



UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

Facultad de Ingeniería

Migración de un Sistema de Correo hacia la Plataforma de Microsoft Exchange.

T E S I S
Para obtener el Título de
INGENIERO EN COMPUTACION
P r e s e n t a n
CARBAJAL BELMONT MARIO
CUERVO ESPINOSA ADDINA
GARCIA MARTINEZ RAFAEL
MUNGUIA CAMPOS SUSANA
OCHOA LOPEZ ARTURO

285731



Director de Tesis:
Ing. Manuel Manriquez Miranda

México, D. F.

2000



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.

Migración de un Sistema de Correo hacia la Plataforma de Microsoft Exchange

**Carbajal Belmont Mario
Cuervo Espinosa Addina
García Martínez Rafael
Munguía Campos Susana
Ochoa López Arturo**

**Director de Tesis
Ing. Manuel Manriquez Miranda**

Agradecimientos:

A mis compañeros de Tesis:

Por el apoyo brindado para concluir esta importante etapa en nuestras vidas.

A nuestro director de Tesis y a nuestros sinodales :

Por su apoyo en la realización de este proyecto.

Al PAT por las facilidades prestadas para la culminación de este trabajo.

CONTENIDO

INTRODUCCIÓN	1
1. ARQUITECTURA	3
1.1 Descripción del Producto Microsoft Exchange	3
1.2 Arquitectura de Implementación	10
2. ANÁLISIS Y DISEÑO DE CONEXIONES	16
2.1 Esquema de Conexiones para Casa Matriz	16
2.2 Servidores Principales de Conexión	20
2.3 Tipos de Conectores	33
3. SOFTWARE DE INSTALACIÓN	38
3.1 Windows NT 4.0	38
3.2 Service Pack 3.0	44
3.3 Microsoft Exchange Server 5.5	48
3.4 IIS 3.0 Acceso vía Web Access	50
3.5 ArcServe Cheyenne	51
3.6 Backup Agent para Microsoft Exchange	53
3.7 Outlook 97 y Outlook 98 para Clientes	56
3.8 Niveles de Seguridad	59
4. PREPARACIÓN DE EQUIPOS	61
4.1 Tipos de Protocolos	61
4.2 Definición de Protocolos a Utilizar	68
4.3 Tipos de Arreglos Redundantes a Fallas	68
4.4 Definición de Arreglos de Discos para S.O. y Datos	75
4.5 Estructura de Discos	76
5. CONFIGURACIÓN DEL AMBIENTE DE TRABAJO	78
5.1 Definiciones de Dominios	78
5.2 Relaciones de Confianza (Trust Relationships)	85
5.3 Definición de Relaciones de Confianza entre México y Casa Matriz	92
5.4 Elementos de Resolución de Nombres	94
5.4.1 DNS	94
5.4.2 WINS	100
5.4.3 LMHOST	108
5.4.4 HOST NAME	110
5.5 Definición de Direcciones Estáticas en WINS para Conexión con Casa Matriz	116
5.6 Quotas	118
5.6.1 Definición de Quotas para usuarios en el servidor	118
5.6.2 Ventajas y Desventajas	119
5.7 Selección de conectores para enlaces WAN	120
5.8 Replicación con el resto del mundo	124
6. INSTALACIÓN DE SERVIDORES FORÁNEOS	126
6.1 Creación de un Site	126

6.2	Definición de Conexiones entre Sites	128
6.3	Definición de servidores Foráneos en un mismo Site	131
7.	ESTRUCTURA DE EXCHANGE PARA EL ALMACENAMIENTO DE INFORMACIÓN	148
7.1	Esquema de almacenamiento de Exchange	148
7.2	BD Pública características	154
7.3	BD Privada características	157
7.4	Archivos de log transaccionales características	158
8.	MIGRACIÓN DE USUARIOS	160
8.1	Procedimientos de Migración de Usuarios	160
8.2	Campaña de Difusión del nuevo correo	166
8.3	Capacitación	172
8.4	Instalación en PC's	174
8.5	Alta de cuentas en el correo	187
8.5.1	Administración de Windows NT	187
8.5.1.1	Alta de usuarios	189
8.5.2	Administración en Exchange	192
8.5.2.1	Alta de Cuentas	196
8.6	Desinstalación del software de correo anterior	205
8.6.1	Administración de Windows NT	205
8.6.1.1	Descripciones de Logon Script	205
8.6.2	Procedimientos Automáticos de Desinstalación.	208
9.	ESQUEMA DE RESPALDO Y RESTAURACIÓN DE INFORMACIÓN	211
9.1	Respaldo fuera de línea	213
9.2	Respaldo en línea	214
10.	HERRAMIENTAS DE OPTIMIZACIÓN Y MONITOREO	216
10.1	Funciones del Procedimiento Run Optimizer	216
10.2	Verificación de la consistencia de las bases de datos	220
10.2.1	Comandos	220
10.2.2	Technet	221
10.3	Verificación de la regeneración de las bases de datos.	223
10.3.1	Comandos	223
10.3.2	Technet	225
10.4	Performance Monitor	227
	CONCLUSIONES	230
	GLOSARIO DE TÉRMINOS	234
	BIBLIOGRAFÍA.	239

INTRODUCCIÓN

Debido a los requerimientos de comunicación que se han dado en los últimos años, muchas compañías han optado por adaptar a sus sistemas de producción los sistemas de mensajería y colaboración que les proporcionen una comunicación eficiente, rápida y segura con el resto del mundo.

El sistema de correo actual de la compañía se encuentra instalado como servidor de producción en un equipo *Digital VAX 4000-100 A* y sobre una plataforma *Alpha*. Actualmente está comunicado con todas las afiliadas que forman parte del corporativo, por lo que la transferencia de información entre las diferentes afiliadas se efectúa por medio del correo electrónico sobre la red.

El sistema de correo actual proporciona únicamente servicio de correo y calendarización de juntas y se han incorporado otras aplicaciones como *TeamRoute* que permiten la asignación de documentos por medio del correo.

Durante éste periodo se ha trabajado con dos protocolos de red; el protocolo *Decnet* se utiliza para establecer la comunicación con la red *WAN* hacia Casa Matriz y el protocolo *TCP/IP* se utiliza en forma local para la red *LAN*. El uso del protocolo *Decnet* será eliminado con la implementación del nuevo sistema de correo ya que como estándar mundial se adoptará el protocolo *TCP/IP* a nivel *WAN*.

La parte central del correo se encuentra ubicado en las oficinas corporativas Casa Matriz ubicadas en New Jersey, por lo que cualquier mensaje que sea enviado de cualquier parte del mundo a otra afiliada deberá pasar por el servidor ubicado en Casa Matriz y de ahí ser retransmitido a la afiliada destino, éste servidor se comporta como un puente de correo entre las afiliadas.

El sistema de correo actual está definido aproximadamente en 50 nodos o países, los cuáles se comunican todos a Casa Matriz, por lo que en un momento dado el acceso a éste servidor puede ser un cuello de botella.

El sistema actual utilizado por todo el corporativo es de tecnología cliente/servidor, por lo que el componente instalado en el servidor llevaba el nombre de *DecMailworks* y el componente instalado en el cliente se conocía como *Teamlinks*, adicionalmente era necesario mantener en el servidor un componente *Message Router* que se encargaba de encaminar los mensajes que no se encontraban en forma local hacia fuera de la filial, así como de mantener el directorio mundial acorde con los demás países del mundo.

El sistema de correo actual proporciona servicio aproximadamente a 18 mil usuarios y se pretende que, con el nuevo sistema de correo, el total de usuarios del corporativo (40 mil) con

equipos de cómputo tengan su cuenta de correo y puedan hacer uso de esta herramienta para desempeñar mejor su trabajo.

Durante el proceso de selección de sistemas de mensajería se evaluaron diferentes características y se consideraron elementos como seguridad de la información, plataformas de implementación, confiabilidad, escalabilidad y hasta proveedor. El *software* de *Microsoft Exchange* como su nombre lo dice está respaldado por *Microsoft*, es un sistema de mensajería universal y se ha implementado ya en muchas corporaciones, su crecimiento es ilimitado y sólo es dependiente del *hardware* con que se cuente, éste fue uno de los factores fundamentales, ya que se considera que se deberían enlazar aproximadamente 40 mil usuarios, la plataforma seleccionada fue *Intel* con *Windows NT*, éste fue otro factor importante ya que todo el corporativo cuenta con esta tecnología, por lo que su implementación sería más fácil para todas las afiliadas, finalmente la seguridad de la información se podía garantizar por medio del manejo de arreglos redundantes a fallas, garantizando el servicio 7x24.

El corporativo cuenta aproximadamente con 40 mil usuarios, los cuáles deberán estar conectados por medio de un sistema de mensajería que pueda soportar la cantidad mencionada y proporcionar un tiempo de respuesta aceptable para todas las filiales.

Durante el proceso de evaluación de sistemas de mensajería se consideraron todas las facilidades y puntos de conexión y escalabilidad de cada sistema, determinando que el sistema de mensajería y colaboración que podría soportar las necesidades de la compañía era *Microsoft Exchange*.

Una vez determinado cual sería el sistema de mensajería nuevo, se inició un proceso de evaluación de la herramienta y planeación de la estrategia de migración de todos los países hacia la nueva plataforma, sin interrumpir el intercambio de mensajes actual en todas las afiliadas.

Como parte de la estrategia de implementación del nuevo sistema de mensajería y colaboración se creó en Casa Matriz un equipo de trabajo que se encargaría de definir las principales bases para iniciar el proceso de migración, éste proceso se dividió en dos fases, la primera fue determinar cuál sería el esquema de conexiones entre los diferentes países y cómo se implementarían los "*Exchange Hubs*" (esta definición será comentada más adelante) y la segunda fase fue determinar que países podrían instalar un *site* independiente en sus localidades o cuáles tendrían que depender de alguna otra filial para contar con el servicio de mensajería.

Exchange está considerado como una organización lógica agrupada por *sites*. Éstos *sites* son básicamente regiones de *Exchange* que contienen uno o varios servidores dentro de su *site*. Los servidores asignados a un *site* no necesariamente deben estar ubicados en la misma localidad geográfica, éstos pueden estar en cualquier parte de una región siempre que pertenezcan al mismo *site*.

Las organizaciones de hoy en día consideran al *Microsoft Exchange* un sistema de mensajería poderoso, confiable, eficiente, escalable y muy seguro.

1.1 Descripción del Producto *Microsoft Exchange*.

Microsoft Exchange es el primer sistema de mensajería cliente/servidor que integra en un mismo sistema diferentes funciones como: el sistema de correo, calendarización de eventos en forma individual o en grupos, manejo de formas electrónicas, uso de contactos y tareas, trabajo en grupo y sincronización *on-line* con correo *Off-line* en el momento de la conexión.

Estas características hacen de *Exchange* un *software* de correo poderoso. Adicionalmente el nivel de seguridad ofrecido por *Internet* hace posible que cualquier organización sin importar el tamaño pueda contar con un sistema de correo poderoso que ofrezca soluciones cliente/servidor y puedan ser accedidas en cualquier parte del mundo.

Microsoft Exchange Server forma parte de la familia *Microsoft BackOffice*, la cual fue diseñada para apoyar a las organizaciones a tomar decisiones y poder ofrecer soluciones cliente/servidor de una manera precisa y mejorada.

La familia *BackOffice* está conformada por los siguientes productos:

- *Microsoft Windows NT Server* como sistema operativo.
- *Microsoft SQL Server* como manejador de base de datos.
- *Microsoft SNA Server* como herramienta de enlace entre plataformas *IBM, AS/400*.
- *Microsoft Systems Management Server* que permite un contacto directo a la PC del usuario por medio de la recolección de inventario, distribución de *software* en forma automática o soporte remoto de *Help-Desk* al equipo.
- *Microsoft Exchange Server* como sistema de correo.

Los negocios hoy en día confían en los sistemas de mensajería y colaboración en mayor escala, esto significa que no sólo se requiere de un sistema de envío y recepción de mensajes sino de una plataforma de mensajería inteligente que incluya todas las herramientas necesarias para generar sistemas de colaboración eficientes. El hecho de poder ofrecer todas las herramientas necesarias para considerarse un correo poderoso ubica a *Microsoft Exchange* como una de las plataformas de mensajería más elegida en el mundo.

A continuación se describen algunas de las características más importantes con que cuenta *Microsoft Exchange*:

Una base de mensajería sólida :

Cualquier plataforma de mensajería debe tener una base sólida de escalabilidad, rentabilidad y seguridad. Además debe tener servicios y una organización soportada, que permita manejar las necesidades tanto de un departamento como de una compañía por muy grande que ésta sea y en forma total.

Exchange Server 5.5 proporciona las características necesarias para crear una plataforma de mensajería confiable.

Escalabilidad :

- Cantidad de Mensajes Ilimitada .- *Exchange Server* proporciona el manejo de una cantidad de mensajes ilimitados, esto se contrapone a la cantidad de usuarios que se podían manejar en cualquier otro sistema de correo o a la cantidad de datos que cada servidor podía manejar, lo cual hacía de los servidores de correo un sistema finito, esto no es aplicable para *Microsoft Exchange*, el cual puede manejar la cantidad de mensajes que el *hardware* permita.
- Una sola Instancia de Almacenamiento .- Se puede maximizar el uso del espacio por medio del manejo de una sola instancia de almacenamiento. Esto provee un alto nivel de *performance* y elimina la necesidad de trabajo administrativo adicional.
- Capacidad de Multiprocesamiento Simétrico (SMP) .- *Exchange Server* habilita la residencia de miles de usuarios por servidor en *Microsoft Windows NT* dependiendo del *hardware*.
- *On-line Backups* .- Dependiendo de los requerimientos, *Exchange Server* proporciona la posibilidad de realizar respaldos en línea, por lo que se puede realizar la copia de los datos sin afectar el servicio en línea proporcionado por el servidor.
- *Fast Backups* .- El *performance* para realizar respaldos también ha sido ampliado, por lo que se cuenta con velocidades de respaldo de 25 Gigabytes por hora, esto se compara en un sistema típico en 2 a 3 Gb por hora.
- Detección Automática .- La infraestructura de *Exchange* permite detectar en forma automática, si ya existe, un servidor en el mismo *site* y permite incorporar el nuevo servidor al mismo esquema de replicación del servidor existente.
- Implementación de Estándares Nativos de *Internet* .- La implementación de los estándares nativos de *Internet* proporciona un acceso mejorado para el usuario, ya que están disponibles los accesos vía los servidores de *Internet MAPI, POP3, IMAP4 y NNTP*.

Rentabilidad :

- Almacenamiento de Transacciones u Operaciones Efectuadas .- Cada transacción que se efectúa en el servidor de envío o recepción de mensajes es escrita en un archivo de *log*, si por alguna razón el servidor deja de trabajar, por medio del archivo de transacciones se pueden recuperar las últimas operaciones realizadas hasta el momento de la falla.
- *Microsoft Cluster Server* .- Un servidor de *cluster* es un grupo de servidores (2 hasta éste momento) interconectados entre sí, manejados como un sólo equipo. Proporciona alta disponibilidad y fácil manejo de datos y aplicaciones, por lo que los usuarios pueden trabajar en forma ininterrumpida aunque uno de los servidores haya sido dado de baja.
- *Server Monitor* .- Esta utilería monitorea el comportamiento del equipo y realiza acciones correctivas que fueron predeterminadas.
- *Link Monitor* .- Esta utilería monitorea el estatus de las ligas de comunicación entre los servidores del mismo *Site* y las conexiones con *Internet* o *X400*.
- Direccionamiento Dinámico .- Si una de las ligas de comunicación se encuentra inactiva, los mensajes son direccionados a otra liga sin intervención de un administrador.
- *Message Tracker* .- Los administradores pueden rastrear un mensaje en cualquier parte de la red *LAN*, *WAN* o dentro de *Internet* por medio de *Message ID*, nombre del destinatario, mensaje enviado o nombre del que envía el mensaje. Se puede determinar si un mensaje fue enviado a su destino e incluso si ya ha sido leído.

Seguridad :

Mantiene el nivel de seguridad integrado con el modelo de *Windows NT*. Cada correo definido por usuario corresponde a una cuenta definida en *Windows NT*, por lo que cada usuario deberá autenticarse en *Windows NT* antes de acceder al contenido de su correo, adicionalmente los usuarios pueden acceder con el mismo *username* a los servicios de *Windows NT*, el correo y otros servicios de red. Por medio del esquema de seguridad, los administradores de *NT* pueden asignar *password* de acceso con un determinado período de expiración, se puede manejar también que el *password* no pueda ser igual al anterior o guardar un histórico de *passwords* que permita que por un determinado número de veces no se pueda teclear el mismo, se habilita también que la cuenta del usuario sea bloqueada después de un cierto número de intentos fallidos, de la misma forma el acceso a los *folders* públicos se puede controlar por medio de la cuenta del usuario.

- *RPC* .- Está disponible el uso de cifrado de mensajes entre los clientes y el servidor. El nivel de cifrado depende del usuario.
- *KMS* .- Maneja firmas digitales o cifrado de mensajes individuales. Una vez que el administrador asigna las claves, los usuarios pueden enviar firmas digitales y mensajes cifrados a otros usuarios dentro de la organización.
- *MTA* .- Sus funciones son determinar si un mensaje pertenece al mismo nodo local o debe ser direccionados a otra localidad, esta función se efectúa para mensajes que salen, o identifica los mensajes que van llegando al servidor local y determina si pertenecen a su nodo o no, el *MTA* también se utiliza para identificar si un mensaje ya ha sido leído y notifica al usuario.

Conectividad :

Los servidores de correo y colaboración deben proporcionar conectividad integral con el sistema *Internet*, con sistemas de mensajería heredados y con diferentes sistemas operativos en cliente.

Microsoft Exchange Server proporciona un sistema de mensajería abierto cumpliendo con las siguientes características :

- *Multiprotocol Server.*
- *Administrative Wizards.*
- *IMAP.*
- *LDAP.*
- *SASL.*
- *MHTML.*
- Soporte *ETRN.*

Conectividad LAN y Host-based.

- Conectividad y Replicación de Directorios .- *Exchange* mantiene habilitadas las opciones de conectividad y replicación de directorios con los sistemas de mensajería de *Microsoft Mail*, *Lotus cc:Mail*, *X.400*, *Lotus Notes*, *Lotus Domino v4.6*, *IBM Office Vision/VM*, *Novel Groups Wise* y *SNADS*.
- Herramientas de Migración .- *Exchange Server* contiene herramientas de migración que le permiten migrar usuarios y datos de los sistemas de correo *Microsoft Mail*, *Lotus cc:Mail*, *Novel Groups Wise*, *Netscape Collabra*, *IBM Office Vision/VM*, *PROFS*, *DEC All-in-One*, *Verimotion MEMO*, *IMAPclients*, *LDAP directories* y *Unix SendMail* hacia *Microsoft Exchange*, cambiando el formato de las cuentas de correo y el formato de los mensajes para un formato reconocido por *Microsoft Exchange*.
- *SMTP Smart-Host* .- El *SMTP smart-host* habilita al *Exchange Server* para direccionar mensajes *SMTP* hacia otro sistema de correo requerido, actuando solo como un puente entre los sistemas de correo, éste puede ser utilizado para el intercambio de mensajes entre diferentes sistemas de correo durante los procesos de migración del mismo.
- *OSI* .- *Exchange Server* cuenta con sistemas integrados de envío de paquetes estándares como *X.400*, *X.500* y *X.25*.
- Replicación entre Organizaciones .- *Exchange Server* permite que diferentes organizaciones puedan compartir directorios e información corporativa.

Cientes :

- *Outlook 98* .- El *software* de *Outlook 98* proporciona el uso de correo electrónico, calendarización en grupos, directorio de contactos y tareas para computadoras de 32-bits.
- *Outlook para Sistemas Operativos de Windows 3.x* .- Esta versión de *Windows* utiliza la misma interface de correo, calendarización de juntas, contactos y tareas que se utilizan en 32 bits, pero para sistemas de 16 bits.
- *Outlook para Sistemas Operativos Macintosh* .- El uso de *Outlook* está adaptado para permitir interoperabilidad con equipos *MAC* con el sistema operativo (*Mac OS 8.5*).
- *Outlook Web Access de Microsoft* .- Se puede utilizar por medio de cualquier *Web Browser* como *Netscape* o *Internet Explorer 4.0*, los usuarios pueden acceder a sus mensajes y opciones de calendarización en forma segura desde cualquier parte de la red por medio de un *browser*, así como las listas corporativas y aplicaciones.
- *Formas HTML* .- Utilizando un *software* de desarrollo de sistemas para aplicaciones *Web* o herramientas autorizadas para desarrollar *HTML*, las formas o desarrollos pueden ser accedadas desde *Outlook* y desplegadas desde cualquier *browser* de *Windows*.

Herramientas de Colaboración :

- *Microsoft Exchange Scripting Agent* .- Permite la creación de soluciones automáticas de procesos por medio de *Workflow* y archivos de instrucciones precisas.
- *ILS* .- Por medio de éste programa se pueden definir juntas, conducir discusiones y participar en documentos y proyectos en línea o en tiempo real.
- *Outlook 98* .- *Outlook 98* provee de un ambiente de desarrollo y modelos de objetos muy completo que proporciona a desarrolladores una herramienta de desarrollo de formas electrónicas o automatización de procesos.

Herramientas de Desarrollo :

- *ASP* .- El *ASP* provee la facilidad de crear aplicaciones *Web* proporcionando acceso a los datos de *Exchange Server* por medio de *VBScript*.
- *CDO* .- El *CDO* permite crear aplicaciones *ASP* más poderosas. Las librerías del *CDO* incluyen objetos de calendario y habilitan a los usuarios a trabajar con calendarización personal y de grupo por medio del *Outlook Web Access*.
- *Design Time Controls and Wizards* .- Permite crear en forma fácil aplicaciones *ASP*.
- *Microsoft Visual InterDev* .- Esta herramienta de desarrollo puede ser utilizada para crear formas *HTML* y otras aplicaciones de sistemas de colaboración.
- *ADSI* .- Construye aplicaciones basadas en *Exchange* que pueden ser integradas con *Microsoft Windows 2000* en servidor y con *Active Directory*.
- *Outlook Forms* .- El ambiente de desarrollo de formas de *Outlook 98* contiene un paquete de herramientas para escribir y debugear *VBScripts*. Incluye el *debugger* y el buscador de objetos que permiten un rápido desarrollo de formas de *Outlook* utilizando scripts y especificando el flujo de las formas. Éstas formas también pueden ser utilizadas en *Outlook 97*.

Manejo y Administración.

Un sistema de mensajería y colaboración debe ser fácil de manejar y administrar, la ventaja de contar con diagnósticos integrados, acceso remoto y con una estructura de directorios flexible, hacen de *Exchange* un *software* de instalación, configuración y administración fácil de utilizar y administrar.

Herramientas de Manejo :

- Integración con las Herramientas de *Windows NT Server* .- Las herramientas de administración de *Windows NT*, el *Performance Monitor* y el *Event Log* son herramientas integradas en *Exchange Server*, permitiendo a los administradores utilizar las mismas herramientas tanto para la administración del sistema operativo como para los servidores de mensajería y colaboración.
- *Server Monitor* .- Esta utilidad funciona en forma proactiva monitoreando el comportamiento del sistema y tomando acciones en el momento en que se presente algún problema.
- *Link Monitor* .- La utilidad de *Link Monitor* funciona también en forma proactiva monitoreando las ligas de comunicación entre los *sites*, la conexión con la *Intranet* y el conector *X.400*.
- *Message Tracker* .- Esta utilidad permite la funcionalidad de rastrear un mensaje en cualquier parte de la red *LAN* o *WAN*, y dentro de *Internet*.
- Recuperación de Mensajes Borrados .- Los registros enviados al *folder* de borrados son marcados con una bandera como borrados y son ocultados de la vista del usuario por un determinado tiempo. Un usuario puede recuperar sus mensajes borrados en cualquier momento durante éste período de tiempo.
- *Simple Network Management Protocol (SNMP)* .- Permite a un administrador manejar en forma eficiente el tráfico de envío y recepción de mensajes, restringiendo cada conector para usos específicos en cada localidad.
- Integración con *Microsoft System Management Server (SMS)* .- Esta integración permite que los clientes de *Exchange* y *Outlook* puedan ser monitoreados y actualizados en forma remota.

Organizaciones Múltiples.

Esta herramienta permite que *Microsoft Exchange* pueda trabajar en forma separada con contenedores virtuales, cada uno de los cuáles puede contener a los usuarios de un área específica. Los accesos pueden ser dados sólo a usuarios que pertenezcan a cada contenedor y éstos solo podrán acceder la información en la que adquirieron permiso.

Arquitectura Multiprotocolos .- Si se requiere toda la funcionalidad de *MAPI* o una solución integral en *Internet*, *Exchange Server* es el único sistema que le permite seleccionar el protocolo y el tipo de cliente que mejor satisfaga sus necesidades sin adquirir un componente adicional.

1.2 Arquitectura de Implementación.

Arquitectura para el Intercambio de Mensajes.

Como parte de la definición de la arquitectura de *Exchange* se deberá considerar principalmente el tamaño de la organización. Existen dos tipos de arquitectura que pueden ser implementadas, la primera *Hub-and-Spoke* y la segunda Arquitectura *Mesh*, la utilización de alguna de éstas arquitecturas es dependiente del tamaño de la organización, si se considera implementar mas de 40 *sites* de *Exchange* en una misma organización, es recomendable utilizar una arquitectura *Hub-and-spoke*. La arquitectura *Mesh* proporciona un buen uso del direccionamiento de tablas pero cuando se consideran organizaciones tan grandes, el redireccionamiento de tablas crece en forma exponencial afectando principalmente las funciones del *MTA*, y haciéndolo ineficiente. Por otro lado la arquitectura *Hub-and-Spoke* utiliza el direccionamiento y la replicación de directorios en servidores independientes dedicados a esta función, llamados *Hub Site*. Los servidores *Spoke Site* están localizados en forma regional y cada uno de ellos se conecta a un *Hub* por medio de conectores.

Como parte del análisis de la arquitectura se determinó utilizar *Hub-and-spoke* para implementar *Microsoft Exchange* en toda la organización. Esta arquitectura proporciona una administración eficiente, y solución de problemas desde una región soportada a otra región soportada.

El diseño de la arquitectura a ser implementada es el resultado de la colaboración tanto del equipo de trabajo de la organización como de los servicios de consultoría de *Microsoft*.

El equipo definirá y construirá la arquitectura necesaria dividiéndola en dos fases. La primera deberá determinar la arquitectura medular que resultará al crear los *Exchange Hubs*. La segunda deberá establecer el criterio y uso de esto, determinando que localidades deberán contar con servidores locales y cuáles de éstos servidores deberán ser construidos dentro de éstas regiones. Cada una de éstas fases se describirá a detalle a continuación:

Definiciones de *Exchange* Necesarias para la Implementación.

Exchange se define como una organización de grupos lógicos llamados *sites*. Éstos *sites* son básicamente *Regiones Exchange* que contienen o pueden contener cierto número de servidores *Exchange*. Éstos servidores no necesariamente deben estar en una localidad geográfica, pueden, esencialmente estar en algún otro lugar.

Los servidores *Exchange* pueden ser utilizados para almacenar correos para cualquier número de usuarios. Éstos también pueden ser utilizados como *Servidores Bridgehead*. El propósito de un *Servidor Bridgehead* es tomar un mensaje y pasarlo a otro servidor dentro de la *Región Exchange*, o también pasar el mensaje a una diferente *Región Exchange*. Con tal de que los servidores *Exchange* sean parte de la misma *Región Exchange*, éstos pueden realizar las funciones de *servidor Bridgehead* y servidor de correos, o las tareas pueden ser divididas entre dos diferentes servidores.

Si una *región Exchange* tiene el potencial de direccionar algunos mensajes con otras *regiones Exchange*, entonces éstas serán más eficientes al tener un servidor dedicado con la función única de *servidor Bridgehead*. Esto será comentado a detalle en las siguientes secciones.

Arquitectura de un Hub.

Microsoft Exchange direcciona mensajes desde una región a otra con base en tablas de direccionamiento, las cuáles almacenan la configuración de cada región. Como resultado, un mensaje enviado desde un servidor a otro puede conseguir llegar a otra región del servidor destino.

Pensando en esto, se determinaron tres regiones principales que serán responsables de direccionar mensajes en toda la organización. Éstas regiones deberán ser identificadas como *regiones Exchange Hub*.

La primer región principal estará ubicada en Casa Matriz (NJ). Las otras dos regiones principales deberán estar ubicadas, una en Alemania y otra en Inglaterra. La Figura 1.1 ilustra la arquitectura de múltiples *Hub*.

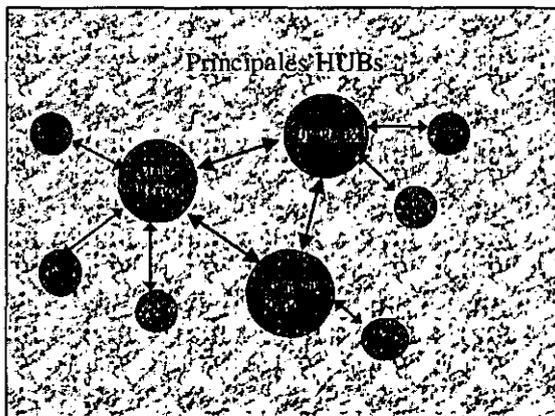


Fig. 1.1 Principales *Hubs*

Consideraciones para Definir un *Hub*.

Si un mensaje es enviado de la región D a la B, el mensaje deberá ser encaminado a través del *Hub* del Reino Unido y enviado al *Hub* de la región Matriz, posteriormente de ahí es enviado a la región B. Cuando se presente algún problema en cualquiera de los *Hubs* principales, los mensajes deberán ser direccionados por el *Hub* que se encuentre funcionando.

Desde ahora éstas tres principales regiones *Hub* deberán ser los factores críticos a tomar en cuenta en el diseño de la *arquitectura Exchange*, cada una de éstas regiones deberá ser configurada para asegurar la redundancia. Esto es recomendado para cada una de las principales *regiones Exchange* debiendo tener un servidor dedicado *Bridgehead* cuyo principal propósito será direccionar mensajes desde una región a la próxima. Un servidor de correos en una región puede funcionar como un respaldo del *servidor Bridgehead* en caso de que el *servidor Bridgehead* esté expuesto a fallas en el *hardware* o *software*.

La siguiente tabla resume las consideraciones para la construcción de un sitio *Hub (Hub site)*.

Ubicación del <i>Hub</i>	El <i>Hub</i> deberá estar ubicado cerca de la red física para minimizar el tráfico de la red.
Fiabilidad	El <i>Hub</i> deberá ser configurado con redundancia para evitar interrupciones de servicio. Además deberá ser lo suficientemente poderoso para administrar el tráfico en el <i>Hub</i> .
Problemas en NT	El administrador del <i>Hub</i> deberá dar soporte al <i>Hub</i> principal. El administrador será el responsable de dar de alta los conectores para cada uno de los sitios que pueda soportar. La ubicación del Dominio es crítico, ya que deberán establecerse relaciones de confianza entre los dominios donde residen los servidores <i>Hub</i> .

Criterios de Ubicación de Servidores/*Sites*.

Una *región Exchange* deberá consistir en un grupo de servidores donde los correos de los usuarios sean almacenados. Cada sitio contendrá un número de servidores. Éstos servidores no necesitan estar físicamente en la misma localidad.

Cada servidor puede dar servicio a más de una localidad desde el mismo *site*.

A continuación se mencionan las regiones existentes, la ubicación de los servidores de correo y las regiones que reciben servicio de correo de la región a la que pertenecen, adicionalmente se identificarán con ** las regiones que manejarán la administración de la región.

Europa:

Región	Ubicación del servidor	Ubicación del servicio
Francia	Colman, Francia	Francia, Colmar
	Courbevoie, Francia **	Francia, Courbevoie
		Francia, Orleans(Posible servidor)
		Morocco, Casa Blanca
		Senegal, Dakar
	Fresnes, Francia	Francia, Fresnes
Alemania	Frelburg, Alemania **	Alemania, Frelburg
		Austria, Viena
		Polonia
		Checoeslovaquia
		Hungría
	Alemania, Melle	Alemania, Melle
	Alemania, Solingen	Alemania, Solingen
Iberia	Barcelona, España **	España, Barcelona
		España, Madrid
		Portugal, Alfragide
	Atenas AE, Grecia	Grecia, Atenas AE
		Grecia, Atenas (LC)
		Egipto, Alejandría
		Libano
	Milan, Italia	Italia, Milan
UK Region	Eastleigh, UK **	UK, Eastleigh
		Scandinavia, Solna
	Cambridge, UK	UK, Cambridge
South Africa	Cape Town **	South Africa

Asia/Australia :

Región	Ubicación del servidor	Ubicación del servicio
Australia	Sidney **	Australia
		Nueva Zelanda
India	Bombay **	India
Japón	Tokio **	Japón
China	Hong Kong(W-L) **	Hong Kong(W-L)
		Hong Kong(SPG)
		Hong Kong(Región SEA)
		China, Guangzhou (W-L)
		China, Guangzhou(SPG)
		Singapur (SPG)
		Malasia (SPG)
Filipinas	Manila **	Filipinas
		Indonesia (W-L)
		Malasia (W-L)
		Singapur (W-L)
Tailandia	Samutprakam **	Tailandia

Sudamérica :

Región	Ubicación del servidor	Ubicación del servicio
Rep. Dominicana	Sto. Domingo **	República Dominicana
Guatemala	Guatemala **	Guatemala
		Costa Rica
		El Salvador
		Honduras
		Nicaragua
		Panamá
Carolina	Carolina, PR **	Carolina
Colombia	Colombia **	Colombia
Perú	Perú **	Perú
		Bolivia
Venezuela	Venezuela **	Venezuela
Argentina	Argentina	Argentina
		Chile (Posible Servidor)
		Uruguay
Brasil	Brasil **	Brasil
México	México **	México
		Ecuador

Norte América :

Región	Ubicación del servidor	Ubicación del servicio
WLBB	MOPS **	MOPS
AA	Ann Arbor **	Ann Arbor
		Sheridan Park
PDMOPS	MOPS(PD) **	MOPS
		EN CBU
		SE CBU
		Central CBU
		West CBU
MOPS	MOPS **	MOPS
ML	Milford **	Milford
Rockford	Rockford **	Rockford
Greenwoot	Greenwoot **	Greenwoot
Lititz	Lititz **	Lititz
Toronto	Toronto **	Toronto
Holanda	Holanda MI **	Holanda MI
Rotchester	Rotchester MI **	Rotchester MI
Vega Baja	Vega Baja PR **	Vega Baja
		Fajardo
Elk Grove	Elk Grove **	Elk Grove
Virginia	Blacksburg **	Blacksburg
	Dublín, VA	Dublín, VA

2.1 Esquema de Conexiones para Casa Matriz.

Conectividad Digital.

