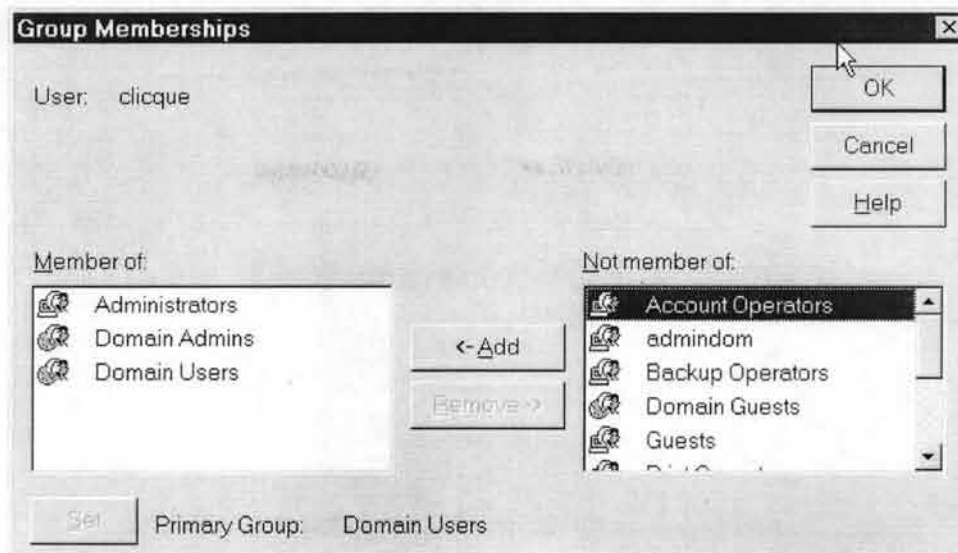
Los pasos a seguir en la creación de usuarios son los siguientes:

- Introducir los datos personales del usuario, en el cuadro de diálogo Nuevos Usuarios se especifican los datos personales del nuevo usuario.

Con el nombre de usuario, especificado en el primer cuadro, los usuarios pueden acceder a Windows NT Server o a cualquiera de los equipos Windows NT Workstation. (figura IV.23)

(figura IV.23)

- Asignarle un grupo al usuario, todos los usuarios deben formar parte de, por lo menos, un grupo. Los grupos de usuario definen los derechos que tiene cada integrante en NT Server y en la red del dominio NT. (figura IV.24)



(figura IV.24)

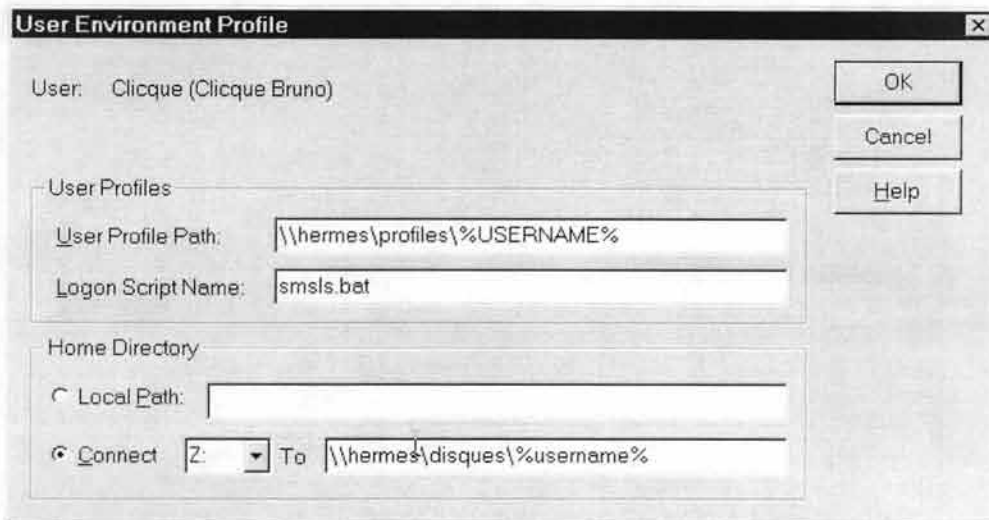
Los grupos globales de usuarios se simbolizan con un globo, los locales con un ordenador.

- Crear un perfil de usuario, al iniciar una sesión local en un ordenador de Windows NT, el nombre de usuario es el encargado, a través del perfil de usuario, de la presentación del escritorio. Al igual que sucede en las estaciones de trabajo, los clientes Windows NT 4.0 también se pueden configurar en una red Windows NT con perfiles de usuario. En el cuadro de diálogo Perfil de entorno de usuarios, se pueden configurar los perfiles de usuario, los scripts de acceso y los directorios base

Los perfiles de usuario guardan las configuraciones de pantalla del escritorio, incluida la lista inicial. Estas configuraciones de Windows NT sólo pueden utilizarse en Windows NT Workstation.

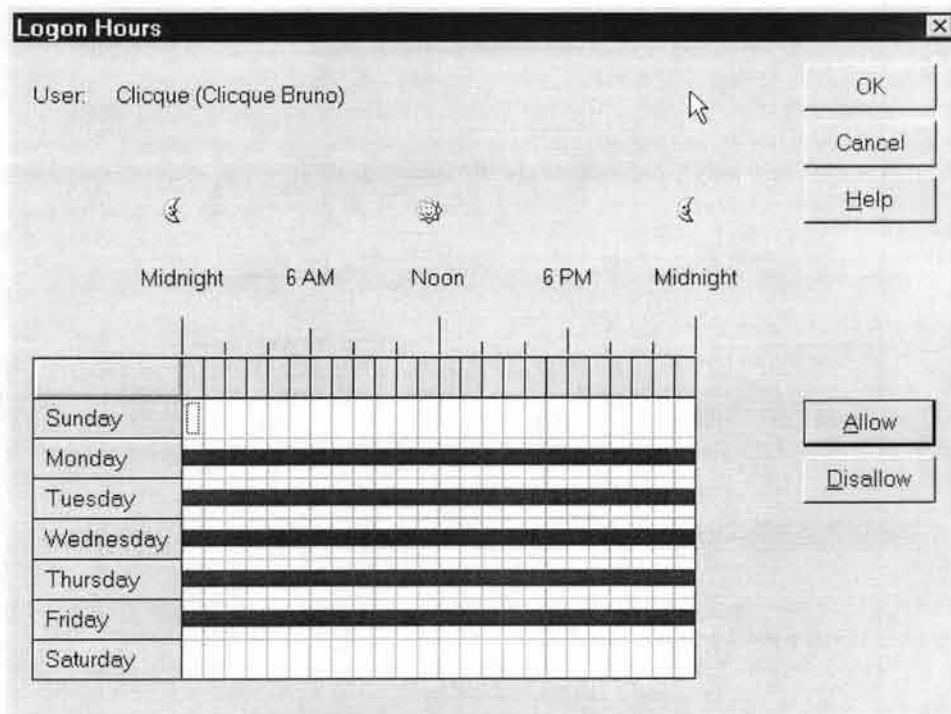
Los scripts de acceso (programas Batch), que se ejecutan en Windows NT Server cada vez que un usuario inicia una sesión en él, pueden asignar variables de entorno y vincular directorios con el ordenador de la estación de trabajo. Los scripts de registro de Windows NT Workstation se pueden ejecutar, además, en ordenadores con sistema operativo MS-DOS, Windows 3.11 y Windows 95. Juegan un papel especial en clientes Windows 3.11 y Windows 95, ya que estos sistemas operativos no son compatibles con los perfiles de usuario y las asignaciones de unidades fijas, por ejemplo, (net use..) sólo son posibles por esta vía.

Los directorios base que se asignan a cada usuario, al inicio de la sesión, son un directorio propio. Este directorio es el primero en que se encuentra el usuario al iniciar la sesión, y con los programas Windows es, además, el directorio estándar para las opciones Archivo, Abrir y Archivo, Cerrar. El directorio base puede ser un directorio local de Windows NT Server o cualquier otra unidad de red del dominio, de libre acceso, tanto de escritura como de lectura para el usuario o su grupo. (figura IV.25)



(figura IV.25)

- Configurar el tiempo de acceso del usuario, cuando el servidor realiza determinadas actividades (por ejemplo la seguridad de los datos), los usuarios no pueden acceder al mismo, o bien sólo pueden hacerlo un número restringido de usuarios. Para paliar este efecto, se puede definir, para cada usuario, un horario en el que se especifique cuándo puede acceder a Windows NT Server y cuándo puede utilizar sólo determinados recursos del sistema. El rigor con que Windows NT Server mantiene estos horarios, se especifica en la configuración de seguridad. Otro motivo para la restricción temporal puede ser determinadas normas de seguridad, por ejemplo para determinados lugares de trabajo en los que no esté permitido a nadie entrar durante el fin de semana a fin de evitar el acceso pirata.(figura IV.26)

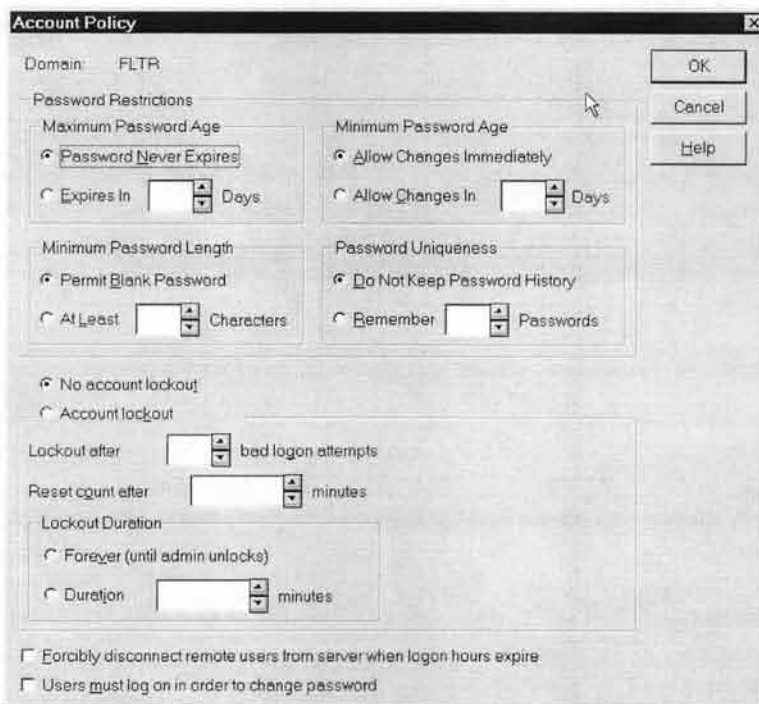


(figura IV.26)

- El liberar estaciones de trabajo para usuario, cuando determinados usuarios sólo pueden acceder a NT Server desde determinadas estaciones de trabajo, éstas se especifican en el botón Iniciar desde de las Propiedades de usuario. Esta restricción en los accesos de los usuarios, sólo existe para

Windows NT Workstation. Otros clientes (MS-DOS, Windows 3.11, Windows 95) pueden acceder en cualquier momento.

- Configurar los parámetros generales de la cuenta, en el primer cuadro de diálogo para la configuración de una cuenta de usuario, hay que definir si la contraseña de la cuenta caducará al cabo de un tiempo o no. En el cuadro de diálogo Información de la cuenta, se especificará si el tipo de cuenta es de duración indefinida o no.(figura IV.27)



(figura IV.27)

En el mismo cuadro de diálogo se define también si la cuenta es una cuenta global o local. La opción predefinida es la cuenta global.

Con esta cuenta los usuarios del dominio de Windows NT Server o de otro dominio de confianza, pueden acceder a NT Server y ejercer los derechos otorgados a su cuenta. Las cuentas locales se utilizan para proporcionar acceso a los recursos de la red NT a usuarios de otros dominios, sin ser de confianza, e incorporarlos a grupos globales de usuarios. Estos usuarios externos no acceden directamente a Windows NT Server, sólo utilizan los recursos de la red.

- Configurar, a través de la red de acceso remoto (RAS), las opciones para el acceso remoto del usuario a la red, para que los empleados de una empresa puedan acceder a la red cuando se encuentren de viaje, o desde casa, es necesario:

- Dotar al equipo Windows NT Server con un módem o una tarjeta RDSI.
- Instalar el servicio de acceso remoto RAS.
- Permitir a los usuarios el acceso a través de ese servicio.

El acceso externo a la red de una empresa debe estar muy bien meditado. Incluso siguiendo todos los estándares de seguridad para redes NT, no es imposible acceder indebidamente a una red utilizando el servicio de acceso remoto RAS. A diferencia de las redes TCP/IP, las redes NT ofrecen medidas adicionales de seguridad como son los servidores proxy y los cortafuegos (Firewalls), para proteger a la red de empresa de la intromisión de terceros. Los servidores proxy y los cortafuegos hacen que el acceso a la red mediante

conexión remota se realice a través de un solo ordenador. Este ordenador no sólo controla todos los accesos externos sino que los envía, también de forma restringida, a los ordenadores de la LAN.

Los datos, además, se transmiten en texto legible a través de la línea telefónica o por tarjeta RDSI, especialmente con las conexiones multiplex, de modo que los técnicos ingeniosos pueden captar fácilmente la comunicación de los empleados de la empresa. Una ayuda para impedir que así sea, la proporciona el protocolo PPTP, el cual posibilita una transmisión segura de datos a través de PPP. En el acceso remoto a su red, lo mejor que puede hacer es restringir fuertemente los derechos de acceso de los usuarios. La administración remota de NT Server se puede realizar por línea telefónica, pero pone en peligro la seguridad de todos los datos y, en consecuencia, la supervivencia de la empresa. En el cuadro de diálogo Información de marcado se define para cada usuario si éste debe poseer acceso remoto a NT Server por línea telefónica y, en caso afirmativo, si el servidor debe responder a la llamada dado el caso.

Cuando haya introducido todos los datos que se piden en cada uno de los cuadros, ya puede incorporar el primer usuario a la lista y seguir introduciendo nuevos usuarios.

4.9.4.1 ADMINISTRAR CUENTAS DE USUARIO.

Las configuraciones de las cuentas de usuario se pueden modificar:

- Si se trata de la cuenta de un usuario, pulse dos veces el usuario en cuestión en el Administrador de usuarios.
- Para modificar las propiedades de varias cuentas a la vez, marque todas las cuentas que se quieren modificar, mientras mantiene pulsada la tecla <Ctrl> y seleccione a continuación, la opción usuario, Propiedades.

Naturalmente, los nombres y las descripciones de los usuarios también se pueden modificar. Windows NT define para cada usuario un ID unívoco enlazado con el sistema de seguridad NT. Este número ID no se puede modificar bajo ningún concepto. Por eso tampoco es posible "pasar" un usuario de un dominio NT a otro dominio NT (porque puede ser que el ID de seguridad del usuario trasladado ya esté asignado en el "nuevo" dominio a otro usuario del mismo).

4.9.5 DEFINIR LAS NORMAS DE SEGURIDAD.

Windows NT soporta diferentes niveles de directivas de seguridad para la red. La seguridad de la cola de impresión y de los derechos de acceso a archivos se configuran en el Explorador; las normas generales de seguridad para usuarios y cuentas, así como las funciones de registro se administran, por el contrario, en el Administrador de usuarios.

4.9.5.1 PROPIEDADES DE CUENTA.

Cada cuenta de usuario está protegida con una contraseña (que también puede estar en blanco). Las contraseñas están para impedir el acceso de terceros al ordenador. Pero sólo cumplen esta función si:

los usuarios:

- Son responsables en el uso de las contraseñas, y
- No utilizan contraseñas demasiado fáciles de adivinar, y

los administradores:

- Controlan las contraseñas (por ejemplo, predefinido una longitud mínima para las mismas y comprobando si han sido utilizadas anteriormente por el mismo usuario)

- Controlando los intentos fallidos de acceso y cerrando las cuentas si es necesario, así como
- Persuadiendo a los usuarios para que modifiquen las contraseñas en intervalos regulares de tiempo.

Las contraseñas están para proteger los recursos contra el acceso de terceros. Pero esto sólo lo consigue si se observan las siguientes reglas:

- No elija contraseñas que sean demasiado cortas (que tengan un mínimo de cinco caracteres).
- Las contraseñas no deben estar formadas por palabras sencillas ni contener fechas de nacimiento, nombres de amigos o de amigas ni matriculas. Todo eso resulta demasiado fácil de adivinar. Palabras como secreto, hay, etcétera forman parte, desde hace mucho tiempo, de la prueba estándar de los piratas informáticos.
- Convenza a los usuarios de que aprendan sus contraseñas de memoria y no las apunten en ningún papel, y sobre todo, que no se les ocurra enganchar ningún papel con contraseñas en el monitor o debajo del teclado.
- Para no olvidar la contraseña, es conveniente relacionarla con algo que resulte fácil de recordar.
- Piense en palabras con faltas de ortografía. Cambie las mayúsculas y las minúsculas.
- La unión de dos palabras a través de un carácter especial, también es un buen sistema para crear contraseñas. Cuanto menos relación guarden las palabras entre sí, tanto mejor.
- Elija un verso de un poema, o un refrán, y utilice la primera letra (o la última) de cada palabra para formar la contraseña.
- Modifique su contraseña periódicamente.
- No utilice la misma contraseña en todos los ordenadores con que trabaja. Si alguien da con ella en uno de los ordenadores, lo hará también en los restantes.

Una parte de estas reglas se puede controlar con las opciones de seguridad para las cuentas.

Aquí están prohibidas las contraseñas demasiado cortas y se puede obligar a los usuarios a que modifiquen su contraseña en intervalos determinados de tiempo. Además, después de un número de intentos fallidos de acceso, por ejemplo 3, se puede cancelar una cuenta, o por lo menos cerrarla durante un tiempo determinado. De ese modo, se evita el peligro de los programas piratas automatizados que van probando diferentes contraseñas según determinados algoritmos (y veces también al azar).

4.10 REDES RAS.

Aún cuando los ordenadores no estén conectados a una red local, siempre es posible conectarlos a una red a través de una línea de marcado. A este tipo de conexiones a la red, a través de líneas de marcado ("*Dial-Up-Networking*") Microsoft las llama RAS (servicio de acceso remoto). Con RAS, los ordenadores se pueden conectar a una red con los protocolos de red TCP/IP, IPX y NetBEUI, soportados por Windows NT, y trabajar con ellos como el resto de los usuarios locales de la red.

La conexión puede establecerse tanto por línea telefónica digital como por módem, RDSI o cualquier otra línea apta para datos (por ejemplo, X.25).

Cuando hay conectados dos ordenadores Windows NT 4.0 directamente entre sí, Microsoft ofrece estrategias de seguridad específicas, por ejemplo: la posibilidad de enviar las contraseñas en clave.

4.10.1 CONFIGURAR RAS.

El servicio RAS se puede configurar durante la instalación de Windows NT o más adelante, por separado. La instalación típica no incluye la instalación del servicio RAS.

En la instalación personalizada hay una opción que permite instalar este servicio.

Fundamentos:

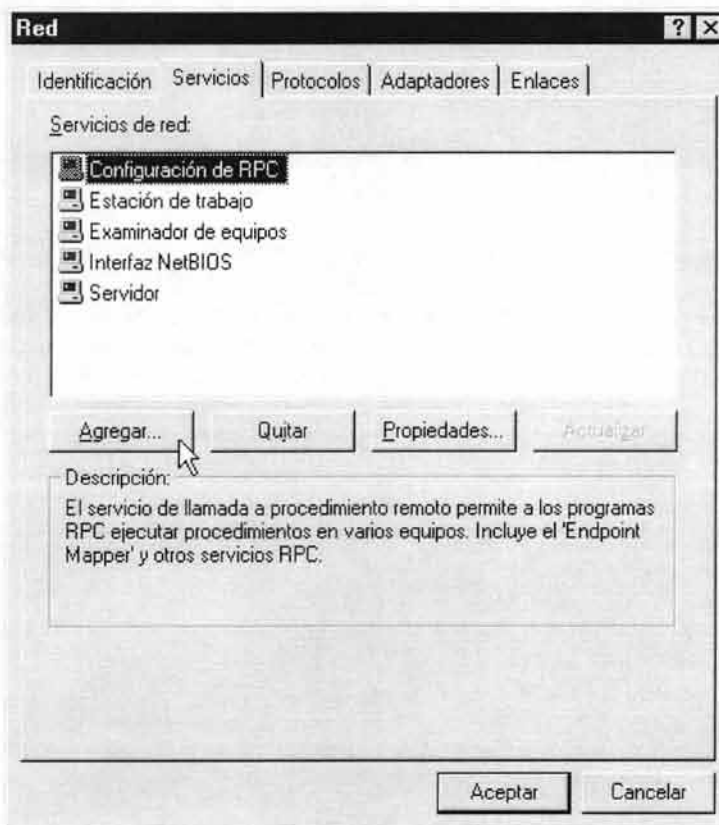
Para utilizar el servicio RAS se necesitan tarjetas adaptadoras para enviar los datos por líneas de conexión remota (líneas telefónicas analógicas, RDSI, X.25). Aquí se supondrá que estos periféricos ya están correctamente instalados.

El servicio RAS se instala a través del icono de red del Panel de Control de Windows NT. Para realizar esta operación es necesario el CD de instalación de Windows NT.

Las siguientes instrucciones indican, paso a paso, todas las operaciones necesarias para instalar el servicio RAS. La instalación es la misma para los servidores y clientes RAS en Windows NT. Cada cliente RAS puede funcionar también como servidor si se le permite que conteste las llamadas. Por eso al describir la instalación aquí no se hará diferencia entre servidores y clientes.

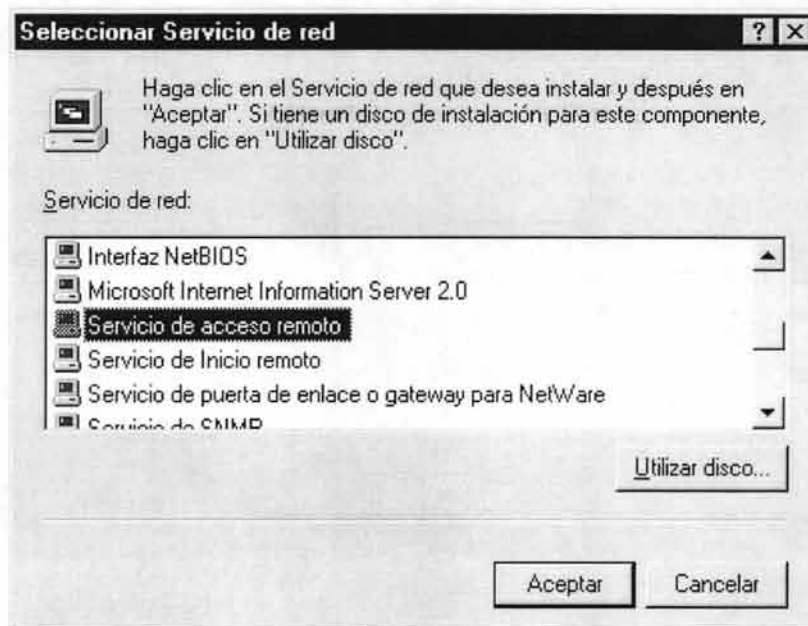
Instalar el servicio RAS:

- Vaya al Panel de control y pulse allí el icono RED.
- En el cuadro de diálogo *Red*, seleccione la ficha Servicios y pulse el botón Agregar. Windows NT le mostrará entonces una lista de los servicios disponibles.(figura IV.28)



(figura IV.28)

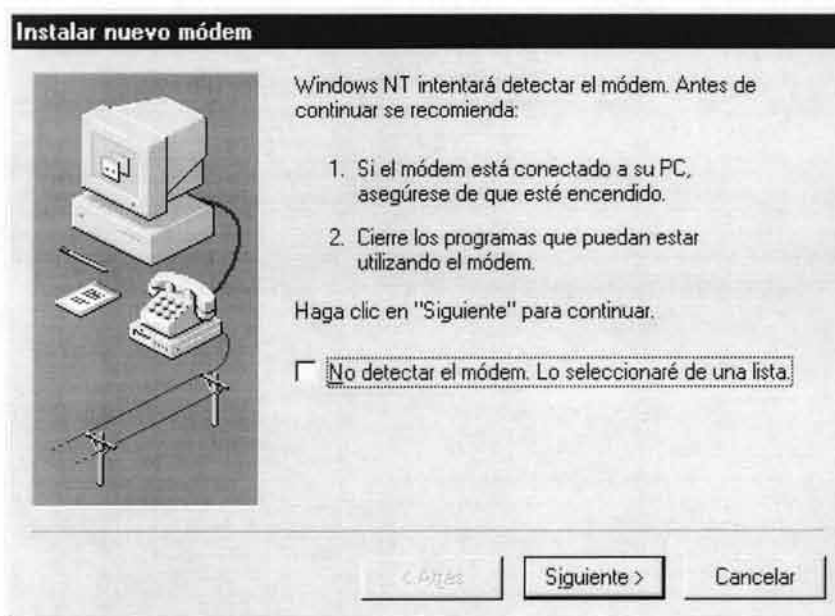
- En el cuadro de diálogo Seleccionar Servicio de red, seleccione la opción Servicio de acceso remoto.(figura IV.29)



(figura IV.29)

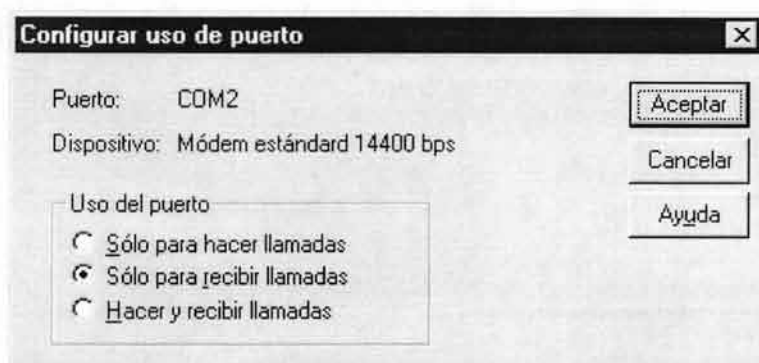
- Ahora debe introducir la ruta de acceso de los archivos de instalación. La encontrará en el subdirectorio \I386 del CD de instalación de Windows NT.
- En el paso siguiente va a configurar el puerto para el servicio RAS. En pantalla se mostrarán todos los puertos de los módems instalados, tarjetas RDSI, tarjetas X.25 y otros puertos WAN. Si instala tarjetas más adelante, siempre puede ampliar el servicio RAS con nuevos puertos.

Windows NT intenta reconocer automáticamente los módems que todavía no estén instalados. Si no lo consigue, deberá seleccionar usted mismo el modelo de su módem.(figura IV.30)



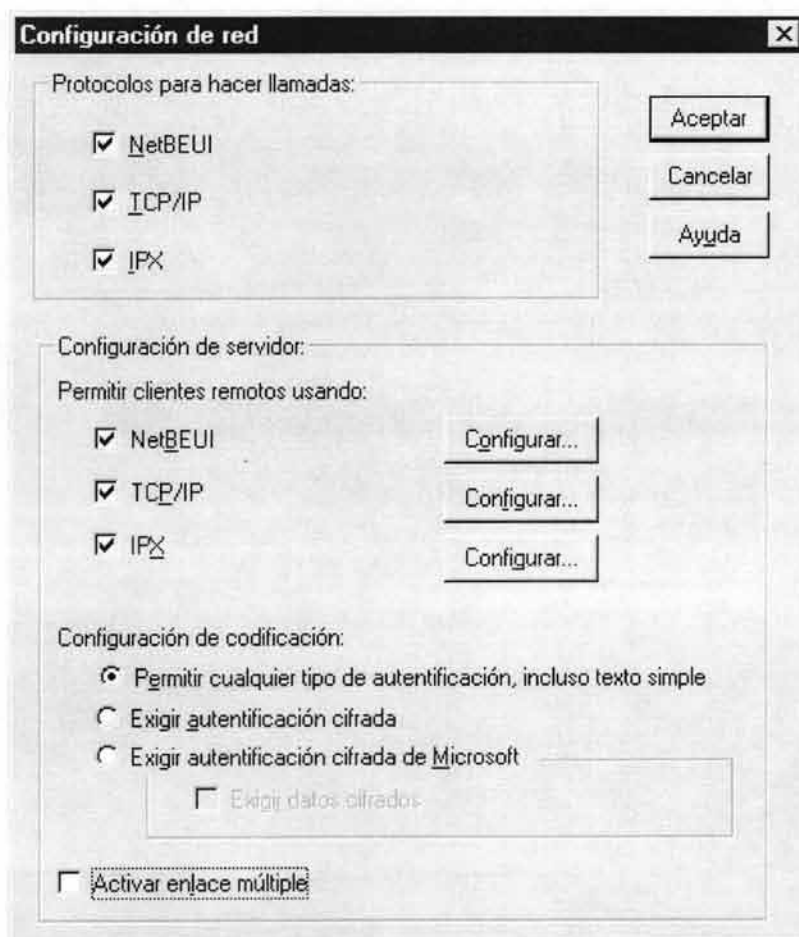
(figura IV.30)

- Para cada puerto de una red RAS se puede definir si tiene que ser sólo de entrada, sólo de salida, o bien ofrecer ambas posibilidades.(figura IV.31)



(figura IV.31)

- Realice ahora las configuraciones de red del servicio RAS. Para ello, pulse el botón Red. En el cuadro de diálogo Configuración de red, configure los protocolos para los servicios de cliente y servidor de su puerto RAS. Puede configurar también otros parámetros como son la codificación de datos o el envío de contraseñas codificadas. Estos parámetros se pueden configurar también más adelante.(figura IV.32)



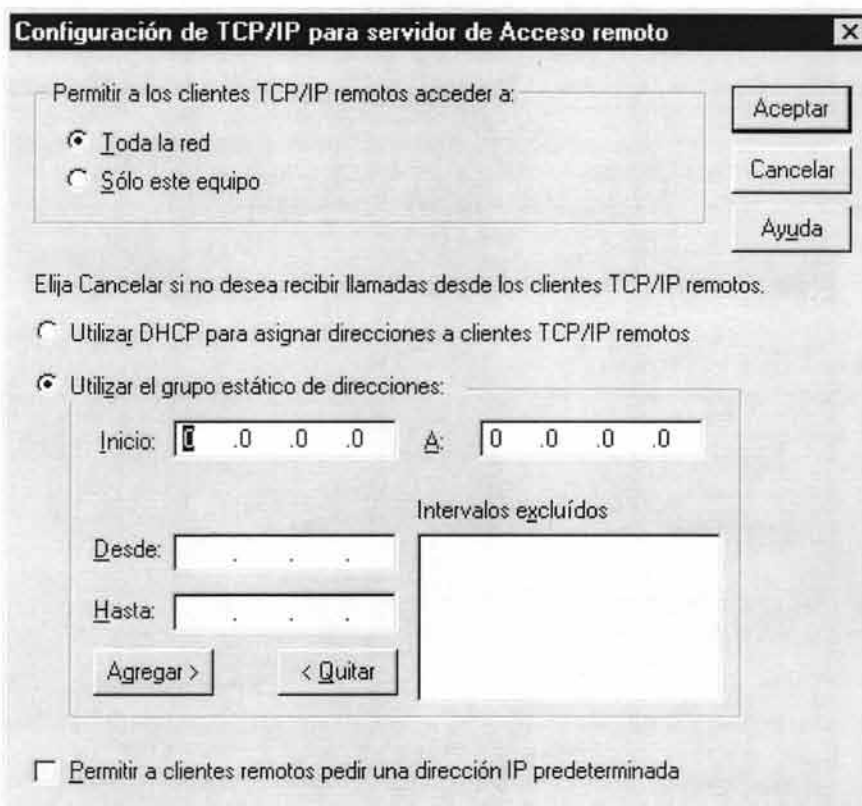
(figura IV.32)

- Con esto quedan finalizadas las configuraciones del servicio RAS. Salga del cuadro de diálogo Instalación de Acceso remoto a través del botón Continuar para regresar al cuadro de diálogo Red. Cierre este cuadro de diálogo para actualizar las configuraciones en el sistema.

A continuación debe iniciar Windows NT de nuevo para que todas las configuraciones nuevas surtan efecto.

Ahora ya ha instalado y configurado el servicio RAS. Puede incluir nuevos módems o tarjetas RDSI siempre que lo desee. Para ello debe utilizar nuevamente el cuadro de diálogo Red, ir a la ficha Servicios y seleccionar Servicio de acceso remoto. Con el botón Propiedades se encontrará otra vez en el cuadro de diálogo de configuración del servicio de acceso remoto., y aquí puede modificar los parámetros de los puertos instalados y agregar puertos nuevos.

Llegados a este punto, vamos a considerar más detalladamente las configuraciones de RAS para un servidor RAS TCP/IP. En las redes TCP/IP todos los ordenadores tienen asignada una dirección IP. La dirección IP la puede traer ya el cliente RAS consigo, o recibirla asignada por el servidor.(figura IV.33)



(figura IV.33)

En una red TCP/IP, las direcciones IP se pueden asignar a través del Dynamic Host Configuration Protocol (DHCP), o mediante las listas estáticas de direcciones IP. Windows NT permite las dos opciones. En la primera opción, las direcciones IP se administran con el protocolo DHC. En la segunda posibilidad, debe indicar a Windows NT un área de posibles direcciones IP y a cada cliente RAS se le asignará exactamente una dirección IP de esta área.

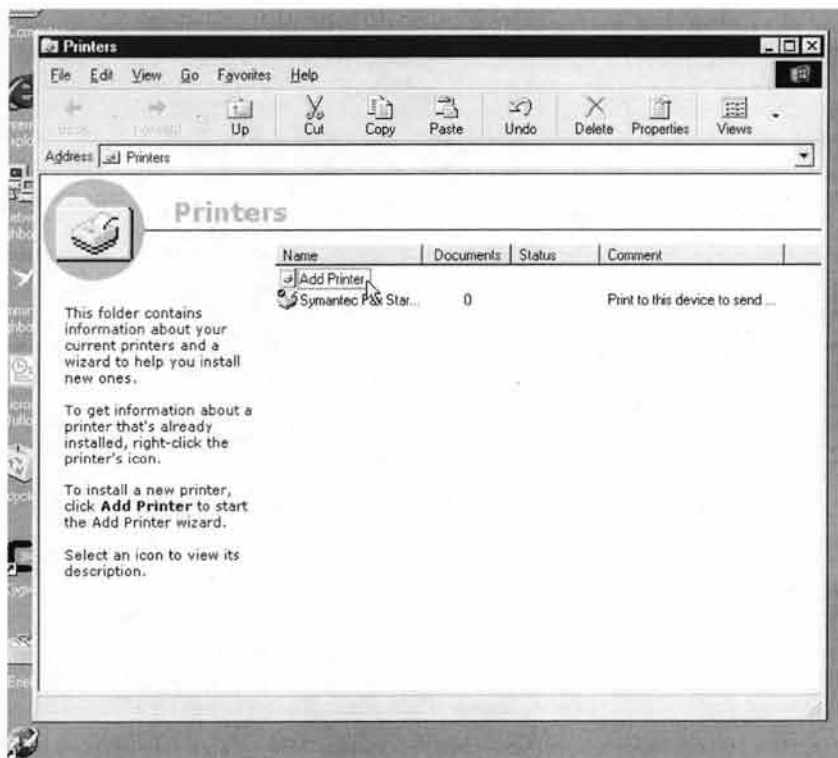
4.11 IMPRESIÓN EN WINDOWS NT.

Una de las principales razones por la que un negocio invierte en una red es para mejorar su acceso a la información. Los servicios de archivo para Windows NT crean un medio ambiente robusto y fácil de manejar para compartir archivos a través de una organización. Asimismo, permite a los administradores, dar a su personal acceso a los recursos disponibles en el sistema, sin importar el sistema operativo que usen.

Los servicios de impresión de Windows NT hacen que el acceso y el manejo de impresoras sean rápido y fácil. Al usar Windows NT Server 4.0 como un servidor de impresión, los administradores pueden maximizar el uso de cada impresora y evitar largas demoras en la impresión. Para optimizar el rendimiento de las impresoras, Windows NT Server 4.0 Enterprise Edition, ofrece una alta disponibilidad de los servicios de impresión, haciendo clusters en el servidor.

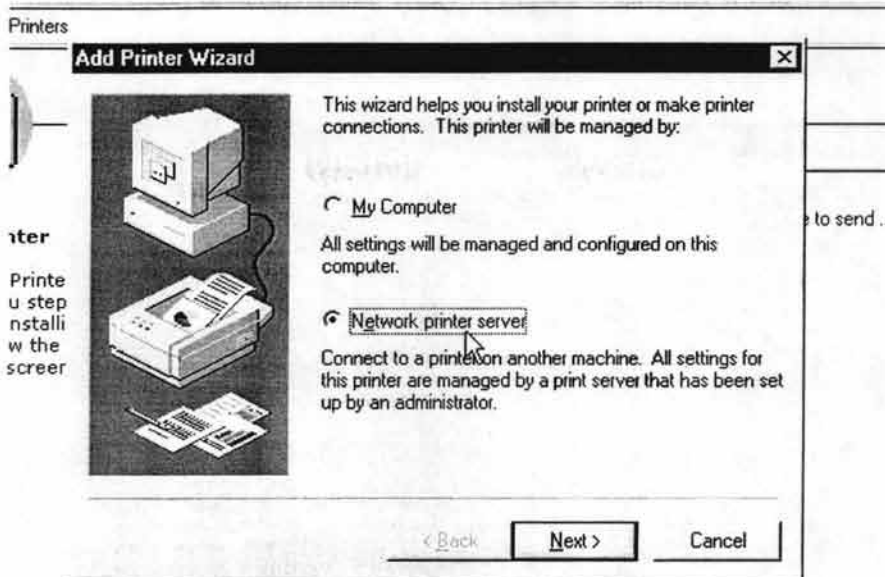
4.11.1 IMPRESORAS.

Normalmente, la mayoría de las aplicaciones ofimáticas necesitan una impresora predeterminada para funcionar. Para instalar una nueva impresora al sistema NT dispone de un sencillo asistente que guía en el proceso de instalación. Para acceder a este asistente se utiliza el ícono Agregar impresora del Panel de control \ impresoras.(figura IV.34)



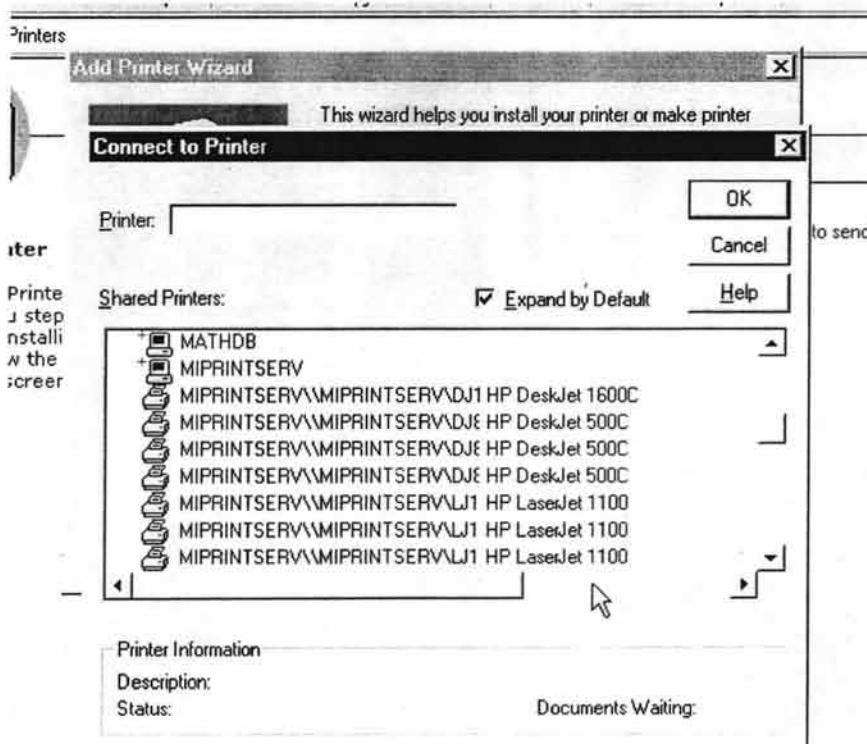
(figura IV.34)

En NT la impresora puede estar instalada en el propio equipo o ser una impresora de red. El caso más sencillo consiste en que la impresora esté conectada a un servidor NT, que la ha compartido. En este caso para conectarse a la impresora basta seleccionar en el asistente la opción *Servidor de impresora de red*. (figura IV.35)



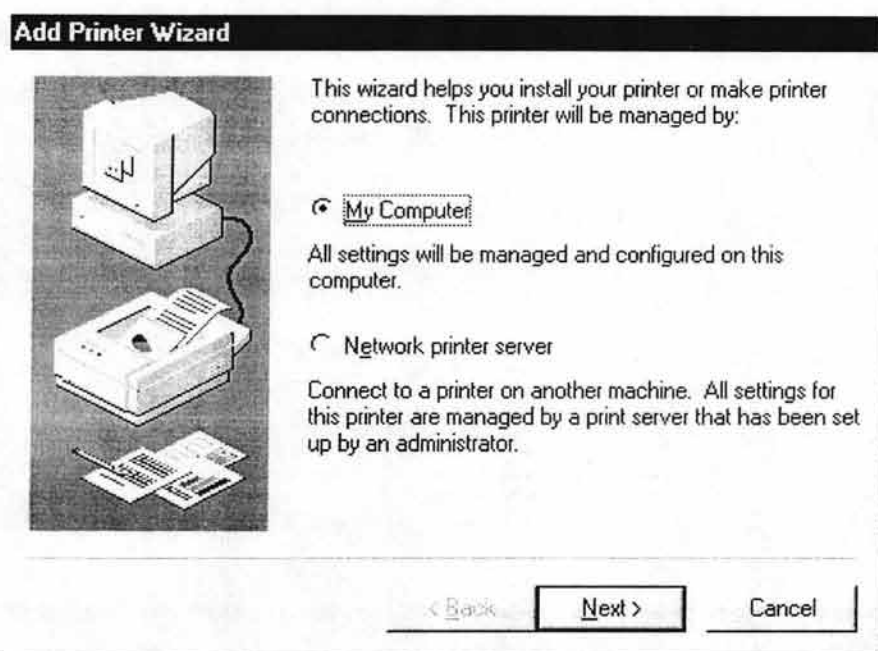
(figura IV.35)

Al seleccionar esta opción aparece un cuadro de diálogo con las impresoras compartidas por los equipos. (figura IV.36)



(figura IV.36)