Algunas organizaciones requieren un ambiente de transmisión más rápido y más seguro que las que proporcionan las líneas analógicas; para éste fin, se pueden utilizar las líneas *DDS*. Las líneas *DDS* proporcionan comunicaciones síncronas punto-a-punto de 2.4, 4.8, 9.6 o 56 Kbps. Los circuitos digitales punto-a-punto son circuitos dedicados que pueden proporcionar varias señales portadoras de telecomunicaciones. Las señales portadoras garantizan un ancho de banda *Full-Duplex* que se instala permanentemente con una liga desde cada punto final.

En algunos casos, las líneas analógicas proporcionan suficiente conectividad. Pero cuando una organización genera mucho tráfico en una red *WAN*, la transmisión generada con una conexión analógica resulta ineficaz y cara, siendo mejor considerar otras alternativas.

La principal razón por la cual se utilizan líneas digitales, es porque éstas proporcionan transmisiones libres de errores en casi un 99 %. Las líneas digitales están disponibles en varias formas, las cuáles incluyen *DDS*, *T1*, *T3*, *T4* y *Switched 56*. Un ejemplo del servicio de línea digital se muestra en la Fig. 2.1.

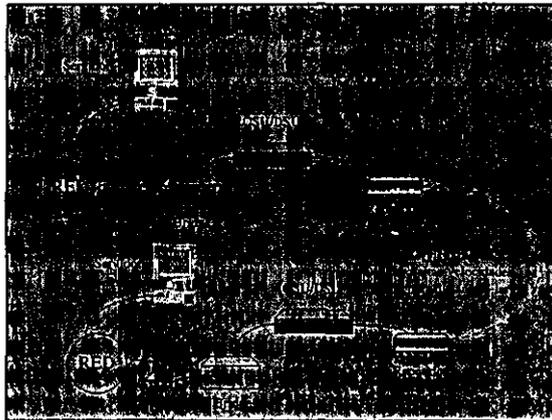


Fig 2.1 Servicio de Línea Digital que une dos redes remotas.

Una causa por la cual se utilizan comunicaciones digitales *DDS*, es porque no se requiere de un modem. Sin embargo, las líneas *DDS* envían datos a través de un *bridge* o un *router* por un

dispositivo llamado *CSU/DSU*. Éste dispositivo convierte señales digitales estándares generadas por una computadora en un tipo de señales digitales (bipolares) que son parte del ambiente de comunicaciones síncronas. Éste esquema, contiene elementos electrónicos que protegen el servicio de red.

Línea Digital *T1*.

T1 es, quizás, el tipo de línea digital más utilizado para transmisión de datos a alta velocidad. Es una tecnología de transmisión punto-a-punto que utiliza dos pares de cables (uno para enviar y otro para recibir) para transmitir una señal *Full-duplex* a una velocidad de 1.544 Mbps. La línea digital *T1* es utilizada para transmisión digital de voz, datos y video.

Las líneas digitales *T1* están consideradas entre las más costosas para conectar redes *WAN*. Los usuarios que no necesitan o no puedan generar el ancho de banda completo de la línea *T1* pueden utilizar uno o más canales *T1* de 64 Kbps conocidos como *FT-1*.

En algunos países, el servicio de líneas digitales *T1* no está disponible. Sin embargo a menudo existe un servicio similar llamado *E1*. La línea digital *E1* es muy similar a *T1*, sin embargo tiene una velocidad de señal de 2.048 Mbps.

***Multiplexing*.**

Las líneas digitales *T1* utilizan la tecnología llamada '*multiplexing*' o '*muxing*', desarrollada por los laboratorios *Bell*, diferentes señales desde diferentes fuentes son concentradas en un dispositivo llamado multiplexor y son alimentadas a un cable de transmisión. Al recibir la señal de finalización, el dato es de-multiplexado hacia su forma original. Esta necesidad surgió cuando los cables de teléfono, que llevaban sólo una conversación por cable, se vieron atestados. La respuesta a éste problema se llamó *T-Carrier network* y fue implementada por los laboratorios *Bell* para llevar varias llamadas sobre un mismo cable.

Dividiendo el Canal *T1*.

Un canal *T1* puede llevar 1.544 megabits de datos por segundo, siendo esta la unidad básica del servicio *T-Carrier*. La línea *T1* divide esta unidad en 24 canales, y muestras por cada canal de 8,000 veces por segundo. Utilizando éste método, *T1* permite mezclar 24 transmisiones de datos simultáneamente por cada par de cables.

Cada canal incorpora muestras de 8 bits. Ya que cada canal obtiene una muestra cada 8,000 veces por segundo, cada uno de los 24 canales puede transmitir hasta 64 Kbps. Esta velocidad estándar de datos es conocida como *DS-0*. La velocidad de datos a 1.544 Mbps es conocida como *DS-1*.

Las velocidades *DS-1* pueden ser multiplexadas para proporcionar velocidades de transmisión iguales o mayores, conocidas como *DS-1C*, *DS-2*, *DS-3* y *DS-4*. Éstas velocidades de transmisión se listan en la tabla siguiente :

Nivel de Señal	Carrier System	T-1 channels	Voice Channels	Data rate (Mbps)
<i>DS-0</i>	<i>N/A</i>	<i>N/A</i>	1	0.0064
<i>DS-1</i>	<i>T1</i>	1	24	1.544
<i>DS-1C</i>	<i>T-1C</i>	2	48	3.152
<i>DS-2</i>	<i>T2</i>	4	96	6.312
<i>DS-3</i>	<i>T3</i>	28	672	44.736
<i>DS-4</i>	<i>T4</i>	168	4032	274.760

El cable de cobre es utilizado para *T1* y *T2*. Sin embargo, *T3* y *T4* requieren un medio de mayor frecuencia tal como microondas o fibra óptica.

Línea Digital *T3*.

Las líneas digitales *T3* y el fraccional *T-3* dan un servicio que proporciona voz y calidad de datos desde 6 Mbps hasta 45 Mbps. Hoy en día, éstas líneas proporcionan la más alta capacidad de servicio disponible. Las líneas digitales *T3* y *FT-3* fueron diseñadas para transportar grandes cantidades de datos con una alta rapidez entre dos puntos fijos, y pueden ser utilizadas para reemplazar a las líneas *T1*.

Línea Digital *Switched 56*.

Las compañías de teléfonos locales y de larga distancia ofrecen el servicio digital para conectar vía modem redes *LAN* a *LAN* que transmiten datos a 56 Kbps. El servicio *Switched 56* es meramente un circuito que cambia de versión para líneas *DDS* a 56 Kbps. La ventaja de *Switched 56* es que se utiliza de acuerdo a la demanda, por eso elimina el costo de una línea especializada. Cada computadora que utiliza éste servicio debe estar equipada con un *CSU/DSU*, éste puede estar conectado a través de una conexión vía telefónica (*dial up*) con otro sitio *Switched 56*.

Criterio Utilizado para Determinar Donde se Definiría un Site.

Uno de los factores más importantes para establecer éste criterio es determinar cuáles son las necesidades de negocio de cada localidad, esta consideracion podría determinar en un momento donde puede ser configurado un servidor y donde sería vital para la empresa contar con un servidor de mensajería.

Crítico y Disponible.

Si un usuario tiene un servicio de correo en un servidor remoto y la línea de comunicación se cae, el usuario pierde su correo por el tiempo que la línea de comunicación esté abajo, pero si se cuenta en forma local con un servidor de correo y la línea de comunicación se cae, el usuario no pierde el servicio de correo local.

Demanda (Número de Usuarios y Volumen de Información).

El número de usuarios y la cantidad de mensajes que serán almacenados deben ser también tomados en cuenta. Las localidades que contienen 100 o más usuarios con servicio de mensajería deberán contar con un servidor en forma local. Aquella localidad que consuma demasiado espacio en mensajes voluminosos o con presentaciones también deberá contar con un servidor específico para el almacenamiento de sus mensajes.

Requerimientos de Tiempo de Respuesta del Cliente.

Si los usuarios tiene uso de sus correos a través de las conexiones *WAN*, el tiempo de respuesta debe ser tomado en cuenta, por lo que sí el usuario va a recibir una cantidad de mensajes ilimitados o con un alto volumen de anexos, no se recomiendan conexiones remotas. Los equipos de cómputo deben tener los recursos suficientes para soportar *Windows NT 4.0*, *Windows 95* y *Outlook*.

Requerimientos y Consideraciones.

Si una localidad es considerada como una localidad para instalar un servidor de *Exchange*, ésta debe contar con los recursos suficientes para soportar *Windows NT* y el ambiente de *Exchange*. El administrador deberá contar con los conocimientos necesarios para dar soporte a ambos ambientes.

2.2 Servidores Principales de Conexión.

Envío de Datos a través de Redes WAN.

Existen tecnologías que no proporcionan la rapidez o el ancho de banda que una organización necesita, por lo que los administradores de red deben considerar otros ambientes más avanzados para las redes WAN que día con día son más populares por su evolución tecnológica. Éstas incluyen :

- X.25.
- Frame Relay.
- ATM.
- ISDN.
- FDDI.
- SONET.
- SMDS.

X.25.

El X.25 es un conjunto de protocolos que se encuentran en las redes *packet-switching*. La red *packet-switching* se creó con el propósito de intercambiar servicios que originalmente se establecieron para conectar terminales remotas hacia sistemas *mainframe*.

Una red X.25 *packet-switching* utiliza interruptores, circuitos y rutas que están disponibles para proporcionar la asignación del mejor camino a cualquier tiempo y lugar en particular, cómo se muestra en la Fig. 2.2.

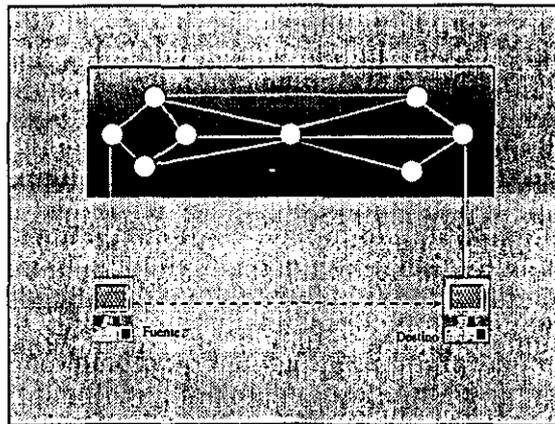


Fig. 2.2 El X.25 Packet Switching utiliza la mejor ruta para cada transmisión.

Las primeras redes X.25 utilizaban líneas telefónicas para transmitir datos. Éste era un medio poco confiable que dió como resultado muchos errores, así X.25 incorporó un sistema extensivo verificador de error. Debido a la verificación de todo error y la retransmisión, X.25 puede parecer estar lento.

Actualmente el conjunto de protocolos X.25 define la interface entre un *host* del paquete-modo síncrono u otro dispositivo, y la *PDN* sobre un circuito dedicado o un circuito de línea rentada. Esta interfase es en realidad un *DTE/DCE*.

Como ejemplos de *DTEs* tenemos los siguientes puntos :

- Una computadora (*host*) con una interfase X.25.
- Un *PAD* que recibe caracteres asíncronos como entrada de una terminal de baja velocidad y los une en paquetes para transmitirlos sobre la red. La *PAD* también desmonta paquetes recibidos a través de la red, así los datos se pueden entregar como caracteres a las terminales.
- Un *gateway* entre el *PDN* y una *LAN* o *WAN*.

Estos tres son ejemplos de *DTE*, el *DCE* que es la mitad del *DTE/DCE* es la *PDN*.

En la Fig. 2.3 se muestran ejemplos de *DTEs* :

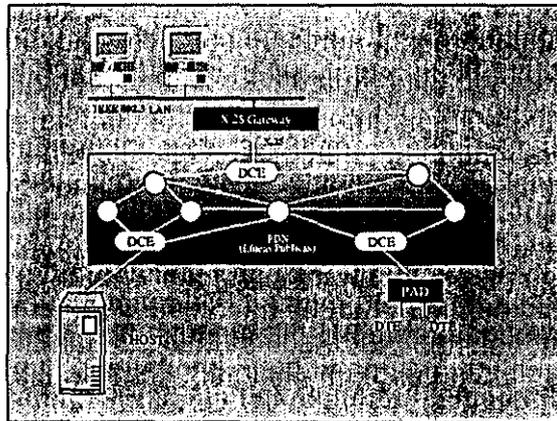


Fig. 2.3 Ejemplos de *DTE's*.

FRAME RELAY.

Debido a que las comunicaciones de red avanzan hacia ambientes digitales y de fibra óptica, las nuevas tecnologías aparecerán con menos errores de verificación comparadas con los primeros métodos analógicos *packet-switching*.

Frame relay es un paquete avanzado y rápido con tecnología digital de longitud variable *packet-switching*. Con esta tecnología, los diseñadores han suprimido muchas de las funciones de verificación de las X.25 que no son necesarias en un ambiente seguro y confiable de circuitos de fibra óptica.

Frame relay es un sistema punto-a-punto (mostrado en la Fig. 2.4) que utiliza un *PVC* que transmite *frames* de longitud variable a la capa *Data Link*. Los datos viajan por la red sobre una línea digital y los introduce a la red *Frame Relay*, éstos fluyen a través de ésta y se entregan a la red destinataria.

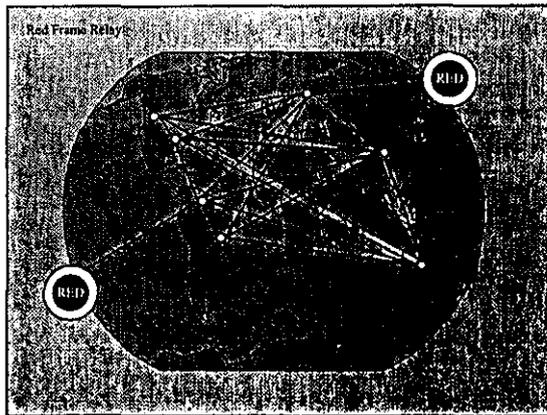


Fig. 2.4 El *Frame Relay* utiliza un sistema punto a punto.

Las redes *Frame Relay* están ganando popularidad porque son mucho más rápidas que otros sistemas de intercambio al ejecutar el funcionamiento básico de *packet-switching*. Esto es porque *Frame Relay* utiliza un *PVC*, así se puede conocer la ruta entera de extremo a extremo. No hay ninguna necesidad de dispositivos de *Frame Relay* para ejecutar la fragmentación y el reensamble o para proporcionar la asignación de la mejor ruta.

Estas redes pueden proporcionar también subscriptores con el ancho de banda de acuerdo a las necesidades, permitiéndolo que el usuario realice casi cualquier tipo de transmisión.

La tecnología *Frame Relay* requiere un competente *router* o *bridge* con buen porcentaje de éxito en la transmisión de datos sobre la red. Un *Frame Relay Router* requerirá por lo menos un puerto *WAN* para una conexión a la red *Frame Relay* y otro puerto para la *LAN*.

ATM.

El *ATM* es una aplicación avanzada de *packet-switching* que proporciona transmisiones de datos a gran velocidad para enviar paquetes de tamaño fijo sobre una banda ancha y una banda base para ambientes *LAN* o *WAN*. El *ATM* puede entregar :

- Voz.
- Datos.
- Fax.
- Video en tiempo real.
- CD- calidad de audio.
- Imágenes.
- Transmisión de datos a Multimegabit.

El *CCITT* definió el *ATM* en 1988 como parte de los servicios integrales de banda ancha de redes digitales. Debido a que los *ATM*'s son poderosos y versátiles, influenciarán el futuro de las comunicaciones de la red. Es igualmente adaptable para ambientes *LAN* y *WAN*, y puede transmitir datos a velocidades muy altas (de 155 Mbps a 622 Mbps o más).

Tecnología ATM.

El método llamado *ATM*, es un método que sustituye un paquete de banda ancha que transmite datos en paquetes de 53 bytes en lugar de *frames* de longitud variable. Éstos paquetes constan de 48 bytes de información de la aplicación con cinco bytes adicionales de *ATM* de datos del *header*. Por ejemplo, *ATM* dividiría un paquete de 1000-bytes en 21 *frames* de datos y pondrá cada *frame* de datos en un paquete. El resultado es una tecnología que transmite un paquete uniforme y consistente.

La Fig. 2.5 muestra el método que utiliza ATM para la transmisión de paquetes de información.

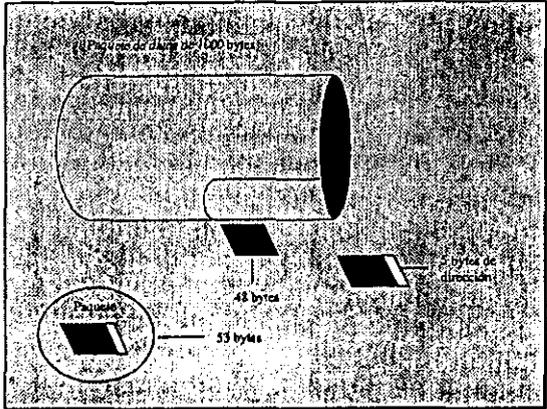


Fig. 2.5 Los paquetes *ATM* contienen 48 bytes de datos y 5 de *header*.

El equipo de la red puede cambiar, direccionar, y mover *frames* de tamaño uniforme mucho más rápidamente que los *frames* de tamaño irregular. El tamaño fijo del paquete normalmente utiliza *buffers* eficaces que reducen el trabajo requerido para procesar datos que entran. El tamaño uniforme del paquete también proporciona ayuda en la aplicación de la planificación del ancho de banda.

Teóricamente, *ATM* puede ofrecer velocidades disponibles de hasta 1.2 gigabits por segundo. Sin embargo, *ATM* mide su rapidez contra las velocidades de la fibra óptica que puede alcanzar tanto como 622 Mbps. El *ATM* más comercial permite transmisiones de datos aproximadamente a 155 Mbps.

Como ejemplo, considerando una rapidez de 622 Mbps, *ATM* puede transmitir todos los volúmenes enteros de la edición más reciente de la Enciclopedia Británica incluyendo las gráficas, en menos de un segundo. Si se prueba la transferencia utilizando 2400 baudios vía modem, la operación tomaría más de dos días.

Se puede utilizar *ATM* tanto en *LAN* y *WAN* aproximadamente con la misma rapidez. *ATM* cuenta con portadores como *AT&T* y *US Sprint* para implementar la aplicación encima de una extensa área. Esto creará un ambiente consistente que terminará con el concepto de lentitud de la *WAN* y las diferentes tecnologías utilizadas en los ambientes *LAN* y *WAN*.

Componentes *ATM*.

Los componentes *ATM* están, comúnmente, disponibles sólo por un número limitado de distribuidores. Todo *hardware* en una red *ATM* tiene que ser compatible con *ATM*. La implicación de esto es que al implementar *ATM* existe la facilidad requerida para reemplazar el equipo común. Esta es una razón por la que no se ha adoptado más rápidamente al *ATM*.

Sin embargo, como el mercado de *ATM* evoluciona, se pueden proporcionar a los usuarios varias ventajas :

- *Routers* y *switches* para conectar servicios de portadores hacia una base global.
- Dispositivos *Backbone* para conectar todas las redes *LAN* dentro de una organización grande.
- *Switches* y adaptadores que enlazan computadoras de escritorio a conexiones *ATM* de gran velocidad para utilizar aplicaciones de multimedia.

Medios de Comunicación *ATM*.

ATM no restringe cualquier tipo de medio de comunicación (tipos de cableado) en particular. Se pueden utilizar medios existentes diseñados para otros sistemas de comunicaciones, incluso:

- Cable Coaxial.
- Par trenzado (*Twisted-pair*).
- Fibra óptica.

Sin embargo, éstos medios tradicionales de comunicación de la red no soportan todas las capacidades de las *ATM*'s. Una organización llamada Foro *ATM* recomienda las siguientes interfaces físicas para *ATM* :

- *FDDI* (100 Mbps).
- *Fiber Channel* (155 Mbps).
- *OC3 SONET* (155 Mbps).
- *T3* (45 Mbps).
- Otras interfaces que incluyen *frame relay* y *X.25*.

Interruptores ATM.

Los interruptores *ATM* son dispositivos multipuerto que pueden actuar en cualquiera de las dos formas siguientes :

- *Hubs* para reenviar datos de una computadora a otra dentro de una red.
- *Routers* como dispositivos para reenviar datos con gran rapidez a redes remotas.

En algunas arquitecturas de red tal como *Ethernet* y *Token Ring*, sólo una computadora transmite a un tiempo. *ATM*, sin embargo, utiliza interruptores como multiplexores que permiten que varias computadoras pongan datos en una red simultáneamente. En la Fig. 2.6, tres *routers* alimentan datos en el interruptor *ATM* y se envían sobre la red *ATM* al mismo tiempo.

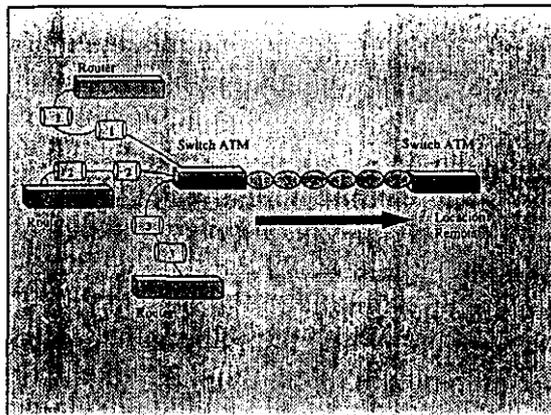


Fig. 2.6 Los *switches ATM* actúan como multiplexores que permiten introducir múltiples datos.

Consideraciones ATM.

ATM es una tecnología relativamente nueva que requiere *hardware* especial y un ancho de banda excepcional para alcanzar su máximo potencial. La actual tecnología *WAN* no tiene el ancho de banda requerido para soportar *ATM* en tiempo real. Las aplicaciones que soportan video o voz saturarían los ambientes actuales de la red y frustraría a los usuarios al tratar de utilizarla para sus negocios. También, implementar y dar el apoyo a *ATM* requiere de especialización que no se encuentra suficientemente disponible.

ISDN.

El *ISDN* es una especificación de conectividad digital interna de ambientes *LAN* que proporciona

- Voz.
- Datos.
- Imágenes.

Una de las metas originales de los diseñadores de *ISDN* era la de unir hogares y negocios con alambres telefónicos de cobre. El primer *ISDN* implementó un plan que exigía convertir los circuitos existentes de teléfono de analógicos a digitales. Éste plan se llevó a cabo mundialmente.

La velocidad básica de *ISDN* divide su ancho de banda disponible en tres canales de datos. Dos de éstos mueven datos a 64 Kbps, y el tercero transmite a 16 Kbps. Los canales a 64 Kbps son conocidos como canales *B*. Éstos canales pueden transportar voz, datos, o imágenes. El canal más lento, que es de 16 Kbps, es llamado el canal *D*. El canal *D* lleva la señalización y el manejo de los datos. El servicio *ISDN* de velocidad básica es llamado *2B+D*.

Una computadora conectada a un servicio *ISDN* puede utilizar los dos canales *B* al mismo tiempo para fusionar 128 Kbps de flujo de datos. Si ambas estaciones extremas soportan compresión, se puede alcanzar una velocidad mucho más alta.

La velocidad primaria de *ISDN* utiliza por completo el ancho de banda de una línea *T1* para proporcionar 23 canales *B* a 64 Kbps y un canal *D* a 64 Kbps. El canal *D* es sólo utilizado para señalización y manejo del enlace.

Las redes que utilizan los servicios de *ISDN* deben considerar si usan velocidad básica o velocidad primaria, basándose en sus necesidades para disponer de los datos. El *ISDN* es el reemplazo digital para las redes telefónicas públicas, y como tal es un servicio *dial-up* solamente.

FDDI.

El *FDDI* es una especificación que describe velocidades altas (100 Mbps) para redes *token-passing ring* que utiliza como medio de comunicación la fibra óptica. Fue creada por el comité *ANSI X3T9.5*, y se liberó en 1986. El *FDDI* fue diseñado para computadoras que se encuentran separadas por grandes distancias, las cuáles no encontraban el suficiente ancho de banda, para éste fin sólo existían las arquitecturas *Ethernet* de 10 Mbps o *Token Ring* de 4 Mbps.

El *FDDI* se utiliza para proporcionar conexiones a gran velocidad para diferentes tipos de redes. *FDDI* se puede utilizar para redes de área metropolitana conectando redes en la misma ciudad con una conexión de cable de fibra óptica a gran velocidad. Se limita a un anillo o circunferencia de máxima longitud de 100 kilómetros, ésta en realidad no fue diseñada para utilizarse como una tecnología *WAN*.

Las redes en ambientes a grandes distancias utilizan *FDDI* para conectar componentes muy grandes y minicomputadoras en un sitio tradicional de computadoras, a veces llamadas redes *back-end*. Éstas redes manejan típicamente la transferencia de archivos mucho más lejos que la comunicación interactiva. Cuando se comunica con un *mainframe*, la minicomputadora o computadora personal a menudo requiere una constante de tiempo real que utilizan los medios de comunicación. Incluso requerirían un exclusivo uso de los medios de comunicación por períodos extendidos de tiempo.

El *FDDI* trabaja con redes *backbone* que otras *LANs* de capacidad baja pueden conectar. No es una medida inteligente conectar todo del equipo de procesamiento de datos en una empresa a una *LAN*, porque el tráfico cargaría excesivamente la red y una falla puede detener el funcionamiento del proceso entero de los datos de la compañía.

Los ambientes *LAN* que requieren altas cargas de datos y un ancho de banda bastante grande puede utilizar conexiones *FDDI*. Éstas son redes que están compuestas por computadoras de alto diseño de ingeniería u otras computadoras que deben soportar aplicaciones con mayor ancho de banda tal como video, diseño asistido por computadora, y diseño industrial por computadora.

Cualquier oficina que requiera un funcionamiento de la red a gran velocidad deberá considerar utilizar *FDDI*. Igual en oficinas de negocios, productores de gráficos para presentaciones y otra documentación que puede saturar y alentar una red.

Token Passing.

Mientras *FDDI* utiliza un sistema estándar de *token passing*, hay diferencias entre *FDDI* y 802.5. Una computadora en una red *FDDI* puede transmitir tantos *frames* como pueda producir dentro de un tiempo predeterminado, antes de permitir que el *token* salga. En cuanto una computadora transmite de un lado a otro, suelta el *token*.

Una computadora suelta el *token* cuando termina de transmitir, en éste momento habría varios *frames* circulando en el anillo uno tras otro. Esto explica porqué *FDDI* ofrece mayor disponibilidad que redes *Token Ring*, por que sólo deja circular uno a un tiempo.

Topología.

El *FDDI* opera a 100 Mbps dentro de una topología *dual-ring* que soporta 500 computadoras en una distancia de 100 kilómetros (62 millas).

El *FDDI* utiliza tecnología de red compartida. Esto significa que más de una computadora puede realizar sus transmisiones a un mismo tiempo. Aunque *FDDI* puede proporcionar un servicio de 100 Mbps, al compartir la red, se puede aproximar a la saturación de ésta. Por ejemplo, si diez computadoras están transmitiendo al mismo tiempo a 10 Mbps, la transmisión total será de 100 Mbps.

En transmisión de video o multimedia, se igualarán los 100 Mbps de velocidad de transmisión con lo cual puede formarse un cuello de botella.

El *FDDI* utiliza el sistema *token passing* en el esquema del *dual-ring*, como se muestra en la Fig. 2.7. El tráfico en una red *FDDI* consiste en dos corrientes similares fluyendo en direcciones opuestas alrededor de dos *counter-rotating rings*. Un anillo es llamado el anillo primario y el otro es el anillo secundario.

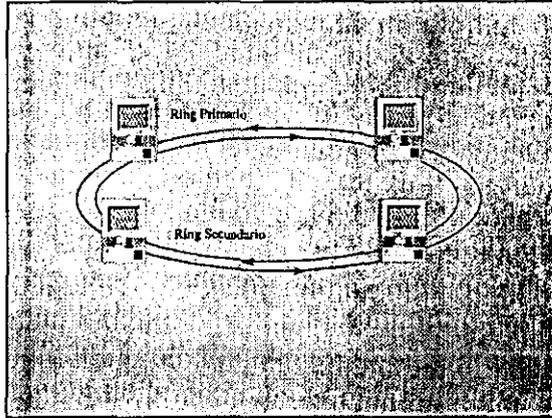


Fig. 2.7 *FDDI* utiliza la topología *dual-ring*

El tráfico normalmente fluye sólo en el anillo primario. Si el anillo primario falla, *FDDI* automáticamente configura la red para que los datos fluyan en el anillo secundario utilizando la dirección opuesta.

Una de las ventajas de la topología del *dual-ring* es la redundancia. Uno de los anillos se utiliza para la transmisión, y otro se usa como respaldo. Si hay un problema, tal como una falla en el anillo o un cable roto, el anillo se configura a sí mismo y continúa con la transmisión.

La longitud total del cable combinada de ambos anillos no debe exceder de 200 kilómetros, y no puede sostener más de 1000 computadoras. Sin embargo, como el segundo anillo redundante protege contra fallas del anillo, las capacidades totales se deben dividir por la mitad. Por consiguiente, cada red *FDDI* se debe limitar a 500 computadoras y 100 kilómetros de cable. También se debe considerar un repetidor, por lo menos, cada dos kilómetros.

Las computadoras pueden conectarse a uno o ambos cables *FDDI* en un anillo. Éstas computadoras (que se conectan con ambos cables) se conocen como Estaciones Clase A, y las que se conectan a un único anillo se llaman Estaciones Clase B.

Si hay una falla en la red, las estaciones Clase A pueden ayudar a reconfigurar la red; las estaciones clase B no pueden realizar esta tarea. Esto es mostrado en la Fig. 2.8.

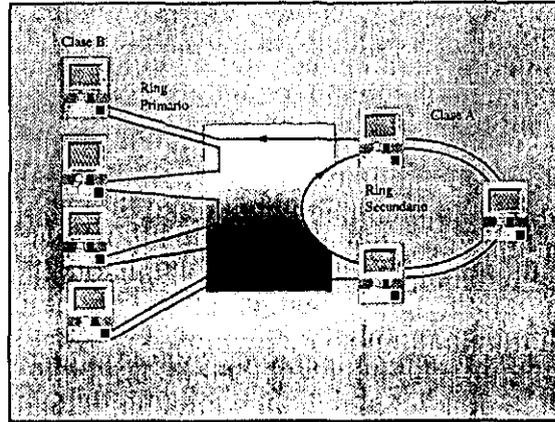


Fig. 2.8 Computadoras clase A conectan dos anillos, las clase B solamente uno.

FDDI en Estrella.

Las computadoras *FDDI* pueden proporcionar enlaces punto a punto hacia un *hub*. Esto significa que *FDDI* puede implementar el uso de la topología estrella-anillo. Esta es una ventaja que puede :

- Ayudar a resolver problemas
- Toma las ventajas del manejo y las capacidades para resolver problemas de los *hubs* avanzados.

Beaconing.

Todas las computadoras en una red *FDDI* son responsables de supervisar el proceso *token passing*, para aislar fallas serias en el anillo. *FDDI* utiliza un sistema llamado *beaconing*. Utilizando *beaconing*, la computadora descubre una falla enviando una señal llamada *beacon* hacia la red. La computadora continuará enviando el *beacon* hasta que se da cuenta la computadora vecina anterior del *beacon*, y entonces se detiene. Éste proceso continúa hasta que la única computadora que envía el *beacon* sea la que directamente da de baja la falla.

Como se ilustra en la Fig. 2.9, la computadora 1 genera una falla. La computadora 3 descubre la falla, se inicia el *beacon*, y continúa así hasta que recibe un *beacon* de la computadora 2. La computadora 2 continúa con el *beacon* hasta que recibe un *beacon* de la computadora 1. Debido a que la computadora 1 es la única con falla, la computadora 2 continuará con el *beacon* y el punto exacto de la falla será en la computadora 1.

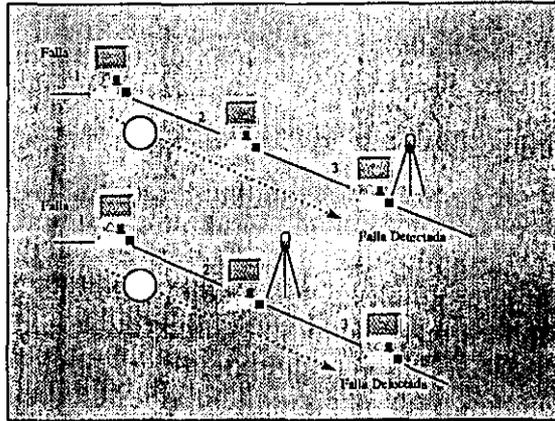


Fig. 2.9 FDDI utiliza el *beaconing* para aislar problemas.

Cuando la computadora del *beaconing* finalmente recibe su propio *beacon*, asume que el problema se ha arreglado, regenera una *token*, y la red le vuelve a su funcionamiento normal.

Medios de Comunicación.

El medio de comunicación principal para *FDDI's* es el cable de fibra óptica. Esto significa que *FDDI* es :

- Inmune a interferencias electromagnéticas o al ruido.
- Seguro porque el cable de fibra óptica no emite señales que no puedan ser controladas.
- Hábil para transmitir en distancias largas antes de requerir un repetidor.

Se puede utilizar *FDDI* también en alambre de cobre, conocido como interface de cobre para datos distribuidos *CDDI*, pero esta limitaría seriamente su capacidad de distancia.

RED SÍNCRONA ÓPTICA (*SONET*).

La red síncrona óptica (*SONET*) es uno de los diferentes sistemas emergentes que aprovechan las ventajas de la tecnología de fibra óptica. Puede transmitir datos a más de un gigabit por segundo. Las redes basadas en esta tecnología son capaces de entregar voz, datos y video sin ningún problema.

SONET es un estándar o norma para transporte óptico creado por la *ECSA* de la *ANSI*. *SONET* se ha incorporado a las recomendaciones de *Synchronous Digital Hierarchy* del *CCITT*, también conocida como la *ITU*, la cual tiene las normas o estándares para telecomunicaciones internacionales.

SONET define un portador óptico (*OC*) el cual nivela y transporta señales eléctricas equivalentes síncronas (*STS's*) para transmisión jerárquica basada en la fibra óptica.

SONET utiliza una tasa básica de transmisión *STS-1*, que es equivalente a 51.84 Mbps. Sin embargo, señales de alto nivel se pueden alcanzar y son múltiplos enteros de la velocidad base. Por ejemplo, *STS-3* es tres veces la velocidad de *STS-1* ($3 \times 51.84 = 155.52$ Mbps) Un *STS-12* sería una velocidad de $12 \times 51.84 = 622.08$ Mbps.

SONET proporciona suficiente flexibilidad, la cual se utiliza como la capa de transporte subyacente para paquetes *BISDN ATM*. *BISDN* es sólo una red *ISDN* que puede manejar voz, datos, y servicios de video. *ATM* es el estándar del *CCITT*, soporta paquetes basados en voz, datos, video, y comunicación multimedia en una red pública bajo *BISDN*. El Forum *ATM* se alinea con *SONET* como la capa de transporte para tráfico basado en paquetes.

SMDS.

El servicio de intercambio de datos a multimegabits es un servicio de cambio provisto por algunos servicios *Exchange Carriers*. Tienen una velocidad de transmisión en un rango de 1 Mbps a 34 Mbps con una conectividad muchos a muchos. Diferente a una red de malla especializada (red con accesos múltiples activos), éste servicio puede ofrecer alto ancho de banda con reducidos costos de red .

El *SMDS* utiliza el mismo paquete de longitud fija que proporciona una tecnología como *ATM*. Una línea con el apropiado ancho de banda conectado hacia el portador local, puede proporcionar conexiones entre todos los sitios sin llamar un iniciador o ejecutar un procedimiento de terminación. El *SMDS* no ejecuta el chequeo de errores o control de flujo; éste es activado cuando comienza la conexión del *site*.

El *SMDS* es compatible con *IEEE 802.6* que es un estándar de las *MAN* así como con *BISDN*, pero *SMDS* proporciona mejor manejo y servicios de facturación no especificados en la *IEEE 802.6*.

El *SMDS* utiliza el *DQDB* como la interface y método de acceso para la red. El *SMDS* es una topología *dual-bus* que forma un anillo que no se cierra.

2.3 Tipos de Conectores.

Microsoft Exchange utiliza conectores de mensajería con el propósito de establecer un medio de intercambio o transferencia de mensajes. No establece conexiones entre *sites*.

MTA.

El *MTA* es un servicio del servidor *Microsoft Exchange*, que se encarga de direccionar los mensajes locales a su destino dentro del mismo *site*, pero si el destino se encuentra fuera del *site* local, el *MTA* identifica el nombre del *site* que se esta tratando de acceder y envía el mensaje al *MTA* del otro *site*.

Todos los servidores de *Exchange* deben configurar y utilizar su propio *MTA*.

De igual forma el *MTA* identifica si algún mensaje es para un diferente sistema de correo al de *Exchange* y modifica el formato del mensaje para enviarlo en un formato válido a su destino, el servidor destino debe identificar el tipo de formato enviado y nuevamente regresarlo a su forma original y enviarlo al servidor de correo elegido.

El *MTA* puede ser configurado para limitar el tamaño de los mensajes, habilitar archivos de log o bitácoras, y reconstruir las tablas de direccionamiento. El *MTA* utiliza tres componentes del servidor *Microsoft Exchange* para dirigir y transferir la información hacia otro servidor o hacia sistemas externos de *e-mail*:

- *Site Connector* del servidor *Microsoft Exchange*.
- Conector *X.400*.
- Conector *RAS*.

Site Connector.

El *Site Connector* conecta dos *sites* utilizando *RPC*. Los *sites* deben estar ligados por medio de conexiones permanentes. El *Site Connector* es fácil de habilitar y configurar por que utiliza *RPC's*, por lo tanto, no es necesario preocuparse por la configuración del transporte de red (el conector utiliza el transporte existente. Esta transparencia permite el uso de múltiples plataformas de red en el sistema).

El *Site Connector* permite que cualquier servidor en un *site* específico, que origina un mensaje, lo entregue a un servidor, en un *Site* remoto. El *Site Connector* está configurado para mantener una lista de servidores destino. Un servidor destino es un servidor en un *Site* remoto, el cual

deberá tener definido en su servidor un servicio *MTA* local para poder conectarse de manera ordenada y entregar el mensaje.

Todos los servidores dentro de un *site* remoto son listados y cualquiera de éstos puede ser seleccionado para ser él o los servidores destino.

Cuando se necesite generar un *MTA* para transferir un mensaje de correo a un *site* remoto éste obtiene el servidor destino de la lista y transfiere la información al servidor. Esto no garantiza que el servidor destino sea el destino final; el servidor destino a su vez podrá retransmitir el mensaje al servidor destino final.

En caso de ser necesario, el *Site Connector* puede ser configurado para monitorear el tráfico de correo a través de las rutas específicas. Éste servicio se proporciona por medio de servidores de correo llamados *bridgehead*; un servidor *bridgehead* recibe mensajes de correo de otros servidores dentro del *site*, y transfiere el mensaje al servidor o a su correspondiente servidor *bridgehead* en un *site* remoto. Esto permite que el administrador identifique el servidor que administrará la comunicación entre los *sites*, el cual podrá descargar el procedimiento de otros servidores.

El *Site Connector* (Fig. 2.10) toma el ancho de banda más alto para transferir información de manera inmediata.

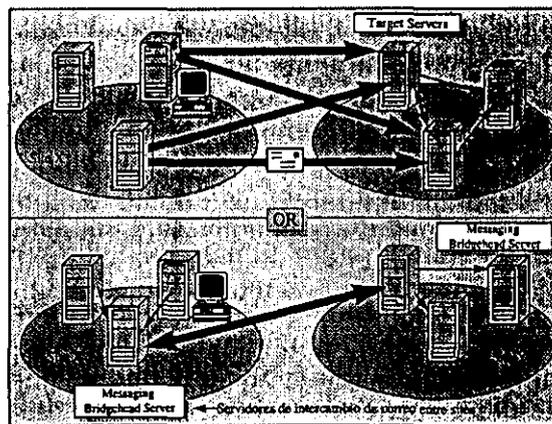


Fig. 2.10 Ejemplo de *Site Connector*

Usos y Beneficios :

- Requiere de una LAN, los RPC y protocolos de conectividad a red como TCP/IP, NetBIOS y NetBEUI, IPX entre otros.
- Es el conector más eficiente, ya que opera más rápido que el conector X.400.
- Es el conector más fácil de configurar.
- Es utilizado típicamente en ambientes con altos anchos de banda. Puede trabajar con anchos de banda bajos dependiendo de la cantidad de información a transferir.
- Provee una configuración automática al lado remoto del conector *site*.

Conector X.400.

El conector X.400 es similar al *Site Connector*, ya que utiliza servidores de mensajería *bridgehead* para monitorear el tráfico de correos, sin embargo, el conector X.400 no puede utilizar los servidores destino como lo hace el *Site Connector*.

El conector X.400 (Fig. 2.11) provee el control sobre el uso de ligas, esto permite al administrador restringir el tiempo en el que estará activo el conector y la especificación de usuarios que pueden enviar correos desde los *sites* remotos.

En lugar de que cada servidor origine un MTA en cada *site* remoto, cada servidor pasará los mensajes al servidor *bridgehead*, el cual se conectará con su contraparte con el *site* remoto para transmitir, una vez que el mensaje arriba del servidor *bridgehead* remoto, éste pasa de ser necesario, al servidor destino final.

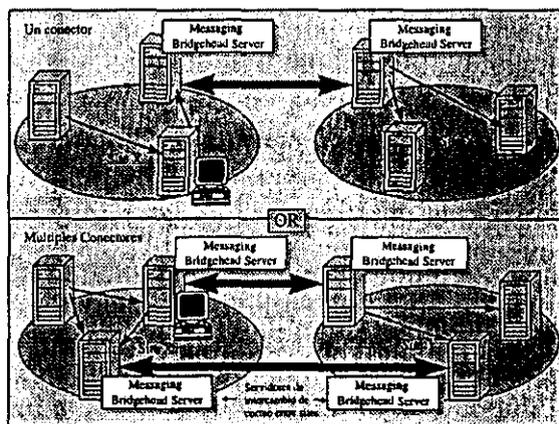


Fig. 2.11 Ejemplo de X.400

Usos y Beneficios :

- Es utilizado con *TCP/IP*, *TP4* y *X.25*.
- Permite mayor control sobre la transferencia de datos de los servidores.
- Es el conector más genérico.
- Puede ser utilizado para conectar cualquier sistema con *X.400*.
- Permite la restricción en el tamaño del mensaje a enviar.
- Su configuración es más compleja que el *Site Connector*.
- Es menos eficiente que el *Site Connector*. El conector *X.400* opera aproximadamente 20% más lento.
- Permite la restricción de los usuarios que pueden acceder a la liga.
- Es menos propenso a la saturación de las ligas que el *Site Connector*, solamente pueden ser definidos dos servidores para cada conector.

Puede resultar un cuello de botella dependiendo del flujo de mensajes.

Conector Dinámico (RAS).

El conector dinámico *RAS* (Fig. 2.12) proporciona el transporte de mensajes entre *sites*, cuando no existe una conexión permanente en las redes *LAN* o *WAN*. Se utiliza *RAS* para proveer el transporte temporal necesario entre dos *MTA*'s. El conector dinámico *RAS* puede ser configurado para activar automáticamente las conexiones *RAS* dentro de un horario establecido.

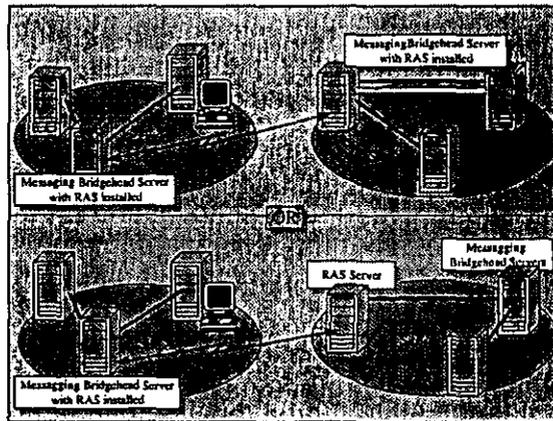


Fig. 2.12 Ejemplo de Conector RAS

Desde *RAS* se puede requerir un procesamiento adicional para contestar llamados y el manejo de las comunicaciones, el administrador puede elegir la configuración para que el servidor llame a un servidor dedicado *RAS* en lugar de llamar directamente a un servidor de *Exchange*. Esto reduce la sobre carga de las respuestas del servidor *RAS* y las llamadas recibidas del servidor *Exchange*.

Este conector también utiliza los conceptos de servicios de mensajería de los servidores *bridgehead* para monitorear el tráfico entre dos *sites*. Tiene algunas de las características del conector *X.400* pero el conector dinámico *RAS* tiene la habilidad de conectarse por demanda.

3.1 *Windows NT 4.0.*

Antecedentes.

Una computadora no es nada sin un sistema operativo. El sistema operativo es el *software* que provee a las computadoras la capacidad básica para comunicarse, almacenar información y ejecutar programas. De igual manera que los sistemas operativos de redes proveen de las herramientas para lograr una administración adecuada de la comunicación entre un conjunto de computadoras.

La creciente necesidad de los usuarios en el intercambio de información y recursos, ha hecho necesario que los sistemas operativos de red evolucionen día a día para poder proveer de las herramientas necesarias para que la administración de la red sea eficiente, confiable y de fácil manejo.

Actualmente *Microsoft Windows NT* es uno de los sistemas operativos de red que ha logrado ofrecer las mejores herramientas en la administración de redes; *Windows NT* es el resultado de una evolución de los siguientes sistemas operativos de red de *Microsoft* :

- *MS-NET* .- Desarrollado por *Microsoft* y licenciado a otros proveedores, pero nunca distribuido directamente.
- *LAN MANAGER* .- Un sistema operativo de red basado en *OS/2* versión 1.3.
- *WINDOWS NT ADVANCED SERVER* .- Basado en *Windows NT* versión 3.1.
- *WINDOWS NT SERVER* .- El producto actual, derivado de la última versión de *Windows NT*, versión 4.

En los últimos dos años, la versión del servidor *Windows NT* se ha establecido básicamente como servidor de archivos y de aplicaciones en red. En éste ámbito ha ido superando a *NetWare*, que dominaba el mercado; dado que se ha prestado especial atención en la fiabilidad del sistema, tiempos de espera y facilidad en la administración gracias a sus herramientas gráficas que facilitan su administración diaria.

Arquitectura Windows NT.

A diferencia de la mayoría de los sistemas operativos (por ejemplo : *Novell Netware*), *Windows NT* trabaja de forma independiente de la arquitectura del procesador. Las partes de programa específicas para cada procesador sólo se encuentran en una pequeña porción del código de programa, denominada *HAL* (Fig. 3.1).

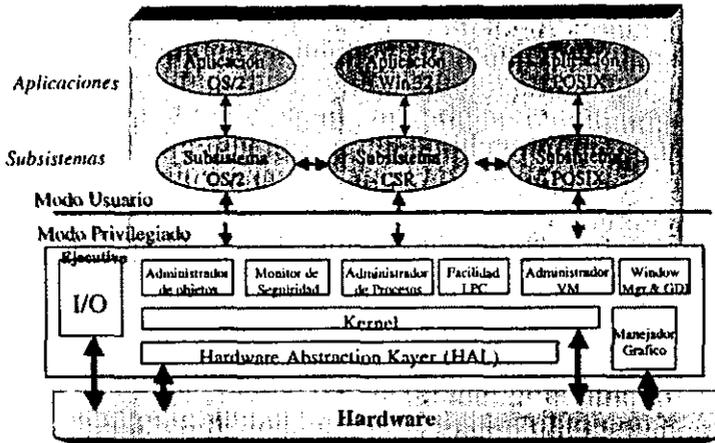


Fig. 3.1 Arquitectura de Windows NT.

Windows NT está construido en componentes modulares. Éstos componentes ejecutan tareas específicas dentro del contexto del sistema operativo como un todo. Esto es realizado a través de subsistemas y servicios ejecutivos. Un subsistema es un proceso separado que provee servicios API a otros programas; los servicios ejecutivos coordinan las actividades del sistema operativo.

Dado que los servicios ejecutivos de *Windows NT* son centrales para las funciones especializadas del sistema operativo, es importante protegerla de las aplicaciones y subsistemas. Esto se realiza teniendo los servicios ejecutivos ejecutándose en modo de procesador privilegiado, el cual provee el acceso a la memoria de la computadora y corre en una área de memoria separada de las demás aplicaciones.

Aplicaciones, subsistemas y el código se ejecutan en un modo de procesador sin privilegios llamado *User Mode*, éste procesador :

- No tienen acceso directo al hardware.
- Están limitados a un espacio de dirección asignada.
- Pueden ser forzados a utilizar espacio del disco duro como memoria virtual RAM.
- Los procesos se ejecutan con prioridad baja.

Características de *Windows NT*.

Windows NT provee el beneficio de una gran variedad de redes, sistema operativo y características de aplicación entre las cuáles se encuentran las siguientes :

Característica	Beneficio
Plataforma múltiple	<i>Windows NT</i> ha sido diseñado para ser soportado por múltiples computadoras; Conjuntos De Instrucciones Complejas de Computadora (CISC) (Intel 80386DX-, 80486 y Pentium.), Conjunto de Instrucciones Reducido (RISC), (MIPS R-1000, DEC ALPHA AXP y Base intergráfica de CLIPPER). <i>Windows NT</i> puede tomar ventaja de múltiples procesadores creando multiprocesos simétricos de sistemas operativos.
Multitareas y Operaciones Simultáneas	Diferentes tipos de aplicaciones pueden ejecutarse a la misma hora. Las aplicaciones <i>Background</i> pueden continuar el proceso mientras los usuarios esta trabajando en sus aplicaciones <i>Foreground</i> .
Seguridad Extensiva	Generadores de seguridad que permiten una mejor protección de los recursos de la red. Nuevas Características que incluyen firmas obligatorias, acceso discrecional, protección de memoria y auditoras.
Soporte MS DOS-, Win 16-, Win 32, OS/2 y POSIX y Aplicaciones Básicas	La mayoría de las aplicaciones existentes se ejecutarán bajo <i>Windows NT</i> ; esto significa que los usuarios pueden trabajar en aplicaciones escritas por otros sistemas operativos en un sólo ambiente. Un usuario solo necesita aprender como usar su aplicación, no diferentes ambientes.
Construcciones en redes	<i>Windows NT</i> fue diseñado pensando en redes. Las utilerías necesarias están incluidas con la habilidad de agregar <i>drivers</i> de red y <i>stacks</i> de protocolos. <i>Windows NT</i> esta soportado en las siguientes redes : <i>Banyan VINES</i> , <i>DEC Pathworks</i> , <i>IBM Lan Sever</i> , <i>IBM SNA Networks</i> (con <i>software</i> adicional, <i>Microsoft LAN MANAGER</i> , <i>Microsoft Windows WorkGroups</i> , <i>Novel NetWare</i> , <i>AppleTalk</i> y <i>TCP/IP Networks</i>).
Soporta 4 Gigabytes de RAM y 16 exabytes de espacio en disco duro	Con el <i>hardware</i> ofertado actualmente, virtualmente no hay límite de capacidad para los recursos utilizados con <i>Windows NT</i> .
Opciones de Conexión Múltiple	<i>Windows NT</i> puede conectar a múltiples tipos de computadoras. Los siguientes protocolos de transporte <i>IDNS</i> están incluidos por <i>Windows NT</i> : <i>TCP/IP</i> , <i>DLC</i> , <i>NetBEUI</i> , <i>AppleTalk</i> y <i>NWLink</i> .
Soporte de Clientes	<i>Windows NT</i> soporta las siguientes <i>workstations</i> : <i>Microsoft Windows</i> , <i>Windows for WorkGroups</i> , <i>Windows NT workstation</i> , <i>MS DOS</i> , <i>Macintosh</i> , <i>OS/2</i> y <i>Novell NetWare</i>
File Systems	<i>Windows NT</i> soporta los siguientes <i>file systems</i> : <i>FAT</i> , <i>NTFS</i> , <i>HPFS</i> y <i>CDFS</i> .

Características del Rendimiento de *Windows NT*.

Multitask y Multithreading.

Windows NT utiliza el método multitarea prioritario (auténtico). Con el mismo se ejecutan simultáneamente varios procesos con distintas prioridades. Las tareas se distribuyen, en las unidades de control, en lapsos de tiempo. Los conceptos multitarea sencillos utilizan el método multitarea cooperativo. Con el mismo también se asumen y administran varios procesos al mismo tiempo. Sin embargo, en cada momento sólo se edita un proceso mientras el resto se trasladan a la cola de espera.

El procesamiento paralelo de varias tareas en una computadora se puede mejorar todavía, si se realizan al mismo tiempo tareas en un programa de aplicación, de poco sirve el método multitarea por sí solo. Para el procesador, éstas tareas son una sola, por lo que solamente se ejecutaran una tras otra.

El remedio para éste problema es el *Multithreading*. Con el mismo, el programa de aplicación diferencia distintas tareas mediante los denominados subprocesos. El número de subprocesos que puede administrar una aplicación depende de los recursos del sistema operativo y del *software* de la aplicación. Algunos programas administran hasta 17 subprocesos.

Un buen ejemplo de *Multithreading* es el trabajo con el navegador *WWW Netscape*. Con un único navegador es posible descargar archivos mediante *FTP* y al mismo tiempo pasar a la página *WWW* siguiente. Allí, se puede iniciar otra sesión *FTP* y asignar un tercer proceso, etc.

Estabilidad y Seguridad.

Junto con el rendimiento, las características de calidad esenciales de un sistema operativo son la estabilidad y la seguridad. Muchos conocen la situación en que *WinCIM* termina una sesión de *CompuServe* y se pierden también *Word* y *Excel* con datos importantes, a veces no guardados. La causa de esta pérdida conjunta es que las aplicaciones no se ejecutan en áreas de memoria separadas. Esto provoca también los conocidos fallos generales de protección como sucede en *Windows (3.x y 95)* a menudo.

En éste caso, suele haber dos aplicaciones distintas que intentan acceder a la misma área de memoria.

Windows NT resuelve éste problema ejecutando cada aplicación en un área de memoria distinta. Durante el funcionamiento normal no pueden interferir en territorio ajeno. Una aplicación que haya dejado de responder puede ser terminada con el administrador de tareas, sin que el resto de aplicaciones o el propio sistema operativo finalicen.

Aunque se ejecuten aplicaciones en distintas áreas de memoria pueden producirse fallos en el sistema. Por ejemplo, si dos programas acceden al mismo tiempo al archivo de sistema *USER.EXE*, pueden bloquearse mutuamente provocando una pérdida de datos y dejar inutilizable el archivo para cualquier otro uso posterior. Los usuarios de *Windows 95* conocen esta situación cuando salen del sistema mientras utilizan programas de 32 bits.

A esta problemática *Windows NT* también ofrece soluciones. Las funciones del sistema operativo, se ejecutan en un área de memoria que no puede ser utilizada por ninguna otra aplicación. Incluso si se hubiera dañado el propio entorno de *Windows NT* mediante el bloqueo de otras aplicaciones, el propio sistema operativo puede tomar el control a activar la aplicación bloqueada y hacer funcionar el sistema.

Naturalmente, la administración separada de programas en áreas de memoria propias requiere mayores recursos del sistema para dividir la memoria. Cada aplicación en *Windows NT* toma como mínimo 3MB de memoria *RAM*. Si se ejecutan algunos servicios estándar o incluso de servidor en segundo plano, la memoria *RAM* se consume rápidamente.

Administración Central.

La gestión central de datos de configuración también contribuye a la seguridad y a la estabilidad de un sistema operativo. *Windows NT* utiliza una base de datos de configuración central, la base de datos de registro. Los antiguos usuarios de *Windows 3.x* se alegrarán de no tener que volver a editar un *WIN.INI*, un *SYSTEM.INI*, un *CONFIG.SYS*, etc.

Para ello es necesario trabajar con cuidado con la complicada base de datos del registro. Si se realizan configuraciones incorrectas se puede bloquear el sistema aunque en éste caso no está todo perdido : al iniciar *Windows NT* basta con recurrir a la última versión buena conocida, guardada por el sistema como copia de seguridad, e intentar de nuevo.

Discos Duros y Administración de Archivos.

Los datos deben de estar seguros no sólo en los servidores. Es por ello que las características y seguridad del sistema de archivos de *Windows NT* son interesantes tanto para usuarios de *NT Workstation* como para los del servidor *Windows NT*.

Windows NT ofrece soporte a ambos niveles. Junto con *FAT* de *DOS* (tabla de asignación de archivos, sistema de archivos de computadoras *DOS*) también puede trabajar con *NTFS* (sistema de archivos propio de *NT*).

La administración de discos duros en *Windows NT* es fundamentada por los conceptos de tolerancia a errores y *RAID*. El primer concepto comprende posibilidades de protección de datos como discos espejo y los conjuntos de bandas. *RAID* es el concepto general para distintos niveles de organización del disco duro como reflejar el disco duro o dividir una sola partición en varios discos duros.

Soporte en Red.

El servidor *Windows NT* es un sistema operativo de red. Detrás de *Windows NT*, como detrás de cualquier sistema operativo de red, se esconde una filosofía de red propia. *Windows NT* administra grupos de trabajo y dominios. Si un servidor *NT* debe trabajar en una "auténtica" red cliente-servidor, uno de los servidores debe asumir el papel de controlador principal del dominio. Por lo tanto, para administrar usuarios y recursos es preciso trabajar a nivel de dominios.

Redes Heterogéneas.

Las redes de área local modernas utilizadas en empresas con frecuencia no sólo conectan computadoras del mismo sistema operativo, sino muchos distintos. Así, es posible encontrar en una red estaciones de trabajo en grupo o *Windows NT* junto con computadoras *Windows 95*, *Macintosh*, *OS/2*, y quizás también *UNIX*. Además, puede haber también un servidor de archivos *NetWare*. Éste entorno mixto debe comunicarse entre sí y permitir que se compartan los recursos mediante protocolos unitarios. *Windows NT* ofrece para ello todos los requerimientos: además del protocolo *Net BEUI* utilizado en redes de *Microsoft*, también son compatibles *IPX/SPX* (*Novell*) y *TCP/IP* (*UNIX*, *OS/2*). *TCP/IP* también se encarga de conectar computadoras *NT* a *Internet*, y, con ello a la red más grande (y más heterogénea). Las computadoras *Apple Macintosh* también se pueden incorporar a redes *NT*.

Como las redes *NetWare* tradicionalmente están muy extendidas en la empresa, *Windows NT* ofrece servicios de cliente y *gateways* para la interconexión con éste tipo de redes.

El protocolo *Data Link Control* (*DLC*, estándar industrial *IEEE 802.2*) *NT* permite la conexión con productos mainframe en *LAN*, *WAN* y por ejemplo, el acceso a impresoras de red.

Administración de Usuarios.

En una red trabajan varias personas que comparten recursos como el espacio de disco duro, el rendimiento del procesador, la impresora y programas de aplicación. Es evidente que en una red de éste tipo, no todo el mundo puede hacerlo todo. Para controlarlo, *Windows NT* soporta :

- Cuentas de usuario, establecen quién puede acceder a qué recursos y de que forma.
- Registro de usuarios, con los cuáles se comprueba quien ha utilizado que recursos.
- Registro de sucesos generales, que ayudan a encontrar el error si se produjera un fallo.

Como sistema operativo verdaderamente multiusuario, *Windows NT* ofrece esta administración de usuarios para todos los usuarios locales. Por lo tanto, para cada usuario que se siente directamente a una computadora *Windows NT* puede establecer los derechos de acceso y perfiles de usuario.

3.2 Service Pack 3.0.

Transporte *RPC*.

El *Service Pack* incluye versiones nuevas de la biblioteca de enlace dinámico (*DLL*) en tiempo de ejecución para *RPC* y del servicio del subsistema *RPC* (*RPCSS.EXE*). Éstos cambios proporcionan compatibilidad mejorada para cola de mensajes *RPC*, que es una característica del futuro *MSMQ*.

Para utilizar colas de mensajes en un programa *RPC* cliente/servidor sobre *Windows NT 4.0*, se debe tener *Service Pack 3* instalado en ambos equipos, tanto en el cliente como en el servidor.

Además, las aplicaciones *RPC* deben admitir colas de mensajes para poder utilizar las siguientes características :

- El atributo [*message*] de *MIDL*.
- La secuencia de protocolo *ncadg_mq*.
- Los indicadores de punto final *RPC_C_MQ_** en la estructura de datos
- *RPC_POLICY*.
- Las funciones *RpcBindingInqOption* y *RpcBindingSetOption*.

CryptoAPI 2.0 (API de cifrado)

La interfaz de programación de aplicaciones de cifrado de *Microsoft* (*CryptoAPI*) proporciona a los desarrolladores funciones básicas de cifrado y certificación.

CryptoAPI 1.0 admite operaciones con claves públicas y claves simétricas, como generación, administración, intercambio, cifrado y descifrado y firma digital de claves, así como la comprobación de dichas firmas.

CryptoAPI 2.0, que es la actualización contenida en el *Service Pack*, incluye la misma funcionalidad básica, así como otras funciones que se basan en certificados. Los desarrolladores pueden utilizar los certificados con esas claves públicas para realizar encapsulaciones y codificación para aplicar a certificados dentro de sus programas.

CryptoAPI 2.0 utiliza un modelo de proveedor de servicios donde el cifrado proviene de los proveedores de servicio de cifrado (*CSP*). Éste modelo permite a los desarrolladores adaptar fácilmente sus programas a las tecnologías de cifrado siempre en continua evolución, así como a las políticas de exportación de algunos gobiernos. En *Service Pack 3* se proporciona un *CSP (Microsoft RSA Base Provider)* que proporciona acceso a técnicas de cifrado exportable a usuarios y desarrolladores.

Esto permite a los programas que utilizan *CryptoAPI* interoperar con otros sistemas basados en certificados.

DirectX 3.0.

Service Pack 3 contiene el *software* completo de *DirectX 3.0*; así como compatibilidad con *hardware* para el componente *DirectDraw* de *DirectX 3.0*. Esto se traduce en las siguientes características principales desde la publicación de *DirectX 2.0* que era compatible con *Windows NT 4.0* :

DirectDraw.

Acceso a las 256 entradas de la paleta en modo exclusivo.

DirectSound.

Localización de audio basada en *software* (interfaces de programación de aplicaciones *Direct3DSound*).

DirectInput.

Interfaz *COM* compatible con datos provenientes del *mouse* y del teclado con documentación y programas de ejemplo.

DirectPlay.

IdirectPlayLobby, una interfase que permite a un programa externo iniciar un programa *Direct 3.0* y dotarlo de la información necesaria para que pueda conectarse a una sesión. Proveedor de servicio *TCP/IP* para aplicaciones de varios jugadores a través de *Internet*.

ODBC 3.0.

Service Pack 3 incluye la última versión del *API Open Database Connectivity (ODBC)* de *Microsoft*. *ODBC 3.0* proporciona un panel de control actualizado y una interfase para el Administrador *ODBC* que utiliza controles de fichas y proporcionan más información sobre los componentes *ODBC* instalados y utilizados por el sistema.

Esta versión actualizada de *ODBC* introduce el concepto de origen de datos de archivos que pueden ser compartidos o situados en un servidor central y utilizado por cualquier usuario con los controladores apropiados instalados.

Firma SMB.

Service Pack 3 contiene una versión actualizada del protocolo de autenticación de bloques de mensajes del servidor (*SMB*), también conocido como protocolo para compartir archivos *CIFS* (*Common Internet File System* o *sistema de archivo de Internet común*). Admite autenticación mutua, que evita un ataque por interposición de intrusos ("*man-in-the-middle attack*"), así como autenticación de mensaje que protege en éste caso de ataques a mensajes activos.

La firma *SMB* permite la autenticación poniendo una forma digital de seguridad en cada *SMB* que es comprobada tanto por el cliente como por el servidor.

Filtrado de Contraseñas.

Service Pack 3 incluye un filtro de contraseñas (*PASSFILT.DLL*) que permite a los administradores del sistema aumentar la confidencialidad de las contraseñas.

Windows NT permite a los usuarios que inician sesión de forma anónima obtener una lista de los nombres de usuario del dominio y de recursos compartidos. Algunos clientes con necesidades más severas, en cuanto a seguridad, han solicitado la posibilidad de restringir esta funcionalidad. *Service Pack 3* proporciona un mecanismo para que los administradores puedan restringir la capacidad de los usuarios anónimos para obtener la lista de cuentas de usuario y de recursos compartidos.

Además, *Service Pack 3* presenta una característica para restringir conexiones remotas de usuarios anónimos al registro. Desde el momento en que se instala *Service Pack 3*, los usuarios anónimos no pueden conectarse al registro ni pueden leer o escribir datos en el mismo.

Service Pack permite la utilización de técnicas de cifrado robusto para aumentar la protección de la información de las contraseñas de las cuentas de usuario que son guardadas en el registro por el *SAM*. *Windows NT* guarda información de cuentas de usuario, incluyendo un derivado de la contraseña de la cuenta de usuario, en una parte especialmente protegida del registro mediante control de acceso y una función de ocultamiento. Sólo los miembros del grupo de administradores tiene acceso a la información de cuentas del registro. *Windows NT*, al igual que otros sistemas operativos, permite a los usuarios con privilegios de administrador tener acceso a todos los recursos del sistema. Para los usuarios que necesiten un alto nivel de seguridad, el cifrado robusto de la información derivada de contraseñas de las cuentas de usuarios proporciona un nivel de seguridad adicional para evitar que los administradores, intencionadamente o no, tengan acceso a los derivados de las contraseñas utilizando interfaces de programación del registro.

El cifrado robusto disponible en *Service Pack 3* es opcional. El cifrado robusto protege la información privada de cuentas utilizando una clave de cifrado aleatoria de 128 bits. Los administradores pueden implementarla definiendo una clave del sistema para *Windows NT*.

Service Pack 3 ofrece compatibilidad limitada con el autenticador *PPP MD5-CHAP* del servidor de acceso remoto que puede ser útil en entornos con pocos usuarios que utilizan clientes de acceso telefónico a redes *PPP* que no sean de *Microsoft*. La compatibilidad es local a un servidor *RAS* determinado. La información de cuentas *MD5* está almacenada en el registro del servidor *RAS* y no está integrada o sincronizada con la base de datos de cuentas del administrador de usuarios.

Servidor *DHCP* de *Microsoft*.

La característica de detección de conflictos de direcciones puede limitar el rendimiento del servidor *DHCP* de *Microsoft*. Para mejorar el rendimiento, reduzca el número de reintentos del comando *PING* en el cuadro de diálogo propiedades del servidor. Esta característica está deshabilitada de forma predeterminada.

Los conflictos de direcciones se ponen de manifiesto reemplazando el nombre del equipo con *BAD_ADDRESS*. Si se especifica un identificador único para la dirección en el cuadro de diálogo propiedades del cliente, entonces la dirección será rechazada por el cliente. Si no se especifica el identificador único, entonces el servidor *DHCP* será quien detectó el conflicto de direcciones. El servidor *DHCP* de *Microsoft* se puede configurar para que haga la *gateway* predeterminada del cliente igual a su dirección *IP*. Esto fuerza al cliente a utilizar el *ARP* para todas las direcciones *IP* de la subred local siendo muy útil para redes sin direccionamiento. Para habilitar esta característica para todos los clientes de un ámbito, agregue el siguiente valor al registro: Esta versión de servidor *DHCP* de *Microsoft* admite clientes *BOOTP*.

Las direcciones *BOOTP* deben reservarse con anticipación creando una reserva de dirección *IP*. Las versiones futuras del servidor *DHCP* de *Microsoft* podrán conceder direcciones dinámicas a clientes *BOOTP*.