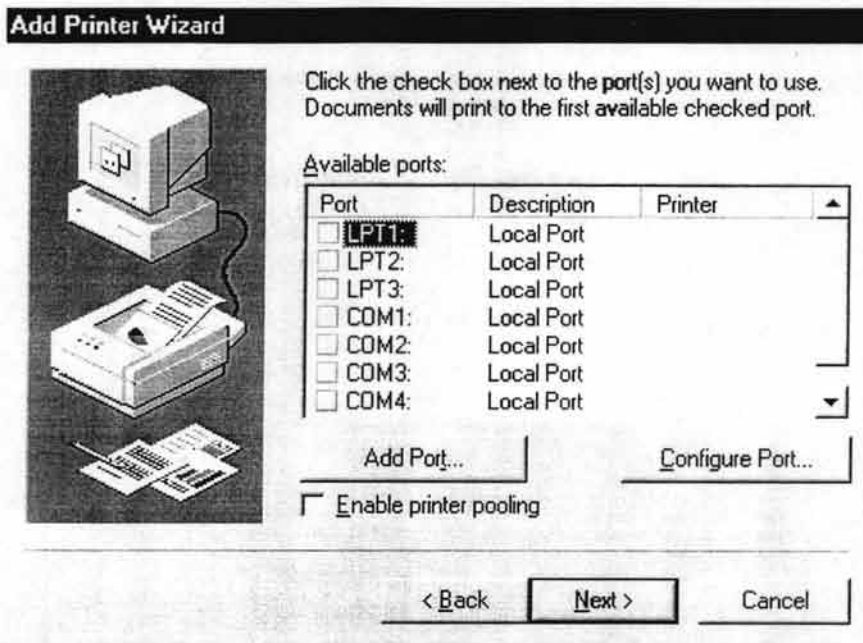
Las impresoras compartidas por los NT aparecen aparte, como elementos separados del equipo que las comparte, haciendo más fácil su localización. La opción instalar la impresora en el propio equipo conduce a una serie de asistentes que nos permiten configurar y compartir la impresora.(figura IV.37)



(figura IV.37)

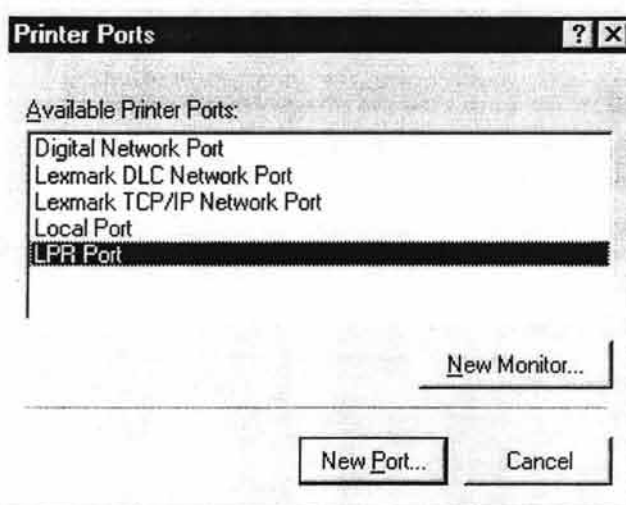
El primer paso consiste en seleccionar el puerto al que está conectada la impresora. Puede ser:

- Un puerto paralelo LPT, normalmente el LPT1.
- Un puerto serie (los trazadores gráficos antiguos los suelen usar).
- Un puerto de red (cuando hay conexiones a impresoras de red).
- Un archivo. En este archivo se almacenarán los comandos necesarios para imprimir el documento en la impresora. Se suele usar para generar archivos Postscript.(figura IV.38)



(figura IV.38)

- Un puerto nuevo, que quizás usa un *hardware* o software especial. Un ejemplo de este tipo son los puertos Jetdirect de red usados por las impresoras HP.(figura IV.39)



(figura IV.39)

En este cuadro de diálogo se puede activar la cola de impresión de NT (normalmente esta opción no se activa por defecto, sino que se imprime directamente en el puerto).

Luego hay que elegir el modelo de la Impresora. El cuadro de diálogo está organizado por Fabricantes y modelos, por lo que se encuentran rápidamente los modelos adecuados. También se puede añadir una impresora no disponible en NT con los controladores proporcionados por el fabricante.(figura IV.40)

Add Printer Wizard



Click the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

Manufacturers:	Printers:
Toshiba ▲	Xerox DocuPrint 4635 v1.3.9 ▲
Unisys	Xerox DocuTech 90 PS2
Varityper	Xerox DocuTech 135 PS2
Wang	Xerox DocuTech 6135 (01.02.00) ┘
Xante	Xerox DCS20 v3.0ER2.26
Xerox ▼	Xerox DCS35 v3.0ER2.26
	Xerox 4215/MRP2 v2013.109 ▼

Have Disk...

< Back Next > Cancel

(figura IV.40)

Tras elegir el modelo hay que ponerle un nombre en el siguiente cuadro de diálogo.

Normalmente NT elige un nombre adecuado, que coincide con el modelo de la impresora.(figura IV.41)

Add Printer Wizard



Type in the name of this printer. When you have finished, click Next.

Note: Exceeding 31 characters in the Server and Printer name combination may not be supported by some applications.

Printer name:

whgfn_e_dt

Do you want your Windows-based programs to use this printer as the default printer?

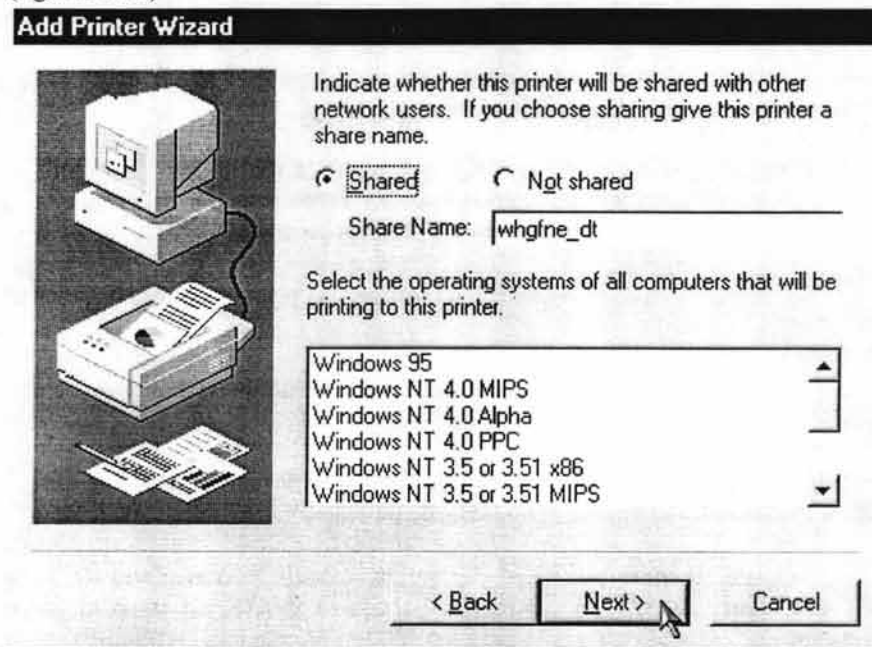
Yes

No

< Back Next > Cancel

(figura IV.41)

El siguiente cuadro de diálogo permite compartir la impresora. Si se comparte NT se debe elegir: (figura IV.42)



(figura IV.42)

- Un nombre para la impresora, que también sugiere el asistente.
- Los controladores que se van a compartir. Se puede añadir el soporte para otras plataformas NT y Windows, aunque hará falta tener los discos correspondientes. Esto permite que los clientes se conecten a la impresora sin necesidad de instalar ellos ningún controlador de impresora. Al conectarse a la impresora los controladores se transfieren al cliente de forma automática.
- El proceso de instalación finaliza con la impresión de una página de prueba opcional, que permite verificar la correcta instalación de la impresora..

4.11.2 EL ADMINISTRADOR DE IMPRESIÓN.

El antiguo administrador de impresión de Windows 3.X y NT se ha sustituido por la Carpeta de Impresoras, que es accesible desde el Panel de Control o desde el menú de Inicio, en el menú de configuración. Con la nueva carpeta de impresoras se puede:

- Abrir el asistente para añadir una nueva impresora.
- Abrir la cola de impresión de una impresora, configurar la impresora y compartirla.
- Conectarse a un servidor de impresión para configurarlo.
- Conectarse a una impresora de red.

En la carpeta de impresoras aparecerá un ícono que permite acceder a la impresora. La ventana de control de la impresora muestra los documentos que se están imprimiendo y permite además, acceder a todas las opciones de configuración de la impresora.

El menú Impresora tiene varias opciones:

- Pausa impresión. Permite detener la impresión de los documentos.
- Establecer como predeterminada. En el sistema sólo puede haber una impresora predeterminada, que será la que usen las aplicaciones por defecto.
- Valores predeterminados del documento. Cuando se crea un documento normalmente la aplicación configura el documento con los parámetros por defecto de la impresora. Normalmente, las aplicaciones luego permiten modificar estos parámetros.
- Compartir. Permite compartir o modificar las opciones utilizadas para compartir la impresora.
- Propiedades. Permite acceder a una serie de cuadros de diálogo para compartir la impresora.

El menú Impresora \ propiedades permite acceder al cuadro de diálogo de configuración de la impresora. Este cuadro de diálogo está formado por una serie de pestañas:

- General. Permite modificar el nombre, modelo y comentario de la impresora. También se puede especificar aquí el controlador para la impresora, así como el procesador de impresión utilizado.
- Configuración del dispositivo. Accede a las opciones de impresión de la impresora, como color, tipo de papel, tipos de letra instalados y otras. Depende del modelo de impresora instalada.
- Plan de impresión. Permite configurar algunas opciones de la cola de impresión que permiten una mayor agilidad en la impresión de documentos
- Puertos. Permite modificar el puerto al que se ha conectado la impresora, así como activar y desactivar la cola de impresión.
- Seguridad. Permite configurar las opciones de seguridad y auditoria de la impresora. Serán explicadas en el tema dedicado a seguridad.
- Compartir. Mediante este cuadro de diálogo se puede compartir de modo sencillo la impresora en red. Al compartirla hay que asignarle un nombre de recurso. Además se pueden compartir los controladores necesarios para que otros usuarios utilicen la impresora sin necesidad de instalar controladores en su equipo.
- Propiedades predeterminadas del documento. Este cuadro de diálogo está dividido en dos pestañas. La primera permite configurar las opciones más sencillas:
 - Tamaño del papel.
 - Origen del papel, para impresoras con varias fuentes de papel, (bandejas, carga manual del papel, sobres, etcétera).
 - Orientación de la impresión: vertical, horizontal (apaisada), o invertida (rotada).
 - Número de copias.
 - Impresión por ambos lados, para impresoras que lo soportan.

- Color, para las impresoras en color y grises.
- Opciones avanzadas. Permiten configurar gran cantidad de opciones:
 - Opciones del papel, como orientación y tipo de papel empleado.
 - Opciones de impresión de los gráficos, para seleccionar la calidad y apariencia de los gráficos.
 - Opciones del documento, como ajustes de los medios tonos o calidad de impresión.

4.11.3 CONEXIÓN A UN SERVIDOR DE IMPRESIÓN.

Quando se establece conexión como administradores a un servidor de impresión es posible configurarlo remotamente, del mismo modo en que se hace con las impresoras locales. Se puede compartir las impresoras del servidor o estación de trabajo NT y configurar las impresoras.

También se puede acceder a las colas de impresión para gestionar los documentos que se están imprimiendo.

El cuadro formularios permite definir los diferentes tamaños de papel soportados por la impresora. NT define los más habituales por defecto.

El cuadro de diálogo avanzadas permite asignar algunas propiedades avanzadas del servidor de impresión. La más importante es el directorio donde se almacena la cola de impresión. Hay que recordar que en este directorio se suelen almacenar ficheros intermedios de gran tamaño. Este directorio normalmente reside en la partición del sistema, por lo que se puede llegar a desbordar el sistema.

El cuadro de puertos permite ver los puertos en los que se puede imprimir, así como añadir, eliminar y configurar los puertos.

4.12 RESPALDOS EN NT.

4.12.1 CREAR UNA COPIA DE SEGURIDAD.

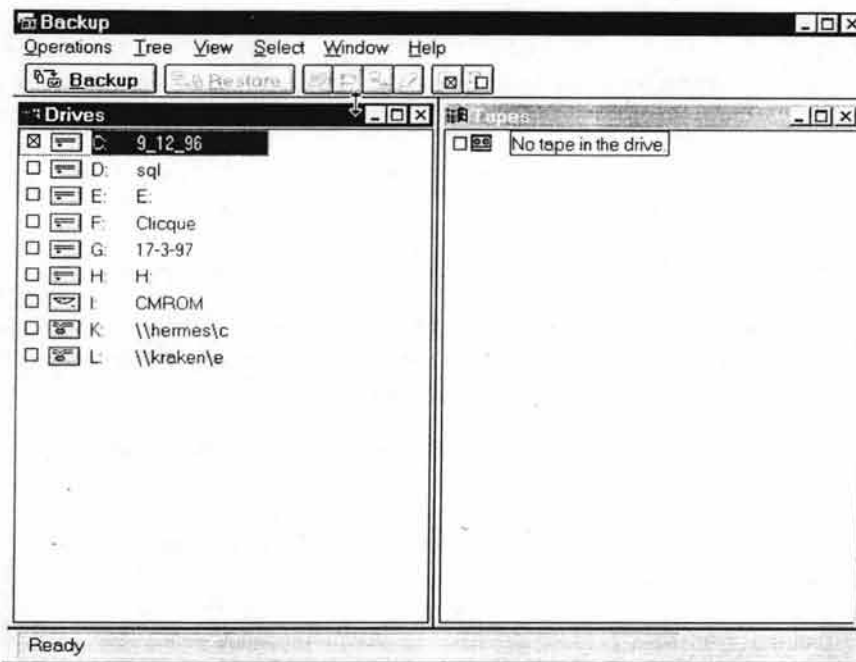
Para crear una copia de seguridad debe utilizar la unidad de cinta instalada en el sistema, ha de iniciarse simplemente el programa copia de seguridad (Backup) de Windows NT. Se trata de un programa de copia de seguridad muy potente. Si la unidad de cinta que posee no estuviese contemplada en el software de Windows NT, deberá solicitar del fabricante el correspondiente controlador para la misma.

Dado que Windows NT utiliza la versión 1.0 del Microsoft Tape Format, es preciso que se dé formato a la cinta antes de poder utilizarla (a menos que viniese ya inicializada expresamente para Windows NT). Los mensajes de error del tipo "Formato de cinta no reconocido" ("*Tape format Not Recognize*") o "La unidad no esta preparada" ("*Drive not Ready*"), suelen indicar que se ha intentado utilizar una cinta sin inicializar. Si desea usar una cinta que ya ha sido utilizada con otro programa de copia de seguridad, seleccione la opción borrar cinta ("*Erase Tape*") en menú de operaciones ("*Operations*").

Haga clic en la opción borrado rápido ("*Quick Erase*") y pulse después el botón continuar ("*Continue*"). Tras la aparición de una serie de mensajes de advertencia, Windows NT habrá dejado lista la cinta para poder ser utilizada. Puede comprobar el éxito de la operación, viendo si aparece el mensaje "The Tape in the Drive is Blank" en el campo cinta actual ("*Current Tape*") del cuadro de dialogo Backup Information.

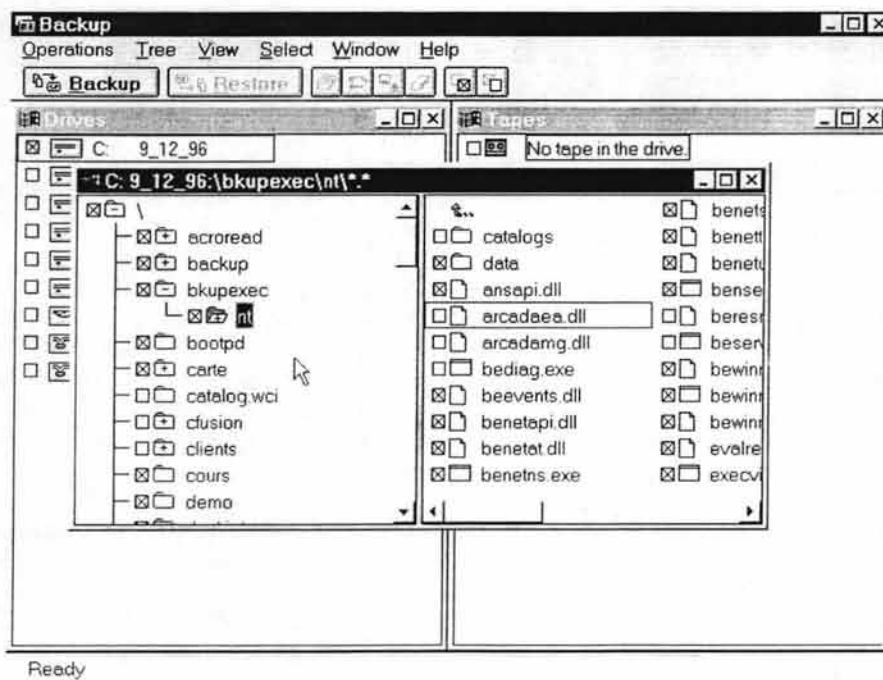
El primer paso para poner en marcha el proceso de copia de seguridad consiste en seleccionar las unidades que se han de incluir en la misma.

En la ventana unidades ("Drives"), puede elegir entre la unidad completa marcando la correspondiente casilla de verificación, o bien hacer doble clic en el ícono de la misma para que aparezca una lista con los directorios y archivos que contiene. (figura IV.43)



(figura IV.43)

Tras esto, puede ir marcando las casillas que correspondan a los directorios o archivos específicos de los que desea tener copia de seguridad. En la mayoría de los casos, la copia de seguridad abarcará la totalidad de la unidad.(figura IV.44)



(figura IV.44)

Una vez seleccionados los archivos de los que desea obtener copia de seguridad, haga clic en el ícono con el nombre copia de seguridad ("Backup") de la barra de herramientas. El programa de copia de seguridad mostrará entonces un cuadro de diálogo, donde puede indicar el tipo de operación que desea realizar.

El programa de copia de seguridad rellena de forma automática los campos Current Tape, Creation Date y Owner. El campo Tape Name permite especificar un nombre para la cinta. Siempre que coloque la cinta en la unidad, podrá identificarla por su nombre. Por omisión, Windows NT utiliza como nombre de cinta la fecha de creación de la copia de seguridad. Puede elegir entre una operación de sustitución o bien de agregadura de archivos; en la operación de sustitución se reemplazan todos los datos de la cinta mientras que en la de agregar, los nuevos datos pasan a ocupar el espacio libre que quede al final de la misma.

Uno de los campos más importantes es el denominado Verify After Backup. Es aconsejable tener siempre activada esta opción, con el fin de asegurar que los datos de la cinta coincidan con los de la unidad original. Naturalmente, esto conlleva una demora en la operación de copia de casi el doble de lo normal.

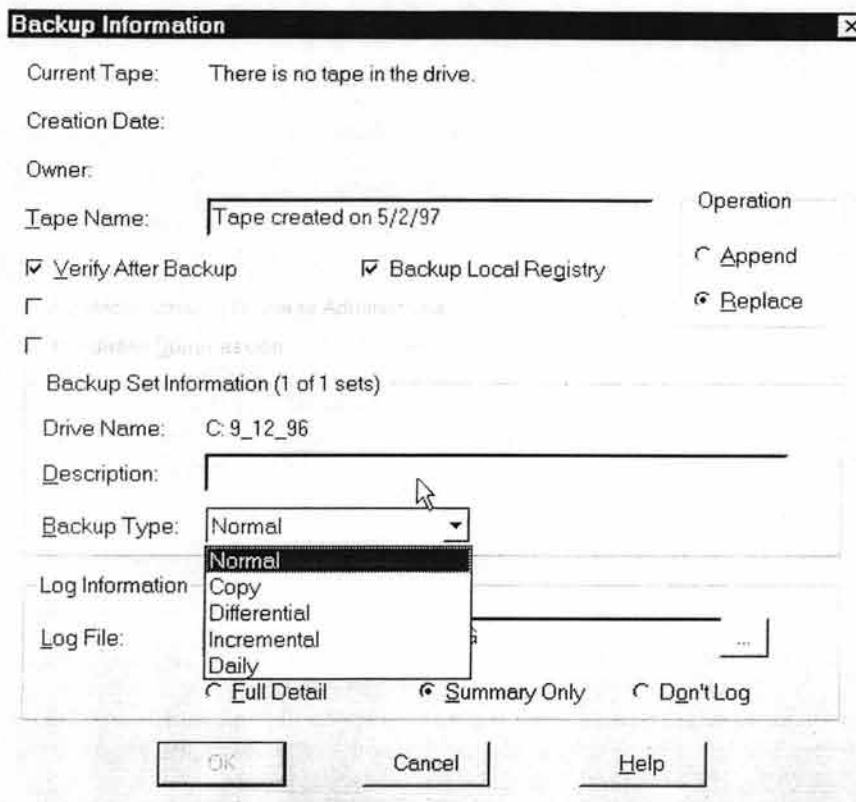
La opción Backup Local Registry permite proteger los datos de configuración, pasándolos también a la cinta.

El campo Restrict Access to Owner or Administrator, permite proteger los datos de posibles intrusiones de otros usuarios.

En Backup set Information se informa de las unidades que el programa de copia de seguridad ha copiado en la cinta. Hay un conjunto de copia de seguridad por cada unidad. En el campo de Descripción, permite describir las condiciones de la copia de seguridad en relación con la unidad. El campo Backup Type permite seleccionar el método de copia de seguridad. Existen 5 métodos entre los cuales elegir:

- Normal. Esta opción permite crear una copia de seguridad completa de una unidad y que posteriormente se empleará para crear la copia de seguridad que sirve de base para posteriores copias diferenciales e incrementales.
- Copy. Esta opción es muy parecida a la opción anterior con la diferencia de que no altera el estado del atributo de modificado de los archivos que va copiando a la cinta. Se recomienda utilizar esta opción cuando no se piense crear copias de seguridad incrementales o diferenciales en el futuro.
- Incremental. Permite agregar los archivos que hubiesen experimentado cambios desde la última copia de seguridad normal o incremental. Este es el método más rápido de obtener copias de seguridad del sistema, pero este ahorro de tiempo se pierde en la operación de restauración posterior.
- Differential. Esta opción es muy similar a la opción incremental, con la excepción de que no altera el estado del atributo de modificado de los archivos agregados.
- Daily Copy. Esta opción permite obtener copia de los archivos modificados en la jornada actual. Esta opción no altera el estado del atributo de modificado.

El apartado Log Information del cuadro de diálogo permite mantener un registro de la operación de copia de seguridad. (figura IV.45)



(figura IV.45)

Una vez concluido el trabajo con el cuadro de diálogo de configuración, puede dar comienzo el proceso. El programa de copia de seguridad de Windows NT presenta un cuadro de dialogo, en donde se informa del estado del proceso. Esta pantalla muestra el número de directorios, archivos y bytes copiados a la cinta, en la parte superior izquierda del cuadro de diálogo. En la esquina superior derecha se informa de los errores en los archivos que hayan sido detectados por el programa de copia de seguridad. En la parte media del cuadro de diálogo existe un indicador de la unidad, directorio y archivo que está siendo enviado a la cinta. En la sección Summary del cuadro de diálogo se informa del desarrollo global de la operación, así como de posibles errores relacionados con el **Hardware**, detectados por el programa copia de seguridad.¹¹

¹¹ Curso de Windows NT , Litz, J. Aprendiendo Windows NT Server 4.0, En línea [URL], <http://webmar.es.vg>

CAPÍTULO V
ANÁLISIS COMPARATIVO DE LAS TRES PLATAFORMAS
(UNÍX, NETWARE®, WINDOWS NT)

5. ANÁLISIS COMPARATIVO DE LAS TRES PLATAFORMAS (UNIX, NETWARE®, WINDOWS NT).

En los capítulos anteriores se analizó cada uno de los sistemas operativos en cuestión, una vez que ya se tiene un panorama más amplio de la administración y configuración de cada uno de los sistemas, a continuación se presenta un análisis comparativo de las tres plataformas.

La metodología empleada para este análisis se basa en la comparación de algunas características técnicas, funcionales o mercadológicas, aunando a este comparativo un muestreo que se realizó en el Valle de México, como también en algunos estudios ya realizados por empresas especializadas.

A continuación se hará un breve compendio de las ventajas y desventajas de los tres Sistemas Operativos que se están estudiando:

5.1 VENTAJAS Y DESVENTAJAS DE LOS SISTEMAS OPERATIVOS¹²:

5.1.1 VENTAJAS DE NOVELL®

- Está diseñado y optimizado para ejecutar redes, administrar servicios de conectividad que incluyen servidores de aplicaciones tales como NETWARE®, Windows NT, UNIX y otros sistemas host.
- NOVELL® Directory Services™ (NDS™) está demostrado en el mercado, con más de 70 millones de usuarios y muchos años de experiencia en todo el mundo.
- Integra el entorno de ejecución Java más veloz, un rápido entorno de programación y la próxima generación de aplicaciones distribuidas basadas en Internet.
- Incluye la base de datos líder en todo el mundo, Oracle8, que permite una entrada única y administración centralizada.
- Incluye herramientas de desarrollo Web con *IBM* WebSphere.
- Su NDS se basan en la arquitectura X.500 estándar del mercado.
- Su NDS proporcionan una organización jerárquica y expansible para todos los recursos de la red.
- Su NDS está disponible para otras plataformas además de NETWARE® y son adoptados por otros fabricantes.
- Su NDS reduce drásticamente el costo de administración de su red.
- Se puede limitar la cantidad de espacio en el disco duro al usuario.
- Soporta múltiples protocolos.
- Soporta acceso remoto.
- Permite instalación y actualización remota.
- Muestra estadísticas generales del uso del sistema.
- Brinda la posibilidad de asignar diferentes permisos a los diferentes tipos de usuarios.
- Permite realizar auditorias de acceso a archivos, conexión y desconexión, encendido y apagado del sistema, etcétera.

5.1.2 DESVENTAJAS DE NOVELL®

- No cuenta con listas de control de acceso (ACLs) administradas en base a cada archivo.
- Algunas versiones no permiten criptografía de llave pública ni privada.
- No ofrece mucha seguridad en sesiones remotas.
- No permite el uso de servidores no dedicados.
- Para su instalación se requiere un poco de experiencia.

¹² Costales F. Sistema Operativo Unix. En línea [URL].
<http://www.monografias.com/trabajos/soredes/soredes.shtml>

- NDS es bastante complejo de instalar y administrar.
- Perdió considerablemente mercado por la complejidad de NETWARE® 4.1 y NDS.
- La actualización de una versión a otra es lenta y compleja.
- Puede ser caro para redes pequeñas.

5.1.3 VENTAJAS DE WINDOWS NT.

- La instalación es muy sencilla y no requiere de mucha experiencia.
- Apoya el uso de múltiples procesadores.
- Permite el uso de servidores no dedicados.
- Soporta acceso remoto.
- El sistema está protegido del acceso ilegal a las aplicaciones en las diferentes configuraciones.
- Ofrece la detección de intrusos.
- Permite cambiar periódicamente las contraseñas.
- Soporta múltiples protocolos.
- Carga automáticamente manejadores en las estaciones de trabajo.
- Trabaja con impresoras de estaciones remotas.
- Soporta múltiples impresoras y asigna prioridades a las colas de impresión.
- Muestra estadísticas de Errores del sistema, Caché, Información del disco duro, Información de Manejadores, Número de archivos abiertos, Porcentaje de uso del CPU, Información general del servidor y de las estaciones de trabajo, etcétera.
- Brinda la posibilidad de asignar diferentes permisos a los diferentes tipos de usuarios.
- Permite realizar diferentes tipos de auditorias, tales como del acceso a archivos, conexión y desconexión, encendido y apagado del sistema, errores del sistema, información de archivos y directorios, etcétera.
- Soporta múltiples procesadores.
- Existe una gran variedad de aplicaciones diseñadas exclusivamente para NT, incluyendo freeware y shareware.
- Es fácil de instalar y manejar.
- Tiene una interfase de usuario muy amigable.
- NT es GUI (Interfase Gráfica de Usuario).
- NT tiene el respaldo de Microsoft, la compañía más poderosa en software del mundo.
- NT está a punto de incorporar soporte completo para UNIX.
- Tiene buen soporte técnico.
- NT es económico para entornos medianos.

5.1.4 DESVENTAJAS DE WINDOWS NT.

- La filosofía de Microsoft de reducir el costo de propiedad de una red consiste en desarmar los entornos de redes existentes y reemplazarlos con soluciones homogéneas de Microsoft a cualquier costo.
- Windows NT no proporciona una infraestructura de administración o de directorio para múltiples plataformas.
- Las redes de Microsoft requieren presupuestos de sistemas mayores y más personal para manejar los crecientes costos de la administración de múltiples dominios, y más *hardware* y tecnología inmadura.
- Microsoft no está comprometido con Java e incluye un entorno de ejecución Java que no está certificado por Java en un 100%.
- El Microsoft Domains de Windows NT es una tecnología más vieja, con una estructura de base de datos que es plana, en vez de jerárquica.
- No se puede limitar la cantidad de espacio en el disco duro al usuario.
- Es un poco lento como servidor de archivos e impresión.

- Presenta serias dificultades en entornos muy grandes.
- Mientras crece la infraestructura, el costo de NT sube.
- Necesita muchos recursos de cómputo para funcionar correctamente.
- Cualquier cambio a la configuración de NT requiere apagar el sistema y reinicializarlo (cambio de IP, gateway, módem, etcétera.).
- Windows NT es estático, es decir no es posible construir un kernel apropiado.
- Microsoft se está convirtiendo en un monopolio, no en un estándar.

5.1.5 VENTAJAS DE UNIX.

- Sistema multiusuario real, puede correr cualquier aplicación en el servidor.
- Es escalable, con soporte para arquitectura de 64 bits.
- El costo de las diferentes variantes de Unix es muy reducido y algunas son gratis, como FreeBSD y Linux.
- Se pueden activar y desactivar drivers o dispositivos sin necesidad de reiniciar el sistema.
- UNIX puede trabajar con CLI (*Command Line Interface*).
- Los kernels de Unix se confeccionan según las necesidades.
- Ofrece la capacidad de realizar cómputo remotamente.
- Es la mejor solución para enormes bases de datos.
- El sistema operativo Unix viene con el programa Sendmail (gratis).
- Unix contempla cuotas en disco duro.
- UNIX puede trabajar en CLI. También existe una variedad de GUI para cada sistema (OpenLook, X11, etcétera).
- Ofrece una variedad de proveedores (no hay monopolio).
- Es escalable.
- Hace uso de los recursos más eficientemente.
- Permite la administración remota del sistema.
- Ofrece la capacidad de realizar cómputo remotamente.
- Posee capacidad de multiusuarios.
- Existe una gran variedad de software.
- Tiene control sobre el espacio de disco de los usuarios.
- No le afectan los virus de hace 10 años diseñados para MS-DOS.
- Corre en cualquier tipo de plataforma.
- UNIX es dinámico, se puede configurar un kernel apropiado a nuestras necesidades.

5.1.6 DESVENTAJAS DE UNIX.

- La interfase de usuario no es muy amistosa en algunas versiones.
- Requiere capacitación, ya que debido a su complejidad, no cualquiera puede usarlo.
- Padece de la falta de aplicaciones comerciales con nombres importantes.

Cada Sistema Operativo tiene Ventajas y Desventajas, las cuales sin duda alguna las empresas propietarias están estudiando a manera de que su Sistema Operativo sea el mejor del mercado. esta labor es difícil, la lucha incesante por ganar la mayor parte del mercado puede resultar la parte más difícil, a continuación se estudiará el movimiento que han tenido los sistemas operativos dentro de este rubro de la mercadotecnia, además de la posición y crecimiento de estos sistemas operativos en el ámbito mundial, aunando a esto una proyección hacia el año 2003.

5.2 PARTICIPACIÓN EN EL MERCADO DE LOS SISTEMAS OPERATIVOS DE RED.

En estos días de globalización de la economía, las cifras presentadas por compañías de renombre encargadas del análisis, investigación, evaluación y presentación de datos, correspondientes al comportamiento de diversos segmentos del mercado, proporcionan una herramienta indispensable en las decisiones que las empresas toman, al momento de realizar una inversión de cualquier índole.

Debido a que existen varios sistemas operativos de red en el mercado, cada uno procedente de diferentes compañías, es necesario observar la manera en que éstos están posicionados en el gusto del comprador. Para decidir cuál de ellos es el que más conviene a las necesidades presentes y futuras de la empresa, se debe considerar su participación actual en números, así como un pronóstico de las tendencias en los años por venir. Las figuras representativas de la participación de los NOS (Sistema Operativo para Redes) en el mercado, se han tomado de investigaciones realizadas por dos de las compañías más prestigiadas en el campo del análisis de datos para computación e informática: International Data Corporation (IDC) y Computer Intelligence, quienes continuamente realizan sondeos en todo el mundo, para conocer el comportamiento de los productos líderes que marcan la pauta en el desarrollo tecnológico de nuestra sociedad.

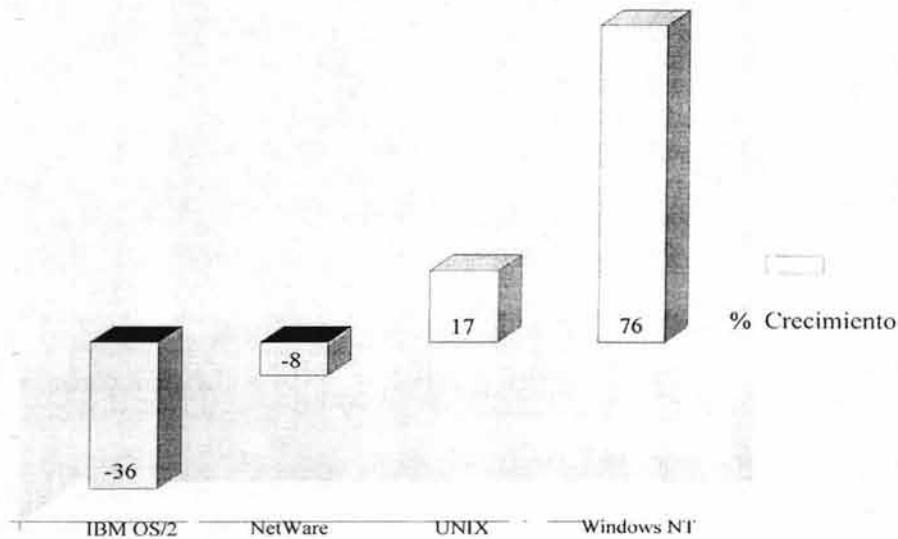
El modelo cliente / servidor se ha convertido en un estándar de las instituciones que desean un sistema robusto y seguro, por lo que los sondeos de mercado para encontrar el sistema operativo de red más requerido con estas características, se han incrementado en los últimos años.

NOVELL® ha sido el principal protagonista en el campo de las redes desde la década de los 80 con sus diferentes versiones de NETWARE®, y aún domina más de la mitad del mercado, donde mantiene gran presencia. Microsoft tuvo un inicio lento con su sistema Windows NT, pero recientemente ha tenido un gran despunte que lo ha llevado a estar en segundo sitio detrás del gigante NOVELL®. Con menos fuerza se reparten lo que resta del mercado el sistema OS/2 de IBM, la solución para redes cliente / servidor AppleShare de Apple y las diferentes variantes de UNIX como Solaris, UnixWare y Linux. La supervivencia de estos sistemas operativos de red, dependerá de la renovación de estrategias tanto productivas como en materia de mercadotecnia en los años por venir, ya que la batalla entre Microsoft y NOVELL® por la supremacía del mercado, parece no querer dejar una tercera opción. A continuación se muestra el mercado de NOS cliente / servidor en 1997 (EE.UU.)

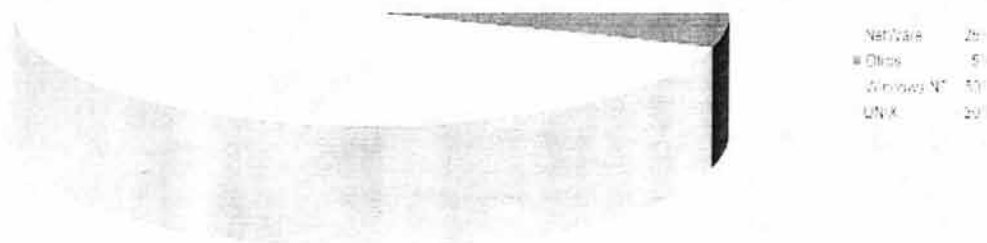


Las necesidades de trabajo en red han causado una demanda muy grande en el área de los NOS, y a la par, las exigencias de parte de los diversos usuarios han hecho que las tendencias en el mercado varíen de manera drástica en muy poco tiempo. Las compañías que dominaban ampliamente la industria de NOS hasta no hace mucho, han sufrido los embates de la competencia de otros poderosos del software, como Microsoft, quien ha sido de los grandes triunfadores en las últimas encuestas.

Han sorprendido en sobremanera los desplomes de NOVELL® e **IBM**, aunque éste último ya había dado muestras de poco crecimiento con su pasiva estrategia mercadotécnica. El resurgimiento de UNIX ha sido una sorpresa agradable y ha puesto los pronósticos sobre el futuro muy inestables para los fabricantes de NOS, pero por otro lado la competencia por ser el mejor en el ramo beneficiará en gran medida al consumidor. En la siguiente gráfica se observa el porcentaje de crecimiento de NOS cliente / servidor en el ámbito mundial en 1997.

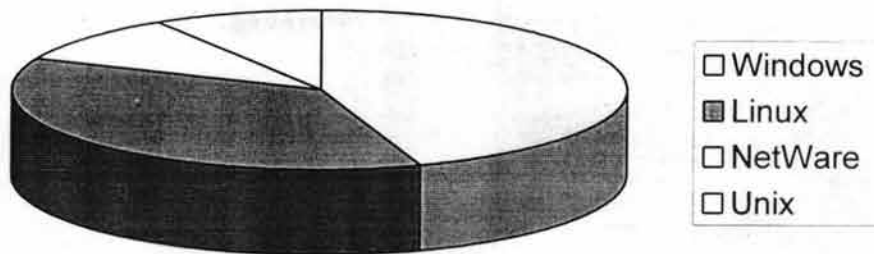


Las tendencias que se encaminaban hacia el año 2000, parecían ser que se inclinaban hacia una solución con Windows NT en sistemas cliente / servidor, superando a NETWARE® de NOVELL® y a las variantes de UNIX, aunque no se descartaba un cambio en los pronósticos dependiendo de cómo les fuera a las nuevas versiones, tanto de NT como de NETWARE®, donde ambas aseguran ser el sistema completo para el siglo XXI. La siguiente figura presenta los pronósticos en los NOS cliente / servidor para el año 2000.



Como se puede observar, Windows NT se posicionó como líder en el mercado de los NOS hacia el año 2000, sin embargo, no se contemplaba en este pronóstico un NOS que venía creciendo de manera exponencial, dicho NOS es LINUX, no importando su derivante, éste ha desarrollado una popularidad impresionante, lo que ha provocado que se le considere como un oponente más en este ámbito de los Sistemas Operativos.

A continuación, se presenta un estudio de la proyección de los Sistemas Operativos hacia el año 2003, en este se puede observar el amplio respeto que se está considerando sobre Linux, debido al enorme crecimiento de éste.



En la gráfica anterior vemos el crecimiento de Windows y Linux además de la caída de NETWARE® y Unix. Es importante considerar que esto es solo una estimación y de ningún modo significa ni se afirma que así será en realidad, esto depende de muchos factores más.¹³

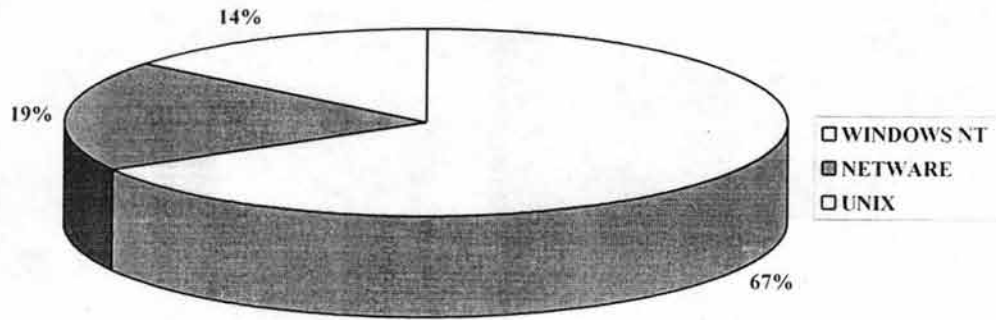
5.3 ESTUDIO COMPARATIVO BASÁNDOSE EN UN MUESTREO EN PEQUEÑAS Y MEDIANAS EMPRESAS (PYMES) DEL VALLE DE MÉXICO.

Se realizó para los fines de este trabajo un muestreo con 60 PYMES ubicadas en el Valle de México, dicho muestreo se basa en la administración de los Sistemas Operativos, apoyándose en las facilidades con las que cuenta dichos Sistemas para la administración, cabe mencionar que el estudio no se realizó con una profundidad técnica de los Sistemas si no desde el punto de vista de los administradores basándose en su capacitación y experiencia.

Se llevaron a cabo 42 entrevistas, en algunas empresas se realizaron varios cuestionarios debido a que existía más de un administrador de red. A continuación se presenta la gráfica que simboliza la preferencia de los Sistemas Operativos en las empresas participantes.