3.3 Microsoft Exchange Server 5.5.

Microsoft Exchange es el primer sistema de mensajería cliente/servidor que integra en un mismo sistema diferentes funciones, el sistema de correo, calendarización de eventos en forma individual o en grupos, manejo de formas electrónicas, uso de contactos y tareas, trabajo en grupo y sincronización *On-line* con correo *Off-line* en el momento de la conexión. Éstas características hacen de *Exchange* un *software* de correo poderoso.

Adicionalmente el nivel de seguridad ofrecido por *Internet* hace posible que cualquier organización sin importar el tamaño pueda contar con un sistema de correo poderoso que ofrezca soluciones cliente/servidor y puedan ser accesadas en cualquier parte del mundo.

Microsoft Exchange es un programa muy eficaz con el que se puede controlar y administrar toda la comunicación electrónica (correo electrónico interno de las empresas, correo electrónico de *Internet*, correo de *CompuServe*, fax) desde un solo programa de aplicación

Gran cantidad de herramientas soportan la comunicación y el trabajo a través de toda la red.

La más difundida es *LOTUS NOTES*. La versión 4 de *LOTUS NOTES* soporta diferentes interfaces de correo electrónico, funciones para trabajo en grupo y servicios de información como el servidor *WWW*.

Microsoft Exchange desempeña las siguientes funciones :

- Envía información electrónica a usuarios dentro y fuera de la empresa. Para tal fin puede recurrir a diferentes interfases de comunicación (sistemas *MAPI*, sistemas *X.400*, correo de *Internet*).
- Guarda y organiza la información tanto de mensajería como de calendarización de juntas o eventos con los grupos de trabajo, tanto de ámbito empresarial como de los que se extienden más allá de éste ámbito.
- En las áreas públicas, pone las informaciones a disposición de todos los miembros que tengan acceso al servidor de *Exchange*.
- Aprovecha las funciones de seguridad del servidor de *Exchange* para proteger los datos personales en las comunicaciones intraempresariales y extraempresariales.

Características.

El servidor *MS Exchange* es más que un simple sistema de correo electrónico. Con él se pueden administrar y planear procesos e información intraempresariales y sincronizar la calendarización de juntas y eventos, incluidos los de todas las empresas filiales.

Con diferentes entornos, *MS Exchange* soporta distintas posibilidades de conexión :

Conexión	Descripción
Conector Estándar	Conexión de dos servidores <i>MS Exchange</i>
<i>Microsoft Mail</i>	Este sistema de comunicación de <i>Microsoft</i> se encuentra disponible tanto para <i>PC</i> como para <i>Apple</i> . Instalado en cualquiera de ellos, éstos podrán utilizar directamente los servicios de <i>MS Exchange Server</i> . El sistema de correo electrónico de <i>Microsoft</i> ofrece además varios gateways hacia otros sistemas de correo electrónico. (<i>P.E. MHS, AT&T Mail, Fax</i>)
<i>X.400</i>	Un estándar específico de correo electrónico que es soportado por algunos sistemas de correo electrónico de <i>Internet</i> .
<i>MS Schedule+</i>	Intercambio de información con el sistema de agenda de <i>Microsoft</i> a través de la interfaz de correo electrónico de <i>Microsoft</i> .
Correo electrónico de <i>Internet Mail</i> . Intercambio de información vía <i>Internet</i>	La información se puede transmitir por otros servicios de correo electrónico de <i>Internet</i> (<i>P.E. MHS, POP3</i>) o por servidores <i>Exchange</i> .

Los requerimientos mínimos de configuración del sistema son los siguientes :

Para plataforma Intel y Compatible :

- Sistema con procesador *Intel Pentium a 133 MHz* o mayor.
- 32 MB de memoria *RAM* y 64 para la edición *Enterprise*.
- 250 MB de espacio en disco libre (500 recomendable)
Sistema *RISC*.

Sistema con un procesador Alpha :

- 48 MB de memoria *RAM* y 64 para la edición *Enterprise*.
- 300 MB de espacio en disco libre (500 recomendable).

Requerimientos Adicionales para Todos los Sistemas.

Políticas de Licenciamiento del Producto.

Una licencia de servidor es necesaria por cada producto instalado. La licencia del servidor únicamente permite al usuario ejecutar el sistema en un servidor standalone.

La licencia de *Exchange Client Access (CAL)* es requerida para cada cliente que se conectara al servidor de *Microsoft Exchange*. Esta licencia no está incluida con *Windows 95* o *Microsoft Office 97* y se puede adquirir en paquetes.

3.4 IIS 3.0 Acceso vía Web Access.

IIS (Internet Information Server).

El *IIS* es un *software* para la administración de servidores de *Web*, el cual provee una gran cantidad de herramientas que permiten al manejo de información y definición de esquemas de seguridad en cualquier red *TCP/IP*. Permite el crecimiento del *Web site* y la utilización eficiente de los recursos de nuestra computadora.

El *IIS* viene incluido en el servidor *Windows NT*. Por medio de éste, se puede instalar lo siguiente :

- Un servidor *World Wide Web*.
- Un servidor *File Transfer Process (FTP)*.
- Un servidor *Gopher*.

Servidor *World Wide Web*.

El *WWW* trabaja según el principio cliente-servidor. Si el servidor de *Windows NT* recibe una petición *WWW* (denominada *HTTP*) en una dirección *IP*, se activará el *IIS*, si éste estuviera disponible.

Servidor *Gopher*.

Gopher es un medio de información muy elemental (y como consecuencia muy rápido) que presenta la información de manera jerárquica, como en el índice de un libro. La gran ventaja ante el *WWW* estriba en el sencillo diseño de las páginas. Durante la búsqueda, ninguna imagen afectara la transmisión de las página. En la actualidad, el servicio *Gopher* ha desaparecido de *Internet*.

Servidor FTP.

Con el *FTP* los usuarios pueden enviar y recibir archivos de red *Intranet* o *Internet*.

Los servidores FTP pueden :

- Ser instalados para permitir al acceso anónimo de usuarios.
- Admitir también como usuarios *FTP* a los usuarios instalados en el dominio *FTP*.
- Poner a disposición del dominio de *Windows NT* la autorización de acceso con contraseña.

3.5 ArcServe Cheyenne.

ArcServe para *Windows NT* es un manejador de datos y programa *Backup* que permite realizar un respaldo de datos de los servidores con *Windows NT* o máquinas ligadas a la red.

ArcServe para *Windows NT* esta disponible en las siguientes versiones :

- Edición *Enterprise* de *backup* para servidor *Windows NT* y *Workstation*.
- Edición sencilla.
- Edición para *Workstation*.

Todas las versiones de *ArcServe* para *Windows NT* pueden trabajar juntas.

Algunas ventajas de *ArcServe* son :

- Calendarización de *Backups* .- Permite calendarizar jobs específicos para que se ejecuten en determinado momento de acuerdo a las necesidades del negocio.
- Rotación de Cintas .- Utiliza una interfase sencilla para el control y la rotación de cintas.
- Compactación de Cintas .- Utiliza el proceso de compactación de la información para permitir grabar mayor información en menos cinta.
- Accesos Paralelos .- Permite la ejecución de diferentes jobs en forma concurrente siempre y cuando se tengan múltiples dispositivos de cintas.
- *Software* de Antivirus Integrado – Realiza el escaneo de virus de archivos en forma automática durante el proceso de *backup*.
- *Scripts* Definidos para Usuarios .- Permite configurar tareas una sola vez y reutilizarlas cuando sean necesarias.
- Proceso de *Restore* de Información Inteligente .- El *ArcServe* permite en forma rápida localizar y restaurar archivos de datos.
- Múltiples Cintas Soportadas .- Se pueden utilizar los formatos de cinta *SCSI 4mm*, *8mm*, *DLT*, y *QIC drivers*.

- Servidor Sencillo .- Reduce el tráfico de la red ya que los datos a respaldar se encuentran en forma local.
- Servicio Remoto .- La versión *Enterprise* permite el manejo de múltiples servidores desde una sola máquina. Permite respaldar, copiar y restaurar archivos de equipos *Windows NT* y *Novel* en la red.
- Sistema de Notificación .- El sistema de alertas de *Cheyenne* notifica cualquier evento ocurrido durante el *backup* o *restore* de información.
- Agente de Soporte al Cliente .- Permite realizar *backup* a diferentes máquinas utilizando el agente del cliente que usa la última versión de la tecnología *PUSH*.
- Agentes de Aplicaciones .- Permite realizar *backup* de bases de datos complejas o grupos de trabajo como *Microsoft Exchange* o *Lotus Notes*.
- El *Dbagent* actúa como un "VE-Entre" para *ArcServe* y las bases de datos de los sistemas, *ArcServe* versión 6.0 soporta los siguientes agentes de Bases de Datos :

DBagent para SQL 6.0

Dbagent para Oracle.

Dbagent para SAP R/3

Dbagent para Microsoft Exchange Server

Dbagent para Lotus Notes.

- Soporte a *Windows NT 3.51* .- Permite la realización de archivos comprimidos, directorios y drives en particiones *NTFS*.
- Compatibilidad con *Netware* .- Compatible con *Windows NT* y redes *Novell NetWare*.
- Interfase fácil de utilizar.
- Descubriendo Servidores en Forma Automática .- *ArcServe* identifica en forma automática todos los otros servidores con *ArcServe* instalados en la red.

Como Trabaja *ArcServe*.

ArcServe está compuesta de dos componentes principales que trabajan en forma conjunta para realizar respaldos, copias y restauraciones de información. Éstos componentes son :

- El *ArcServe Manager*.
- El *ArcServe Server*.

ArcServe Manager : El *ArcServe manager* permite controlar todas las operaciones de *ArcServe* desde una sola máquina. Es utilizado para lanzar procesos de *backup* o *restore*, manejar las bases de datos o buscar reportes, etc.

ArcServe Server : Utilizando la información especificada por el *ArcServe manager*, el *ArcServe server* se encarga de ejecutar las operaciones seleccionadas. Se encarga de controlar y administrar los procesos de *Job Engine*, *Tape Engine* y *Database Engine* :

- *Job Engine* .- Es responsable de procesar los trabajos en la fecha y hora seleccionada, monitorea si algún proceso ha sido enviado y lo ejecuta.
- *Tape Engine* .- Es responsable de la comunicación entre el *software* y la unidad controladora de cintas.
- *Database Engine* .- Es responsable de mantener la historia de archivos, directorios o máquinas que *ArcServe* ha respaldado, de los trabajos que se han ejecutado, los resultados de un *backup*, cintas formateadas y con que nombre, etc.

En general todo lo que ocurre en el *ArcServe* es registrado por la *Database Engine*.

3.6 Backup Agent para Microsoft Exchange.

Cheyenne Backup Agent para el servidor *Microsoft Exchange* es un componente adicional del sistema de respaldo que permite realizar respaldos y restauraciones de las bases de datos de *Exchange*, *Mailboxes* independientes y otros objetos.

Utilizando el agente de *backup de Exchange* es posible realizar las siguientes actividades :

- Manejar y realizar respaldos de las bases de datos de *Exchange*, de los *mailboxes* y de los *folders* públicos.
- Realizar respaldos de las bases de datos en forma *on-line* tomando ventajas de las funciones *API* del *Exchange Server backup/restore*.
- Calendarizar los respaldos por medio del programa de *ArcServe manager*.
- Realizar respaldos de dispositivos conectados en arreglos de discos.

El sistema de mensajería de *Microsoft Exchange* está organizado en unidades administrativas, donde la mayor se conoce como organización. La organización esta conformada por *sites* que a su vez están formados por uno o más servidores locales que comparten la misma base de datos de directorios.

Los servidores locales trabajan con los componentes del cliente para realizar tareas y funciones entre las redes. Los componentes del cliente solicitan instrucciones como búsqueda de nombres, envío de mensajes de almacenamiento de información en las bases de datos privada y *folders* públicos.

Cada servidor local contiene componentes esenciales y opcionales. Los componentes esenciales proveen transferencia de mensajes y entrega, almacenamiento y servicios de directorios. Los componentes opcionales proveen conectividad, entre la base de datos de directorios de *Exchange* con otros sistemas.

El agente de *Backup de Exchange* le permite realizar respaldos de los siguientes componentes en el servidor local.

Bases de Datos de *Exchange* .- Está compuesto por las dos bases de datos más importantes de *Exchange* que son la de directorios y la del *Information Store*.

También esta permitido respaldar los componentes del *Information Store* públicos y privados.

Como Trabaja el Agente de Respaldo.

El Agente de *Backup* permite respaldar y restaurar las bases de datos del servidor *Exchange* o sus componentes como *Mailboxes*. El Agente de *Backup* actúa como un interprete entre *ArcServe* y el servidor *Exchange*, controla todo el flujo de información entre los dos sistemas y habilita los datos para ser manipulados por éste sistema.

El Agente de *Backup* se instala en el servidor de *Exchange*, cuando *ArcServe* levanta el producto de *Backup* para realizar el respaldo de las bases de datos o de sus componentes, éste envía un requerimiento al Agente de *Exchange*, éste recibe la solicitud y recupera la información solicitada del servidor *Exchange* y la envía a *ArcServe*, donde los datos son respaldados hacia la unidad de cinta, el proceso de restauración es similar al de respaldo.

Respaldos en Línea.

El Agente de *Backup* utiliza las funciones de *Backup/Restore* del API del servidor *Exchange* para realizar respaldos en línea.

El respaldo en línea es una gran ventaja ya que permite realizar el respaldo de la información cuando el sistema se encuentra activo y no hay necesidad de retirar el servicio a los usuarios.

Así mismo, el respaldo en línea lanza un proceso de limpieza de *logs* de transacciones, los cuáles se generan en forma diaria y son almacenados en un disco del sistema, si éstos archivos no son depurados, el sistema los sigue generando y se corre el riesgo de saturar el disco físico.

El formato de limpieza de los archivos de *log* se realiza cuando se efectúan respaldos completos.

Flujo del Proceso de Respaldo.

Los siguientes pasos describen el flujo de datos cuando *ArcServe* utiliza el Agente de *Exchange* para realizar respaldos en línea de las bases de datos de *Exchange* :

- *ArcServe* envía un requerimiento al Agente de *Backup de Exchange* para realizar un respaldo de la base de datos.
- El Agente de *Backup de Exchange* da instrucciones al servidor de *Exchange* para que habilite los siguientes archivos en modo de respaldo :

Bases de Datos de Exchange	Archivos en Línea.
Directorios	DIR.EDB DIR.PAT EDBXXXXX.LOG
<i>Information Store</i>	PRIV.EDB PRIV.PAT PUB.EDB PUB.PAT EDBXXXXX.LOG

- El Agente de *Backup* recupera los archivos de la base de datos del servidor *Exchange* y los transfiere hacia *ArcServe*.
- *ArcServe* escribe las bases de datos hacia la unidad de cinta.
- El Agente de *Backup de Exchange* le da instrucciones al servidor *Exchange* para indicar que el modo de *Backup* ha finalizado.

3.7 Outlook 97 y Outlook 98 para Clientes.

Outlook 97

El *Outlook 97* es una aplicación que permite administrar el correo electrónico, calendarizar citas, agendar contactos, tareas, compartir archivos, siendo una interfase intuitiva y fácil para los usuarios :

- Permite compartir información con un grupo utilizando el correo electrónico, programación de grupo y carpetas públicas.
- Comparte información con otras aplicaciones de *Office*, así como explora y busca archivos de *Office* desde *Outlook*.
- Permite conectarse y compartir información a través de *World Wide Web*.
- También se puede utilizar para enviar correo electrónico a través de *Internet*.
- Cuenta con opciones de programación para personalizar el *Outlook* (programación en lenguaje C)
- Tiene una total compatibilidad con la interfase de extensiones de *Microsoft Exchange Client*.
- Tiene un completo modelo de objeto de automatización. Los programadores que utilizan *Visual Basic* para aplicaciones pueden manipular fácilmente los datos de *Outlook* como objetos.
- Los programadores pueden definir y ejecutar un código de *Visual Basic Scripting Edition* que responda cuando los usuarios concluyan acciones: Por ejemplo, se puede escribir un código que abra, cierre, envíe o cambie propiedades de elementos de *Outlook*.

Outlook 98

Se creó con la misma finalidad que el *Outlook 97* pero se le dió más importancia y seguridad al área de soporte en *Internet*, lo cual permite una excelente integración con el *Microsoft Internet Explorer 4.0*.

Outlook provee de un ambiente de desarrollo y modelos de objetos muy completo que proporciona a desarrolladores una herramienta de desarrollo de formas electrónicas o automatización de procesos.

El *software* de *Outlook 98* proporciona el uso de correo *e-mail*, calendarización en grupos, directorio de contactos y tareas para computadoras de 32-bits.

Outlook para sistemas operativos de *Windows 3.x* .- Esta versión de *Windows* utiliza la misma interfase de correo, calendarización de juntas, contactos y tareas que se utilizan en 32 bits, pero para sistemas de 16 bits.

Outlook para sistemas operativos *Macintosh* .- El uso de *Outlook* esta adaptado para permitir interoperabilidad con equipos *MAC* con el sistema operativo (*Mac OS 8.5*).

Microsoft Outlook Web Access .- Se puede utilizar por medio de cualquier *Web Browser* como *Netscape* o *Internet Explorer 4.0*, los usuarios pueden acceder sus mensajes y opciones de calendarización en forma segura desde cualquier parte de la red por medio de un *browser*, así como las listas corporativas y aplicaciones.

Outlook Forms .- El ambiente de desarrollo de formas de *Outlook 98* contiene un paquete de herramientas para escribir y debugear *VBscripts*. Incluye el *debugger* y el buscador de objetos que permiten un rápido desarrollo de formas de *Outlook* utilizando *scripts* y especificando el flujo de las formas. Éstas formas pueden ser utilizadas en *Outlook 97*.

Permite el manejo y envío de archivos *HTML*, además de enviar y recibir archivos por *Internet* con el formato *Vcard*

Principales Características del Outlook 97 y el Outlook 98.

En el *Outlook 97* se tiene :

- Bandeja de Entrada (*Mailbox*) .- En donde recibe y envía mensajes.
- Calendario (*Calendar*) .- Mantiene un seguimiento de la programación y organización de las reuniones con los usuarios.
- Contactos .- Permite administrar la información de sus contactos personales y profesionales.
- Tareas .- Organiza una lista de tareas en una única ubicación fácil de administrar. Determina rápidamente la prioridad de las tareas y asigna tareas a los demás.
- Diario .- Lleva un registro de las interacciones con contactos importantes, guarda mensajes de correo y archivos importantes, y registra todo tipo de actividades, para poder realizar un seguimiento.
- Notas .- Almacena información personal tales como: notas para recordar preguntas, ideas, instrucciones, etc.
- Archivos .- Permite abrir, ver y compartir archivos de otras aplicaciones desde *Outlook*.

En el *Outlook98* se tiene :

- *Outlook Today*, en él se realiza lo que se hacía en la bandeja de entrada, el Calendario, Contactos, Tareas, Diario, Notas y Archivos, del *Outlook 97*, además de permitir ligar las páginas de *Internet*, haciendo un *click* puede acceder a la información.
- Los menús están mejor estructurados, para que puedan ser utilizados en forma fácil y rápida por el usuario final.
- Permite administrar todos los recursos del *Outlook* de una forma rápida.
- Permite manejar archivos con los estándares de *Internet*, *SMTP/POP3*, *IMAP4*, *NNTP*, *s/MIME* y *ical* y *Vcal*, así como *HTML*, y *Vcard*, desde el correo electrónico.
- Utiliza un *script debugger*, lo cual permite crear formularios y ejecutarlos al mismo tiempo, y así corregirlos en el instante.
- Utiliza *Outlook Forms* contiene *VBScript* y el *script debugger*.
- Utiliza un mejor editor de texto *script*, además de agregar una barra de herramientas, para su fácil manejo.
- Permite la programación con *VBA*, *VB*, *C/C++* o *Java*.

Además cuenta con el *Digital IDs*, que es una identificación digital, para garantizar la seguridad del envío y recepción de la información por *Internet*.

3.8 Niveles de Seguridad.

Windows NT proporciona un conjunto de servicios de seguridad muy completo algunos de los cuales se dividen de la siguiente forma:

Seguridad de Acceso.

- Uso de Logon ID y password.
- Longitud mínima de password de 6 caracteres.
- Expiración de password cada 90 días.
- Bloqueo de la cuenta después de 3 intentos fallidos.
- Auditoría de Logon.
- Desconexión automática de la sesión después de 15 minutos de inactividad.

Seguridad de la Información.

Respaldos de la información en forma diaria.

- Bases de Datos.
- Sistema Operativo.
- Otro Software.

Servidores con tolerancia a fallas en componentes críticos.

- Fuentes de poder.
- Discos.
- Procesadores.

Configuración de arreglos Raid nivel 1 y 5 para garantizar la conectividad del servicio y protección a los discos.

Software detector de virus.

- GroupShield para Bases de Datos de Exchange por Computer Associates.
- NetShield para Sistema Operativo y otros datos por Computer Associates.

Cifrado de la Información.

- Producto SecurPC versión 1.1 de la compañía RSA Security.

Particiones NTFS con diferentes niveles de seguridad a nivel archivo y directorio.

- Read.
- Write.
- Delete.
- Execute.
- Access.

Seguridad de Acceso Remoto.

Dentro del corporativo no se permite el acceso a la red de Warner por medio de una red pública de telefonía.

El acceso remoto a la compañía solo está permitido por medio de dos alternativas:

SecurID – Componente con Autenticación válida.

Server ID y password para el segundo nivel de autenticación.

Seguridad en el uso de Internet.

La red mundial de internet provee la oportunidad de acceder y compartir información de negocios, investigaciones, entretenimientos, etc.

Con esta gran oportunidad vienen implícitos ciertos riesgos para la compañía como son: la transmisión de virus o pérdida o alteración de la información.

El acceso directo a internet desde la red de la compañía estará disponible solo a través de los Gateways corporativos. Si el negocio requiere la transmisión de información via internet deberá ser cifrada .

Se establecen políticas de uso para todos los usuarios de internet.

Como parte de la seguridad se configuran restricciones de acceso a subredes específicas.

CAPÍTULO 4 PREPARACIÓN DE EQUIPOS

4.1 Tipos de protocolos

Los protocolos son reglas o procedimientos para establecer la comunicación entre computadoras. En el sentido físico, esto se realiza por medio de una tarjeta de red, y una conexión entre las tarjetas generalmente un cable, pero también pueden ser conexiones por radio o láser.

Los protocolos trabajan de la siguiente forma :

Se debe de establecer un orden en las computadoras de la red. En la computadora que va a mandar la información, éstos procedimientos se efectuarán de arriba hacia abajo, y en la máquina receptora los procedimientos de comunicación se efectuarán de abajo hacia arriba.

A continuación se describe el envío y recepción de información entre dos computadoras :

Computadora que envía información :

1. El protocolo dividirá la información en secciones pequeñas, llamadas paquetes, mientras el protocolo se dirige a la otra máquina, para verificar que esta activa
2. Se agrega la dirección a los paquetes de información, que serán enviados a la computadora destino, para que reconozca la información que se envía.
3. Prepara la transmisión de datos a través de la tarjeta y el cable de la red.

Computadora que recibe la información :

1. Verifica que una máquina le enviará información, y toma la información del cable de red.
2. Envía los paquetes de información a la computadora a través de la tarjeta de red.
3. Extrae de los paquetes toda la información que agregó la computadora que envía.
4. Copia los datos de los paquetes al buffer para juntarlos nuevamente y los válida.
5. Pasa los datos ya unidos a la aplicación que se está usando.

A mediados de 1980, la mayoría de las redes *LAN* eran aisladas. Sólo se ocupaban de un departamento en específico, pero no se conectaban a otros ambientes. Se fueron expandiendo y fortaleciendo, y surgió la necesidad de comunicarse de redes *LAN* a redes *LAN* y a los protocolos que soportan éste tipo de comunicación, se les llamo protocolos direccionables. Éstos protocolos permiten unir varias *LAN* y con ello crearon las redes *WAN*.

Protocolos de Arquitectura en Capas.

El modelo *OSI*, se desarrolló entre 1977 y 1984, es un modelo en capas donde cada una de ellas tiene una tarea específica dentro del proceso de comunicación. Para que pueda operar una capa requiere de los servicios de la capa inferior, y cuando dos capas del mismo nivel, pero en nodos diferentes de la red quieren comunicarse, esta comunicación se efectúa por medio de protocolos.

Son 7 capas y se describe la función que realizan :

- Capa de Aplicación .- Inicia una petición o la rechaza.
- Capa de Presentación .- Asigna una sintaxis a los datos, los muestra, y descifra la información de los paquetes.
- Capa de Sesión .- Ofrece un mecanismo organizado del intercambio de datos entre usuarios y determina cuando se enviarán los datos.
- Capa de Transporte .- Detección de error, envía información para ser validada.
- Capa de Red .- Es el control de red, la coordinación entre nodos adyacentes, direccionamiento y manejo de paquetes. Administra conexiones a través de la red para las capas superiores, así como controlar la secuencia y la dirección que se les asignó a los paquetes.
- Capa de Enlace .- Es el control de enlace lógico, direccionamiento, detección y corrección de errores, es el responsable de la transferencia de datos por el canal. Proporciona a los datos la sincronización necesaria para delimitar el flujo de bits en el nivel físico.
- Capa de Nivel Físico .- Es el que conforma el paquete de bits que será transmitido. Define las características físicas del medio de red.

En éste modelo (Fig. 4.1) las capas inferiores determinan que máquinas se conectarán con que máquinas. Y las capas superiores especifican los medios de comunicación y la interpretación de las aplicaciones.

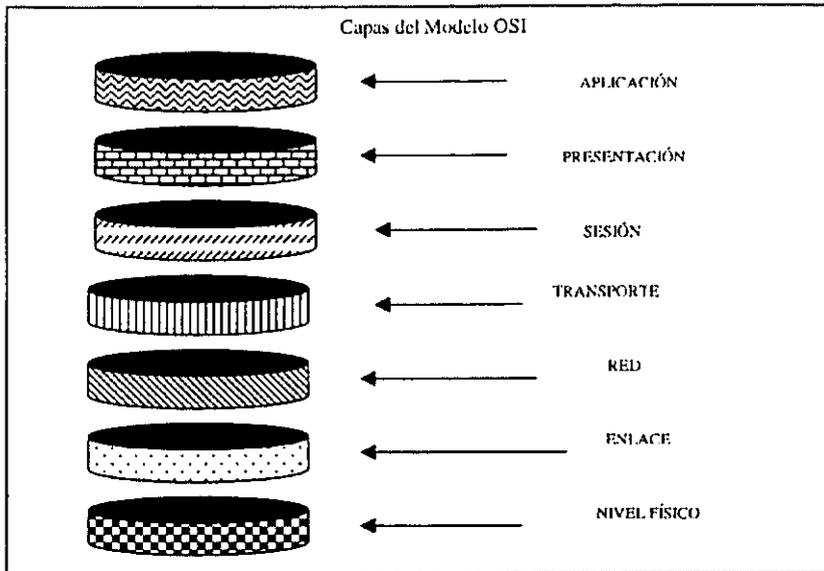


Fig. 4.1 Las 7 capas del Modelo OSI.

A la combinación de varios protocolos se le conoce como *suite* o *stack* de protocolos.

El Proceso de Unión.

Al unirse varios protocolos dan una gran flexibilidad, tanto los protocolos como las tarjetas de red se pueden mezclar de acuerdo a las necesidades, por ejemplo dos *stacks* de protocolos como lo son el *IPX/SPX* y el *TCP/IP* pueden funcionar con una sola tarjeta de red. Los modelos de protocolos estándar más importantes son :

- Protocolo *Suite ISO/OSI*.
- Arquitectura de Sistema de Red *IBM (SNA)*.
- *DecNet* de *Digital*.
- Red de *Novell NetWare*.
- Red *Apple Talk*.
- Protocolo de *Internet, Suite, TCP/IP*.

A continuación se listan los protocolos que trabajan en cada una de las 7 capas del modelo *OSI*, realizando un trabajo específico por cada capa:

Los protocolos que trabajan en la capa de aplicación son :

- *APPC (Advanced Program-to-Program Communication)*.
- *FTAM (File Transfer Access and Management)* y el protocolo *OSI* en archivos de acceso.
- *X.400* Protocolo para transmisiones de correos internacionales.
- *X.500* Protocolo para acceso de archivos y directorios por varios sistemas.
- *SMTP (Simple Mail Transfer Protocol)* Protocolo de *Internet* para la transferencia de correos electrónicos.
- *FTP (File Transfer Protocol)* Protocolo de *Internet* para transferencia de archivos.
- *SNMP (Simple Network Management Protocol)* Protocolo de *Internet* para el monitoreo de redes y sus componentes.
- *Telnet* Protocolo de *Internet* para acceder a servidores remotos y procesamiento local de datos.
- *Microsoft SMB (Server Message Blocks)* Servidor de mensajes por bloques y redirecciones *shells* a los usuarios.
- *NCP (Novell NetWare Core Protocol)* Protocolo para *Novell*.
- *Apple Talk* y *Apple Share* Protocolo de red *Suite* para equipos *Apple*.
- *AFP (Apple Talk Filing Protocol)* Protocolo para equipos *Apple* para acceso remoto de archivos.
- *DAP (Data Access Protocol)* Protocolo de acceso de archivos *DecNet*.

Protocolos que trabajan en la Capa de Transporte :

- *TCP (Transmission Control Protocol)*.
- *UDP (User Datagram Protocol)* *ARP (Address Resolution Protocol)*.
- *ICMP (Internet Control Message Protocol)*.
- *SPX* Parte de *Novell* es *IPX/SPX (Internetwork Packet Exchange/Sequential Packet Exchange)* Protocolo *suite* para controlar la secuencia de los datos.
- *NWLinks* es una implementación de *Microsoft* del protocolo *IPX/SPX*.
- *NetBEUI [NetBIOS] (Network Basic Input/Output System)* Sistema Básico de entrada y salida de redes, es no direccionable. Establece sesiones de comunicación entre computadoras (*NetBIOS*) y proporciona el servicio de transportación de datos (*NetBEUI*).
- *ATP (Apple Talk Transaction Protocol)*, *NBP (Name Binding Protocol)* Protocolo de comunicación y transporte de datos de *Apple*.

Protocolos que trabajan en la capa de red :

- *IP (Internet Protocol)* El *TCP/IP* habilita el direccionamiento.
- *IPX (Internetwork Packet Exchange)* Protocolo de *Netware* para envío y direccionamiento de paquetes.
- *NwLink* Implementación de *Microsoft* para el protocolo de *Netware*.
- *NetBEUI* Protocolo de transporte que suministra los servicios de transporte de datos para las sesiones o aplicaciones del *NetBIOS*.
- *DDP (Datagram Delivery Protocol)* Protocolo de transporte de datos de *Apple Talk*.

Protocolos que trabajan en la capa física :

- *802.3 (Ethernet)*.
- *802.4 (Token Passing)*.
- *802.5 (Token Ring)*.

Junto con la Capa de Liga de Datos, el *IEEE* define un protocolo que facilita la comunicación activa dentro de las subcapas mediante un Control de Acceso de las Subcapas.

En la capa *Datalink* el control de acceso a medios es un dispositivo que está localizado en la subcapa del Control de Acceso al Medio. Éste controlador es conocido como un controlador de tarjeta de red. Es el que proporciona acceso a los niveles y a los adaptadores de red que soportan la transmisión de algunas funciones de los adaptadores.

El protocolo de Control de Acceso al Medio determina que computadora de la red está utilizando un cable y cual está tratando simultáneamente de utilizarlo. *CSMA/CD* y el protocolo *802.3*, verifica quien usa el medio y si ambas transmiten el *CSMA/CD* detiene la transmisión de una para evitar colisiones.

Protocolos Comunes :

- *TCP/IP*.
- *NetBEUI*.
- *X.25*.
- *Xerox Network System (XNS)*.
- *IPX/SPX and NWLink*.
- *APPC*.
- *Apple Talk*.
- *OSI protocol suite*.
- *DecNet*.

TCP/IP.

La serie de protocolos de *Internet*, comúnmente conocidos como *TCP/IP*, fue desarrollado a mediados de los 70's por el Departamento de Defensa de E. U. Para esto la Defensa avanzaba en la investigación del proyecto de administración de redes (*ARPANET*). *ARPANET* fue la primera demostración pública de redes con conmutación de paquetes. Esto fue una colección de instalaciones de redes individuales entre el gobierno, militares, universidades e industrias. El *ARPANET* interconectó las redes formando la *Internet*.

Con éste protocolo se establece comunicación en ambientes heterogéneos. *TCP/IP* proporciona un protocolo direccionable, y permite acceder al mundo de *Internet*.

Se considera un protocolo estándar para múltiples computadoras, ésta es una de sus principales ventajas y todas las redes soportan a éste protocolo.

Otros de los protocolos escritos específicamente para el *suite de TCP/IP* son :

- *SMTP (Simple Mail Transfer Protocol)* Correos Electrónicos.
- *FTP (File Transfer Protocol)* Para extraer archivos de otras computadoras donde se esté ejecutando el *TCP/IP*.

SNMP.

Históricamente se le consideran al *TCP/IP* dos desventajas principales que son: el tamaño y la velocidad. El *TCP/IP* es relativamente un protocolo grande que causa problemas a los clientes basados en el *MS-DOS*, en la *GUI* basada en el sistema operativo, como puede ser *Windows NT* o *Windows 95*, el tamaño no es un problema y la velocidad es igual al *IPX*.

NetBEUI.

El *NetBEUI* es una interfase extendida para el usuario del *NetBIOS*. Originalmente, *NetBIOS* y *NetBEUI* pudieron trabajar en conjunto, considerados como un solo protocolo.

NetBIOS el cual trabaja en la capa o nivel de sesión de las redes *LAN* de *IBM*, y el cual utiliza a otros protocolos direccionables, es el que proporciona las herramientas para que el programa establezca la sesión o comunicación con otra computadora de la red.

NetBEUI es pequeño, rápido y eficiente como protocolo que trabaja en la capa de transporte el cual es sustituido por los productos de la red de *Microsoft*, es el que ha estado disponible desde 1980 y fue sustituido por el primer producto de la red de *Microsoft* llamado *MS-NET*.

Las ventajas del *NetBEUI* es su pila de tamaño pequeño lo cual es importante para las computadoras que tienen solamente el sistema operativo, la velocidad de transmisión de la red es mediana y existe una gran compatibilidad con todas las redes que trabaja *Microsoft Network*.