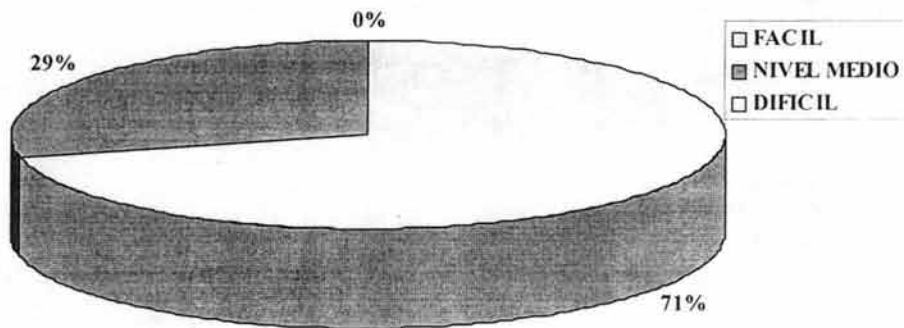
¹³ Selección de un sistema operativo, Espinoza Curiel M. Selección de un Sistema Operativo, En línea [URL], <http://www.geocities.com/SiliconValley/8195/selec.html#temas>

PREFERENCIAS DEL SISTEMA OPERATIVO

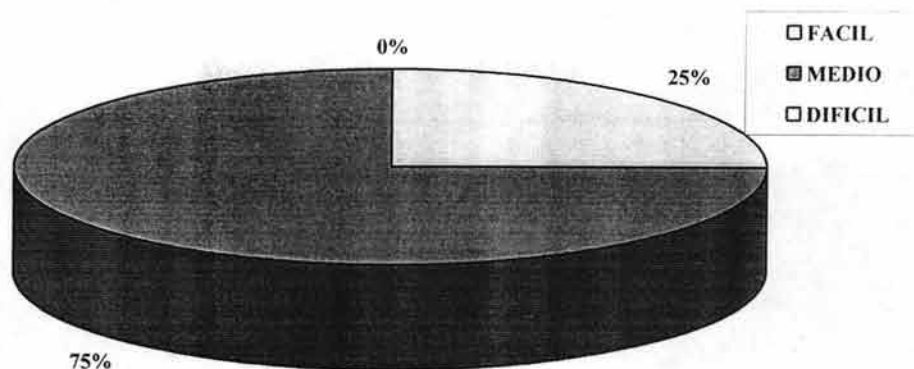


Como siguiente punto se muestran las graficas que exponen la opinión de los administradores con respecto a la dificultad que encontraron en la instalación de los Sistemas Operativos.

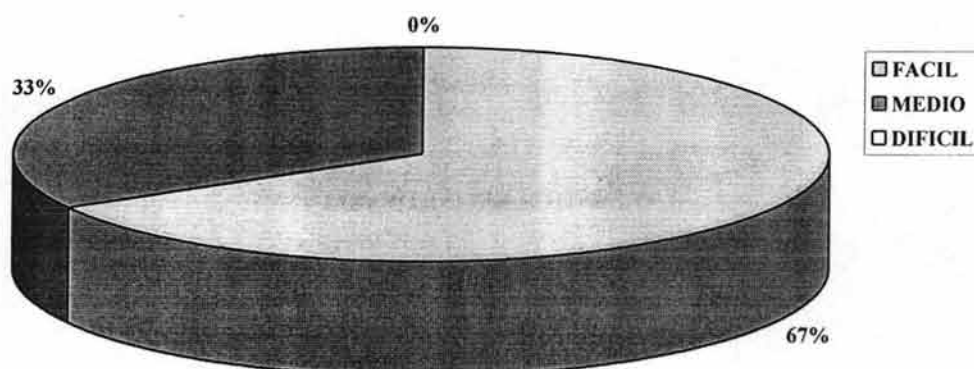
INSTALACION DE WINDOWS NT (28 CUESTIONARIOS)



INSTALACION (NETWARE)



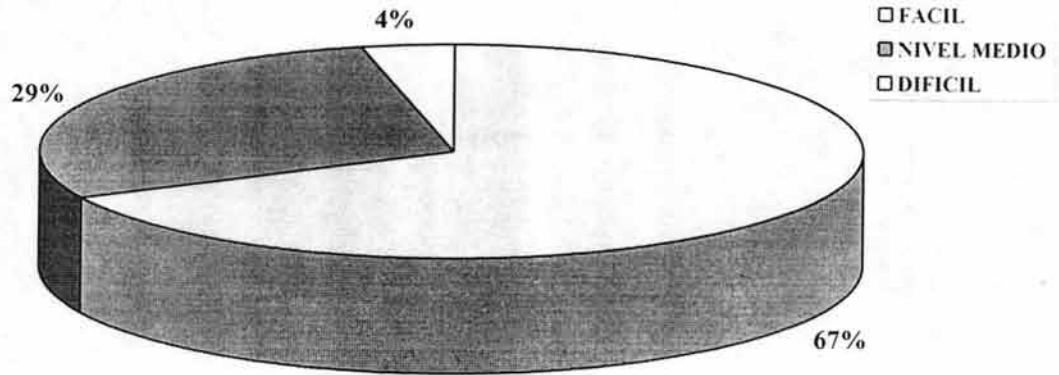
INSTALACION (UNIX)



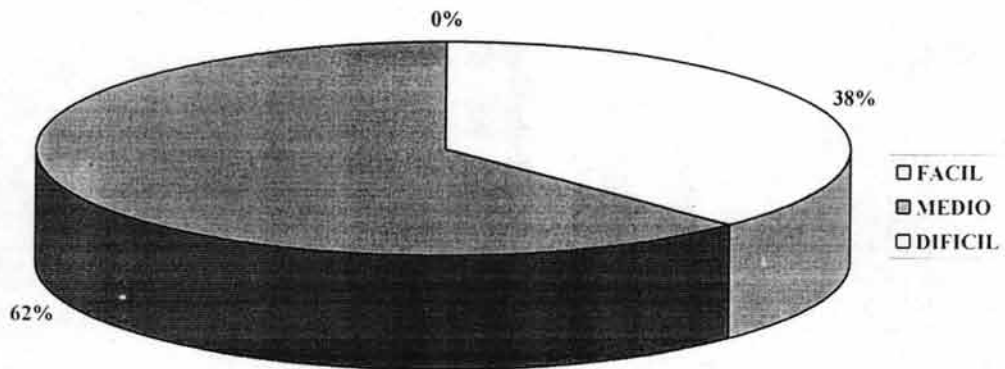
Como se puede observar en las tres gráficas el Sistema más fácil de instalar es Windows NT tomando en cuenta que los porcentajes están expresados por Sistema Operativo. Con el 71% de los administradores de este sistema a favor, en segundo lugar encontramos a Unix con el 67% y como ultimo lugar a NETWARE® con el 25%.

En el segundo estudio realizado se toma en cuenta la complejidad de la administración de los Sistemas Operativos basándose en el punto de vista de los administradores encuestados.

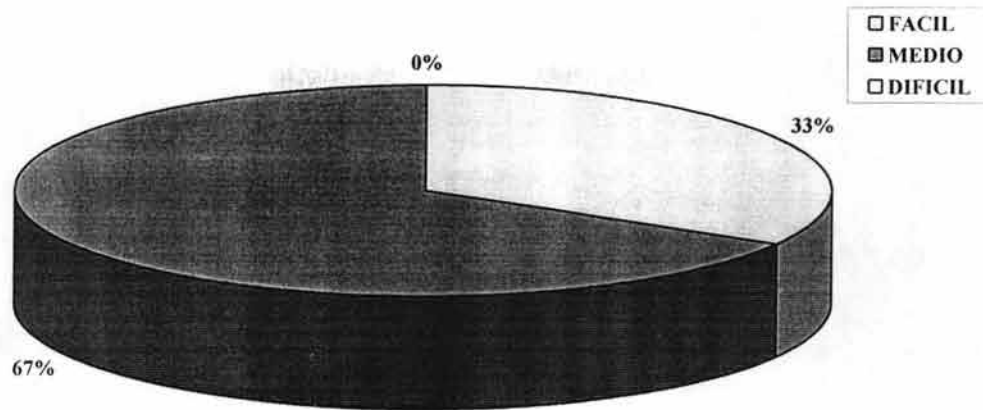
ADMINISTRACION DE WINDOWS NT
(28 CUESTIONARIOS)



ADMINISTRACION (NETWARE)



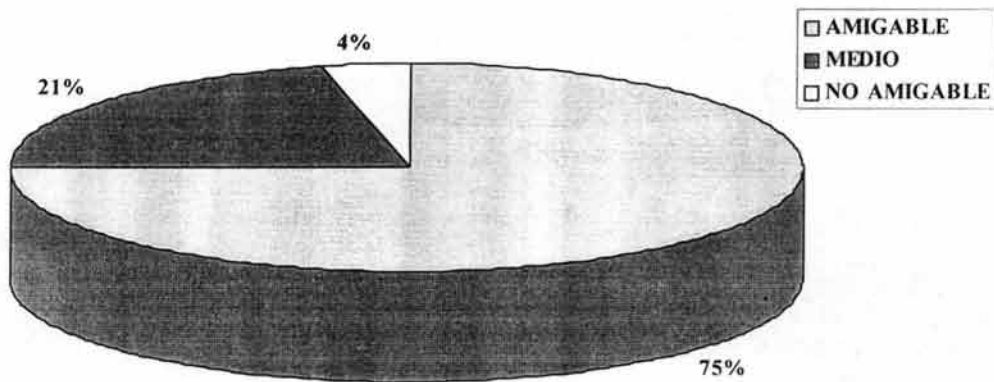
ADMINISTRACION (UNIX)



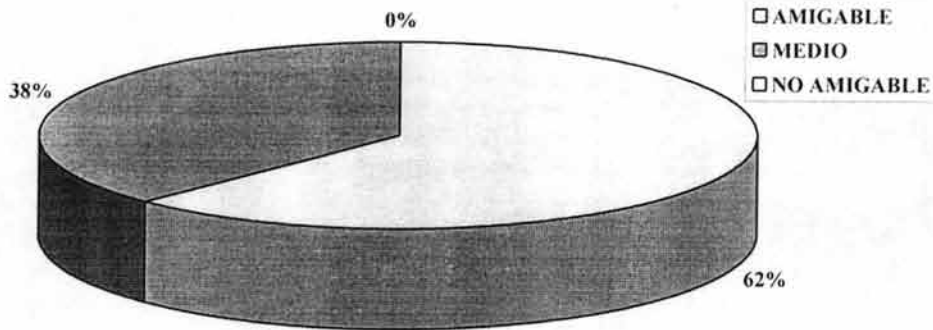
En lo referente a la resultante de la administración, se denota que Windows NT es el más fácil de administrar con el 67% de los entrevistados a favor, en segundo lugar se encuentra NETWARE® con el 38% y Unix en tercer lugar con el 33%.

Continuando con los resultados de las entrevistas, ahora se presenta la resultante en cuanto a interfaces de comunicación se refiere.

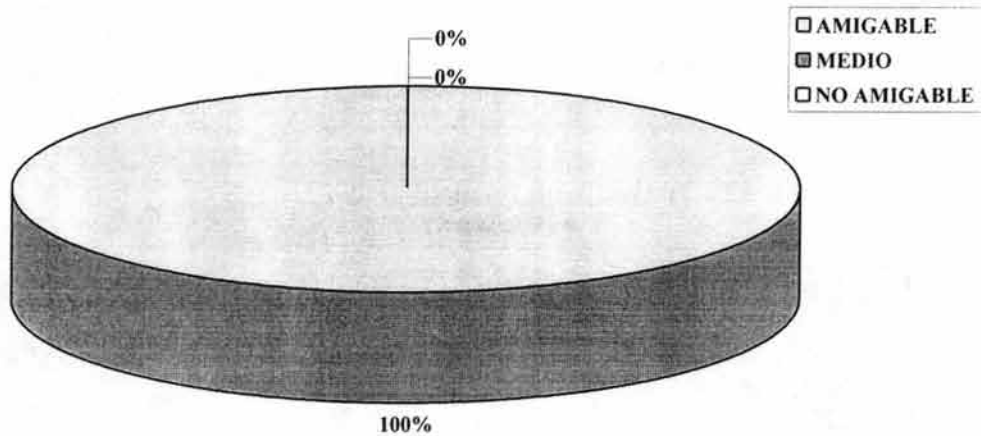
INTERFASE DE COMUNICACIÓN WINDOWS NT



INTERFASE DE COMUNICACION (NETWARE)



INTERFASE DE COMUNICACION (UNIX)

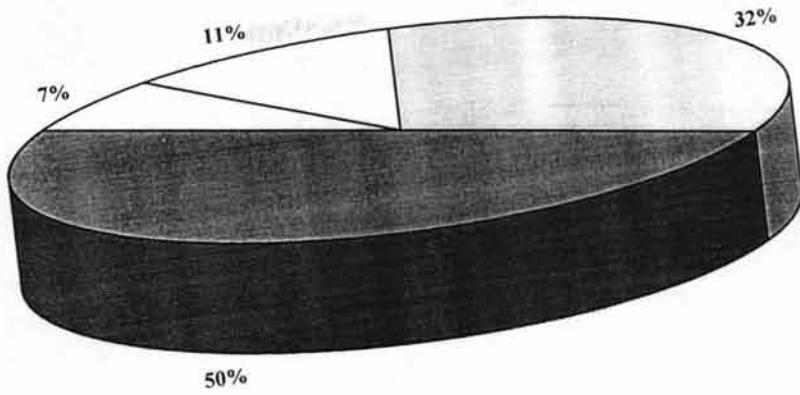


En las gráficas anteriores se puede observar un fenómeno no muy común pero quién llevó la delantera en cuanto a lo amigable de su interfase de comunicación fue Unix con el 100% de los entrevistados, es importante mencionar que los entrevistados administran Unix con alguna interfase gráfica de apoyo y no por línea de comando como se pudiera pensar en un principio, en segundo lugar quedó Windows NT con el 75% y en tercero NETWARE® con el 62%.

Ahora se analizará en las siguientes gráficas el punto de vista de los administradores en cuanto a servicios web se refiere.

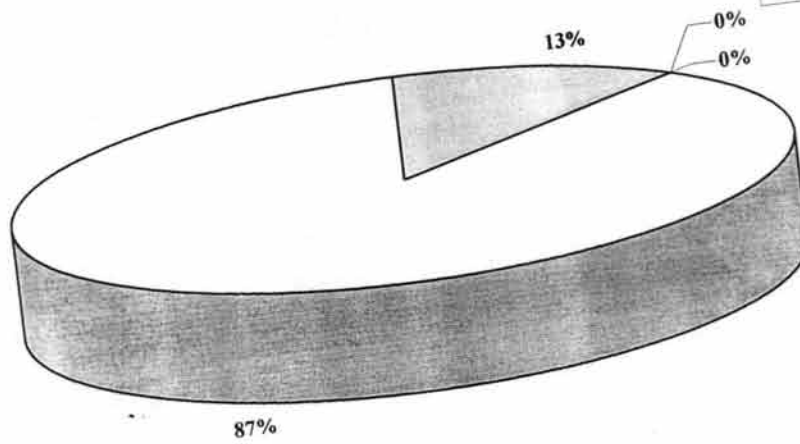
SERVICIOS WEB

- EFICIENTES
- MEDIO
- DEFICIENTES
- PROXY

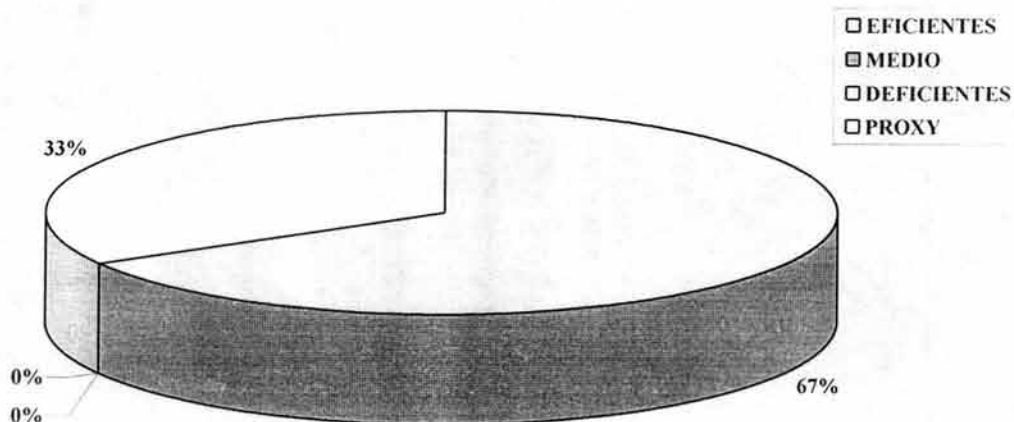


SERVICIOS WEB (NETWARE)

- EFICIENTES
- MEDIO
- DEFICIENTES
- PROXY



SERVICIOS WEB (UNIX)



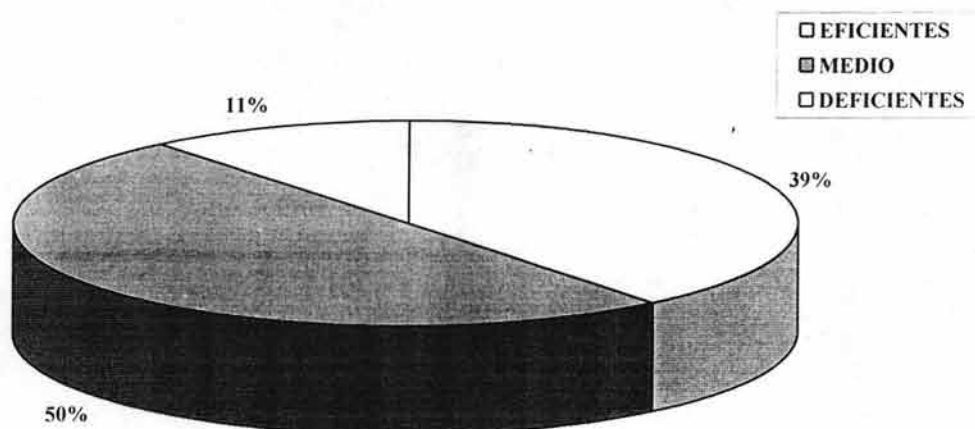
En estas gráficas se evalúa la capacidad de los servicios web de los Sistemas operativos desde el punto de vista de los administradores de redes, en cuanto Windows NT el 50% de los entrevistados consideran que el servicio web tiene un nivel medio de eficiencia, el 32% opina que es eficiente, el 7% opina que es deficiente y el 11% opina que se apoyan en un proxy externo al sistema.

En lo que a NETWARE® concierne el 13% de los administradores consideran que los servicios web son eficientes, el 87% restante utilizan un proxy externo como apoyo.

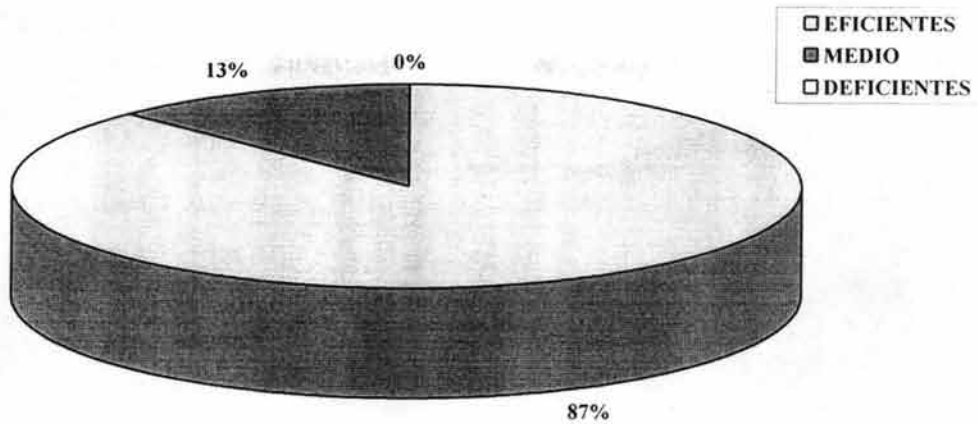
Y finalmente, analizando los resultados de Unix el 67% de los administradores opina que los servicios web de Unix son eficientes y la parte complementaria utiliza un proxy externo como apoyo.

Continuando con las gráficas representativas, ahora se presenta en estudio realizado con respecto a la eficiencia de los controles de seguridad de los Sistemas Operativos.

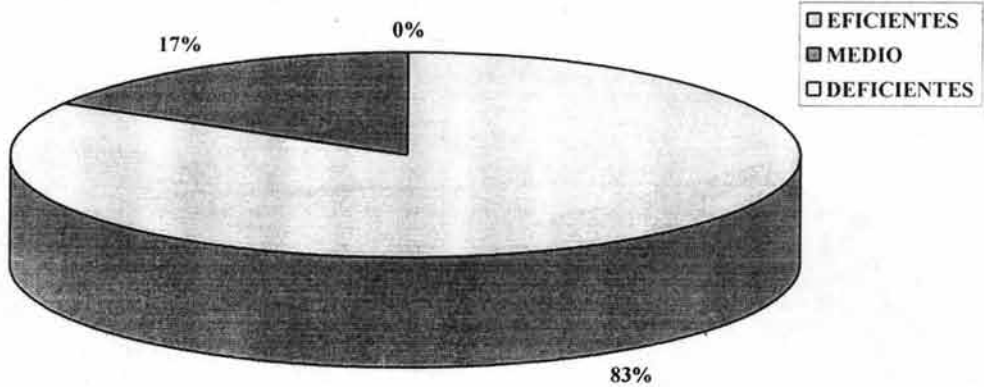
CONTROLES DE SEGURIDAD



CONTROLES DE SEGURIDAD (NETWARE)



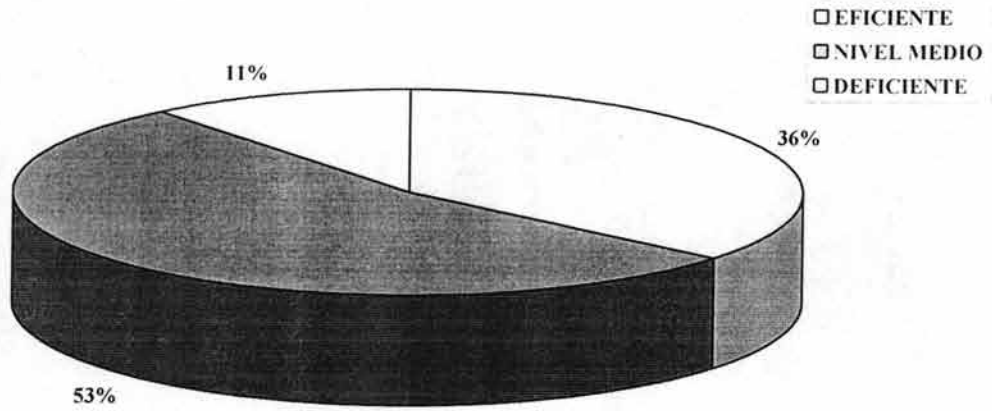
CONTROLES DE SEGURIDAD (UNIX)



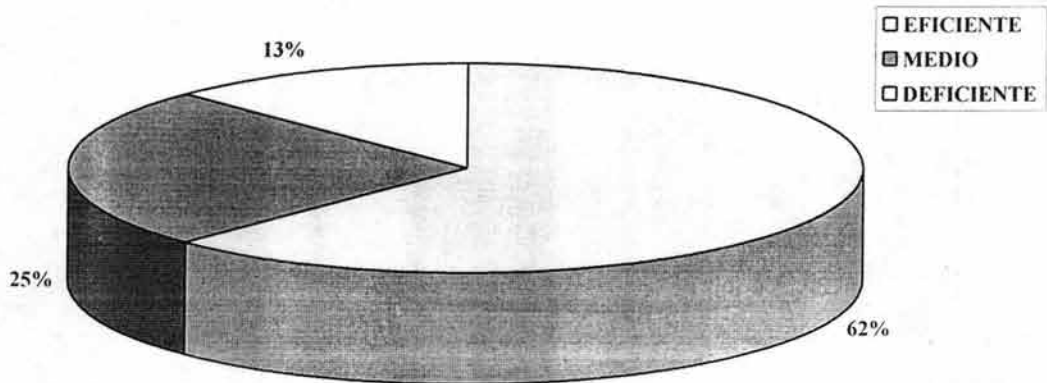
En estas gráficas encontramos en la delantera a NETWARE® con el 87% de votos a su favor, en segundo lugar esta Unix con el 83% y Windows NT se encuentra en último lugar con el 39%, deduciendo de esta manera según los administradores de redes participantes, que Windows NT es el Sistema Operativo con controles de seguridad menos eficientes.

A continuación, se presenta el estudio realizado a los módulos de respaldo de los Sistemas Operativos, midiendo en las siguientes gráficas su eficiencia.

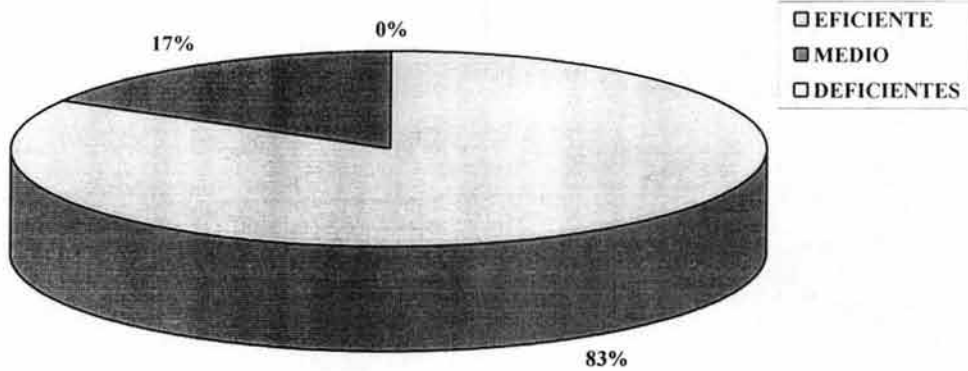
MODULO DE RESPALDO (NT)



MODULO DE RESPALDO (NETWARE)



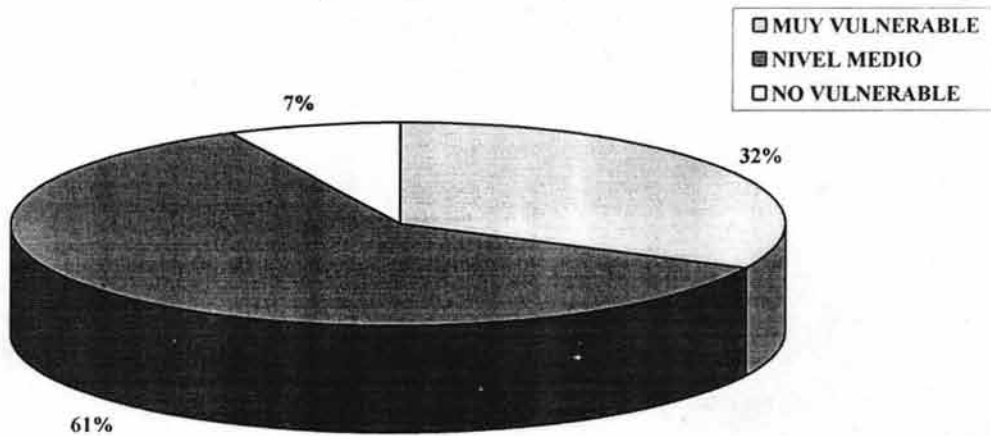
MODULO DE RESPALDO (UNIX)



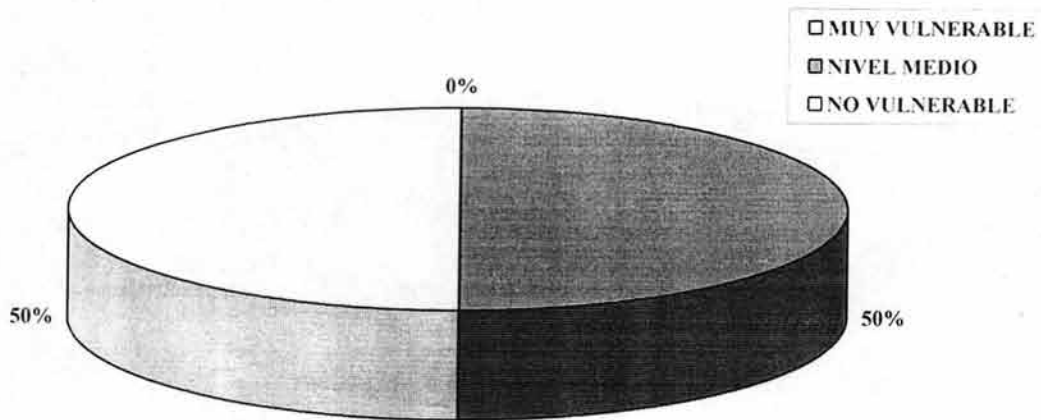
En las anteriores gráficas se puede observar que Unix ocupa el primer lugar con el 83%, en segundo lugar encontramos a NETWARE® con el 62% y por último tenemos a Windows NT con el 36%.

Ya como último punto del estudio, se analiza la vulnerabilidad de los Sistemas Operativos en cuanto a seguridad ante virus y *hacker's* se refiere.

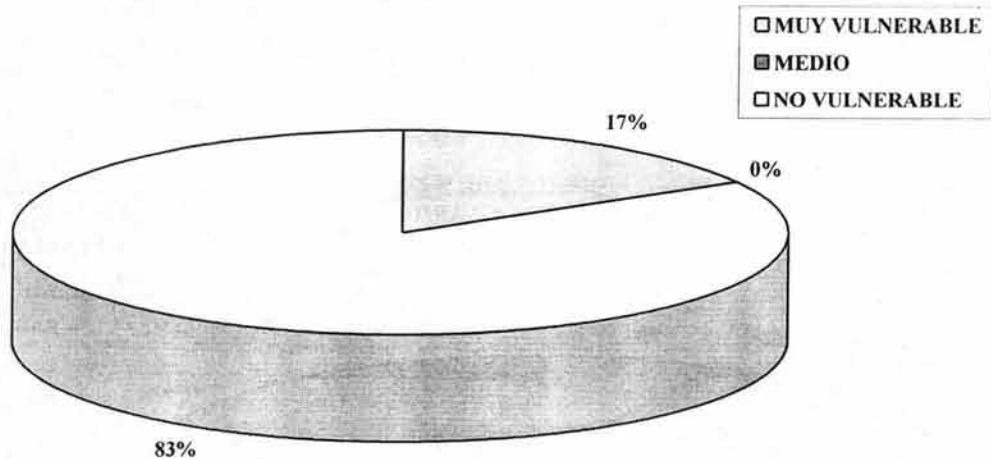
VULNERABILIDAD DE WINDOWS NT (28 CUESTIONARIOS)



VULNERABILIDAD DE NETWARE



VULNERABILIDAD (UNIX)



En las gráficas anteriores se puede analizar que Unix ganó terreno en este rubro con el 83% de los administradores de Unix entrevistados opinando que no es vulnerable, en segundo lugar se encuentra NETWARE® con el 50% y en tercer lugar quedó Windows NT con el 7%.

El horizonte y los límites de la investigación se han fijado de manera que se permita presentar información tecnológica útil para un administrador de redes, al mismo que tiempo que se presenta el enfoque administrativo y no técnico a detalle.

Durante el análisis de estas gráficas se pueden encontrar resultados que tal vez van en contra de lo que supuestamente se debería de obtener. sin embargo es parte de un muestreo real en el Valle de México y no de opinión propia.

Es importante mencionar que se tuvieron algunas dificultades para poder conseguir entrevistas con los administradores de las redes, en primer lugar, que no tenían mucho tiempo, en segundo lugar pensaban que se trataba de una auditoria, este tipo de obstáculos dificultó en cierta forma un análisis más detallado del estudio.

Se obtuvo que al preguntarle a los administradores encuestados qué porcentajes de conocimiento tenían sobre su sistema operativo algunos contestaban que el 100%, 90%, 80%, no se sabe si realmente es verdad, pero se deduce que no fueron tan reales al contestar, debido que muchas veces hasta los administradores certificados en algún producto no dominan al 100% un sistema operativo debido al amplio ramo de conocimientos que se deben de tener para administrar completamente el SO.

Cabe señalar que aproximadamente el 85% de las empresas en el Valle de México y en la Republica Mexicana son PYMES¹⁴, esto tiene como consecuencia que no se capacite al nivel de certificación a los administradores de redes, la mayoría de los administradores han aprendido desde su formación académica, en pequeños cursos básicos, o a través de la experiencia que obtienen en alguna empresa que maneja algún Sistema Operativo.

5.4 UNA VISION A OTROS COMPARATIVOS.

5.4.1 ESTUDIO COMPARATIVO ENTRE SISTEMAS OPERATIVOS (POR CENTENIAL NETWORKING LABS).¹⁵

A continuación se presenta un comparativo de los Sistemas Operativos que realmente tienen presencia en el mercado en el ámbito mundial, es importante mencionar que en este estudio se considera a Windows 2000 Server , NETWARE® 5.1 de NOVELL®, Unixware 7.1.1 de SCO y Linux 6.1 de Red Hat Software, esto como parte de la actualización de Windows NT, NETWARE® 5 de NOVELL® y Unix SCO respectivamente; esto a consecuencia de la rápida evolución de los Sistemas Operativos durante la elaboración del presente trabajo, se considera que es conveniente tomar en cuenta estas evoluciones y compararlas para que se tenga una visión actualizada de los Sistemas Operativos.

En lo que se refiere a sistemas operativos de red, existen en el mercado productos para cada tipo de necesidad. Así quedó patente en el comparativo realizado para IDG Communications por Centennial Networking Labs de la North Carolina State University con Windows 2000 Advanced Server de Microsoft, NETWARE® 5.1 de NOVELL®, Linux 6.1 de Red Hat Software y UnixWare 7.1.1 de The Santa Cruz Operation (SCO). Aunque NETWARE® ganó en cuanto a rendimiento, Windows 2000 resultó ser superior globalmente.

Todo se reduce a lo que se espera de un sistema operativo de red. Si lo que se busca es un sistema tan flexible que pueda instalarse de cualquier modo que se desee, quizá habrá que centrarse en las cuestiones de administración y gestión. Puede, sin embargo, que lo que se pretenda es obtener un sistema operativo que sea lo suficientemente robusto como para no preocuparse demasiado de él. Por suerte, hoy el mercado cubre toda clase de necesidades.

En las pruebas realizadas por Centennial Networking Labs para IDG -en las que Sun declinó participar aduciendo que en estos momentos prepara una nueva versión de Solaris- Windows 2000 fue el ganador gracias a su interfase de gestión, herramientas de monitorización del servidor, funciones de gestión de almacenamiento y medidas de seguridad. Sin embargo, en rendimiento no pudo superar a NETWARE® 5.1 en las exhaustivas pruebas de red y de servicio de ficheros. Con su administración basada en NDS y su excelente rendimiento, el producto de NOVELL® representa una muy buena solución para una red corporativa.

¹⁴ Moreno J. y Osorio C. Artículo estadístico Informático de México, En línea [URL], <http://www.chein.com.mx/articulos/4mar-2002.htm>

¹⁵ Badas Cañabate, J y Vélez Isasmendi, I. Sistemas Informáticos en Tiempo Real. Escuela Superior de Ingenieros Industriales, Universidad de Navarra. España

Por detrás se situó la última versión del Linux comercial de Red Hat, del que hay que destacar la flexibilidad de su diseño modular, que permite, entre otras cosas, crear scripts de múltiples comandos para automatizar tareas a través de un entorno distribuido.

Aunque UnixWare de SCO no sobresalió por su rendimiento en servicios de ficheros y en características de administración, su escalabilidad le convierte en un fuerte candidato para correr aplicaciones de empresa.

Instalación de los sistemas operativos de red

	Tiempo de instalación	Comentarios
Red Hat Linux	30 minutos	Soporta instalaciones remotas de clientes.
Windows 2000 Advanced Server	30 a 45 minutos	Realiza consultas de todos los aspectos de la instalación.
NETWARE®	30 a 45 minutos	La modificación de los archivos de configuración de red requiere reiniciar.
UnixWare	1,5 a 2 horas	Los confusos <i>scripts</i> de instalación son difíciles de usar.

5.4.1.1 SERVICIOS DE FICHEROS Y DE RED.

Con independencia de la tarea a la que se vaya destinar el servidor, tendrá que tener un buen rendimiento a la hora de leer y escribir ficheros y enviarlos por la red. Para la evaluación se diseñaron dos conjuntos de pruebas para medir ambas categorías en cada sistema operativo de servidor. Para reflejar un entorno de producción real, las pruebas tenían en cuenta un amplio rango de condiciones de servidor.

NETWARE® fue el líder en la evaluación del rendimiento, ocupando el primer lugar en las dos terceras partes de las pruebas de ficheros y en todos los de red. El Linux de Red Hat siguió a NETWARE® en el rendimiento total de ficheros e incluso le desplazó en las pruebas donde las cargas de lectura / escritura eran pequeñas. Sin embargo, no rindió bien al tratar grandes cargas, es decir, en aquellas pruebas con más de cien usuarios. En estos casos, el producto manifestaba una clara tendencia a detener el servicio de peticiones de ficheros durante un corto periodo de tiempo, transcurrido el cual volvía a comenzar de nuevo.

Windows 2000 demostró un rendimiento modesto en cuanto a escritura de ficheros. De hecho, obtuvo un resultado que suponía el 10% del rendimiento conseguido en lectura. Después de consultar con Microsoft, se llegó a la conclusión de que esto podría ser debido a la existencia de un posible problema de rendimiento con el driver SCSI para el *hardware* utilizado. Pero no se pudo constatar este extremo.

Más significativa fue, sin embargo, una cuestión que se produjo con el software de prueba empleado. El *Benchmark Factory* utilizado envía una señal de escritura en cada una de sus peticiones para que el servidor actualice la caché, si resulta apropiada, y entonces forzar una escritura al disco. Cuando ésta se produce, la llamada de escritura es liberada y puede ser enviada la siguiente petición.

A primera vista parecía como si Windows 2000 fuera el único sistema operativo en cumplir esta señal de escritura debido al tan pobre rendimiento obtenido. Así que se procedió a realizar una segunda ronda de pruebas de escritura con el sistema de señal desactivado. En estas circunstancias, el rendimiento de escritura de NETWARE® se incrementó un 30%, escribiendo en el disco de un modo más eficiente al tratar en conjunto bloques contiguos de datos en la caché y escribir todos ellos en el disco de una sola vez.

Asimismo, en esta modalidad el rendimiento del Linux de Red Hat se incrementó entre un 10% y un 15%. Cuando se examinó el código de sistema de ficheros Samba, se encontró que tiene un tiempo óptimo durante la secuencia de lectura / escritura para escribir en el disco.

Esta segunda ronda de pruebas demostró que Windows 2000 depende de su caché del sistema de ficheros para optimizar el rendimiento de escritura. Los resultados sin escritura a través de señal fueron mucho mayores; concretamente, hasta 20 veces más rápidos. Sin embargo, aun en esta modalidad quedó por debajo de NETWARE® y Linux.

SCO potencia la escritura a través de señal por defecto, puesto que su sistema de ficheros está construido para maximizar la integridad de los datos mediante la escritura en el disco de todas las peticiones. Los resultados con señal y sin señal de escritura fueron muy similares.

Para las pruebas de red, se realizaron dos tandas de pruebas. Una transacción TCP larga medía el ancho de banda que puede soportar el servidor, mientras que una transacción TCP corta evaluaba la capacidad de cada servidor para manejar números elevados de sesiones con transacciones de ficheros pequeñas.

En esta ronda de pruebas, Windows 2000 logró los mejores resultados con las transacciones TCP largas. Tanto el producto de Microsoft como UnixWare disponen de pilas IP que les permiten tratar peticiones de red con múltiples procesadores. NOVELL® y Red Hat aseguraron estar trabajando para integrar también esta funcionalidad en sus productos.

NETWARE® y UnixWare ocuparon el segundo y tercer puesto, respectivamente, en las pruebas de transacciones TCP largas.

En las pruebas con transacciones TCP cortas, NETWARE® fue el claro vencedor, seguido por Linux, pese a carecer de la función por la que se puede rápidamente deshacer conexiones TCP fracasadas; una posibilidad que utiliza el software de pruebas utilizado, Chariot de Ganymede Software.

Puntuaciones

	Microsoft Windows 2000 Advanced Server	NOVELL® NETWARE® 5.1	Red Hat Linux 6.1	SCO UnixWare 7.1.1
Pruebas de rendimiento				
Servicios de archivos (15%)	5,6	9,4	6,7	3,3
Red (10%)	8,4	9,6	7,4	7,5
Administración / gestión				
Interfase de gestión (5%)	8	8	5	7
Monitorización de servidor (5%)	8	6	6	6
Administración de clientes (5%)	7	8	4	6
Gestión de archivos / impresoras (5%)	8	8	5	6
Gestión de almacenamiento (5%)	9	7	6	5
Escalabilidad (20%)	8	5	6	8
Seguridad (10%)	9	8	7	5
Estabilidad y tolerancia a fallos (10%)	8	6	7	7
Instalación (5%)	9	7	8	3
Documentación (5%)	7	8	6	8
Puntuación total (100%)	7,78	7,61	6,35	6,10

5.4.1.2 GESTIÓN.

A medida que las empresas crecen, requieren más servidores y un mayor soporte de usuarios finales. Es aquí donde las herramientas de gestión de los sistemas operativos de servidor se vuelven cruciales para mantener las redes bajo control. En la evaluación se examinaron las interfases de gestión de cada producto y cómo cada servidor trata la monitorización, la administración de cliente, la gestión de ficheros e impresión y la gestión de almacenamiento.

Tanto NETWARE® como Windows 2000 proporcionan interfaces de gestión muy útiles. Microsoft Management Console (MMC) es la utilidad que unifica la mayor parte de la gestión de Windows 2000. Esta interfase gráfica configurable permite trabajar con applets de Microsoft y de terceros que personalizan su funcionalidad. Se trata de una interfase similar a Windows Explorer, con una lista anidada en la parte izquierda y detalles de selección en la derecha.

La consola es fácil de usar y permite configurar un buen número de elementos de servidor local, incluyendo usuarios, discos y sistema, para establecer, por ejemplo, horario y fecha. MMC permite, además, implantar políticas de gestión para grupos de usuarios y ordenadores utilizando Active Directory, el nuevo servicio de directorio de Microsoft. Desde la herramienta de gestión de Active Directory que está dentro de MMC, se puede configurar usuarios y cambiar políticas.

Las herramientas de configuración de red se encuentran en una aplicación distinta que se abre cuando se hace "click" en el icono *Network Places* de la sobremesa. Dentro de esta ventana se lista cada interfase de red, y se puede añadir y cambiar protocolos, así como configurar, activar y desactivar interfaces sin tener que reiniciar.

NETWARE®, por su parte, ofrece varias interfaces de gestión y configuración de servidor. Estas herramientas proporcionan doble funcionalidad, útil cada una en función del lugar donde se encuentre el administrador a la hora de gestionar el sistema. System Console aporta herramientas de configuración de servidor, de las que NWConfig resulta de las más útiles al permitir cambiar ficheros, instalar módulos del sistema y configurar el subsistema de almacenamiento. NWConfig es simple, intuitivo y predecible.