La mayor desventaja del *NetBEUI* es que no soporta el direccionamiento.

X.25.

Es un conjunto de protocolos que se incorpora a los paquetes de *switches* de la red en los servicios de *switches*. El servicio de *switches* se estableció para conectar sistemas remotos hacia *mainframes*. Busca rutas a través de la red y transmite paquetes.

XNS.

Sistema de red *Xerox (XNS)* fue desarrollado por *Xerox* para redes *Lan Ethernet*, es un protocolo largo y muy lento, produciendo más *broadcast* y causando mayor tráfico para la red.

IPX/SPX y NWLink

Internetwork Packet eXchange/Sequence Packet eXchange es un *stack* de protocolo el cual lo utilizan las redes *Novell*, es relativamente pequeño y rápido a diferencia del *NetBEUI* es direccionable.

También el protocolo *NWLink* es una versión del protocolo *IPX/SPX*, es un protocolo de transporte y es direccionable.

APPC.

APPC es un protocolo de transporte de *IBM* desarrollado como parte del Sistema de Arquitectura de Red (*SNA*) fue diseñado para permitir a los programas de aplicación de diferentes computadoras el comunicarse e intercambiar datos directamente.

Apple Talk.

Es el protocolo propietario de las computadoras *Apple* para permitir el compartir archivos e impresoras en un ambiente de red.

Protocolos OSI.

Es un conjunto de protocolos. Cada uno de ellos mapea directamente hacia una capa del modelo *OSI*. El conjunto de protocolos *OSI* incluye el direccionamiento y protocolos de transporte a la serie de protocolos *IEEE*, protocolos a nivel sesión, así como protocolos del nivel de presentación, y varios protocolos del nivel de aplicación diseñados para proveer a la red una funcionalidad completa incluyendo, los archivos de acceso, impresión y emulación de terminales.

DecNet.

Es un conjunto de protocolos propietarios de equipos Digital. Es un grupo de productos de *hardware* y *software* para implementar la arquitectura de Red Digital (*DNA*) define la comunicación de redes sobre redes *Ethernet* de área local, y en redes de distribución de datos vía fibra en área metropolitana, y redes de cobertura amplia (*WAN*) para facilitar la transmisión pública o privada de datos.

DecNet puede usar también el *TCP/IP* y el protocolo *OSI* de igual forma que los suyos, es un protocolo direccionable.

4.2 Definición de Protocolos a Utilizar.

El protocolo a utilizar es el *TCP/IP*. El *TCP* es un protocolo de paquetes orientado a la conexión perteneciente al protocolo de *Internet (IP)*. Su función dentro del transporte consiste en garantizar la secuencia adecuada y el control de la transmisión de datos mediante sumas comprobatorias. Si la transmisión se pierde o se daña algún paquete, el *TCP* tendrá que volver a incorporar el paquete a su ruta. Esto requiere la inclusión, en cada paquete, de numerosos *headers* que deben contener toda la información necesaria para la recomposición de los datos fragmentados.

El *TCP/IP* habilita el direccionamiento. Se encarga sólo del transporte de los datos, desconociendo toda corrección y control de la secuencia de los mismos. El *IP* sólo comprueba la corrección en el *header* del paquete *IP*.

4.3 Tipos de Arreglos Redundantes a Fallas.

El servidor *Windows NT* cuenta con un *software* de aplicación para implementar la tecnología de tolerancia a fallas *Fault Tolerance* conocida como *RAID*, la tecnología de *RAID* es un estándar que se subdivide en varios niveles.

Un arreglo no es más que una colección de discos duros agrupados, donde cada nivel de arreglo distribuye los datos a través de los discos del arreglo de una manera diferente.

El manejo de arreglos fue desarrollado por la Universidad de *Barkley* en 1987, su principal objetivo fue desarrollar un método que permitiera clasificar los diferentes arreglos de discos de acuerdo a la capacidad del equipo y a la disponibilidad del usuario, el servidor *Windows NT* soporta los niveles de *RAID* 1 al 5 para proporcionar *Fault Tolerance*.

Actualmente existen al menos 8 niveles de arreglos *RAID* diferentes. Cada definición puede resultar la opción adecuada dependiendo del ambiente de trabajo, por lo que no es posible decir que un *RAID-5* es siempre mejor que un *RAID-1* o que un *RAID-4* es mejor que un *RAID-3*, la selección del arreglo deseado depende exclusivamente de las necesidades de la empresa, cada nivel de *RAID* ofrece diferentes escalas de *performance*, disponibilidad, capacidad, rentabilidad y costo.

Un *RAID* proporciona tolerancia a fallas porque implementa un sistema de redundancia de datos. Con el uso de redundancia en datos se permite que la información sea escrita en más de un disco, de manera que si un disco falla pueda ser recuperado conforme a la información de algún otro disco.

Tolerancia a fallas *RAID* puede ser implementada por medio de *hardware* o *software*, la selección del tipo de *RAID* puede ser realizado de acuerdo a los siguientes criterios :

- La definición de tolerancia a fallas por medio de *software* es más barata que por *hardware*.
- El *performance* del equipo es normalmente mayor cuando se implementa la tolerancia a fallas por *hardware*.
- El uso de tolerancia a fallas por medio de *hardware* podría hacer que el equipo sea dependiente de un sólo proveedor, lo cual no ocurre por medio del *software* ya que es definido en el sistema operativo de *Windows NT*.
- En algunos arreglos de tolerancia a fallas por *hardware* es posible reemplazar el disco fallado sin necesidad de darle un *shutdown* al equipo.
- El sistema de tolerancia a fallas por *software* sólo funciona para el servidor *Windows NT*, no está implementado en *Windows NT Workstation*.

Una vez ocurrida una falla en algún disco, el sistema queda vulnerable y por el momento que dura la reconstrucción ya no hay tolerancia a fallas, por lo que si se presenta un segundo suceso y algún otro disco falla, el sistema no podrá soportar la pérdida de dos discos simultáneamente. Ningún sistema de tolerancia a fallas soporta la pérdida de más de un disco físico.

Implementación de un *RAID* por *Hardware*.

En una solución de redundancia a fallas por medio de *hardware*, la interfase de la controladora de discos se encarga de la creación y regeneración de la información. Algunos equipos ya son configurados por el vendedor para soportar *RAID* directamente en el *hardware* por medio de sus tarjetas controladoras de arreglos (*RAID*).

Debido a que éstos métodos son específicos del proveedor en sus equipos no utiliza los *drivers* del sistema operativo para tolerancia a fallas, lo cual incrementa el *performance* del equipo comparado contra la implementación vía *software*.

Implementación de un RAID por Software.

Windows NT únicamente puede definir por *software* dos tipos de arreglos redundantes a fallas *RAID 1 (Mirror set)* y *RAID 5 (stripe sets with parity)*.

Los tipos de arreglos *RAID* manejados por *Windows NT* son :

RAID 1 : (Mirror Sets) Espejo.

El nivel de arreglo *RAID 1* (Fig. 4.2) es manejado por un archivo de *Windows NT* llamado (*Fdisk.sys*) que permite escribir simultáneamente en dos discos físicos la misma información. Éste arreglo permite tener una copia idéntica de la información en cada uno de los discos, normalmente éste tipo de arreglos se utiliza para los discos donde se instala el sistema operativo.

Cualquier partición incluyendo las particiones de *booteo* o de sistema pueden ser configuradas como *Mirror*. Éste tipo de arreglo protege únicamente al disco de falla.

Este tipo de arreglo puede resultar un poco caro ya que la cantidad de espacio total del disco que se utiliza es un 50%, ya que del total de los discos físicos se debe dividir entre dos por el *Mirror*.

El *performance* es otra característica que se ve afectada con éste tipo de arreglo, para efectos de lectura el *performance* se incrementa porque puede acceder la información de cualquiera de los dos discos, pero para efectos de escritura el *performance* se ve un poco degradado ya que debe escribir la misma información en ambos discos. En el momento en que se presenta una falla en algún disco del arreglo el sistema regresa a su operación normal ya que únicamente tiene un disco para grabar y el mismo disco para leer mientras se recupera el otro disco.

La confiabilidad de éste tipo de arreglos es del 100%, ya que la información es duplicada en su totalidad en ambos discos.

Otra característica que tiene éste arreglo es que es configurado únicamente con una controladora de discos.

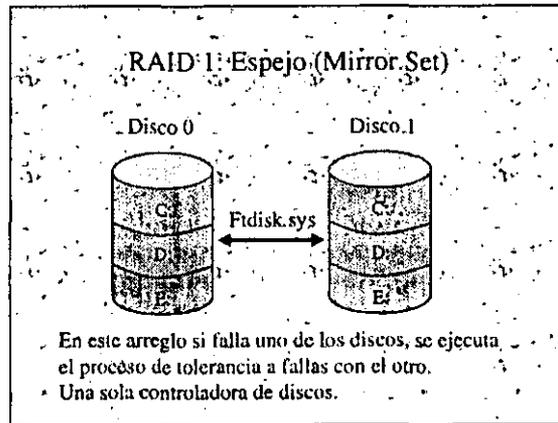


Fig. 4.2 Raid 1. Mirror.

Disk Duplexing.

Disk Duplexing tiene el mismo comportamiento que un arreglo *Mirror* en todos los aspectos, sin embargo un *Disk Duplexing* se define con dos controladoras de discos, por lo que el sistema está aún más redundante a fallas.

En el arreglo *Mirror* definido con una controladora, si la controladora de discos llega a fallar todo el arreglo falla y la información no puede ser accesada.

Adicionalmente a esto el arreglo de *Disk Duplexing* incrementa el *performance* de lectura y escritura del equipo ya que cuenta con dos controladoras independientes eliminando los tiempos de espera.

RAID 0 : (Striping) Bloques.

Este arreglo distribuye la información por medio de pequeños bloques a través de todos los discos conectados al arreglo, éste sistema no es redundante a fallas, su ventaja es que incrementa el *performance* de lectura y escritura, ya que la información esta distribuida en diferentes discos. Otra ventaja de éste arreglo es que la cantidad de espacio utilizada y desplegada por el *drive* lógico es la suma de las cantidades físicas ocupadas por cada disco.

Este tipo de arreglo es el único nivel de *RAID* que no proporciona ninguna tolerancia a fallas, por lo que si uno de los discos falla, todo el sistema falla y la información ya no es posible accederla.

RAID 4 : (Striping by Block).

Este tipo de arreglo es muy similar al arreglo generado por el *RAID 5*, la información es dividida en bloques y distribuida en todos los discos que forman el arreglo, éste sistema sí presenta tolerancia a fallas ya que cuenta con uno de los discos para almacenar la paridad de los otros discos, esto es, si se cuenta con 4 discos físicos para datos únicamente se utilizan 3 de ellos y el cuarto es ocupado para almacenar la paridad de los primeros 3 discos.

Este tipo de arreglo es más lento que el manejo de un *RAID 0* o un *RAID 1*.

Una ventaja de éste arreglo es un rápido acceso a discos para lectura pero lento para escritura. Y una desventaja es que toda la información de paridad de los discos almacenados se encuentra en un solo disco, por lo que puede llegar a ser un cuello de botella principalmente si se inicia un proceso de recuperación de falla en otro disco, ya que la controladora tendría que estar recuperando el disco dañado con la información del disco de paridad y a su vez almacenando la nueva información generada por los discos en línea. En la Fig. 4.3 se muestra este tipo de arreglo.

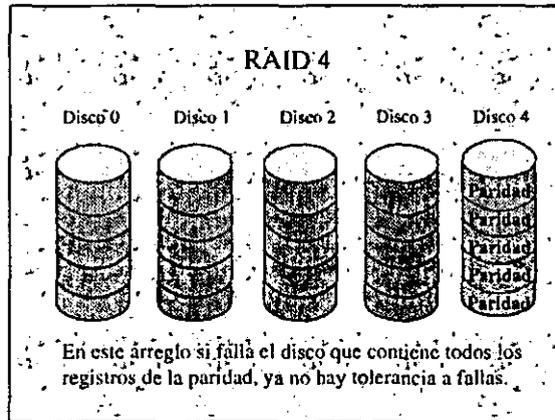


Fig. 4.3 Raid 4. Striping by Block.

RAID 5 : (Stripe Set with Parity).

Como parte importante de un arreglo *RAID 5* se debe definir en que consiste un *Stripe Set* y cuáles son sus características.

Stripe Set .- Es un área de espacio en disco no formateada que puede ser accedida por los archivos del sistema como una sola entidad y es conocido como una sola unidad lógica o *drive*.

Un *Stripe Set* se maneja como un bloque de tamaño fijo que se graba en cada uno de los discos físicos, en el momento en que se efectúa una escritura a los discos, la escritura se realiza en forma secuencial a cada *Stripe Set*, la información es prorrateada entre todos los discos físicos que forman el arreglo, por lo que el proceso de escritura es muy rápido. El proceso de escritura de la paridad se realiza simultáneamente en otro disco físico, por lo que si algún disco llega a fallar toda la información es recuperada del disco que mantuvo la paridad del disco dañado.

Un *Stripe Set* requiere de al menos dos discos físicos para funcionar, por lo que un arreglo *RAID 5* requerirá al menos de 3 discos físicos para formar el arreglo.

La cantidad de discos máxima que puede ser configurada en un *Stripe Set* es de 32 discos físicos y puede combinar discos de diferentes tipos como *SCSI*, *ESDI* e *IDE*. Es importante considerar que el tamaño de los discos para crear un *RAID 5* debe ser igual o el arreglo debiera ser formado con el tamaño de la partición más pequeña de discos.

En un *Stripe Set* los datos son escritos a través de todos los discos físicos uno por uno, en el correspondiente tamaño de bloque, *Windows NT* maneja el tamaño de éste *Stripe* de 64 KB.

Todos los discos duros que forman el *Stripe Set* efectúan las mismas funciones comportándose como un sólo disco duro. Esto permite que los comandos de *I/O* sean utilizados y procesados en todos los discos en forma simultánea. El uso de *Stripe Sets* puede incrementar el *performance* de accesos *I/O* si el sistema cuenta con discos que puedan ser accedidos simultáneamente.

Consideraciones para *Stripe Sets* :

Los archivos del sistema y de *boot* de *Windows NT* no deberán ser almacenados en *Stripe Set*.

Una computadora ejecutando el sistema operativo de *Windows NT* puede tener una partición con doble *boot* como *Windows 95*, pero si éste sistema operativo no soporta *Stripe Set*, no deberá acceder información contenida en el mismo.

Un *Stripe Set* por sí sólo no proporciona ninguna tolerancia a fallas debido a que no es redundante a datos.

Los *Stripe Set* son sensibles a generar fallas en discos ya que su acceso es a varios discos en forma simultánea.

Stripe Set with Parity es reconocido como un *RAID 5*, y no es otra cosa que un *Stripe Set* con un mecanismo de tolerancia a fallas, el cual es soportado por *Windows NT*.

Paridad es un método matemático de verificación de la integridad de la información. El proceso de tolerancia a fallas se consigue añadiendo un *Stripe* de paridad de información en cada partición. El *Stripe* de paridad de información es utilizado para reconstruir los datos de un disco dañado. Un *Stripe Set* con paridad puede soportar de 3 a 32 discos para generar el arreglo.

El *Strip Set* con paridad se escribe a través de todos los discos en el arreglo para soportar la tolerancia a fallas.

El proceso en que la tolerancia a fallas se efectúa en éste arreglo es por medio de los discos físicos, si un disco falla, los datos no se pierden ya que la información de éste disco está contenida en los otros discos, en cuanto éste disco es reemplazado empieza el proceso de recuperación de la información y los otros discos proporcionan la información necesaria para regenerar el disco reemplazado.

Todas las operaciones de escritura que se efectúan en un *Stripe Set* con paridad son más lentas que las operaciones que se realizan en un *Stripe* sin paridad debido al proceso de generación de la paridad de la información. Por el contrario el proceso de lectura mantiene un mayor *performance* que cuando se tiene definido un *Mirror Sets*, esto se debe principalmente a que los datos están distribuidos en diferentes discos. Por el contrario, si un disco falla en un *Stripe* con paridad el proceso de lectura se vuelve lento ya que se debe realizar el proceso de reconstrucción utilizando la información de paridad de cada disco.

La definición de un arreglo *RAID 5* (Fig. 4.4) tiene un costo menor que la definición de un arreglo *RAID 1*, debido a que en el *Mirror* el espacio sacrificado es del 50 % y en un *Raid 5* es del 25%.

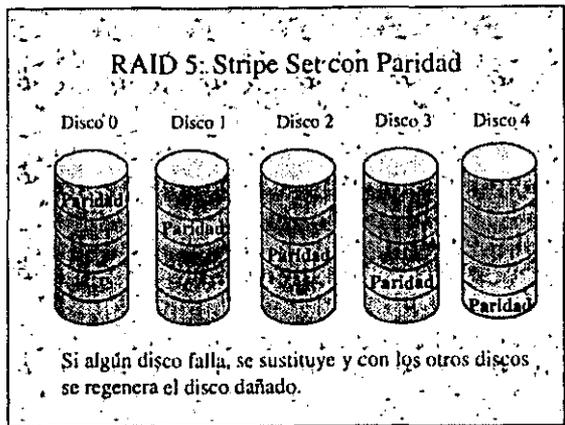


Fig. 4.4 Raid 5. Stripe Set with Parity.

4.4 Definición de Arreglos de Discos para S.O. y Datos

Comparativo entre *Raid 1* y *Raid 5*.

A continuación se presenta una tabla comparativa entre los dos principales arreglos de redundancia a fallas :

RAID 1 (Mirror Set)	RAID 5 (Stripe set with Parity)
Soporta particiones FAT y NTFS.	Soporta particiones FAT y NTFS.
Puede respaldar archivos del sistema y de boot.	No puede soportar archivos del sistema o de boot en un arreglo RAID 5.
Requiere 2 discos duros	Requiere al menos 3 discos duros.
Tiene un mayor costo por Megabyte de disco ya que el porcentaje de utilización es del 50%.	Tiene un menor costo por Megabyte.
Tiene un buen performance de lectura y escritura.	Tiene un performance de escritura medio y un excelente performance de lectura.
Consumo menos recursos de memoria.	Requiere mayor consumo de memoria.
Utiliza particiones del mismo tamaño.	Soporta máximo 32 discos duros.

El *RAID 1* y el *RAID 5* proporcionan diferentes niveles de tolerancia a fallas. La elección entre éstos dos métodos depende del nivel de protección deseada y de las posibilidades del *hardware* utilizado.

La mayor diferencia entre éstos dos arreglos son el *performance* y el costo.

RAID 1 : (Mirror Set) Espejo.

Normalmente éste tipo de arreglo ofrece un mejor *performance de I/O*. Un arreglo *Mirror* soporta además dentro de su esquema de trabajo la tolerancia a fallas para los archivos del sistema y las particiones de *boot*. El costo de implementar un arreglo *Mirror* se considera alto ya que el porcentaje de utilización del disco es al 50%, pero si el costo de los disco disminuye el costo de éste arreglo también.

RAID 5 : (Stripe Sets with Parity).

Este tipo de arreglo ofrece un mejor *performance* de lectura que un arreglo *Mirror*, principalmente si se le puede implementar utilizando múltiples controladoras que permitan la distribución de la información tanto de lectura como de escritura.

Sin embargo el proceso de cálculo de la paridad consume más memoria de la que consume el arreglo *Mirror*. El costo de implementar éste arreglo es menor en cuanto a discos, ya que consume el 33% de la cantidad de espacio total del arreglo de discos.

4.5.- Estructura de Discos

Implementar Diferentes Arreglos.

Los tipos de arreglo *RAID 1* y *RAID 5* pueden coexistir al mismo tiempo en el mismo equipo debido a que ambos arreglos tienen funciones diferentes, el arreglo *RAID 5* no puede incluir como parte de su redundancia a fallas las particiones de *boot* ni los archivos de sistema, por lo que esta redundancia queda a cargo del arreglo *Mirror* y la redundancia a fallas en el *RAID 5* se utiliza específicamente para datos.

Consideraciones para Definir o Crear un *RAID 5*.

El espacio disponible en cada disco que formará el *RAID 5* debe ser del mismo tamaño, en caso de no ser así, el sistema formatea las unidades al mismo tamaño y en algunos discos dejará marcado un espacio como no utilizable.

Es necesario dar un *shutdown* al equipo después de haber definido el arreglo *RAID 5*.

Es muy importante considerar que cuando un arreglo *Mirror* o *Stripe Set* con paridad son borrados, todos los datos almacenados en éstos arreglos son borrados.

Cuando uno de los componentes involucrados en *RAID 1* o *RAID 5* entra en falla, el sistema tolerante a fallas se activa con los demás discos que se encuentran funcionando para continuar dando el servicio.

Si la falla de los discos involucra la partición del sistema será necesario utilizar un disco de *boot* para iniciar el proceso de tolerancia a fallas y arrancar el sistema con el otro disco.

Si la falla de los discos se presenta en uno de los componentes del *RAID 5*, la computadora continúa operando y dando acceso a todos los datos existentes, como consecuencia de la recuperación de la información el sistema se ve degradado ya que al mismo tiempo que está recuperando el disco en falla está trabajando con los bits de paridad de la información para continuar dando el servicio.

Cuando se está efectuando un proceso de recuperación de un disco y dependiendo del *hardware* es muy común que el sistema no sea dado de baja y únicamente se retira el disco dañado, se incluye uno nuevo y se da la opción de regenerar disco, la información de éste disco nuevo es obtenida de la información de paridad que se encuentra en los otros discos.

Los discos C y D, se encuentran configurados en un *Mirror*, cada disco es de 4.2 Gb, por lo que la cantidad total del disco 0 desplegada es de 4 Gb.

Para el Disco 1 se configuraron 7 discos para formar el *RAID 5*, cada disco es de 4.2 Gb, por lo que la cantidad desplegada es de 25 Gb, eliminando el porcentaje usado en cada disco físico por *RAID 5*.

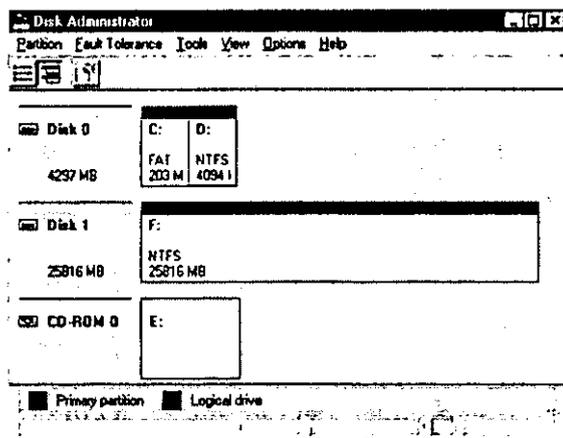


Fig. 4.5 Estructura de Discos.

CAPÍTULO 5

CONFIGURACIÓN DEL AMBIENTE DE TRABAJO.

5.1 Definiciones de Dominios.

Modelo de Dominio.

El concepto de modelo de dominio de red es una forma de estructura que permite a una organización administrar de forma fácil sus recursos y grupos de trabajo, se conoce también como modelo de la empresa y fue definido por *Microsoft* para facilitar la administración en grandes empresas.

El modelo del dominio se caracteriza porque mantiene una sola base de datos centralizada con la información de cuentas de usuarios y privilegios. Esto permite que el administrador del dominio tenga un alto nivel de seguridad en todos sus recursos, ya que sólo él puede asignar permisos y accesos a los usuarios a la base de datos que se encuentra centralizada.

La estructura de un dominio de red, permite manejar redes de diferentes tamaños con servidores, computadoras y usuarios, ubicados en diversas regiones geográficas. Un dominio se puede definir en diferentes arquitecturas de red, utilizar diferentes protocolos, y trabajar con diferentes plataformas, lo cual brinda una arquitectura abierta y flexible

Los dominios de *Windows NT* se componen de dos elementos, servidores y estaciones de trabajo :

Servidores : Un servidor es un equipo que se encarga de poner disponibles sus recursos y aplicaciones para que sean accesadas por las estaciones de trabajo, esta información normalmente esta centralizada. Un servidor se configura con *Windows NT 4.0* de alguna de las siguientes formas :

- Servidor de aplicaciones.
- Servidor de base de datos.
- Servidor de RAS.
- Servidor de impresión.
- Servidor de archivos.

Estaciones de Trabajo : Las estaciones de trabajo son los equipos que accesan las aplicaciones o recursos existentes en los servidores. Los sistemas operativos que pueden acceder a servidores son :

- *Windows NT Workstation 4.0.*
- *Windows 95.*
- *Windows for Workgroup 3.11*
- *MS-DOS.*
- *Sistema 7 de Apple Macintosh.*
- *DOS o OS/2 de Lan Manager.*

El dominio de *Windows NT 4.0* se caracteriza por utilizar una base de datos centralizada con la información de cuentas de usuarios y sus características.

Cuando un usuario intenta acceder algún recurso o aplicación que se encuentre definida en un servidor, debe acceder al dominio con un *username* y *password* válidos, esta información es enviada a un servidor de autenticación, el cual verifica que la información sea correcta y además a que servicios o aplicaciones tiene acceso éste usuario.

El servidor que se encarga de validar y autenticar la cuenta del usuario se conoce como controlador de dominio.

Los servidores pueden identificarse en tres formas únicamente :

- *PDC Primary Domain Controller* .- Controlador de dominio primario
- *BDC Backup Domain Controller* .- Controlador de dominio secundario
- *Server* .- Servidor Standalone conectado al dominio.

PDC (Primary Domain Controller) :

Es el primer servidor con *Windows NT* instalado en un dominio y configurado como *Primary Domain Controller*. éste servidor almacena la base de datos de usuarios y grupos del dominio.

BDC (Backup Domain Controller) :

Los servidores *BDC* mantienen una base de datos de usuarios y grupos idénticos los existentes en el *PDC*, esta base de datos es replicada por el servidor primario a cada servidor *BDC* con los cambios registrados durante ese periodo de tiempo.

**ESTA TESIS NO SALE
DE LA BIBLIOTECA**

Si el servidor *PDC* experimenta una falla de *hardware* y debe ser dado de baja del dominio, algún servidor configurado como *BDC* es promovido al rol de *PDC* y se encargará de la administración de la Base de datos del dominio.

Cada servidor *PDC* debe tener configurado en el mismo dominio un servidor *BDC*. Los servidores *BDC* también son requeridos para proporcionar servicio de validación de cuentas de usuarios ya que cuentan con la misma Base de Datos del servidor *PDC*.

Server :

Es una computadora trabajando en forma *Stand-Alone* pero que puede o no pertenece al dominio. Éstos servidores pueden hacer uso de las cuentas de usuarios y grupos definidas en la base de datos de los controladores del dominio (*PDC*, *BDC*) pero no pueden administrar esta base de datos.

Los modelos de dominio existentes se pueden definir de las siguientes 4 formas :

- *Single Domain Model.*
- *Master Domain Model.*
- *Múltiple Master Domain Model.*
- *Complete Trust Model.*

Para elegir el modelo de dominio a seguir se deben tomar en cuenta los recursos que se tienen, la cantidad de cuentas de usuarios, el tamaño de la empresa y su estructura.

TRUST.

Las relaciones de confianza proporcionan un canal de comunicación seguro entre dos dominios. Por medio de una relación de confianza un dominio existente puede aceptar como válidas las cuentas de usuarios creadas en otro dominio y darle acceso a sus recursos sin necesidad de que éstas cuentas existan en su propio dominio.

SINGLE DOMAIN MODEL

Todas las cuentas de usuarios y todos los recursos están dentro de un dominio *enterprise-wide*. No es necesario establecer relaciones de confianza en éste modelo de dominio (Fig. 5.1). La administración de las cuentas de usuarios esta centralizada en el *PDC*, y los recursos los mantiene el servidor de recursos el cual pertenece al dominio.

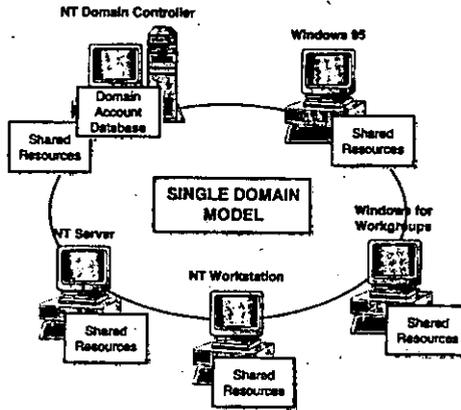


Fig. 5.1 Modelo de Dominio Simple.

Ventajas :

- Este modelo es aceptable para pequeñas empresas, donde no necesitan que sus computadoras participen en un ambiente *WAN*.
- Este modelo permite manejar mas de 40,000 cuentas.
- La administración es centralizada.
- Los grupos de trabajo y las cuentas de usuarios sólo se definen una vez.

Desventajas:

- Es lento el trabajo dentro del dominio

MASTER DOMAIN MODEL.

Este modelo de dominio (Fig. 5.2) trabaja con más de un dominio, uno para administrar las cuentas de usuarios en la base de datos y otro para administrar los recursos que serán accedidos por los usuarios.

En éste modelo de dominio sólo va a existir un servidor *PDC* y uno o varios *BDC's*, el cual es un servidor de respaldo.

Este modelo es común en las organizaciones donde los recursos se comparten entre varios departamentos y cada departamento administra la seguridad de sus recursos, cada departamento necesita tener autoridad para asignar accesos a sus recursos.

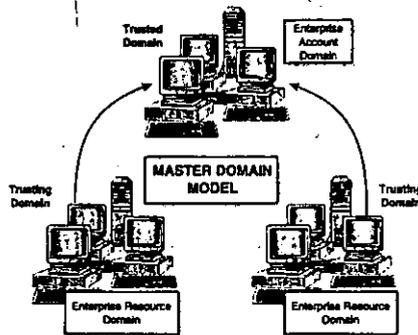


Fig. 5.2 Modelo Master Domain.

Ventajas :

- Soporta más de 10,000 usuarios.
- Debe tener una buena comunicación.
- Debe tener una red confiable.
- Se deben establecer relaciones de confianza.
- Permite una red eficiente.
- Ayuda a escalar una red grande.
- El modelo es transparente para el usuario.

Desventajas :

- La definición de las relaciones de confianza entre los dominios participantes deben establecerse en forma segura, evitando así poner en riesgo la integridad del dominio.

MULTIPLE MASTER DOMAIN MODEL.

Este modelo (Fig. 5.3) es similar al *Master Domain Model* donde las cuentas se manejan centralizadas por uno o varios servidores *PDC*, los recursos están agrupados lógicamente y se manejan de acuerdo a las necesidades, existen relaciones de confianza entre los recursos y las cuentas de usuarios del dominio. La diferencia principal es que la base de datos de las cuentas puede estar distribuida en dos o más dominios de cuentas. Ello puede dar como resultado la forma en que los usuarios están distribuidos en la red *WAN*, con sus ubicaciones físicas, el tamaño de la base de datos de cuentas, el *hardware* del controlador de dominio, la organización cultural o estructura de la empresa.

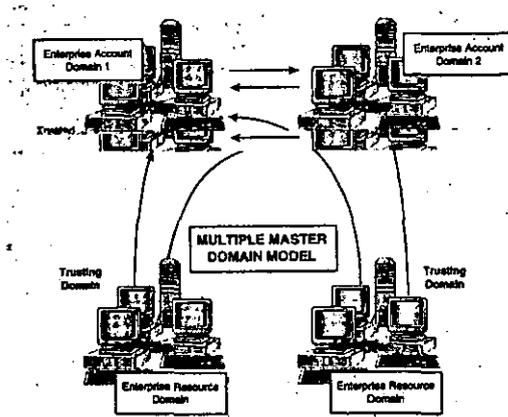


Fig. 5.3 Modelo *Multiple Master Domain*.

Ventajas :

- Este modelo se utiliza para grandes organizaciones donde varios de sus usuarios están localizados en diferentes áreas.
- Modelos a gran escala.
- Máquinas confiables.
- Se manejan 20,000 usuarios.

Desventaja :

- La mayor desventaja es el exceso de relaciones de confianza, ya que se deberán definir por cada servidor que se integra a éste dominio y genera complejidad en la administración.
- Administración problemática.
- Modelo complejo.

En éste modelo cada dominio de recursos confía en cada dominio de cuentas. La fórmula para calcular el número de relaciones de confianza en éste modelo es $M*(m-1) + (r*m)$ donde M representa el número de Dominio Maestro de cuentas y R representa el número de dominios de recursos

COMPLETE TRUST DOMAIN MODEL.

En éste modelo (Fig. 5.4) cada dominio confía en el otro dominio. La administración de las cuentas como la administración de los recursos está distribuido según la estructura de la empresa. Cada dominio cuenta con su propia base de datos de cuentas de usuarios.

Los administradores de recursos proveen el acceso de recursos a los usuarios de otro dominio.

El número de relaciones de confianza que se requieren para éste modelo se obtienen con la siguiente fórmula : $n*(n-1)$ donde n representa el número de dominios que se incluirán en el modelo.

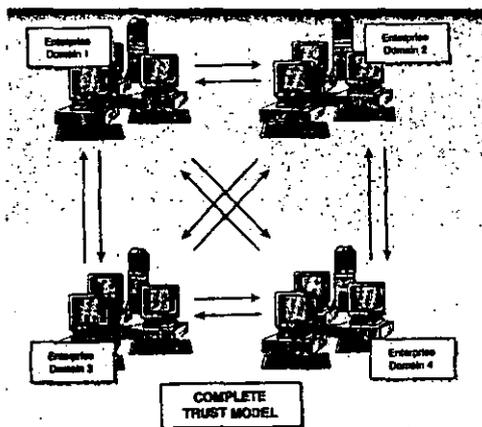


Fig. 5.4 Modelo Complete Trust Domain.

Ventajas :

- Fácil de implementar
- Cada dominio tiene el control de sus cuentas de usuarios.
- Se definen relaciones de confianza de ambas partes entre todos los dominios.
- Se requiere un nivel de confianza en los otros dominios muy alta.

Desventajas :

- Como existen varios administradores de cuentas de usuarios, se pueden duplicar las cuentas de los usuarios, y generar conflictos en la asignación de privilegios.
- Pueden tener un acceso inapropiado por parte de los usuarios a los recursos de la red.
- Es difícil garantizar la seguridad de la red, ya que intervienen varios administradores y varios servidores de recursos, lo cual puede generar que un administrador asigne permisos a un servidor de recursos que no le corresponde.