ConsoleOne® es una interfase basada en Java con unas cuantas herramientas gráficas para gestionar y configurar NETWARE®. Admite herramientas de administración de terceros y permite gestionar múltiples servicios. NOVELL® proporciona, asimismo, una aplicación de gestión accesible vía Web llamada NETWARE® Management Portal que permite gestionar servidores NETWARE® remotamente desde un navegador. También cuenta con NWAdmin32, una herramienta cliente relativamente simple para administrar NDS (NOVELL® Directory Services) desde un puesto Windows 95, 98 o NT.

La interfase de gestión de sistemas de Red Hat, denominada LinuxConf, puede correr como una aplicación gráfica o basada en texto. La interfase gráfica, que recuerda a MMC, funciona bien pero a veces su uso resulta algo complicado. Por ejemplo, algunas aplicaciones se muestran en un tamaño superior al de la pantalla de la sobremesa.

Con todo, desde LinuxConf se puede gestionar perfectamente casi cualquier cosa, y se puede utilizar en modo local o remoto por la Web o vía Telnet. Es posible configurar parámetros del sistema como direcciones de red y establecer sistemas de ficheros y cuentas de usuario, así como servicios adicionales como Samba -que permite a los clientes Windows acceder a ficheros residentes en servidores Linux- y servidores FTP y Web. La realización de los cambios no exige reiniciar el equipo.

Por encima de todo y pese a su apariencia, la interfase de Red Hat resulta de gran utilidad, con unas herramientas subyacentes potentes y flexibles.

SCOAdmin consiste en una funcionalidad "*front-end*" basada en interfase gráfica que da servicio a alrededor de 50 herramientas de gestión y configuración de UnixWare. Cuando se hace "click" en una de ellas, aparece en una ventana la aplicación correspondiente. Algunas de las herramientas de SCO están basadas en interfase gráfica mientras que otras se basan en texto. Y, aunque para efectuar determinados cambios fue necesario reiniciar el servidor, SCOAdmin permite gestionar múltiples servidores UnixWare.

SCO ofrece, además, una muy útil herramienta de administración remota basada en Java, denominada WebTop, que funciona desde un navegador.

5.4.1.3 MONITORIZACIÓN DE LOS SERVIDORES.

Dentro de la administración, una tarea de las más importantes es la monitorización interna del servidor, un área donde destaca Microsoft. Windows 2000 System Monitor permite ver gráficos en tiempo real de operaciones del sistema tales como utilización de la red y de la CPU, y nivel de uso del disco y de la memoria. En la evaluación se utilizaron estas herramientas para determinar el efecto de las pruebas en el sistema operativo. Otra herramienta, llamada Network Monitor, dispone de un analizador de paquetes básico que permite ver los tipos de paquetes que entran en el servidor. Con ambas utilidades juntas es posible medir y comparar el rendimiento y la capacidad a través de múltiples servidores Windows 2000.

La utilidad Monitor de NETWARE® muestra la utilización del procesador, de la memoria y del buffer de un servidor local. Sabiendo qué buscar, es ésta una poderosa herramienta a la hora de diagnosticar cuellos de botella en el sistema. Sin embargo, aprender el significado de cada uno de los parámetros monitorizados lleva su tiempo. Además, *Web Management Portal* permite realizar estadísticas de rendimiento de múltiples servidores.

Para monitorizar el servidor, Red Hat ofrece las herramientas de línea de comandos que ofrece en este campo el Linux estándar, como "iostat" y "vmstat". Como sucede con cualquier sistema operativo Unix, es posible escribir *scripts* para automatizar dichas herramientas a través de servidores Linux. Sin embargo, estas herramientas resultan demasiado crípticas y usarlas eficazmente requieren una gran experiencia.

UnixWare, por su parte, proporciona diferentes herramientas de monitorización. System Monitor es una simple pero limitada interfase gráfica para monitorizar los procesadores y el uso de la memoria. Juntas, las líneas de comandos "sar" y "rtpm" ofrecen el nivel de utilización del buffer, de las CPU y de los discos, aportando una idea muy aproximada del grado de carga del servidor.

5.4.1.4 ADMINISTRACIÓN DE LOS CLIENTES.

No es sorprendente que los dos sistemas operativos de red que vienen de origen con un servicio de directorio integrado ocupan los mejores puestos en lo que se refiere a las pruebas de las herramientas de administración de clientes.

Tanto con Active Directory de Microsoft como con la administración de directorio de MMC fue posible configurar permisos de usuario. Asimismo, permiten agrupar usuarios y ordenadores en unidades organizacionales y aplicar las políticas.

Para gestionar clientes NETWARE® y NDS se puede utilizar ConsoleOne®, NW Admin o NETWARE® Management Portal. Cada una de estas utilidades permite crear usuarios, gestionar espacios de ficheros y establecer permisos y privilegios. Adicionalmente, NETWARE® viene con una versión de cinco usuarios de la herramienta ZENworks de NOVELL®, que ofrece servicios de administración de sobremesas (como inventario de *hardware* y software), distribución de software y servicios de control remoto.

El Linux de Red Hat no aporta demasiado en este apartado. Los usuarios se han de controlar localmente mediante los mecanismos de configuración de permisos de Unix.

UnixWare es muy similar a Linux en cuanto a administración de clientes, pero SCO proporciona algunos binarios Windows en el servidor para establecer remotamente permisos de ficheros y directorio desde un cliente Windows, así como para crear y cambiar usuarios y sus configuraciones.

SCO y Red Hat ofrecen soporte de *Network Information Service* (NIS), basado en Unix. NIS actúa como un almacén de información de red relativa a aspectos como contraseñas y nombres de acceso y directorios, información que, al estar integrada, resulta de gran utilidad.

5.4.1.5 FICHEROS E IMPRESIÓN.

Nada es un sistema operativo de red sin sus prestaciones de compartición de ficheros e impresoras. Y también en esta área Microsoft y NOVELL® se colocaron a la cabeza.

En Windows 2000 resulta muy sencillo añadir y mantener impresoras mediante el "wizard" de administración de impresión, y es posible añadir compartición de ficheros usando las herramientas de gestión de Active Directory. El sistema operativo ofrece además *Distributed File Services*, que permite combinar ficheros que residan en más de un servidor en una compartición única.

NOVELL® Distributed Print Services (NDPS) incorpora rápidamente impresoras a la red. Cuando detecta una nueva impresora, define un *Printer Agent* que corre sobre ella y se comunica con NDS, de modo que se puede utilizar el servicio de directorios para definir sus políticas.

Red Hat incluye la utilidad "printtool" de Linux para establecer impresoras de red conectadas a un servidor. Esta interfase gráfica se puede utilizar también para crear entradas "printcap" a fin de definir accesos de impresora.

Linux cuenta con herramientas de configuración del sistema de ficheros basadas en líneas de comandos para crear y eliminar particiones. Además, Samba proporciona ciertos niveles de integración para clientes Windows. Es posible configurar Samba mediante una rudimentaria herramienta basada en Web y denominada "swat".

UnixWare aporta una flexible herramienta de establecimiento de impresoras basada en interfase gráfica llamada *Printer SetUp Manager*. Para la gestión de volúmenes y ficheros, SCO ofrece la herramienta VisionFS, que permite a los clientes NT acceder al servidor UnixWare. Este servicio resulta muy sencillo de configurar y usar.

5.4.1.6 GESTIÓN DEL ALMACENAMIENTO.

Windows 2000 proporciona las mejores herramientas de gestión de almacenamiento. Su herramienta gráfica Manage Disk para la configuración del disco local incluye gestión RAID, de modo que se puede añadir dinámicamente discos a un volumen determinado sin tener que reiniciar el sistema. Adicionalmente, en cada uno de los discos de un "array" se escribe una firma que permite moverlo a otro servidor 2000 sin tener que configurar su volumen. El nuevo servidor reconoce los discos como miembros de un conjunto RAID y añade dinámicamente el volumen al sistema de ficheros.

NWConfig -la herramienta de gestión de volúmenes de NETWARE®- es muy sencilla de usar, pero puede resultar algo confusa a la hora de establecer un volumen RAID. Una vez que se conoce el mecanismo, no aparecen problemas en la inicialización de los discos y en la creación de volúmenes RAID. La herramienta tiene una apariencia un tanto primitiva, pero resulta de gran sencillez y funcionalidad.

El Linux de Red Hat no proporciona herramientas de configuración RAID gráficas, pero sus herramientas de líneas de comandos realizan la tarea fácilmente.

Para configurar discos en el servidor UnixWare, se utilizó la herramienta gráfica de administración de volúmenes de discos Veritas Volume Manager del sistema operativo. Inicialmente, aparecieron algunos problemas a la hora de que la herramienta reconociera los discos al momento de ser inicializados; problemas que desaparecieron al usar una función de las herramientas de línea de comandos.

5.4.1.7 SEGURIDAD.

Aunque los sistemas operativos no se probaron exhaustivamente en lo que respecta a sus puntos flacos de seguridad, se revisaron las funciones que proporcionan en este apartado.

El producto de Microsoft destacó por encima del resto, seguido a corta distancia del de NOVELL®. Windows 2000 soporta certificados de clave pública Kerberos como mecanismo de autenticación primario en un dominio, pero permite utilizar autenticación adicional con tarjetas inteligentes. Microsoft proporciona Security Configuration Tool, que se integra con MMC para gestionar fácilmente objetos de seguridad en el sistema Active Directory Services, así como un nuevo Encrypting File Systems que permite designar volúmenes sobre los cuales se almacenan automáticamente los ficheros usando encriptación.

NOVELL® ha añadido a NETWARE® 5 soporte de infraestructura de clave pública (PKI) mediante un esquema de certificado público desarrollado por RSA Security que permite utilizar NDS para generar certificados.

Red Hat ofrece un mecanismo de autenticación Kerberos básico. Con su Linux, como con la mayoría de los sistemas Unix, los servicios de red pueden ser controlados individualmente para incrementar la seguridad. La compañía aporta *Pluggable Authentication Modules* como un modo de permitir establecer políticas de autenticación a través de programas que corren en el servidor. Las contraseñas son protegidas con un fichero oculto. Red Hat proporciona además servicios incorporados de red privada virtual (VPN) y de "cortafuegos".

UnixWare viene con un conjunto de herramientas de seguridad, denominadas *Security Manager*, que permite establecer diversos niveles de protección contra intrusiones, desde acceso libre a una restricción total a los servicios de red. Estas herramientas representan un medio excelente para ahorrar tiempo dedicado a la gestión, aunque se pueden conseguir los mismos resultados modificando los servicios manualmente.

5.4.1.8 ESTABILIDAD Y TOLERANCIA A FALLOS.

De nada le vale a un sistema operativo de red contar con un amplio conjunto de muy buenas prestaciones si es incapaz de mantener el servidor activo. En este sentido, Windows 2000 ofrece RAID 0, 1 y 5 al objeto de proporcionar a los discos tolerancia a fallos, y cuenta con una característica de equilibrio de las cargas de la red que permite a un grupo de servidores aparecer como uno solo, compartiendo el mismo nombre de red y dirección IP. El grupo decide qué servidor dará servicio a cada petición.

Este enfoque no sólo distribuye la carga de la red entre diferentes servidores, sino que también aporta tolerancia a fallos en caso de que alguno de ellos se venga abajo. A menor escala, se puede utilizar Failover Clustering de Microsoft para aportar servicios de "failover" básicos entre dos servidores.

Como NT 4.0, Windows 2000 ofrece protección de memoria, es decir, cada procesador corre en su propio segmento. Asimismo, el producto cuenta con funciones de recuperación y backup.

NOVELL® tiene un producto adicional para NETWARE®, denominado NOVELL® Cluster Services, que permite agrupar hasta ocho servidores y gestionarlos desde un punto central mediante ConsoleOne®, NETWARE® Management Portal o NWAdmin32. Pero, actualmente, la compañía no ofrece productos de "clustering" que proporcionen balanceo de cargas para aplicaciones o servicios de ficheros. Lo que sí aporta es un muy elaborado esquema de protección de memoria para segregarse la memoria usada por el kernel y las aplicaciones, así como un módulo *Storage Management Services* que proporciona un sistema de recuperación y backup muy flexible. El backup puede cubrir la totalidad de la red o partes determinadas, así como almacenar "instantáneas" diferenciales.

El producto de Red Hat provee una utilidad de equilibrio de cargas denominado "piranha". Este paquete ofrece balanceo de cargas TCP entre los servidores de un grupo, cuyo número de miembros puede ser muy amplio. Linux proporciona, además, soporte RAID de software a través de herramientas de líneas de comandos, y cuenta con funciones de protección de memoria y una facilidad de *backup* rudimentaria.

SCO ofrece una característica opcional para agrupar servidores en un entorno de equilibrio de cargas con un alto nivel de tolerancia a fallos en su *Non-Stop Clustering*, que actualmente soporta grupos de seis servidores. UnixWare aporta, además, soporte de todos los niveles RAID estándar, gestionado por *On-Line Data Manager*. También viene con ArcServeIT 6.6 de Computer Associates para realizar las tareas de recuperación y backup, y ofrece, asimismo, funciones de protección de memoria.

5.4.1.9 DOCUMENTACIÓN.

Debido a que la comparativa se realizó antes del lanzamiento comercial de Windows 2000, no se pudo evaluar su documentación en papel. Pero por lo que respecta a su documentación *online* sobre CD se puede decir que es amplia, útil y bien organizada.

NETWARE® 5 viene con dos manuales: uno detallado para la instalación y configuración del sistema operativo con muy buenas explicaciones de conceptos y características con una visión global de la configuración, y un folleto de tarjetas de inicio rápido. Su documentación *online* resulta muy útil.

Red Hat ofrece tres manuales (una guía de instalación, una guía de inicio y un manual de referencia) muy sencillas de seguir.

A pesar de ser el producto más difícil de instalar, UnixWare proporciona la mejor documentación. Viene con dos manuales: uno sobre el sistema y otro de inicio. El primero es una referencia para llevar a cabo la instalación del sistema operativo; el segundo está bien redactado y organizado, y cubre muchas de las herramientas necesarias para configurar y mantener el sistema operativo. La documentación *online* tiene una buena presentación y es fácil de seguir.

5.4.1.10 CONCLUSIONES.

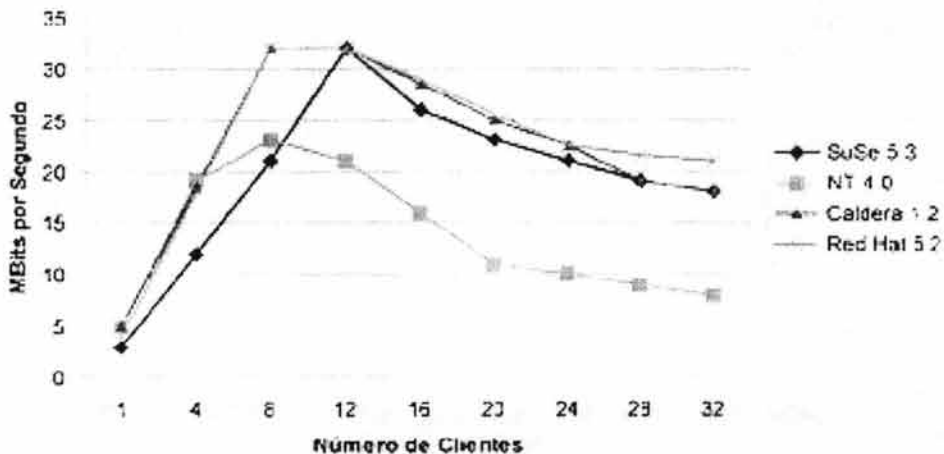
1.- Tras la evaluación, quedó patente que los sistemas operativos de red ofrecen un amplio rango de características y proporcionan a los usuarios corporativos una muy buena solución. Si lo que se desea es un sistema operativo bueno y de propósito general capaz de suministrar servicios a escala corporativa con todas las prestaciones imaginables, Windows 2000 es la elección adecuada.

2.- Sin embargo, si lo que se pretende es disponer de altos niveles de rendimiento y muy potentes servicios de ficheros e impresoras, NETWARE® sigue siendo la mejor opción.

3.- Cuando no importa pagar un alto precio por contar con una gran escalabilidad y fiabilidad, hay que volver los ojos a UnixWare.

4.- Y si, finalmente, lo que se precisa es una alternativa barata que nos proporcione servicios de red no demasiado complejos con un rendimiento aceptable, el producto Linux de Red Hat ofrece una muy buena alternativa.

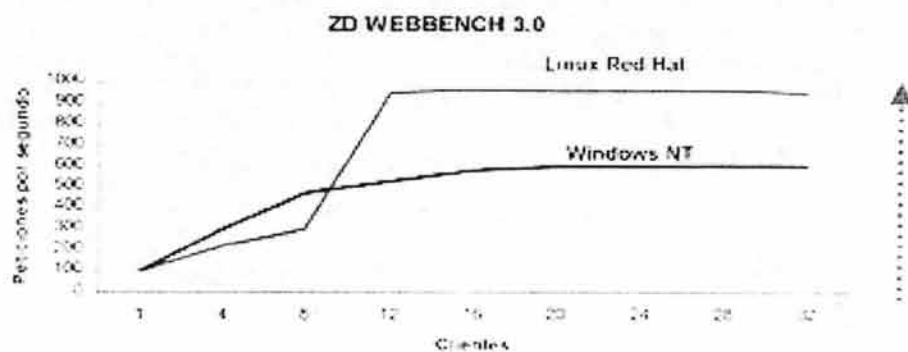
Los ensayos consisten en realizar peticiones a un servidor Web en el mismo ordenador cambiando únicamente el sistema operativo (NT y varias distribuciones de Linux). Los resultados del primer ensayo son:



Peticiones de varios clientes a un servidor

Como se puede ver en esta figura, Windows NT tiene peor rendimiento que Red Hat, Caldera y SuSE (tres distribuciones de Linux) a partir del momento en que más de 8 clientes (8 ordenadores u 8 ventanas de un navegador) solicitan páginas del servidor Web.

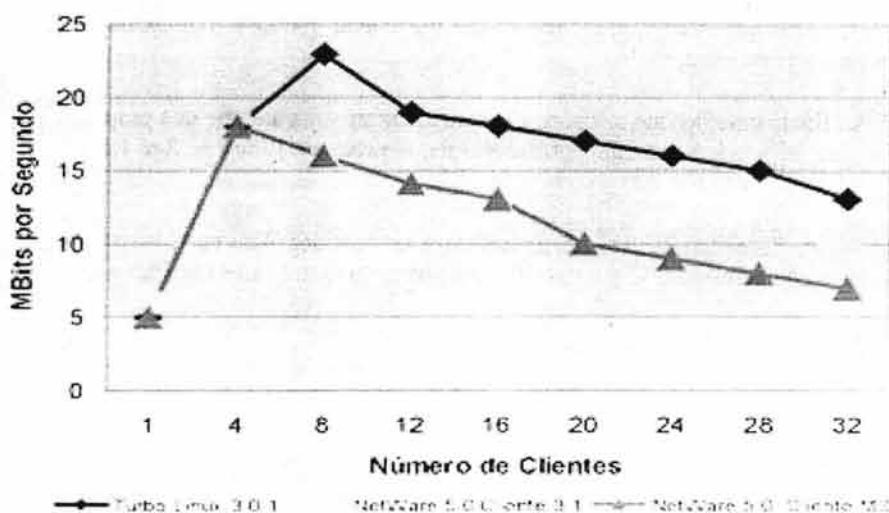
En esta otra comparación ocurre lo mismo, pero los resultados han sido medidos de forma diferente utilizando el software de medición ZD WebBench 3.0.



Comparativa Linux/Windows

Como puede verse, se han comparado los rendimientos del mismo ordenador utilizando Windows NT y Linux de Red Hat resultando claramente vencedor este segundo.

En cuanto a servidor de ficheros se refiere, se presentan aquí los resultados de comparar los rendimientos de un servidor Linux-Samba y un servidor NETWARE®. Como se ve, a partir de 4 clientes (4 ordenadores leyendo del disco duro del servidor), el servidor Linux es más rápido.



Comparación del rendimiento a escala local.

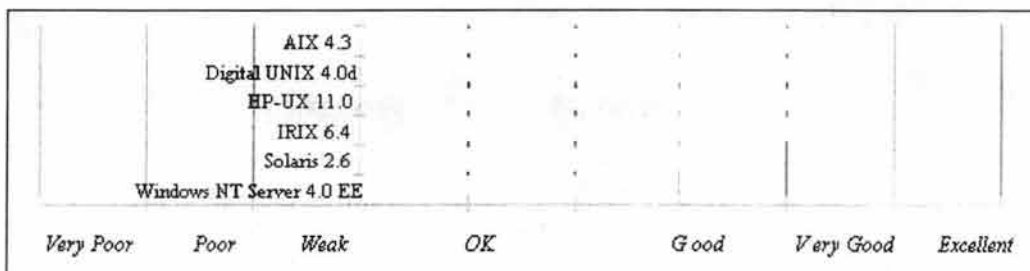
El estudio comparativo acaba exponiendo la conclusión de que se puede afirmar que, por la décima parte de lo que cuestan NT o NETWARE®, se obtiene un 30% más de rendimiento utilizando Linux.