5.2 Relaciones de Confianza (Trust Relationships).

Un dominio se establece cuando se designa a un controlador de dominio primario (PDC), el cual permitirá la creación de las cuentas de usuarios, grupos de acceso y configurar las relaciones de confianza entre los demás dominios, un PDC tiene un identificador de seguridad (SID) el cual registra funciones y relaciones de seguridad que tiene ese dominio.

El primer objetivo de crear las relaciones de confianza (Trust Relationship, Fig. 5.5) es que cada usuario pueda utilizar la red con una misma cuenta, y pueda acceder de forma fácil y rápida a todos los recursos de la misma, independientemente del lugar donde se encuentren, así como centralizar la administración para un mejor manejo de los usuarios.

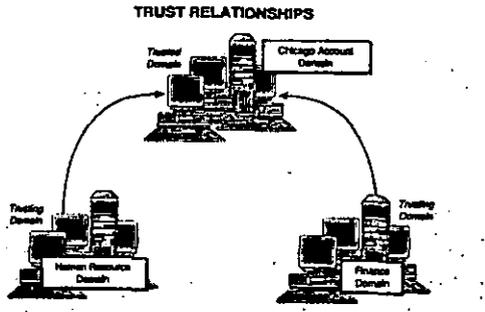


Fig. 5.5 Relaciones de Confianza.

Una relación de confianza (Trust Relationship) establece conexiones seguras, entre dos o más dominios, lo que permite la verificación de los usuarios y el acceso a los recursos de una forma segura entre los dos dominios. La confianza se establece para los usuarios de un dominio que desean acceder a los recursos en el otro dominio en el cual se les ha dado acceso.

La relación de confianza sólo se puede establecer entre los dos servidores controladores del dominio primarios.

El dominio que tiene los recursos que serán accedidos por los usuarios de otro dominio se llama *Trusting Domain*.

El dominio que maneja las cuentas de usuarios que accederán el dominio de recursos se llama *Trusted Domain*.

Trusting vs. Trusted Domains.

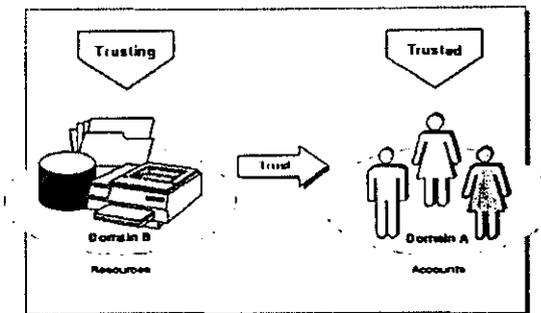


Fig. 5.6 Trusting vs. Trusted Domains.

Cuando la confianza se ha establecido, la administración de los recursos en el *trusting domain* permite crear *ACL's* para sus recursos, agregando cuentas desde su propio dominio, como se hace con las bases de datos de las cuentas en un *trusted domain*, como se muestra en la Fig. 5.6.

Por ejemplo : El usuario *B* del Dominio *B* necesita acceder a los recursos en el Dominio *A*, el administrador de recursos para los recursos en el Dominio *A* puede agregar al usuario *B* a la *ACL* del Dominio de recursos *A* por la relación de confianza establecida.

Cuando el usuario *B* trata de acceder al Dominio *B*, el usuario *B* puede acceder a todos los recursos que tenga en el Dominio *B*, así como a todos los recursos que necesite usar en el Dominio *A*, nuevamente por las relaciones de confianza establecidas. Resumiendo, podremos decir, la relación de confianza da al usuario *B* la habilidad de acceder a cualquier computadora que pertenece al Dominio *A* y así poder acceder al conjunto de recursos de la red, (como se muestra en la Fig. 5.7).

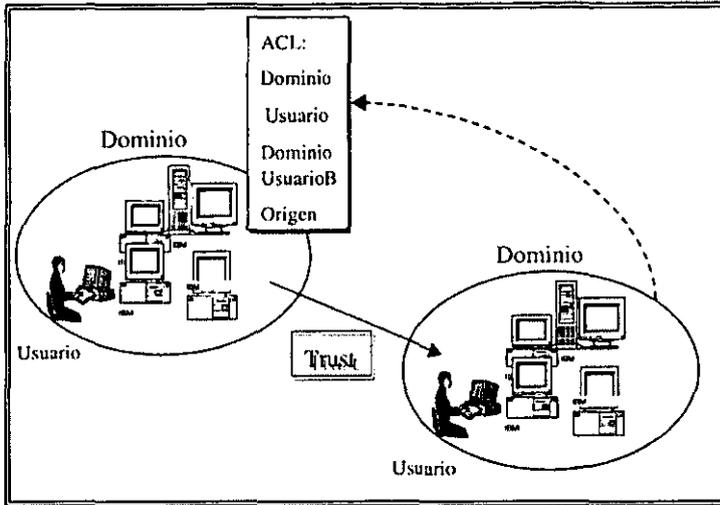


Fig. 5.7 Ejemplo de *Trusting* vs. *Trusted* Domains.

Este tipo de *Trust Relationship* que se describe en la figura se conoce como *one-way-trust*, (relaciones de confianza de un solo lado). Las relaciones de confianza son por naturaleza unidireccionales, generalmente se direccionan del dominio que tiene los recursos hacia el dominio que contiene las cuentas de usuarios y grupos de acceso. *Microsoft* generalmente las representa por medio de una flecha, el inicio de la flecha será el dominio de recursos (*Trusting*) y se dirigirá al dominio de cuentas (*Trusted*).

Esta relación de confianza, *one-way trust* es directa de un dominio de recursos a un dominio de cuentas (*trusting to trusted*) lo cual permite que los usuarios del dominio de cuenta puedan acceder a los recursos en el otro dominio y permitan conectarse a cualquier máquina del dominio, dentro de éstos dominios.

También se puede establecer la relación *two-way trust* que existe entre dos dominios. Lo cual permite que los usuarios de un dominio puedan acceder a los recursos del otro dominio, y tengan acceso a todas las máquinas que forman parte de éstos dominios, con una sola cuenta.

Como los dominios, las relaciones de confianza son canales de comunicación lógicos, la ubicación física de los dominios no es importante, lo que es importante establecer es :

- La ubicación de los recursos y ubicación de cuentas de usuarios, por ejemplo, dominio de recursos y dominio de cuentas.
- Cuáles dominios se requieren que confíen en otros.
- Cual será el tipo de relación de confianza que se deberá establecer, *one-way o two-way*.
- Cual es el número de relaciones de confianza que deberá establecer una empresa para satisfacer sus necesidades.

Los elementos necesarios para establecer las relaciones de confianza entre dos dominios son :

- Un dominio se identifica con su *PDC*.
- No debe existir ninguna sesión conectada entre los dos *PDC's* para poder definir las relaciones de confianza.
- Cuando se establece la relación de confianza, el proceso de verificación de la cuenta del usuario, se efectúa en forma automática en el *PDC* del dominio al que nos conectaremos.
- Los administradores establecen las relaciones de confianza. Se debe estar seguro de poder acceder a los dos dominios con la clave de administrador.
- Se utilizará la herramienta del manejador de dominios (*User Manager*) para establecer las relaciones de confianza.

El proceso de definición de una relación de confianza se puede efectuar por dos formas:

Trusted :

El *trusted domain* debe identificar a cual dominio confiará (dominio de recursos).

Trusting :

El *trusting domain* debe identificar cual es el dominio que confía (dominio de cuentas).

Se deberá establecer primero el *trusted domain* para que de forma automática se establezca el *trusting domain* el cual confiará en el otro dominio.

Deben seguir los siguientes pasos para definir una relación de confianza de tipo *trusting domain* (Fig. 5.8):

1. Utilizar la herramienta *User Manager for Domain* para definir una relación de confianza.
2. Seleccionar *Policies y Trust Relation Ships* como se muestra en el siguiente cuadro :

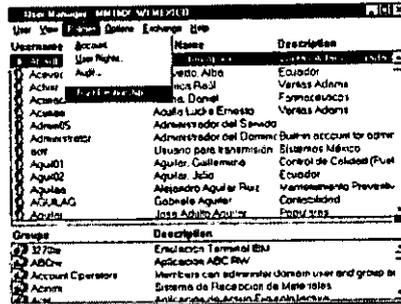


Fig. 5.8 Cuadro 1.

3. Seleccionar *Add* para agregar el *Trusting Domain* de la lista :

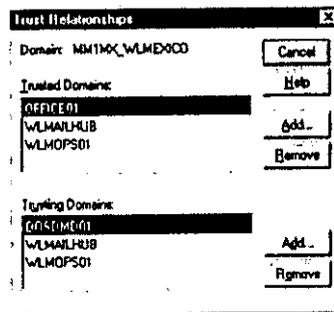


Fig. 5.8 Cuadro 2.

4. Anotar el nombre del *Trusting Domain* en la caja de texto de *Trusting Domain*.

2. Seleccionar *Policies* y *Trust Relation Ships* como se muestra en el siguiente cuadro.

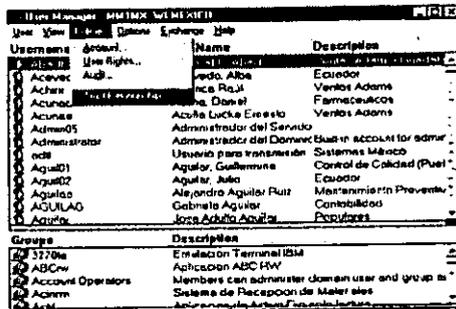


Fig. 5.9 Cuadro 2.

3. Seleccionar *Add* para agregar el *Trusted Domain* de la lista :

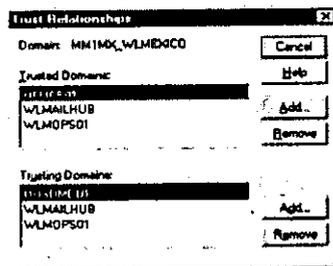


Fig. 5.9 Cuadro 3.

4. Anotar el nombre del *Trusted Domain* en la caja de diálogo *Domain* :

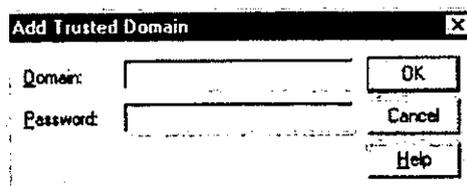


Fig. 5.9 Cuadro 4.

5. Teclear el nombre de la contraseña definida en la definición del *Trusting Domain*.
6. Seleccionar *Ok*.
7. Si el *trusted domain* permite que el otro dominio confíe y la contraseña tecleada es correcta se desplegará un mensaje indicando que se establecieron las relaciones de confianza con éxito, en caso contrario también aparecerá otro mensaje, indicándole el error.

5.3 Definición de Relaciones de Confianza entre México y Casa Matriz.

Todas las regiones de *Exchange* se deberán conectar a la región central o *Hub Central* definido como parte de la configuración.

Para establecer la conexión entre los diferentes *sites* y el *Hub Central* se deberá establecer una relación de confianza (*Trust RelationShip*) de ambas partes (dual).

La definición para establecer una relación confianza dual se comentó en el inciso anterior (definiciones de *Trust RelationShip*).

Los elementos necesarios para definir una relación de confianza entre dos dominios diferentes son :

- Nombre del dominio con el que se desea establecer la relación de confianza
- Nombre del servidor *PDC* del otro dominio.
- Direcciones *IP* del servidor *PDC* del otro dominio.
- Nombre de todos los servidores *BDC* del otro dominio.
- Direcciones *IP* de todos los servidores *BDC* del otro dominio.
- Nombre del servidor de *Exchange* del otro dominio.
- Dirección *IP* del servidor de *Exchange* del otro dominio.

Será necesario que el servidor con el que se desea establecer la relación de confianza cuente también con la información anterior y defina las direcciones en su servidor de *WINS*.

Se deberán definir en el servidor de *WINS* local las direcciones *IP* del otro dominio en forma estática.

El procedimiento de definición de direcciones estáticas en el servidor de *WINS* se documentó en el capítulo 5 (elementos de resolución de nombres).

La definición de las cuentas de usuarios, los privilegios y los recursos que se instalarán en cada afiliada son responsabilidad exclusivamente de la afiliada y el uso de los recursos siempre es posible compartirlos estableciendo relaciones de confianza con la afiliada que solicita acceso a los recursos.

Actualmente la afiliada de México tiene definidas relaciones de confianza con el servidor de Casa Matriz en *NJ* y con las oficinas de *Greenwood*.

La primera relación de confianza definida con Casa Matriz es para utilización del correo electrónico y para permitirle al servidor de Casa Matriz la actualización con todos los servidores del corporativo.

La segunda relación de confianza definida es para permitir al personal de *Greenwood* que accese recursos de la afiliada de México pero con sus propias cuentas de usuarios definidas en su localidad.

El uso de las relaciones de confianza entre diferentes dominios, permite compartir recursos entre diferentes afiliadas, incrementado el volumen de productividad y reducción de costos, ya que al contar una filial con los recursos que otras pueden acceder, no es necesario definir nuevamente esos recursos en la otra filial.

5.4 Elementos de Resolución de Nombres.

5.4.1 DNS.

Windows NT con *TCP/IP* necesita una dirección *IP* única y un nombre para cada equipo de la red. Debe existir un mecanismo en toda red *TCP/IP* para establecer una correspondencia entre los nombres de los equipos y sus direcciones *IP*. Éste mecanismo se llama Servicio de Resolución de Nombres.

Resolución de Nombres Utilizando el Sistema de Nombres de Dominio.

El *DNS* es una base de datos distribuida que proporciona un sistema de nomenclatura jerárquico para identificar *host* en *Internet*. *DNS* se desarrolló para resolver los problemas que surgieron cuando el número de *host* de *Internet* aumentó considerablemente a principios de la década de los '80. Las especificaciones para *DNS* están definidas en las *RFC 1034* y *1035*. Aunque *DNS* puede parecer similar a *WINS*, hay una diferencia principal: *WINS* es totalmente dinámico, mientras que *DNS* necesita configuración estática para la asignación de nombres de equipos a direcciones *IP*.

Servidores de Resolución de Nombres.

DNS utiliza un modelo cliente-servidor donde los servidores *DNS* contienen información de una parte de la base de datos *DNS* (zona) y hacen que esta información esté disponible para los *resolvers*. Un *resolver* realiza una consulta de un servidor de nombres pidiendo información acerca del espacio de nombres *DNS*. Éste servidor de nombres puede, a su vez, consultar otros servidores del mismo tipo al intentar responder a la consulta realizada por el *resolver*.

Un administrador de una zona *DNS* configura uno o más servidores de nombres para la zona:

Un servidor de nombres principal. Éste servidor tiene una copia maestra de los archivos de la base de datos con los registros de recursos de todos los subdominios y *host* de la zona.

Un servidor de nombres secundario. Éste servidor recibe una copia duplicada de los archivos de la base de datos del servidor principal. Cuando la estructura de la zona cambia, los archivos de la base de datos maestra se modifican y se copian a los servidores secundarios. Los archivos de los servidores secundarios nunca se tocan.

Un servidor de nombres de sólo-obtener. A diferencia de los servidores principales y secundarios, un servidor de sólo-obtener no está asociado a ninguna zona *DNS* específica y no contiene archivos de base de datos. Cuando se inicia un servidor de sólo-obtener no conoce la estructura del dominio *DNS* y debe confiar en la información que le dan otros servidores. Cada vez que un servidor de sólo-obtener consulta un servidor de nombres y recibe una respuesta, almacena la información en su memoria *caché*. Cuando otras consultas solicitan esta información, el servidor de sólo-obtener les responde directamente con la información de la memoria *caché*. Con el tiempo, la memoria *caché* crecerá hasta llegar a incluir la información que se solicita con más frecuencia.

Aunque el *software DNS* no lo necesita, los servidores secundarios son convenientes por las siguientes razones :

- Equilibran la carga .- Los servidores secundarios alivian la carga del servidor principal. Esto puede ser significativo en redes con mucho tráfico en las que las consultas al servidor de nombres pueden llegar a 20,000 a la hora e incluso más.
- Tolerancia a fallos .- Los servidores secundarios permiten que la resolución de nombres *DNS* continúe cuando el servidor principal no esté disponible.
- Reducen el tráfico de red .- Los servidores secundarios ubicados en la proximidad de los equipos cliente reducen el tráfico entre redes a través de los ruteadores.

Windows NT Server 4.0 incluye funcionalidad de servidores de nombres DNS compatible con RFC. Windows NT Server, Windows NT Workstation, Windows 95 y Windows para Trabajo en Grupo 3.11 con Microsoft TCP/IP-32 instalado incluye toda la funcionalidad de resolución DNS.

Además del servicio servidor de nombres DNS, Windows NT Server 4.0 incluye una herramienta de administración gráfica basada en RPC, el administrador DNS, que permite a los administradores realizar su función de forma remota a los servidores de nombres DNS. El administrador DNS tiene funciones similares al administrador WINS de Windows NT Server 4.0. Para obtener más información acerca de la instalación y el uso de éstas herramientas.

Espacio de Nombres de Dominio.

La base de datos DNS es una estructura de árbol denominada espacio de nombres de dominio, en la cual cada dominio (nodo en la estructura de árbol) tiene un nombre y puede contener subdominios. El nombre de dominio identifica la posición del dominio en la base de datos con respecto a su dominio principal y utiliza un punto (.) para separar cada parte de los nombres de los nodos de la red del dominio DNS. Por ejemplo, el nombre de dominio *DNS csu.edu* especifica el subdominio *csu* cuyo dominio principal es *edu*; *csu.com* especifica el subdominio *csu* cuyo dominio principal es *com*. La Fig. 5.11 muestra las relaciones principal-secundario de los dominios DNS.

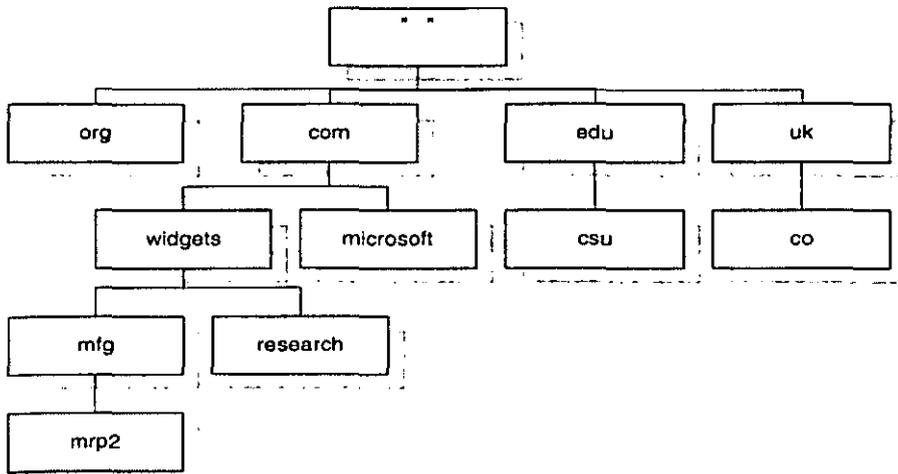


Figura 5.11 Relaciones principal-secundario de los dominios DNS.

Como se muestra en la figura anterior, el nodo raíz de la base de datos *DNS* no tiene nombre (*null*). Se hace referencia a él en los nombres *DNS* con un punto al final (.). Por ejemplo, en el nombre *estudio.widgets.com.*, el punto que hay después de *com* indica el nodo raíz *DNS*.

Dominios de Nivel Superior.

InterNIC administra la raíz y los dominios de nivel superior de la base de datos *DNS*. Los nombres de dominio de nivel superior se dividen en tres áreas principales :

- Dominios basados en organizaciones (nombres de tres caracteres).
- Dominios geográficos (códigos de país de dos caracteres que se encuentran en *ISO 3166*).
- Dominio *in-addr.arpa*. (dominio especial que se usa para las asignaciones dirección-nombre)

Los nombres de dominio basados en organizaciones se empezaron a utilizar originalmente en Estados Unidos, pero a medida que *Internet* empezó a crecer internacionalmente, se hizo evidente que una división basada en organizaciones era inadecuada para una entidad global. Entonces se introdujeron los nombres de dominio geográfico. Incluso cuando existe un dominio de país *us*, los nombres de dominio en Estados Unidos se basan aún en su mayoría en organizaciones. Como se muestra en la tabla 5.12, hay siete dominios basados en organizaciones en la actualidad.

Tipo de organización o institución	Tipo de organización o institución
<i>com</i>	Comercial
<i>edu</i>	Educativa
<i>gov</i>	Gubernamental
<i>org</i>	Organizaciones no comerciales
<i>net</i>	Organizaciones de conectividad en red
<i>mil</i>	Militar
<i>int</i>	Internacional

Tabla 5.12 Los dominios *DNS* basados en organizaciones

Delegación.

InterNIC delega en otras organizaciones la responsabilidad de administrar el espacio de nombres de dominio *DNS* por debajo del nivel superior. Éstas organizaciones posteriormente subdividen el espacio de nombres y delegan responsabilidades. Éste modelo administrativo descentralizado permite que *DNS* se administre de manera autónoma en los niveles que sean razonables para cada organización involucrada.

Zonas.

La unidad administrativa en *DNS* es la zona. Una zona es un subárbol de la base de datos *DNS* que se administra como una entidad separada. Puede consistir en un único dominio o en un dominio dividido en subdominios. Los subdominios del nivel inferior de una zona también se pueden dividir en una zona o zonas separadas. La Fig. 5.13 ilustra la relación entre los dominios *DNS* y las zonas :

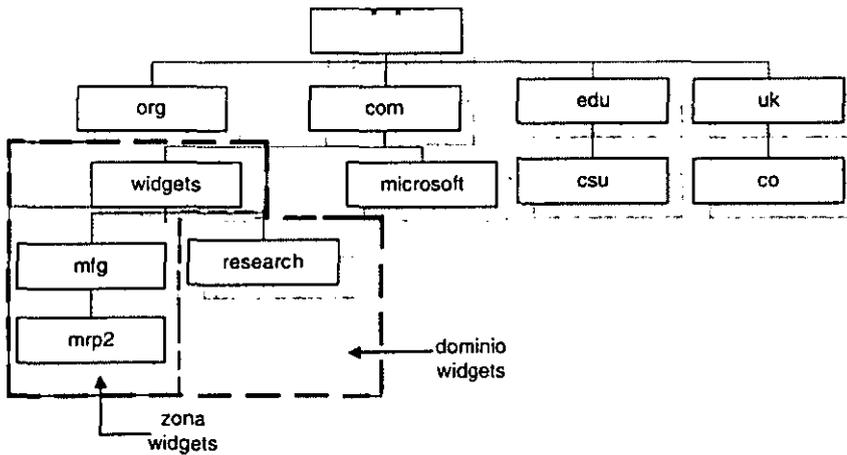


Figura 5.13 Relación entre los dominios *DNS* y las zonas.

Nombres de Dominio Completos.

Con excepción del nodo raíz, cada nodo de la base de datos *DNS* tiene un nombre (etiqueta) con un máximo de 63 caracteres. Cada subdominio debe tener un nombre único dentro de su dominio principal. Esto asegura la unicidad del nombre en el espacio de nombres *DNS*. Los nombres de dominio *DNS* se forman siguiendo la ruta desde la parte inferior del árbol *DNS* a la raíz. Los nombres de los nodos se concatenan y un punto (.) separa cada parte. Éstos nombres se conocen como nombres de dominio completos (*FQDN*). He aquí hay un ejemplo :

mrp2.widgets.mfg.universal.co.uk.

En la práctica, la mayoría de las entradas de *host DNS* no aparecen en un nivel inferior al quinto nivel del árbol *DNS*, siendo tres o cuatro el nivel más habitual.

Resolución de Nombres.

La tarea clave de *DNS* es presentar nombres sencillos a los usuarios y resolver esos nombres en direcciones *IP*, como requiere el conjunto de redes. La resolución de nombres la proporcionan los servidores de nombres a través de *DNS*, interpretando la información de un *FQDN* para obtener su dirección específica. Como se muestra en la Fig. 5.14, el proceso empieza cuando un *resolver* pasa una consulta a su servidor de nombres local. Si el servidor de nombres local no tiene los datos solicitados en la consulta, los solicita a otros servidores de nombres en nombre del *resolver*. En el caso peor, el servidor de nombres local se inicia por la parte superior del árbol *DNS* con uno de los servidores de nombres raíz y funciona de esta forma hasta que se encuentran los datos solicitados.

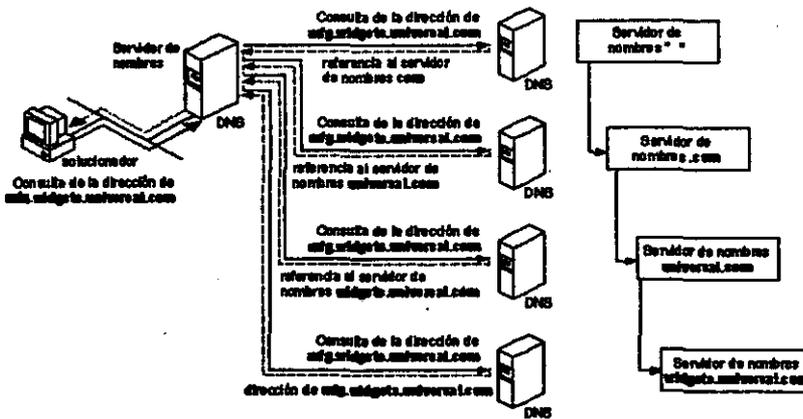


Fig. 5.14 Proceso de resolución de nombres.

La resolución de nombres *DNS* se basa en tres conceptos claves: recursividad, iteración y obtención.

- **Recursividad** .- Un *resolver* pasa una petición de resolución recursiva a su servidor de nombres local. Una petición de resolución recursiva indica al servidor de nombres que el resolver espera una respuesta completa a la consulta, no sólo un puntero a otro servidor de nombres. La resolución recursiva pasa de manera efectiva la carga de trabajo al servidor de nombres y permite que el resolver sea pequeño y simple.
- **Iteración** .- Si el servidor de nombres local no puede resolver la consulta por completo, obtiene la ayuda de otro servidor de nombres *DNS* a través del espacio de nombres *DNS*. Un servidor de nombres local realiza la tarea de procesamiento él mismo y pasa sólo la resolución iterativa a otros servidores de nombres. Una petición de resolución iterativa indica el nombre del servidor del que el peticionario espera recibir la mejor respuesta sin la ayuda de otros servidores de nombres. Si el servidor de nombres tiene los datos solicitados, los devuelve; de lo contrario, devuelve punteros a los servidores de nombres que tienen más probabilidad de tener una respuesta. Sin embargo, si un servidor de nombres principal no es capaz de resolver una petición de datos de su zona, devuelve un error al peticionario.
- **Obtención** .- A medida que los servidores de nombres locales procesan de manera recursiva las peticiones, descubren mucha información sobre el espacio de nombres de dominio *DNS*. Para aumentar el rendimiento de *DNS* y facilitar las tareas en el conjunto de redes y en los otros servidores de nombres, éstos últimos mantienen temporalmente esta información en la memoria *caché* local. Cuando llega una petición del *resolver*, el servidor de nombres local comprueba la información estática y la memoria *caché* para dar una respuesta. Incluso si la respuesta no está en la memoria *caché*, la identidad del servidor de nombres de la zona puede estar, lo que reduce el número de peticiones iterativas que el servidor de nombres tiene que procesar.

5.4.2 WINS.

Windows Internet Name Service (WINS) y Resolución de Nombres por Difusión.

WINS proporciona una base de datos dinámica y duplicada para el registro y la consulta de las asignaciones entre nombres de equipos *NetBIOS* y direcciones *IP* en un entorno de red encaminado. *WINS* se ha diseñado para resolver los problemas que surgen con la resolución de nombres en conjuntos de redes complejas.

WINS reduce el uso de difusiones locales para la resolución de nombres y permite a los usuarios localizar fácilmente sistemas en redes remotas. Más aún, cuando el direccionamiento dinámico a través de *DHCP* da como resultado direcciones *IP* nuevas para los equipos que se trasladan de subred, los cambios se actualizan automáticamente en la base de datos de *WINS*. En éste caso, ni el usuario ni el administrador de la red necesitan hacer cambios manualmente.

El protocolo *WINS* se basa y es compatible con los protocolos definidos para *NBNS* en las *RFC 1001* y *1002*, por lo que puede funcionar conjuntamente con cualquier otra implementación de éstas *RFC*.

Esta sección proporciona una introducción a la manera en que *WINS* y las difusiones de consultas de nombres proporcionan la resolución de nombres.

***WINS* en un Entorno Encaminado.**

WINS consta de dos componentes :

- El servidor *WINS*, que administra las consultas y los registros de nombres.
- El *software* cliente, que consulta la resolución de nombres de equipo.

Los clientes de red de *Windows* (equipos con *Windows NT*, *Windows 95*, o *Windows* para Trabajo en Grupo 3.11 con *WINS* activado) pueden utilizar *WINS* directamente. Los equipos que no disponen de *WINS* y que son compatibles con el nodo b, como se describe en las *RFC 1001* y *1002*, pueden tener acceso a *WINS* a través de agentes *Proxy*, que son equipos con *WINS* activado que escuchan las difusiones de consultas de nombres y a continuación responden para los nombres que no están en la subred local o que son equipos nodo *p*.

En una red *Windows NT*, los usuarios pueden examinar de forma transparente los recursos que hay al otro lado de un ruteador. Para permitir éste examen sin *WINS*, el administrador de la red debe asegurarse de que el dominio principal de *Windows NT* de los usuarios tiene equipos con *Windows NT Server* o *Windows NT Workstation* en ambos lados del ruteador para que actúen como examinadores principales. Éstos equipos necesitan archivos *LMHOSTS* correctamente configurados con entradas para los controladores de dominio de *Windows NT* de la subred.

Con *WINS*, no es necesario emplear éste tipo de estrategias porque los servidores de *WINS* y los agentes *Proxy* proporcionan el soporte necesario para examinar lo que hay al otro lado de los ruteadores allí donde los dominios de *Windows NT* los atraviesan.

La Fig. 5.15 muestra un pequeño conjunto de redes formado por tres de ellas de área local conectadas por medio de un ruteador. Dos de las subredes contienen servidores de nombres *WINS* utilizables por los clientes de las dos subredes. Los equipos con *WINS* activado, incluidos los agentes *Proxy*, tienen acceso directamente al servidor *WINS*, y los equipos que utilizan difusiones tienen acceso al servidor de *WINS* a través de los agentes *Proxy*. Los agentes *Proxy* interceptan los mensajes difundidos y los envían directamente al servidor *WINS*.

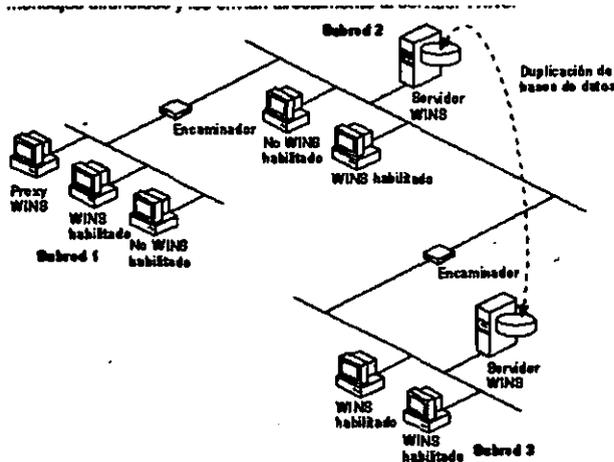


Fig. 5.15 Redes conectadas por un ruteador.

El *Proxy* se comunica con el servidor *WINS* para resolver nombres y después los guarda en memoria *caché* durante cierto tiempo. El *Proxy* funciona como intermediario, ya comunicando con el servidor de *WINS* o suministrando una asignación entre un nombre y una dirección *IP* desde su *caché*. La Fig. 5.16 muestra las relaciones existentes entre los servidores y los clientes *WINS*, incluyendo los agentes *Proxy* para los equipos que no utilizan *WINS*.

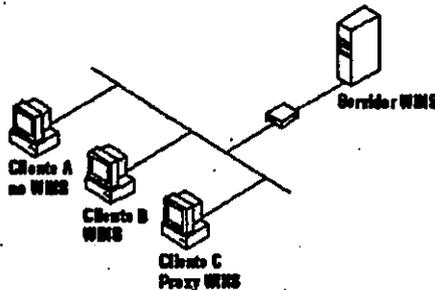


Fig. 5.16 Relaciones entre servidores y sus clientes.

En la figura anterior (Fig. 5.16), el cliente *A* no está habilitado para *WINS*, el cliente *B* está habilitado para *WINS* y el cliente *C* es un agente *Proxy WINS*. La tabla 5.17 muestra los pasos típicos que el cliente *A* y el cliente *B* realizan cuando están resolviendo nombres.

Cliente <i>A</i> (no <i>WINS</i>)	Cliente <i>B</i> (<i>WINS</i>)
El cliente <i>A</i> envía una consulta (como un mensaje de difusión) para la dirección <i>IP</i> del cliente <i>X</i> . El cliente <i>X</i> (que no aparece en la figura) no está en la subred local. (1)	El cliente <i>B</i> hace una consulta al servidor <i>WINS</i> para la dirección <i>IP</i> del cliente <i>A</i> .
El cliente <i>C</i> (<i>Proxy WINS</i>) intercepta el mensaje de difusión y lo envía directamente al servidor <i>WINS</i> . (2)	El servidor <i>WINS</i> responde directamente al cliente <i>B</i> con la dirección <i>IP</i> del cliente <i>A</i> . (3)
El servidor <i>WINS</i> responde directamente al cliente <i>C</i> con la dirección <i>IP</i> del cliente <i>X</i> .	Si no está disponible el servidor <i>WINS</i> , la consulta falla. El cliente <i>B</i> cambia al nodo <i>b</i> y envía la consulta como un mensaje de difusión a la subred local.
El cliente <i>C</i> responde directamente al cliente <i>A</i> con la dirección <i>IP</i> del cliente <i>X</i> .	El cliente <i>A</i> recibe la difusión y responde directamente al cliente <i>B</i> .

- (1) Si el cliente *X* está en la subred local, responderá directamente a la consulta del cliente *A*.
- (2) Puede que el cliente *C* tenga ya la información pedida en la memoria *cache*. Si es así, el cliente *C* responde directamente al cliente *A* sin pasar por el servidor *WINS*.
- (3) Ambos ejemplos asumen que la información solicitada está disponible en la base de datos *WINS* en el servidor.

Tabla 5.17 Resolución de nombres en clientes *WINS* y no *WINS*

Si el equipo cliente de *Windows NT* también tiene activado *DHCP* y el administrador especifica la información del servidor de *WINS* como parte de las opciones de *DHCP*, normalmente el equipo estará configurado automáticamente con información del servidor de *WINS*.

En un entorno *WINS* y en un entorno de resolución de nombres por difusión, un equipo cliente con *WINS* se comportará de manera diferente de un cliente no *WINS*. Éstas diferencias se notarán en la forma en la que éstos clientes realizan la resolución, registro, liberación y renovación.

Resolución de Nombres.

Con los servidores *WINS* en el conjunto de redes, los nombres de equipos *NetBIOS* se resuelven usando dos métodos básicos, dependiendo de si la resolución *WINS* está disponible y habilitada en el equipo cliente. Cualquiera que sea el método de resolución utilizado, el proceso es transparente para el usuario una vez configurado el sistema.

- Si *WINS* no está activado en el cliente : El equipo registra su nombre enviando paquetes de petición de registro de nombre (como mensajes de difusión) a la subred local. Para encontrar un equipo en particular, el equipo que no utiliza *WINS* envía paquetes de petición de consulta de nombre (como mensajes de difusión) en la subred local. (Esta difusión no puede atravesar ruteadores de *IP*.) Si falla la resolución local de nombres, se consulta el archivo *LMHOSTS* local. Éstos procesos se llevan a cabo si el equipo es un servidor de red, una estación de trabajo u otro dispositivo.
- Si *WINS* está activado en el cliente : El equipo consulta primero al servidor *WINS* y, si no obtiene ningún resultado, envía sus peticiones de registro y de consultas de nombres (como mensajes de difusión) siguiendo los pasos que se indican a continuación:

Durante la configuración de *TCP/IP*, el equipo cliente registra su nombre en el servidor *WINS*. Esto se muestra en la Fig. 5.18. (se observa que la base de datos de *WINS* se duplica en todos los servidores *WINS* del conjunto de redes.)

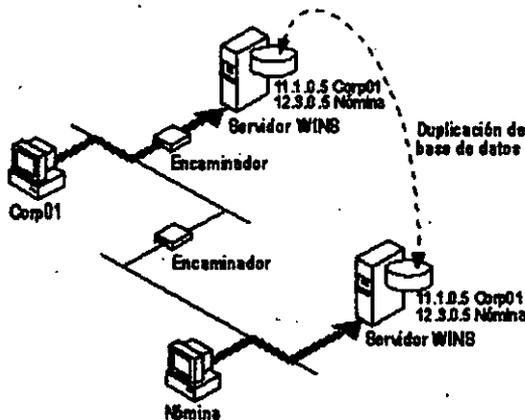


Fig. 5.18 Configuración *TCP/IP*.

Como se describe en la figura anterior (Fig. 5.18) primero se envía una petición de consulta de nombre al servidor de *WINS*. Si se encuentra el nombre en la base de datos de *WINS*, el cliente puede establecer una sesión basada en la asignación de direcciones recibida del servidor de *WINS* (Fig. 5.19).

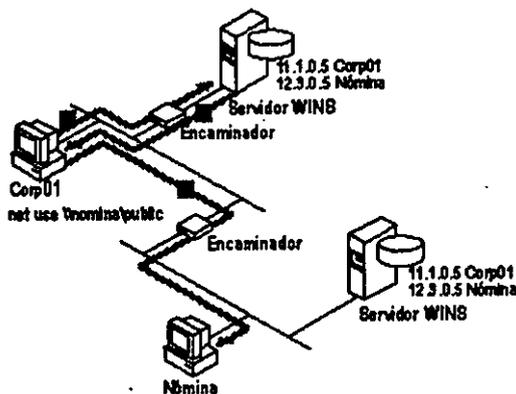


Fig. 5.19 Asignación de direcciones.

Si al consultar al servidor de *WINS* no se obtiene un resultado satisfactorio y el equipo cliente está configurado como nodo *h*, el equipo cliente envía paquetes de petición de consulta de nombre (como mensajes de difusión) de la misma forma que un equipo que no tenga activado *WINS*.

Finalmente, si fallan otros métodos, se comprueba el archivo local *LMHOSTS*. (Se incluyen en la búsqueda archivos centralizados *LMHOSTS* referenciados por instrucciones *#INCLUDE* en el archivo local.)

Los servidores *WINS* aceptan y responden a las consultas de nombres *UDP*. Cualquier asignación entre nombre y dirección *IP* registrada en un servidor *WINS* puede constituir una respuesta fiable a una consulta de nombre. Sin embargo, una asignación de la base de datos no garantiza que el dispositivo relacionado esté funcionando en ese momento, sólo que un equipo ha solicitado esa dirección *IP* en particular y actualmente tiene una asignación válida con un nombre de dispositivo.

Registro de Nombres.

El registro de nombres asegura que el nombre *NetBIOS* y la dirección *IP* del equipo sean exclusivos para cada dispositivo.

Si *WINS* está activado en el cliente : La petición de registro de nombre se envía directamente al servidor *WINS* para que lo agregue a la base de datos. Un servidor *WINS* acepta o rechaza un registro de nombre de equipo dependiendo del contenido actual de su base de datos :

- Si la base de datos contiene una dirección diferente para ese nombre, *WINS* pide a la entrada actual que determine si el dispositivo sigue solicitando ese nombre.
- Si otro dispositivo está utilizando ese nombre, *WINS* rechaza la nueva petición de registro.
- De lo contrario, *WINS* acepta la entrada y la agrega a su base de datos local junto con una marca de hora, un número de versión único progresivo y otros datos.

Si *WINS* no está activado en el cliente : Para registrar su nombre, un equipo que no utilice *WINS* difunde un paquete de petición de registro de nombre a la red local, indicando su nombre de equipo *NetBIOS* y su dirección *IP*. Cualquier dispositivo de la red que haya solicitado ese nombre con anterioridad contesta al registro de nombre (con una respuesta negativa de registro de nombre) provocando un error al intentar registrar el nombre duplicado. Si la petición de registro de nombre no recibe una respuesta durante un período de tiempo determinado, el equipo solicitante adopta ese nombre y esa dirección.

Una vez que un equipo que no utiliza *WINS* ha solicitado un nombre, debe contestar a los intentos que se produzcan de registrar su nombre por duplicado (con una respuesta negativa de registro de nombre) y responder afirmativamente a las consultas de nombres emitidas con su nombre registrado (enviando una respuesta afirmativa de consulta de nombre). La respuesta afirmativa de consulta de nombre contiene la dirección *IP* del equipo para que los dos sistemas puedan establecer una sesión.

Liberación de Nombres.

Cuando un equipo deja de utilizar un nombre determinado (como por ejemplo, cuando se detienen los servicios estación de trabajo o servidor de *Windows NT*), ya no contesta a las solicitudes de registro emitidas para ese nombre. Esto se denomina liberar un nombre.

Si *WINS* está activado en el cliente : Siempre que un equipo se cierra adecuadamente, libera su nombre para el servidor *WINS*, el cual marca como liberada la entrada correspondiente de la base de datos. Si la entrada sigue liberada durante un período de tiempo determinado, el servidor *WINS* la marca como extinguida, actualiza el número de versión y notifica los cambios a otros servidores *WINS*.

- Si un nombre está marcado como liberado en un servidor *WINS* y llega un nuevo registro que utiliza ese nombre pero con una dirección diferente, el servidor *WINS* puede dar inmediatamente ese nombre al cliente que lo solicita porque sabe que el cliente antiguo ya no utiliza ese nombre. Esto puede ocurrir, por ejemplo, cuando un equipo portátil con *DHCP* activado cambia de subred.
- Si ese equipo ha liberado su nombre durante un cierre ordenado del sistema, el servidor *WINS* no contestará al nombre cuando se vuelva a conectar el equipo. Si no se produce un cierre del sistema ordenado, el registro del nombre con una nueva dirección provocará que el servidor *WINS* conteste al registro, pero la contestación fallará y el registro se llevará a cabo porque el equipo ya no tiene la dirección antigua.

Si *WINS* no está activado en el cliente : Cuando un equipo que no utiliza *WINS* libera un nombre, se realiza una difusión para permitir que cualquier sistema de la red que contenga ese nombre en su memoria *caché* lo elimine. Después de recibir los paquetes de consulta de nombre que especifican el nombre eliminado, los equipos simplemente ignoran la petición, permitiendo que otros equipos de la red adquieran el nombre que ha liberado.

Para que los equipos que no utilizan *WINS* sean accesibles desde otras subredes, sus nombres deben agregarse como entradas estáticas a la base de datos de *WINS* o al archivo o archivos *LMHOSTS* de los sistemas remotos, ya que sólo responderán a las consultas de nombres que se originen en su subred local.

Renovación de Nombres.

Periódicamente, es necesario que los equipos cliente renueven sus registros de nombres *NetBIOS* con el servidor *WINS*. Cuando un equipo cliente se registra primero con un servidor *WINS*, éste devuelve un mensaje que indica cuándo necesita el cliente renovar su registro :

- El intervalo de tiempo predeterminado de renovación de las entradas en la base de datos *WINS* es de cuatro días.
- Los clientes *WINS* se registran y actualizan cada dos días.
- Los servidores *WINS* primario y de reserva deben tener el mismo intervalo de renovación.
- Las entradas definidas como estáticas nunca caducan.

Si la entrada pertenece al servidor *WINS* local, el nombre se libera en el momento especificado a menos que el cliente lo haya renovado. Si la entrada pertenece a otro servidor *WINS*, se volverá a validar en el momento especificado. Si la entrada no existe en la base de datos del servidor *WINS* que es su propietario, se elimina de la base de datos del *WINS* local. Las peticiones de renovación de nombres se tratan de la misma forma que los registros nuevos.

Un ajuste incorrecto de éste intervalo puede afectar de manera negativa al rendimiento de la red y del sistema.

5.4.3 *LMHOSTS*.

Éste es un ejemplo del archivo *LMHOSTS* utilizado por *Microsoft TCP/IP* para *Windows NT*.

Este archivo contiene los mapas de direcciones *IP* para nombres de computadoras *NT* (*NetBIOS*). Cada elemento debe tener una línea individualmente. La dirección *IP* debe estar ubicada en la primera columna seguida por el correspondiente nombre de la computadora. La dirección y el nombre de la computadora deben estar separados por un espacio o tabulador. El carácter “#” es generalmente usado para denotar el comienzo de un comentario.

Este archivo es compatible con los archivos *LMHOSTS Microsoft LAN Manager 2.x TCP/IP* y se compone de las siguientes extensiones :

- # PRE
- # DOM:< dominio>
- # INCLUYE< nombre del archivo>
- # BEGIN_ALTERNATE
- # END_ALTERNATE
- \0xnn (non-printing character support)

Seguido a un elemento en el archivo con los caracteres “ # PRE” deberá estar el elemento a ser precargado dentro del *name cache*. Por default, los elementos no son precargados, pero son revisados solo después de fallas en la resolución de *host names* dinámicos.

Seguido al elemento “ # DOM: < domain>” se debe asociar el elemento con el dominio específico en < domain>. Éste afecta tanto al browser y a los servicios de *logon* los cuáles tienen buen funcionamiento en ambientes *TCP/IP*. Para preinstalar el *host name* asociado con el elemento “# DOM”, es necesario también agregar un # PRE a la línea. El <domain> está siempre precargado aunque éste se muestra cuando el *name cache* es visto.

Especificando la sentencia "# INCLUDE <filename>" forzará al *software RFC NetBIOS* (NBT) a ver el <filename> especificado y revisar éste como si fuera local. El <filename> es generalmente un nombre *UNC-based*, permitiendo a un archivo centralizado *LMHOSTS* darle mantenimiento en un servidor. Esto es siempre necesario para proporcionar un mapeado de direcciones *IP* del servidor priorizado por el # INCLUDE. Éste mapeado debe utilizar la directriz # PRE. En suma, la porción "public" en el ejemplo abajo mencionado debe estar en la lista de *LanManServer* del "NullSessionShares", con un orden para máquinas cliente y ser habilitado de lectura el archivo *LMHOSTS* satisfactoriamente. Esta clave es la siguiente :

```
\machine\system\currentcontrolset\service\lanmanserver\parameters\nullsessionshares
```

En el registro, simplemente se agrega "public" a la lista encontrada.

Las palabras clave # BEGIN_ y # END_ALTERNATE proporcionan el uso de múltiples sentencias # INCLUDE para agrupar declaraciones. Cualquier elemento exitoso causará que el grupo tenga éxito.

Finalmente, los caracteres "non-printing" pueden ser insertados en mapas por los primeros *NetBIOS names* entre comillas, entonces se utiliza la notación "\ 0xnn" para especificar un valor hexadecimal para un carácter "non-printing".

El siguiente ejemplo ilustra todas éstas extensiones :

```
# 102.54.94.97 rhino # PRE # DOM: networking # net group's DC
# 102.54.94.102 "appname \0x14" # special app server
# 102.54.94.123 popular # PRE # source server
# 102.54.94.117 localsrv # PRE # needed for the include
#
## BEGIN_ALTERNATE
## INCLUDE \\localsrv\public\LMHOSTS
## INCLUDE \\rhino\public\LMHOSTS
## END_ALTERNATE
```

En el ejemplo anterior, el servidor "*appname*" contiene un caracter especial en éste nombre, el servidor "*popular*" y el "*localsrv*" son precargados, y el servidor "*rhino*" es especificado para poderse utilizar con el # INCLUDE centralmente dando mantenimiento desde el archivo *LMHOSTS*, si el servidor "*localsrv*" no está disponible.

NOTA : cuando éste archivo es revisado se incluyen los comentarios sobre cada *lookup*, éste guarda así los comentarios a un mínimo para mejorar la ejecución.

Por consiguiente, no es aconsejable agregar entradas al archivo *LMHOSTS* en el extremo de éste mismo.

5.4.4 HOST NAME.

Los *host names* se utilizan en casi todos los ambientes *TCP/IP*. La siguiente lista proporciona una descripción de un *host name*:

- Un *host name* es un alias asignado a una computadora por un administrador para identificar un *TCP/IP host*. El *host name* no necesariamente tiene que coincidir con el nombre del *NetBIOS* de la computadora, y puede serle dado una longitud de 256 caracteres. Para un mismo *host* se pueden asignar múltiples *host name*.
- Un *host name* simplifica la forma de utilizar referencias de otros *TCP/IP hosts*. El *host name* es fácil de recordar como una dirección *IP*.
- Un *host name* puede ser usado en lugar de una dirección *IP* cuando se utilice *PING* u otra utilidad *TCP/IP*.
- Un *host name* siempre corresponde a una dirección *IP*, esta es almacenada en un archivo *HOST* o en una base de datos sobre un *DNS* o en un servidor de nombres *NetBIOS*. *Windows NT 3.5* también utiliza el archivo *LMHOSTS* para mapear *host names* a direcciones *IP*.
- La utilidad *HOSTNAME* debe desplegar el *host name* asignado al sistema. Por default, el *host name* es el nombre de la computadora en *Windows NT*.

Resolución del *Host name*.

La resolución del *host name* es el proceso de mapeo del *host name* para una dirección *IP*. Antes de que la dirección *IP* pueda ser resuelta por la dirección del *hardware*, el *host name* deberá ser resuelto por una dirección *IP*.

Microsoft TCP/IP puede utilizar cualquiera de los métodos conocidos para resolver *host names*. Los métodos de resolución para *Windows NT* de un *host name* pueden ser configurables.

Método Estándar de Resolución	Descripción
Local <i>host name</i>	La configuración del <i>host name</i> es por computadora. Este nombre es comparado con el <i>host name</i> destino.
Archivo <i>HOSTS</i>	Es un archivo de texto en el mismo formato que el archivo 4.3 <i>Berkeley Software Distribution (BSD) UNIX</i> etc\hosts file. Éste es el archivo de mapas de los <i>host names</i> para las direcciones <i>IP</i> . Es utilizado típicamente para resolver <i>host name</i> para las utilerías <i>TCP/IP</i> .
<i>Domain Name System (DNS) server</i>	Es un servidor que mantiene un base de datos de direcciones <i>IP</i> /nombres de computadoras (<i>host name</i>) mapeados.

Métodos <i>Microsoft</i> de Resolución	Descripción
<i>NetBIOS Name Server (NBNS)</i>	Es un servidor implementado bajo <i>RFC 1001/1002</i> que proporciona resolución de nombre del <i>NetBIOS</i> de la computadora. Esta implementación de <i>Microsoft</i> es <i>WINS</i> .
<i>Local broadcast</i>	Un <i>broadcast</i> sobre la red local para la dirección <i>IP</i> del nombre del <i>NetBIOS</i> destino.
Archivo <i>LMHOSTS</i>	Es un archivo de texto que contiene las direcciones <i>IP</i> de los nombres del <i>NetBIOS</i> de las computadoras que trabajan con <i>Windows</i> en redes remotas.

Resolviendo Nombres con un Archivo *HOSTS*.

A diferencia del archivo *LMHOSTS*, el cual es utilizado para *host* remotos solamente, el archivo *HOSTS* contiene mapas de *host names* tanto para *host* locales como remotos para sus direcciones *IP*. Éste proceso es como se describe a continuación en la Fig. 5.20:

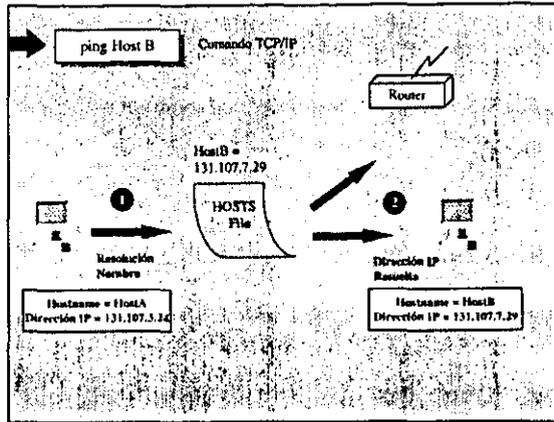


Fig. 5.20 Proceso de Resolución de Nombres con el archivo *HOSTS*.

1. La resolución del *Host name* comienza cuando un usuario teclea un comando utilizando el *host name* asignado para el *HOST* destino.

Windows NT verifica si el *host name* es el mismo nombre que el del *host* local. Si son diferentes, el archivo *HOSTS* es revisado. Si el nombre del *host* está en el archivo *HOSTS*, éste es resuelto a una dirección *IP*.

Si el *host name* no puede ser resuelto y ninguno de los otros métodos de resolución está configurado (tal como *DNS*, el servidor de nombres *NetBIOS* o el archivo *LMHOSTS*) el proceso se para y el usuario recibe un mensaje de error.

2. Después de que el *host name* es resuelto a una dirección *IP*, se intenta resolver la dirección *IP* del *host* destino para su dirección de *hardware*.

Si el *host* destino está en una red local, *ARP* obtiene su dirección de *hardware* consultando la dirección *IP* del *host* destino por el *ARP cache* o por *broadcasting*.

Si el *host* destino está en una red remota, *ARP* obtiene su dirección de *hardware* a través de un *router* y el requerimiento es dirigido hacia el *host* destino.

Resolviendo nombres con servidores *DNS*.

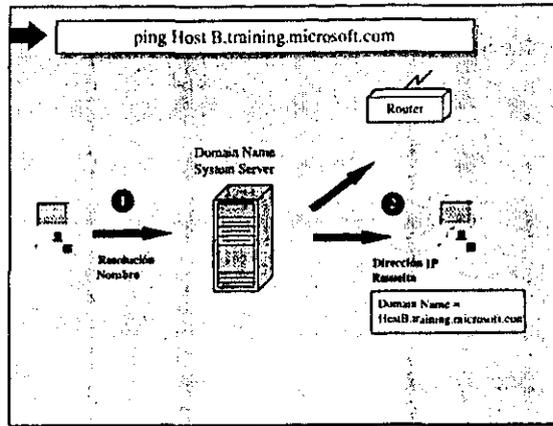


Fig. 5.21 Proceso de Resolución de Nombres con servidores *DNS*.

Un servidor *DNS* (Fig. 5.22) es una base de datos centralizada utilizada en ambientes *UNIX* para resolver *Fully Qualified Domain (FQDN)* y otros *host names* a direcciones *IP*. *Windows NT 4.0* puede utilizar servidores *DNS* para proporcionar éstos servicios. Resolver el nombre de un dominio utilizando un servidor *DNS* es muy similar a usar a un archivo *HOSTS*.

Si *Windows NT* es configurado para resolver *host names* con un servidor *DNS*, el proceso es como sigue :

1. Cuando un usuario teclea un comando usando un *FQDN* o un *host name*, el servidor *DNS* busca el nombre en su base de datos y lo resolverá para una dirección *IP*.

Si el *DNS* servidor no responde a éste requerimiento, intentara hacerlo en intervalos de 5,10,20,40,5,10, y 20 segundos. Si el servidor *DNS* no responde cualquier de los intentos, y no hay ningún otro método de la resolución configurado, tal como el servidor *NetBIOS* o el archivo *LMHOSTS*, el proceso se detiene y se reporta un error.

2. Después de que el *host name* ha sido resuelto, *ARP* obtiene la dirección de *hardware*. Si el *host* destino está en una red local, *ARP* obtiene las direcciones de *hardware* consultando la dirección *IP* por *ARP cache* o por *broadcasting*. Si el *host* destino está en una red remota, *ARP* obtiene la dirección de *hardware* a través de un *router* que entrega el requerimiento. Si el servidor *DNS* está en una red remota, *ARP* debe obtener la dirección de *hardware* por un *router* antes de que el nombre pueda ser resuelto.

Métodos de Microsoft para Resolver HOST Names.

Windows NT puede ser configurado para resolver *host names* (Fig. 5.22) utilizando un servidor de nombres *NetBIOS*, *broadcast*, y un archivo *LMHOSTS* en adición al archivo *HOSTS* y al servidor *DNS*. Si uno de éstos métodos falla, los otros métodos proporcionan un respaldo.

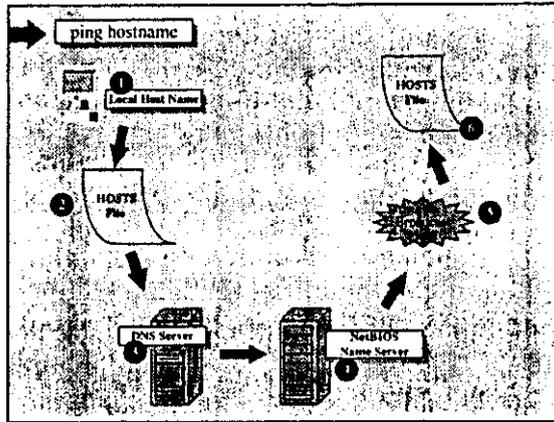


Fig. 5.22 Proceso de Microsoft para Resolver HOST Names.

Si *NBNS* y *LMHOSTS* son configurados, el orden de resolución es el siguiente :

1. Cuando un usuario teclea un comando haciendo referencia a un *host name*, *Windows NT* verifica si el *host name* es el mismo que el del *host name* local.
Si el *host name* y el *host name* local son los mismos, el nombre ha sido resuelto y el comando es ejecutado, sin generar actividad en la red.
2. Si el *host name* y el *host name* local no son los mismos el archivo *HOSTS* es revisado.
Si el *host name* es encontrado en el archivo *HOSTS*, éste es resuelto para una dirección *IP* y ocurre la resolución de dicha dirección. El archivo *HOSTS* debe residir en el sistema local.
3. Si el *host name* no puede ser resuelto utilizando el archivo *HOSTS*, el *host* fuente envía un requerimiento para configurar el *DNS* (*Domain Name Server*). Si el *host name* es encontrado por un servidor *DNS*, éste es resuelto para una dirección *IP* y la resolución de esta se realiza.

Si el servidor *DNS* no responde a dicha petición, adicionalmente se realizan varios intentos a intervalos de 5, 10,20,40,5,10 y 20 segundos.

4. Si el servidor *DNS* no puede resolver el *host name*, el *host* fuente revisa el nombre del *caché* del *NetBIOS* local antes de realizar tres intentos para contactar al servidor de nombres *NetBIOS* que esta configurado. Si el *host name* se encuentra en el *NetBIOS* nombre *caché* o en el servidor de nombres *NetBIOS*, éste es resuelto para una dirección *IP* y la resolución es terminada.
5. Si el *host name* no se resuelve por el servidor de nombres *NetBIOS* el *host* fuente genera tres mensajes de *broadcast* en la red local. Si el *host name* se encuentra en la red local, éste es resuelto para una dirección *IP* y la resolución se completa.
6. Si el *host name* no es resuelto usando los *broadcast* el archivo local *LMHOSTS* es revisado. Si el *host name* se encuentra en el archivo *LMHOSTS*, éste se resuelve para una dirección *IP* para completar la resolución.

Si ninguno de éstos métodos resuelve el *host name*, la única manera de comunicarse con otro *host* es especificando la dirección *IP*.

Archivo *HOSTS*.

El archivo *HOSTS* es un archivo estático utilizado para los mapas de *host names* para direcciones *IP*. Éste archivo es compatible con el archivo *HOSTS* UNIX. Las siguientes características describen al archivo *HOSTS* (Fig. 5.23):

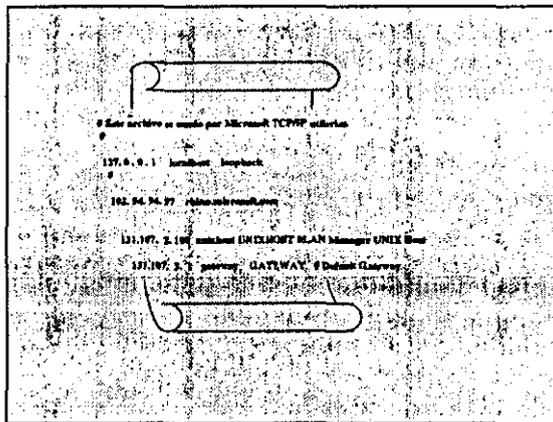


Fig. 5.23 Archivo *HOSTS*.

- Una sola entrada consiste de una dirección *IP* correspondiente a uno o más *host names*.
- El archivo *HOSTS* debe residir en cada computadora.

- Es utilizado por *PING* y otras utilerías de *TCP/IP* para resolver *host name* para una dirección *IP* sobre redes locales y remotas.
- Este archivo es revisado cuando un *host name* es referenciado. Los nombres son leídos en forma lineal. Los nombres más comúnmente utilizados deberán estar colocados al comienzo del archivo.
- También es utilizado para resolver nombres del *NetBIOS* (especificación -32- *TCP/IP*).
- Por default, el *host name local host* es un elemento en el archivo *HOSTS*.
- Este archivo se puede editar con cualquier editor de texto. Éste se localiza en un directorio con un nombre de la siguiente forma:

systemroot\SYSTEM32\DRIVERS\ETC

- Cada elemento *host* esta limitado a 255 caracteres.

5.5 Definición de Direcciones Estáticas en *WINS* para Conexión con Casa Matriz.

Como parte del proceso de conexión entre los diferentes *sites* y Casa Matriz es necesario definir en forma estática las direcciones y nombres de los servidores del *Hub* Principal con el que se conecta el nodo de México.

El proceso de definición de las direcciones se efectúa desde el servidor de *WINS* (Fig. 5.24) en el servidor primario *PDC* y se deberá contar ya con todas las especificaciones que serán dadas de alta en el servidor de *WINS*.

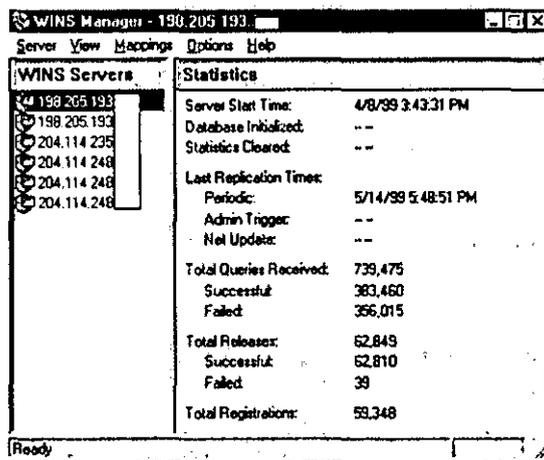


Fig. 5.24 Ventana de configuración de *WINS*.

Dentro del servidor de WINS se selecciona la opción de *Mapping* y dentro de esta se selecciona la opción de *Static Mappings*.

Se desplegará la ventana de entradas de direcciones estáticas (Fig. 5.25) se deberá seleccionar el botón de *Add Mapping* y teclear la información solicitada.

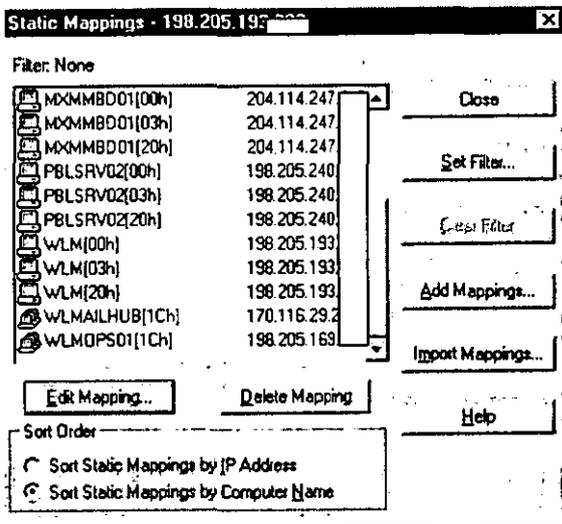


Fig. 5.25 Ventana de configuración de Direcciones Estáticas

La ventana de acceso a las direcciones (Fig. 5.26) estáticas requiere el nombre del servidor y la dirección IP.

Para cada dirección que se va capturando se deberá oprimir el botón de *Add*.

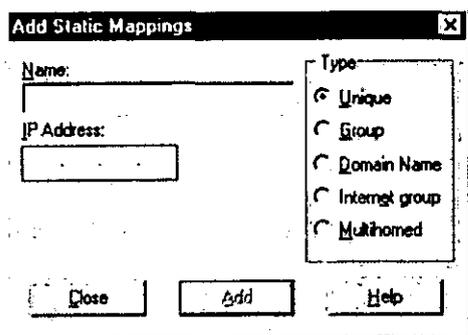


Fig. 5.26 Configuración de Direcciones Estáticas

5.6 Quotas.

La cuota se considera el espacio de disco asignado a cada *Mailbox* de usuario, la cantidad de espacio para almacenar toda la información recibida y enviada en el *Mailbox* del servidor, pueden ser mensajes, anexos, juntas, contactos o notas.

5.6.1 Definición de Quotas para usuarios en el servidor.

La definición de Quotas se puede establecer por dos medios, el primero genérico para todos los *Mailboxes* pertenecientes al *Site*, y el segundo en forma individual para cada *Mailbox*.

El primero se define por default para controlar el espacio a todos los *mailboxes* en forma global y el segundo se utilizará solo si algún usuario justifica la ampliación de su cuota.

El espacio definido es suficiente para almacenar un gran número de mensajes para la mayoría de los usuarios, pero se han detectado usuarios especiales, los cuáles reciben en forma constante mensajes con anexos grandes que les satura en forma rápida la cantidad de espacio asignado, por lo que solicitan una ampliación de sus cuotas de correo.

El sistema se limita a 20,000 Megas de espacio en el servidor para cada *Mailbox* de usuario, y esta condicionado a permitir la entrada de mensajes aun cuando la cuota permitida se rebase, pero ya no permite el envío de mensajes, por lo que el usuario automáticamente detecta que la cantidad de espacio asignada ha sido rebasada. La ventana siguiente (Fig. 5.27) ejemplifica la configuración del servidor en el primer caso, en que se limita el espacio en forma genérica para todos los *Mailboxes* de usuarios.

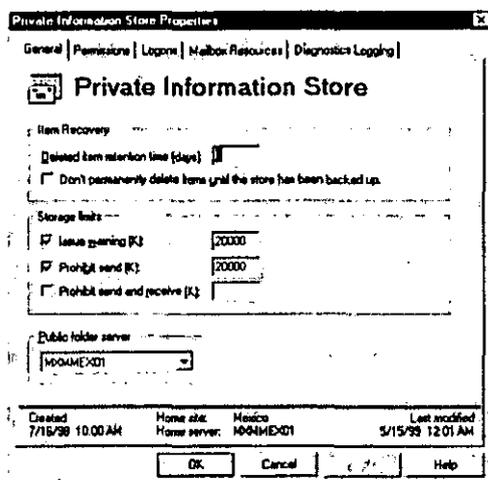


Fig. 5.27 Ventana de configuración del *Information Store*

La siguiente ventana (Fig. 5.28) ejemplifica la configuración de un *Mailbox* en forma independiente que ya ha rebasado la cuota asignada y que ha solicitado una ampliación de su cuota.

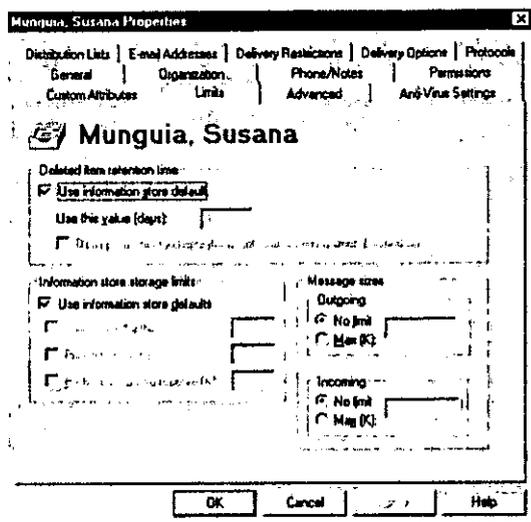


Fig. 5.28 Ventana de configuración de un *Mailbox*

De igual forma cuando un usuario ha saturado su cuota el administrador de *Exchange* en forma automática inicia un proceso de envío de mensajes a la cuenta de usuario saturada indicándole cual es la cantidad de espacio permitido y por cuanto ha rebasado su cuota, así como solicitando la depuración de su correo.