5.5 ESTUDIO COMPARATIVO POR COPYRIGHT DIGITAL EQUIPMENT.¹⁶

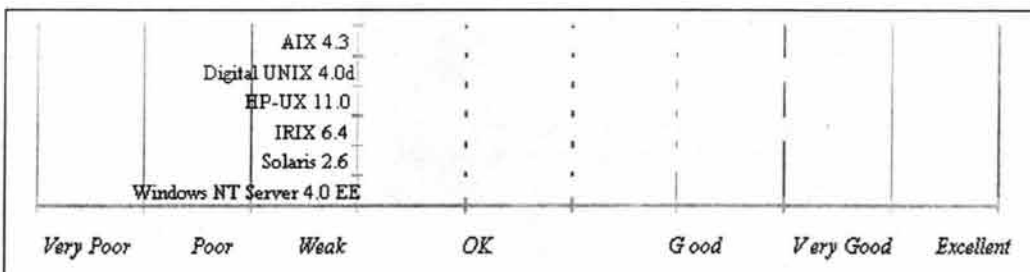
A continuación se presenta un estudio comparativo presentado por Copyright Digital Equipment Corporation durante 1998 en el cual se compara Windows NT contra las diferentes versiones de Unix.

¹⁶ Kirch, J. (1999). Microsoft Windows NT Server 4.0 versus Unix. En línea [URL], <http://kirch.net/unix-nt/>

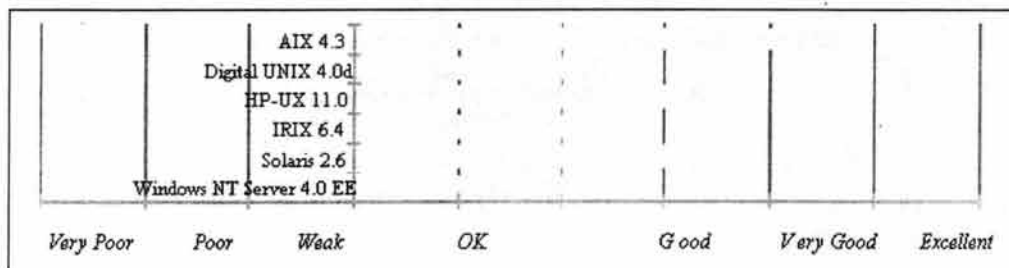
Características en redes internet / Intranet
INTERNET / INTRANET NETWORKING FEATURES



FIABILIDAD Y ESCALABILIDAD



GESTIÓN DEL SISTEMA



Copyright Digital Equipment Corporation 1995-1998. All Rights Reserved.

Los estudios anteriormente presentados proponen una visión diferente de la que se presentó en el muestreo ya que éstos fueron hechos desde la funcionalidad interna de los Sistemas Operativos en un laboratorio preparado y destinado con tales fines.

Es importante mencionar que el primer estudio hecho por CENTENIAL NETWORKING LABS difiere un poco de los demás comparativos, hay que tomar en cuenta que este estudio fue hecho con sistemas operativos más actualizados, lo cual es un parámetro a considerar ya que cada compañía realiza importantes esfuerzos para mejorar sus productos.

Así de esta manera, se han presentado diferentes análisis comparativos, con diferentes perspectivas, buscando como objetivo principal, beneficiar a la sociedad informática mexicana con una herramienta de información que les ayude en la toma de decisiones para llegar a la elección adecuada con la que trabajará su compañía.

CONCLUSIONES

En los capítulos anteriores, se analizó desde los requerimientos que necesita cada plataforma hasta la administración, pero se tiene que ver que hay detrás de todo esto, tal vez por su facilidad en cuanto a manejo y administración se puede decir que se prefiere Windows NT, sin embargo hay que tomar en cuenta las herramientas que brinda cada plataforma, porque hoy en día no basta con solo administrar recursos compartidos.

La elección de un sistema operativo para servidor con el que vivirá por años una organización no se basa simplemente en la funcionalidad de la versión en particular de un producto. Se trata de una decisión estratégica de largo plazo, guiada por las necesidades de la organización en cuanto a una plataforma en que construir soluciones para sus problemas de negocios. Por otra parte, los requerimientos que las organizaciones exigen en los sistemas operativos para servidor se expanden rápidamente. De la necesidad básica de compartir archivos e impresoras, los requerimientos han crecido e incluyen las comunicaciones, Internet, administración y aplicaciones distribuidas de gran escala. Estos requerimientos tan diversos implican que el sistema operativo de servidor debe ser una plataforma de propósito múltiple, capaz de proporcionar un conjunto extenso e integrado de servicios, que sean excelentes en cada función individual.

Realmente decir que Sistema Operativo es el mejor, es difícil, cada uno tiene sus puntos fuertes y sus puntos débiles, todo depende de la empresa que lo este utilizando, y la magnitud de esta misma, puede ser un PYME o un corporativo transnacional, las necesidades y requerimientos de los dos tipos son diferentes.

Normalmente el crecimiento de la empresa esta ligado al crecimiento de su infraestructura informática, hay que asegurarse de que la elección de un sistema operativo permitirá un crecimiento razonable y adaptación adecuada de las necesidades que se susciten después de su implantación.

Otro punto primordial a considerar en la elección de un sistema operativo es el mantenimiento; el administrador de la red debe estar adecuadamente capacitado, considerando que hay sistemas como Windows NT que tiene una curva de aprendizaje bastante aceptable, motivo por el cual hay una gran cantidad de administradores que son autodidactas, en su contraparte tenemos a Unix o Linux que en realidad se requiere cierto nivel de capacidad para su adecuada administración, motivo por el cual se necesita una capacitación más profesional para su correcta administración, lo cual implica un gasto, además, cada sistema operativo o plataforma cuanta con pros y contras en el aspecto de la administración diaria.

Cada sistema operativo tiene bondades específicas que difieren de los demás, la elección de este, puede recaer en la seguridad o capacidad que tenga el administrador para la administración y mantenimiento del sistema, en México la elección de sistemas operativos recae en la mayoría de los casos a la decisión que tome el administrador de la red o la persona encargada de Informática, y este nos puede llevar a una elección incorrecta, debido a que esta se basa en la capacidad del administrador y no en un análisis profesional de las verdaderas necesidades que tiene la empresa, un ejemplo de esto es, si el administrador de la red tiene más conocimientos sobre Windows NT, desde luego que elegirá este sistema operativo, sin contemplar los gastos que este sistema requiere y si la empresa podrá en algún momento soportar económicamente el mantenimiento y crecimiento de su red, esto es motivado a que la mayoría de las empresas en México son PYMES y no destinan grandes cantidades presupuestales a los ámbitos informáticos, teniendo como consecuencia la contratación de personal con escasos conocimientos para tomar una decisión de tal magnitud y mucho menos para pagarle una adecuada capacitación.

GLOSARIO DE TÉRMINOS

Administrador Es la persona o programa encargado de gestionar, realizar el control, conceder permisos, etc. de todo un sistema informático o red de ordenadores.

ASCII (*American Standard Code for Information Interchange*): Es el código numérico utilizado mundialmente para representar todos los caracteres del alfabeto, números, símbolos, etc. Está compuesto por 128 códigos estándares representados por un conjunto de 7 dígitos binarios.

Bit Es la unidad más pequeña de la información digital con la que trabajan los ordenadores.

Buffer Es una memoria intermedia utilizada para guardar temporalmente la información que se transfiere entre diferentes dispositivos informáticos o entre los componentes de un mismo sistema informático.

Byte Es una unidad que mide la cantidad de información, tamaño y capacidad de almacenamiento. Un Byte, equivale a 8 Bits.

bps (bits por segundo): Es la unidad en que se mide la velocidad de transmisión de los datos entre las máquinas. Un módem de 28,8 Kbps, puede mover 28.800 bits por segundo.

Cliente: Corresponde a la denominación de un programa (software) utilizado para contactar y obtener datos desde un software servidor que se encuentra generalmente en otro ordenador. En la arquitectura cliente-servidor, existe un software cliente corriendo en un ordenador y un software servidor corriendo en otro ordenador que interactúan entre ellos y ejecutan alguna tarea específica.

Cluster Son varios sectores consecutivos de un disco.

Driver Es un programa, conocido como controlador, que permite la gestión de los dispositivos conectados al ordenador generalmente, periféricos como impresoras, unidades de CD-ROM, etc.

Ethernet: Es uno de los protocolos de red más comunes para una red de ordenadores local (LAN, *Local Area Network*). Ethernet es capaz de transportar hasta 10,000,000 bits-por-segundo y puede ser usada casi con cualquier clase de ordenador.

FAT: Acrónimo de *File Allocation Table*. Lista o tabla por el **sistema operativo** para manejar el espacio utilizado en el almacenaje de **archivos**. Los archivos son almacenados en un **disco** como grupos de **bytes** de tamaño fijo en vez de una cadena contigua de texto o números, por lo que un **archivo** puede estar dividido en segmentos que pueden estar en varias áreas separadas físicamente. El mapa de la FAT permite marcar los espacios ya utilizados, encontrar y unir los segmentos correspondientes a un archivo determinado.

FTP (*File Transfer Protocol*): Es uno de los servicios Internet más comunes para mover archivos entre un ordenador y otro. Es habitual usar FTP desde un sitio en Internet para rescatar o enviar archivos. Existen muchos sitios Internet que suministran información gratuita contenida en archivos y a los que se puede acceder usando el protocolo FTP con el nombre de cuenta anonymous.

GUI Graphic User Interface. Interface Gráfico de Usuario. Interface de comunicación gráfico entre el Sistema Operativo y el usuario.

Hardware: Incluye todos los componentes electrónicos, eléctricos y mecánicos que componen una computadora.

Host: Representa a cualquier clase de ordenador conectado a la red y que presta servicios a los otros ordenadores de la red. Es muy común que una misma máquina (host) provea varios servicios, tales como WWW, News, FTP, etc.

ID user (nombre de usuario): Corresponde al nombre del usuario o identificación de la persona que tiene autorización para acceder a algún servicio en particular, por ejemplo: modificar su sitio web. El ID está asociado a la password y entre ambos dan acceso a la administración del espacio que ocupa el sitio web en el servidor.

IFS *Instalable File System*. Sistema que se encarga de gestionar las transferencias de información de entrada y de salida, correspondientes a un grupo de dispositivos informáticos (de la red o de otras redes) y ficheros.

Interface Es el sistema que permite a los usuarios dialogar (comunicarse e interactuar) con el ordenador y el software que éste tiene instalado. A su vez, este software se comunica mediante un sistema de interfase con el **hardware** del ordenador.

Internet: Corresponde al conjunto de redes de ordenadores que se encuentran interconectadas alrededor del mundo y que utilizan el protocolo TCP/IP.

Intranet: Corresponde a una red de ordenadores privada o al interior de una organización que utiliza la misma tecnología de Internet y que es solamente para uso interno.

Dirección IP: Es un número único a nivel mundial separado en cuatro partes por puntos. Cada uno de estos números puede ser desde 0 hasta 255. Un ejemplo de dirección IP es: 200.27.90.2. El orden de jerarquía de los números es de izquierda a derecha, donde el primer número es el más general y así sucesivamente hacia la izquierda. Cada máquina que está conectada a Internet tiene su propia **dirección IP** y es única en todo el mundo.

DNS: Acrónimo de ***Domain Name System*** (Sistema de Nombre de Dominio) o de **Domain Name Service** (Servicio de Nombre de Dominio). El DNS permite que un usuario de **Internet** tenga tanto un nombre de dominio (ej: ficticia.org) como una **dirección IP** (ej: 127.0.0.1). El DNS Servicio es la **utilidad de Internet** que implementa el DNSistema. Los **servidores DNS** mantienen las **bases de datos** que contienen las direcciones.

ISP (*Internet Service Provider*): Es el término genérico para representar a cualquier empresa u organización que provee servicios de acceso a Internet.

Kernel: Núcleo o corazón de un **SO**. Maneja la **memoria**, **archivos**, dispositivos periféricos, fecha y hora, lanza **aplicaciones** y asigna los recursos del **SO**

Kilobyte (KB): Corresponde a 1.024 bytes.

LAN (*Local Area Network*, red de área local): Representa una red de ordenadores limitada a un área contigua y específica, por ejemplo un mismo edificio o el mismo piso de un edificio.

Login (dos significados): El nombre dado a una cuenta y que permite el acceso a un ordenador o bien la acción de entrar a un sistema de ordenadores.

Megabyte (MB): Representa un millón de bytes.

Memoria (memory): Circuito que permite el almacenamiento y devolución rápidos de datos. Ver **ROM, RAM, PROM, EPROM y EEPROM**

Módem (*MODulator, DEModulator*): Es el dispositivo que conecta un ordenador a una línea telefónica y que permite enviar y recibir datos desde otro ordenador.

Nodo: Representa a cualquier ordenador conectado a una red.

Password: Es el código secreto utilizado para acceder a un sistema protegido.

Protocolo Descripción formal de formatos de mensaje y de reglas que dos ordenadores deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina-a-máquina o intercambios de alto nivel entre programas de asignación de recursos.

Proxy (servidor proxy): Componente de un **firewall** que maneja el tráfico de una **LAN** desde y hacia **Internet**. Permite la descarga más rápida de documentos o **páginas Web** de uso frecuente y el control de acceso.

Puerto: Son vías que permiten a una PC el intercambio de datos, su salida y entrada.

RAM: Acrónimo de *Random Access Memory* (**memoria de acceso aleatorio**). Memoria basada en semiconductores que puede ser leída y escrita por el CPU u otros dispositivos de *hardware*. Las locaciones de almacenaje pueden ser accedidas en cualquier orden. Algunos tipos de **ROMs** pueden ser accedidas de igual manera pero no ser escritas. Por lo general el término RAM es comprendido generalmente como la memoria volátil (los datos e instrucciones se borran al apagarse la PC) que puede ser escrita y leída.

Restore: Restaurar. La carpeta **RESTORE** contiene varios respaldos de días, semanas y meses atrás, configurados según ciertas reglas. Ello permite restaurar el **Sistema** cuando ha sido dañado.

ROM: Acrónimo de *Read Only Memory* (**memoria de solo lectura**). Circuito semiconductor que sirve como **memoria** y que contiene datos o instrucciones (colocados durante la fabricación o por una programación posterior) y que puede ser leído pero no modificado (a diferencia de la **RAM**). Ver **PROM**, **EPROM**, **EEPROM**.

Servidor: Es un ordenador o un software que provee una clase especial de servicio a los software clientes que están corriendo en otros ordenadores y al que acceden para realizar una función determinada. Un ordenador funcionando como servidor puede tener operando varios software servidores para prestar servicios, por ejemplo: servidor de WWW, servidor de Mail, etc.

Setup: Lugar donde se realiza la declaración de las opciones con las que se trabajará, puede ser de la computadora o de un **programa** determinado.

Shell En un sistema UNIX se trata del programa que interactúa con el usuario, toma sus órdenes y hace que el sistema operativo las ejecute; en MS-DOS sería el intérprete de comandos COMMAND.COM. Por otra parte, en ambientes hacker se habla de cuenta Shell para referirse a conjuntos de login y password que dan acceso a un sistema.

Sistema operativo: Programa diseñado especialmente para controlar el *hardware* de un sistema específico de procesamiento de datos de manera que permita ser empleado fácilmente por los usuarios y los programas que este emplea. Ej: MS-DOS, Windows, Unix, etc.

TCP/IP (*Transmission Control Protocol/Internet Protocol*): Es el conjunto de protocolos que definen a Internet. Originalmente diseñado para el sistema operativo UNIX, hoy en día existe software TCP/IP disponible para la mayoría de los sistemas operativos. Para poder utilizar Internet, su ordenador debe tener software TCP/IP.

Telnet: Herramienta para acceder a otras computadoras conectadas a **Internet**, con la posibilidad de leer **archivos** y ejecutar **programas** ubicados en esas computadoras remotas.

Terminal: Un dispositivo que permite enviar comandos hacia un ordenador en cualquier lugar que éste se encuentre.

UNIX: Es el sistema operativo usado en muchos ordenadores. UNIX está diseñado para ser usado por muchas personas al mismo tiempo (multiusuario) y tiene incorporado el protocolo de comunicaciones TCP/IP. Es uno de los sistemas operativos más utilizado entre los servidores conectados a Internet.

WAN: Es el nombre dado a cualquier red de ordenadores que cubre un área geográfica mayor a un lugar físico contiguo. Internet es un caso de WAN.

Web Telaraña Mundial. Red de documentos HTML de Internet, relacionados entre ellos y dispersos por servidores de todo el mundo. Para muchos la WEB es Internet, para otros es sólo una parte de ella. Podríamos decir, estrictamente, que la WEB es la parte de Internet a la que accedemos a través del protocolo HTTP y en consecuencia gracias a navegadores (browsers) como Opera, Netscape o Internet Explorer.

APENDICE I.

Instrumento de medición utilizado en el capítulo V, donde los resultados se presentan en forma grafica.

Compañía: _____
Sistema Operativo _____

1.- ¿Por qué eligió este S.O?

- a) Ya residía b) Porque se tiene conocimiento c) Por mercado

2.- ¿Cuántas caídas de sistema ha sufrido en el último año?

R: _____

3.- ¿Cómo considera la administración del sistema?

- a) Fácil b) Nivel Medio c) Difícil

4.- ¿Cuántas estaciones de trabajo tiene su red?

R: _____

5.- ¿En cuanto a drivers para el S.O le es difícil conseguirlos?

- a) SI b) NO d) A veces

6.- ¿Cómo considera los controles de seguridad del S.O.?

- a) Eficientes b) Nivel Medio c) Deficientes

7.- ¿A contemplado alguna vez cambiar de S.O?

- a) SI b) NO

8.- ¿Qué tan vulnerable considera el S.O contra Virus o Hackers?

- a) Muy vulnerable b) Nivel Medio c) No vulnerable

9.- ¿Qué porcentaje de conocimiento tiene con respecto al S.O?

R: _____

10.- ¿Cómo considera la instalación del S.O?

- a) Fácil b) Nivel Medio c) Difícil

11.- ¿Cómo considera el módulo de respaldo en el S.O?

- a) Eficiente b) Nivel Medio c) Deficiente

12.- ¿Cómo considera los servicios de impresión del S.O?

- a) Eficientes b) Nivel Medio c) Deficientes

13.- ¿Sabe ud. Cuales son los puntos más vulnerables del S.O?

R:

14.- ¿Cómo considera la interfase de comunicación del S.O?

- a) Amigable b) Nivel Medio c) No amigable

15.- ¿Cómo considera los servicios Web del S.O?

- a) Eficientes b) Nivel Medio c) Deficientes

16.-¿ Tiene alguna plataforma alterna instalada en su empresa?

- a) SI b) NO

Motivo _____

OBSERVACIONES O COMENTARIOS

REFERENCIAS Y BIBLIOGRAFÍA

- ¹ Magaña, Saúl y Magaña, Adrian. (2000). Introducción a redes de microcomputadoras. Universidad Nacional Autónoma de México, Facultad de Ingeniería, División de Educación Continua; Diplomado de redes de Computadoras y Telecomunicaciones. México D.F.
- ² García, J. Sistema Operativo de Netware® de Novell® V.5. En línea [URL], <http://www.monografias.com/trabajos6/sinov/sinov.shtml#histo>
- ³ Netware® 5.1. En línea [URL], <http://www.NOVELL.com/documentation/spanish/nw51/docui/index.html>
- ⁴ ConsoleOne 1.3. En línea [URL], <http://www.novell.com/documentation/spanish/consol13/index.html>
- ⁵ Raya Cabrera, J. y Raya Pérez E. (2000). Netware® 5 Instalación, Configuración y Administración. México: Alfaomega, 286-340pp
- ⁶ Raya Cabrera, J. y Raya Pérez E. (2000). Netware® 5 Instalación, Configuración y Administración. México: Alfaomega, 659-672pp
- ⁷ Raya Cabrera, J. y Raya Pérez E. (2000). Netware® 5 Instalación, Configuración y Administración. México: Alfaomega, 659-672pp
- ⁸ Rey de Perea Campos J. Escuela de Administración de Negocios, E . A . N . ; Taller práctico sobre el sistema operativo unix; diplomado en informática; Universidad de Almería España. En línea [URL], <http://www.ual.es/~jperea/documentacion/unix/Taller.exe>
- ⁹ Correa García I. Instalación del Sistema Operativo SCO Unix. En línea [URL], <http://software.uaemex.mx/documentos/SCO/indice.html>
- ¹⁰ Rey de Perea Campos J. Escuela de Administración de Negocios, E . A . N . ; Taller práctico sobre el sistema operativo unix; diplomado en informática; Universidad de Almería España. En línea [URL], <http://www.ual.es/~jperea/documentacion/unix/Taller.exe>
- ¹¹ Litz, J. Aprendiendo Windows NT Server 4.0, En línea [URL], <http://webmar.es.vg>
- ¹² Costales F. Sistema Operativo Unix. En línea [URL], <http://www.monografias.com/trabajos/soredes/soredes.shtml>
- ¹³ Espinoza Curiel M. Selección de un Sistema Operativo, En línea [URL], <http://www.geocities.com/SiliconValley/8195/selec.html#temas>
- ¹⁴ Moreno J. y Osorio C. Artículo estadístico Informático de México, En línea [URL], <http://www.chuin.com.mx/articulos/4mar-2002.htm>
- ¹⁵ Badas Cañabate, J y Vélez Isasmendi, I. Sistemas Informáticos en Tiempo Real. Escuela Superior de Ingenieros Industriales, Universidad de Navarra, España
- ¹⁶ Kirch, J. (1999). Microsoft Windows NT Server 4.0 versus Unix. En línea [URL], <http://kirch.net/unix-nt/>