5.6.2 Ventajas y Desventajas.

El proceso de definición de las Quotas es dependiente de cada localidad, cada administrador de un *Site* deberá asignar el tamaño que considere necesario en su afiliada, considerando esencialmente el espacio en disco duro del servidor, ya que cuando más cuota se asigna al usuario, mayor es la cantidad de espacio que se utiliza en el servidor.

Una de las ventajas de contar con la asignación de cuotas es controlar el espacio a cada usuario de la información que puede tener almacenada en el servidor, forzándolo a su vez a bajar su información a su disco duro y evitar saturar el servidor.

En caso de no contar con espacio suficiente de disco en el servidor, se pueden limitar las cuotas a un tamaño menor y evitar así la compra de mas discos.

La asignación de una cuota, permite que los planes de crecimiento o compra discos se calcule de acuerdo al espacio que se asignará a los usuarios y así evitar un gasto innecesario.

Una desventaja es recibir demasiados mensajes con anexos y estar recibiendo constantemente la notificación del administrador para efectuar la depuración.

5.7 Selección de conectores para enlaces WAN.

Después de que se han definido los límites del site, se debe decidir que conector usar para unir a estos. Las opciones principales son:

- *Site conector (RPC)*
- *Conector X.400*
- *Conector Dinámico RAS*
- *Internet Mail Service*

Algunos casos indican un tipo de conector bastante obvio. Por ejemplo, si una compañía ya paga por una conexión pública X.400 a un proveedor, el conector X.400 es una opción obvia para la red Exchange. Otros casos requieren de una decisión con mucho más análisis. Por ejemplo, si la empresa tiene disponible sólo un par de módems y líneas telefónicas normales, se puede obtener la conectividad requerida de tres maneras:

- Para una transmisión punto-a-punto, usar el Conector Dinámico RAS.
- Utilizando una conexión dial-up para Internet, usar el *Internet Mail Service*.
- Usando *Windows NT* con tecnología de asignación de ruta la cual proporciona una conectividad de acuerdo a la demanda, si usa el conector X.400

Quizás un gran dilema es cuando una WAN usa líneas arrendadas o conexión dial-por demanda de *Intregated Services Digital Network (ISDN)*. Se podría usar el *Site Conector*, el *Conector X.400* o *Internet Mail Service* para unir los sitios al mismo tiempo.

Se recomienda usar el *Site Conector* la mayor de las veces que sea posible por que es el más rápido y proporciona la mayor flexibilidad. Cuando se utiliza, la red debe soportar *RPC* sincrónos y la autenticación de *Windows NT*. Aunque se puede configurar un *Site Conector* en el modelo de *Windows NT* donde no existen relaciones de dominio, se tiene que implementar temporalmente el llevar a cabo la autenticación el tiempo que dura la instalación del *Site Conector*. Esta instalación envuelve el confiar y asignar los permisos Exchange para los servicios de cuentas del site local en el site adyacente. Después de que el conector esta colocado, se puede eliminar la relación de confianza.

La regla del dedo pulgar dice que se debe usar el *Site Conector* cuando el ancho de banda es bueno, el Conector *X.400* cuando se limita el ancho de banda, y el *Internet Mail Service* cuando se unen *sites* sobre *Internet*. Muchas personas se ven demasiado precavidas cuando estiman el ancho de banda del cual se dispone, ya que usan el conector "más seguro" (*X.400*). Éste usa menos ancho de banda que otros conectores, pero introduce flexibilidad y emisiones de seguridad. También se debe considerar la cantidad de latencia de la red. Por ejemplo, los satélites se unen, como se sabe, por latencia alta, esto puede causar errores que aparecen en el *Event Log*, aunque la red tenga el suficiente ancho de banda .

Las tablas siguientes muestran como se ven los datos en la red cuando se transmite un mensaje entre dos sitios usando cada uno de los conectores disponibles.

Un simple mensaje de texto - tráfico incluyendo binding y la autenticación de MTAs

Concetor	Tráfico enviado (bytes)	Tráfico recibido (bytes)	Total frames	Comentarios
<i>Site (RPC)</i>	7,484	3,889	60	Conexión segura. Sesión Completa Cifrada
<i>X.400</i>	4,087	751	19	Título de mensaje y parte del nombre en texto claro
<i>Internet Mail</i>	6,962	1,376	30	Usa NTLM Service autenticación y cifrado

Un simple mensaje de texto - MTAs terminado

Concetor	Tráfico enviado (bytes)	Tráfico recibido (bytes)	Total frames	Comentarios
<i>Site (RPC)</i>	4,744	1,434	24	Conexión segura. Sesión completa cifrada
<i>X.400</i>	3,653	319	13	Título de mensaje y parte del nombre en texto claro
<i>Internet Mail</i>	6,962	1,376	30	Usa NTLM Service autenticación y cifrado

Un mensaje con un attachment de 304 KB - MTAs terminado

Conector	Tráfico enviado (bytes)	Tráfico recibido (recibido)	Total frames	Comentarios
<i>Site (RPC)</i>	342,302	19,629	471	Conexión segura. Sesión completa cifrada
<i>X.400</i>	332,366	12,279	454	Título de mensaje y parte del nombre en texto claro
<i>Internet Mail</i>	453,164	13,258	523	Usa NTLM Service autenticación y cifrado

Como se puede ver en las tablas, el Conector *X.400* es más eficaz en la red. Sin embargo, no proporciona el nivel de seguridad que los otros conectores ofrecen. También podemos ver que también no hay mucho sobre la cabeza en el *Site Conector* como el tamaño de los mensajes incrementados. Todo *RPC* demandado para el *Exchange MTA* se fabrica en serie. Si un *MTA* no responde rápidamente, puede ocurrir un *thread blocking*, previniendo al *MTA* local de comunicarse con otros servidores, igual con enlaces rápidos. Se requiere de un análisis cuidadoso para asegurar que el desempeño del servidor *Exchange* no sea degradado por enlaces de la red lentos. En general, los diseñadores de sistemas de mensajería, se inclinan por el *Site Conector* por su capacidades de flexibilidad.

A continuación se listarán los nombres de las regiones en la región *Exchange* y la ubicación del servidor, el tipo de conector *Site* que se usa y con quien se establecerá la conexión del Sitio.

Los datos registrados en la siguiente tabla se han determinado de acuerdo a la topología de la red y el ancho de banda de cada filial.

Asia/Australia	Nombre del Site	Tipo de conector	Región conectada
	Australia	X400	WLBB
	India	X400	WLBB
	Japón	X400	WLBB
	Región China	X400	WLBB
	Filipinas	X400	WLBB
	Tailandia	X400	WLBB
Europa			
	Sur Africa	X400	Región UK
	Región Benelux	RPC	Región UK
	Capsugel Europa	X400	Región UK
	Región Francia	X400	Región UK
	Región Alemania	RPC/X400	Región UK/WLBB
	Región España	X400	Región UK
	Región UK	RPC/X400	Región Alemania/WLBB
	Irlanda	X400	Región UK
Latino/Sur América			
	República Dominicana	X400	WLBB
	Guatemala	X400	WLBB
	Carolina	X400	WLBB
	Colombia	X400	WLBB
	Perú	X400	WLBB
	Venezuela	X400	WLBB
	Argentina	X400	WLBB
	Brasil	X400	WLBB
	México	RPC	WLBB
Norte América			
	WLBB	X400/X400	Región UK/Región Alemania
	AA	RPC	WLBB
	PDMOPS	RPC	WLBB
	MOPS	RPC	WLBB
	ML	RPC	WLBB
	Rockford	RPC	WLBB
	Greenwood	RPC	WLBB
	Lititz	RPC	WLBB
	Toronto	X400	WLBB
	Holanda	RPC	WLBB
	Rochester	RPC	WLBB
	Vega Baja	RPC	WLBB
	Elk Grove	RPC	WLBB
	Virginia	X400	WLBB

5.8 Replicación con el resto del mundo.

Como parte de la replicación se encuentran dos procesos que pueden efectuarse en un *Site*, una replicación dentro del mismo *Site* y una replicación con otros *sites*.

La replicación dentro del mismo *Site* se efectúa en forma constante cada 5 minutos entre servidores que pertenecen al mismo *Site*, por ejemplo si se define el servidor de *Exchange* de México y se anexa un servidor en la ciudad de Puebla que se conecta al mismo *Site* se efectúa un proceso de *Join* entre ambos servidores al mismo *Site*, el proceso de replicación entre éstos servidores no requiere de una configuración adicional ya que se efectúa en forma automática cada 5 minutos.

La replicación entre diferentes *Sites* se efectúa de la siguiente manera:

El proceso de replicación de directorios trabaja sobre la conectividad proporcionada por el servicio *Message Transfer Agent (MTA)*, éste servicio se encarga de monitorear y dirigir aquellos mensajes que no pertenezcan al *site*, de igual forma se encargará de dirigir la información necesaria fuera del *site* y de extraer de otros *sites* la información que falte por configurar en su *site* local.

El proceso de replicación debe considerar una relación de confianza con el servidor *Bridgehead server* principal, para mantener actualizada la información del servidor local.

El servidor local envía un requerimiento de actualización al servidor remoto y éste envía la información de los cambios que se hayan generado, de igual forma cuando un *site* efectúa cambios, envía la información al *Bridgehead* principal y éste se encarga de enviar las actualizaciones a los otros *sites* y a otros *Bridgehead* con los que se encuentre conectados.

En forma inicial cuando la replicación no ha sido configurada, únicamente se despliegan los *folders*, la *Global Address List*, el *Address Book* y el *site* local, pero una vez que se ha configurado un conector de replicación se inicia el proceso de replicación entre los diferentes *Sites* por medio de los servidores *Bridgehead* y se empieza a desplegar toda la información referente a otros *Sites* como se muestra en la Fig. 5.29.

Este proceso de replicación es variable y depende del número de *Sites* configurados o *folders* existentes.

CAPÍTULO 6

INSTALACION DE SERVIDORES FORANEOS

6.1 Creación de un *Site*.

Organización y Nombre de *Site*.

La organización y el nombre del *site* son utilizados para generar la dirección de *e-mail* y la base de datos de directorios, que es donde se encuentran definidos todos los nombres de *site* pertenecientes a una misma organización. El nombre de la organización y el nombre del *site* deben ser únicos y no mayores a 64 caracteres.

La organización y el nombre del *site* deben estar incluidos en la base de datos de directorios e identificar a todos los objetos de un *site*, como son :

- *Mailboxes*
- *Public folders*
- Listas de distribución

Estos directorios no pueden ser modificados después de ser creados.

Nombre del Directorio para Instalación.

El nombre del directorio default es *C:\Exchsrv*, pero puede ser modificado.

Service Account

La cuenta de servicio llamada *Service Account*, es la cuenta con la que será instalado el producto de *Exchange* y deberá tener todos los permisos y privilegios especificados para poder levantar todos los servicios de *Exchange*, esta cuenta se define antes de iniciar la instalación del producto.

CD Key.

Durante la instalación, aparecerá una caja de diálogo la cual pedirá la *CD Key* o el *PID*. La *CD Key* es un número único de 11 dígitos, la cual se encuentra especificada en el disco compacto. Cada paquete de productos contiene una *CD Key* o un número de serie, el cual es necesario para instalar todo *software*.

Adicionando un Servidor a un Site.

Otro contexto organizacional de instalación es adicionar un servidor *Exchange* a un *site* existente.

Requerimientos de Seguridad *Windows NT*.

Para adicionar un servidor de *Exchange* a un *site* existente, se debe contemplar lo siguiente:

- Especificar el nombre del servidor *Microsoft Exchange* en el *site*. El programa *Setup* intentará contactar al servidor existente por medio de un *RPC* y, cuando lo encuentra, deberá buscar en el directorio la organización y el *site* que se accederá.
- Conocer la *password* de la cuenta de servicio con la que fue instalado el primer servidor, ya que esta es necesaria para realizar la unión entre los dos servidores.
- Tener disponible el papel de *Permissions Admin* para los tres niveles: Organización, *site* y configuración.
- Tener un administrador de *Windows NT* sobre el servidor *Microsoft Exchange* en el *site*.

Razones para adicionar un nuevo servidor a un *site* existente :

A continuación se listan algunas razones para adicionar servidores:

- Crear un servidor dedicado : Un servidor dedicado puede ser un servidor *Public Folder*, un servidor de correo privado o un servidor de comunicación utilizando el servicio de correo de *Internet* o el conector *X.400*.
- Crecimiento : Una ventaja de *Microsoft Exchange* es su habilidad de crecer con la organización.

Ventajas para definir más de un Servidor en un *Site* :

- Tener servidores dedicados asignados a diferentes funciones. Permite que la carga de funciones de un servidor sea distribuida en diferentes servidores, dando todos éstos el servicio a todas las cuentas de correo existentes en el *site* con un mejor tiempo de respuesta y conexión.
- Mantener una sola base de datos de información y permitir que otras zonas foráneas se enlacen de manera rápida a los servicios de correo más cercanos a su región.
- El tiempo de acceso de la información de correo y del envío de mensajes en forma local se incrementaría, ya que no habría dependencia de medios de comunicación para resolver el mensaje.
- La carga de un servidor estaría distribuida.

- Disminución de riesgos de perder todo el correo, ya que aunque un servidor que pertenezca al *site* sea dado de baja, los otros servidores del *site* continúan dando servicio a las cuentas que pertenezcan a ese servidor.

Desventajas al definir más de un Servidor en un *Site* :

- Costo de adquisición de otros servidores.
- Costo de administración en servidores foráneos.
- Conexión *RPC* entre servidores del mismo *site*, por lo que se requiere un buen nivel de conexión *WAN*.

Como parte de una implementación a nivel mundial, se debe definir que ciudades deben quedar configuradas con un *site* en su región y cuáles ciudades tomarían los servicios de correo de los *sites* definidos, en algunas ciudades como México se considero que se definiría un servidor principal y uno foráneo para cualquier otra ciudad importante de la afiliada y que formará parte del mismo *site*, en éste caso se seleccionó la ciudad de Puebla que se enlazará al servidor de México en el mismo *site*.

6.2 Definición de Conexiones entre *Sites*.

Comunicación de Servidores *Multisite*.

Los servidores *Microsoft Exchange* son altamente adaptables y confiables por diversos procesos. Un proceso importante es la comunicación entre servidores en *sites* separados. Cuando dos *sites* son conectados y la información es transferida entre ellos, a esta acción se le denomina comunicación de servidores *intersite*. Como las organizaciones crecen, es importante que la información sea actualizada entre los *sites* sobre una base continua. Dichos *sites* son geográficamente remotos.

Esto ofrece la ventaja de que cada oficina remota puede ser iniciada como un *site* servidor *Exchange* individual para hacer más eficiente el uso del ancho de banda de red entre los *sites* o los modelos administrativos.

Cuando dos *sites* son conectados para transferencia de información, se da el nombre de comunicación *intersite*.

En un ambiente *multisite*, los servidores se comportan de la misma forma que en un ambiente con un sólo *site* cuando hacen la transferencia de información relacionada con la organización.

La principal diferencia de un ambiente *multisite* radica en que el *MTA* es el responsable de toda la transferencia de datos (Fig. 6.1) de cualquier tipo. La información de directorio es encapsulada en un mensaje de *e-mail* y esta es direccionada por el *MTA* a los servidores en los diferentes *sites*. Esto difiere de un *site* simple o del ambiente *intrasite*, donde un *Directory Service* pasa la información de directorio directamente al *Directory Service* del otro servidor en el mismo *site*. Los servidores *Exchange* envían sólo una copia de un mensaje entre dos servidores o *sites*. Esto hace más eficiente el uso del enlace por ancho de banda por la mínima transferencia de datos entre los dos *sites*.

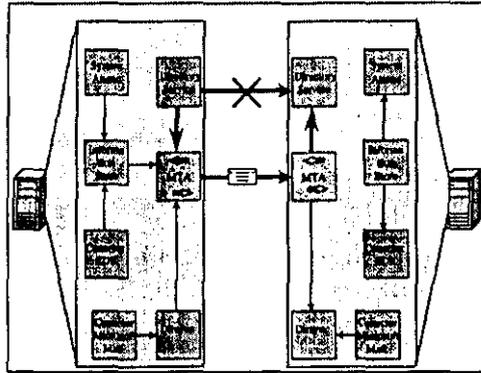


Fig. 6.1 Entre 2 *sites* no existe comunicación entre *Directory Services*, la única forma de comunicación entre *sites* es a través de *MTA*.

Hay dos tipos de conectores utilizados para transmitir información entre *sites* de servidores *Exchange* y éstos son los conectores de mensajería y el conector de Replicación de Directorio.

Conectores de Mensajería.

Los servidores *Exchange* utilizan conectores de mensajería para conectar dos *sites* con el propósito de transferir mensajes. Típicamente, los siguientes conectores son utilizados para estabilizar la conectividad de mensajería entre *sites* :

- *Site Conector.*
- Conector *X.400.*
- Conector Dinámico *RAS.*
- *Internet Mail Service.*

Conector de Replicación de Directorio.

En suma, para transportar mensajes entre *sites*, los servidores *Exchange* pueden intercambiar información de directorios. Dicha información es manejada utilizando un conector de Replicación de Directorio. El conector de Replicación de Directorio utiliza cualquier conector de mensajería disponible para transmitir la información de directorio entre servidores.

No se puede instalar un conector de Replicación de Directorio si no existe un conector de mensajería instalado.

Estrategia del Corporativo.

Como parte de la implementación y transferencia de información *Intersites*, es importante considerar que se definieron tres *hubs* principales que se encargarán de la transferencia de información entre las diferentes regiones, al mismo tiempo que administrarán la comunicación entre *sites* de la misma región.

Los tres *hubs* principales realizarán el proceso de transferencia de información entre diferentes regiones, apoyados en el proceso *MTA* de cada *site*.

La definición de los tres *hubs*, permite particionar la carga en un sólo servidor central, el cual podría ser un cuello de botella para todos los *sites*, si todos los requerimientos van hacia ese servidor, adicionalmente se genera una estructura redundante que permita mantener el servicio activo con mayor seguridad, ya que si algún *hub* principal tuviera problemas de comunicación, el envío de mensajes entre los otros dos *hubs* no se ve afectado.

6.3 Definición de servidores Foráneos en un mismo Site

Comunicación de Servidores *Intrasite*

Un diferente tipo de información puede ser intercambiada y transferida en una organización para su correcto funcionamiento. Cuando los servidores intercambian o transfieren información y éstos pertenecen al mismo *site*, recibe el nombre de comunicación de servidores *Intrasite* (Fig. 6.2).

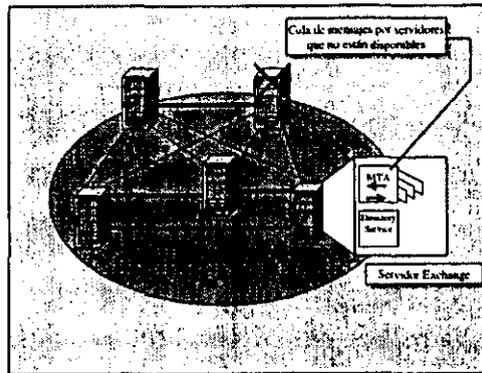


Fig.6.2 No existe direccionamiento de mensajes entre servidores del mismo *site*. La ejecución de la ruta solo se efectúa fuera del *site*.

Servidores Comunicados en un *Site* Utilizando *RPC's*.

Dentro de cada servidor en una configuración *Intrasite* (dos o más servidores conectados al mismo *site*) la información es transferida directamente desde cada servidor a todos los demás, utilizando *RPC*. La comunicación *RPC* entre servidores *Exchange* requiere una conexión permanente y de alta velocidad sobre el tráfico de red que es generado. En un *site* de servidores *Exchange*, todos los servidores utilizan *RPC's* para distribuir los datos al correspondiente servidor que los recibe en el *site*.

Servidores *Originating* que Almacenan Mensajes no Entregados.

Si un servidor destino se encuentra deshabilitado, el servidor *originating* almacena la información hasta que el servidor destino es nuevamente habilitado. Si la información es un mensaje de *e-mail* y el servidor destino no está habilitado con un *administrator-configured amount of time*; el servidor *originating* regresa el mensaje al usuario.

Transfiriendo Información.

Los dos componentes que manejan la transferencia de información en una organización son el *Directory Service* y el *MTA*. Los datos pueden ser desde un mensaje individual hasta actualizaciones de directorios o información de carpetas públicas. La siguiente tabla lista los tipos de datos que pueden ser transferidos y el servicio responsable para dicha transferencia.

Tipo de dato	Servicio Responsable
Replicar cambios en directorios	<i>Directory Service</i>
Replicar cambios a folders	<i>Public Information Store</i>
Cambios de jerarquía a folders públicos	<i>Public Information Store</i>
Mensajes de mail	<i>Private Information Store</i>
Mensajes "Link Monitor"	<i>System Attendant</i> (utilizando almacenamiento de información)
Directorio de sincronización de mensajes	<i>Directory Synchronization</i>

RPC's y WAN's Intrasite

Cuando se diseña un *site* con servidores *Exchange*, se debe considerar el impacto del tráfico de red. En la Fig. 6.3 se ilustra una red corporativa compuesta por dos *LAN*'s separadas, unidas por una conexión *WAN* simple. Cuando son configuradas para operar como un *site* simple, cada servidor abre una conexión *RPC* directamente a todos los servidores. Esta facilidad ofrece excelentes resultados en un ambiente de tráfico pesado de red entre servidores. Éste tráfico puede causar severos problemas a la red sobrecargando la unión *WAN*.

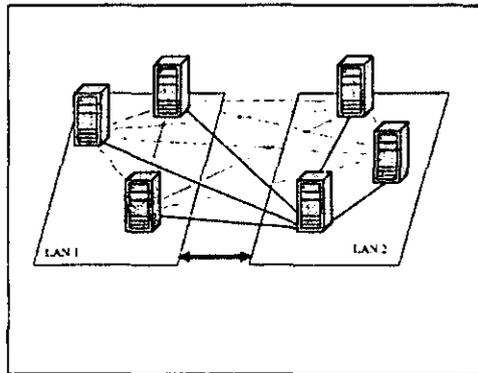


Fig.6.3 Cada servidor levanta una sesión directa en cada servidor del otro lado de la WAN.

Una solución a éste problema es la creación de múltiples *sites* y utilizar conectores para estabilizar la comunicación entre ellos.

MTA

EL *MTA* es un componente primario responsable de la transferencia de información entre servidores y *sites*. Algunos otros componentes del servidor *Exchange* también utilizan el servicio del *MTA* para enviar información. La completa comprensión de los conceptos que se ligan con el *MTA* es esencial para entender como trabaja un servidor *Exchange* en un sólo *site* y en un ambiente de multiservidores.

Proceso *MTA*.

Cuando los datos son transferidos entre dos *MTA*'s (Fig. 6.4) éstos deben tener siempre la forma de mensaje. Cualquier dato que no está en formato de mensajes de *Exchange* se convierte y se direccionan al destino apropiado. El *MTA* utiliza la información almacenada en el *Directory Service* para determinar el *MTA* destino.

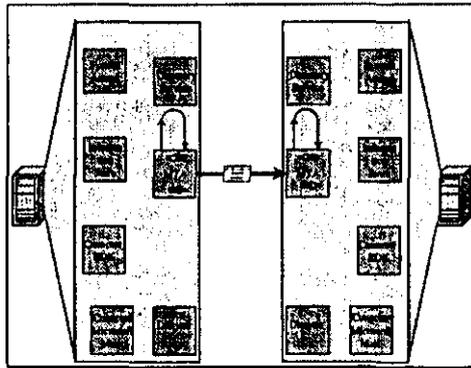


Fig. 6.4 Proceso *MTA*.

Los siguientes pasos determinan el procedimiento utilizado para actualizaciones :

1. El *MTA* busca el servidor destinatario desde el *Directory Service*.
2. El *MTA* verifica si debe dirigir el mensaje fuera del sitio.
3. Una sesión *RPC* es abierta para el *MTA* destino utilizando el *Site Service* el cual cuenta con un contexto de seguridad. Esto es llamado una *asociación*.
4. El mensaje es enviado al servidor destino utilizando la conexión *RPC* abierta.
5. En la transmisión exitosa del mensaje, el *MTA* receptor busca al destinatario de su local *Directory Service* y entonces verifica si el mensaje necesita pasarse a otro servidor. En el contexto del *site* simple el *MTA* receptor es siempre el destino final.
6. El *MTA* coloca el mensaje en una cola y notifica al *Information Store* que el mensaje se entrego.
7. El *Information Store* recupera el mensaje del *MTA* y le notifica a los destinatarios.

Asociaciones *MTA*.

Si el *MTA* realiza un intento de envío de mensaje para más de un usuario sobre múltiples servidores, éste crea de primera instancia un mensaje simple para cada servidor destino y entonces procede a transferir el mensaje a cada *MTA* remoto. El *MTA* envía una copia a cada servidor utilizando el ancho de banda de la red para mayor eficiencia (Fig. 6.5).

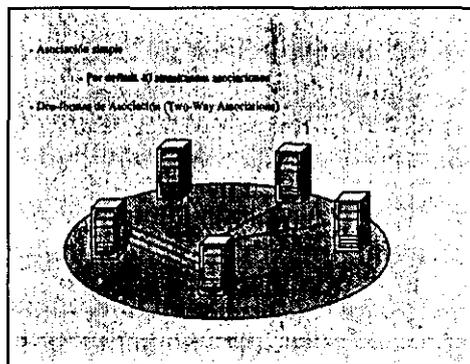


Fig. 6.5 Asociaciones *MTA*.

Asociaciones Simples.

Típicamente, esto se define como una conexión simple a un servidor destino, sin embargo, si se llegara a dar un súbito incremento de mensajes de correo, un *MTA* puede abrir múltiples asociaciones para el mismo servidor. Esta propiedad permite al servidor reducir algunos mensajes de *Backlog*. El *MTA* soporta de 20 a 240 *MTA*'s simultáneamente. Durante esta optimización, el *Performance Wizard* determina un ajuste correcto.

Asociaciones *Two-Way*.

Cuando una asociación ha sido creada, todos los mensajes son entregados a, y recibidos desde, el *MTA* remoto. Entregar y recibir mensajes al mismo tiempo se nombra como una asociación *Two-Way*. Cuando el mensaje a transferir es completado, el *MTA* espera 300 segundos, por *default*, antes de desconectar la asociación. Esta pausa permite el tiempo necesario para que el *site* remoto envíe una señal al *MTA* local, si éste necesitara mantener la asociación abierta (Fig. 6.6).

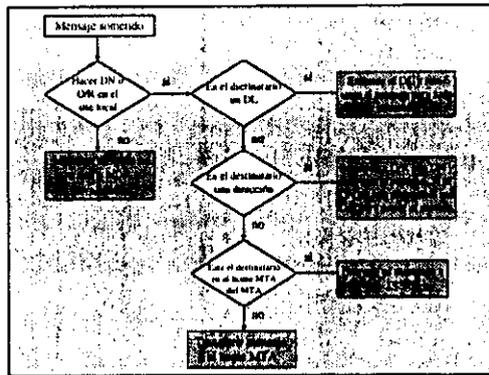


Fig. 6.6 *MTA* y Asignación de la ruta.

Servicio de Comunicaciones *Intrasite*.

Los servicios de servidores *Exchange*, con excepción del *Directory Service*, transfieren información a través de mensajes de *e-mail*. Si éste servicio no es capaz de crear el mensaje, cuenta con el *Information Store* para crear el mensaje. En éste caso, típicamente el servicio tiene su propio buzón oculto dentro del *Information Store* (Fig. 6.7).

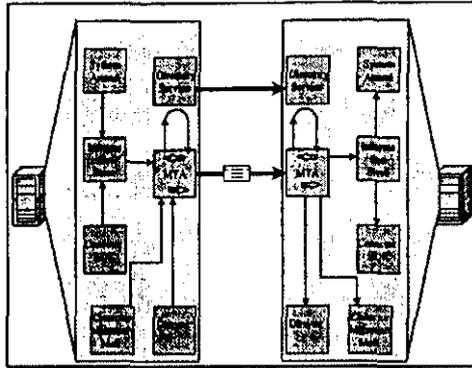


Fig. 6.7 Servicio de comunicación *Intrasite*.

Estos servicios no pueden entregar mensajes sin su propia infraestructura de mensajería proporcionada por el *MTA* para enviar información. Los siguientes tipos de servicios son utilizados por el *MTA* para ejecutar éstas funciones :

- *Information Store*.
- *System Attendant*.
- *Connectors*.
- *Microsoft Mail for PC and Apple Talk Networks Directory Synchronization*.

Proceso del *Directory Service*.

Dentro de un *site*, cada *Directory Service* (Fig. 6.8) mantiene una copia completa de la base de datos de directorios, teniendo la información almacenada en un área central. Éste modelo es nombrado modelo *Multi-Maste*, el cual reduce el tráfico de la red asegurando que cada servidor tenga el mismo directorio. Esto proporciona una tolerancia a las fallas que permite a los servidores de un *site* estar fuera de línea sin afectar la información del directorio en otros servidores.

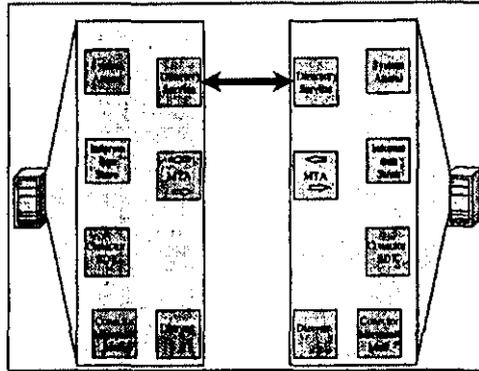


Fig. 6.8 Proceso del *Directory Service*.

Cambios de Comunicación entre *Directory Service*.

Cuando son realizadas modificaciones a los objetos del directorio, como a un correo o *DL*, o a algún servidor dentro de un *site*, el *Directory Service* envía éstos cambios a todos los demás *Directory Service* en el *site*, esto permite que los cambios puedan ser aplicados y guardados en todos los directorios consistentemente.

A continuación se presenta una cronología de los pasos (Fig. 6.9):

1. Después de que los cambios son realizados al directorio, éstos son replicados con una demora de 300 segundos, por *default*, éste proceso recibe el nombre de *Replication Latency*. Éste proceso permite al sistema replicar los cambios en procesos *batches* al mismo tiempo.
2. El *Directory Service* local mantiene una lista de todos los servidores en el *site* que recibirán las modificaciones. Una vez terminado el período del *Replication Latency*, el *Directory Service* envía una notificación a cada servidor, esta pausa de notificación se traslada de servidor en servidor. Esto permite la notificación al servidor para aplicar los cambios. Por *default*, esta pausa es de 30 segundos.
3. El servidor remoto recibe esta notificación de revisión sobre la actualización del *USN*, en éste se determina el último momento de recepción de una actualización. El *USN* es utilizado para determinar que modificaciones necesitan ser replicadas.
4. El *Directory Service* remoto requiere todas las modificaciones realizadas por el *Directory Service* local donde fueron ejecutados los cambios al directorio.
5. El *Directory Service* local, donde fueron realizados los cambios, se conecta al *Directory Service* remoto utilizando *RPC's* y es entonces cuando transfiere la información de las modificaciones en el directorio.
6. El servidor remoto actualiza el directorio local.

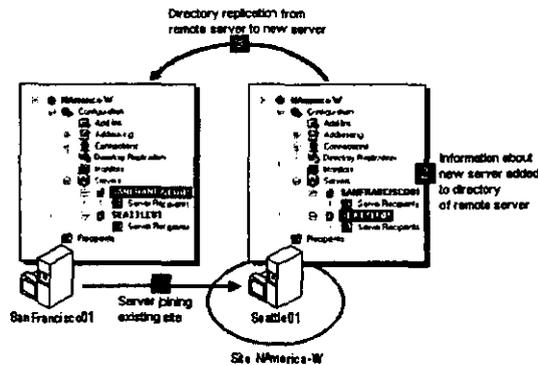


Fig. 6.9 Proceso del *Directory Service*.

Information Store.

La comunicación de mensajes entre servidores dentro de un *site*, es enviada desde el *Information Store* (Fig. 6.10) directamente al *MTA*. El *MTA* es el encargado de dirigir el mensaje al servidor apropiado.

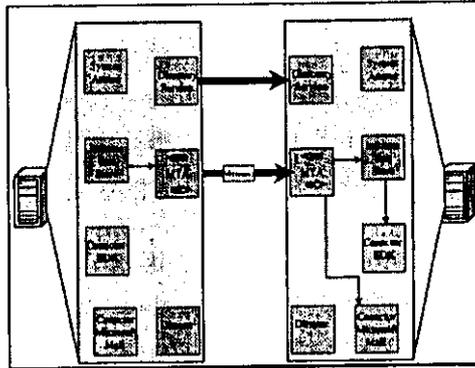


Fig. 6.10 *Information Store.*

Information Store Privado.

El *Information Store* privado mantiene el envío y recepción de mensajes de los usuarios. Cuando un mensaje es enviado a un usuario residente en un correo de diferente servidor, el *MTA* determina el servidor destino y coloca el mensaje en una cola de salida para dicho servidor.

El *MTA* intenta entregar los mensajes en espera desde el *Information Store*, y entonces se conecta al *MTA* del servidor destino utilizando una conexión *RPC*. El *MTA* de origen mantiene esta conexión abierta durante 300 segundos. Si no se realizan transmisiones subsiguientes, el *MTA* cierra la conexión.

Information Store Público.

El *Information Store* público mantiene la información al corriente en carpetas públicas. A continuación se mencionan dos clases de información manejada por el *Information Store* público :

- *Public Folder Hierarchy* .- El *Public Folder Hierarchy* es una lista de carpetas públicas. Esto se da porque todos los servidores dentro de un *site* no deben contener todas las carpetas públicas en su *Information Store*, la jerarquía debe ser habilitada por el cliente para poder ser desplegada. La replicación del *Public Folder Hierarchy* es en forma automática y obligatoria.
- Réplicas del *Public Folder* .- Si una carpeta pública es replicada a más de un servidor en el *site*, los contenidos también son replicados.

Cuando es necesaria una actualización, ya sea por jerarquía o por réplica, el *Information Store* notifica al *MTA* de la actualización. Al mismo tiempo, el *MTA* ejecuta la actualización y envía esta al servidor remoto.

System Attend.

El *System Attendant* (Fig. 6.11) es responsable de varias funciones en una organización. Con respecto a la comunicación dentro del *site*, una responsabilidad del *System Attendant* es proporcionar la funcionalidad de *Link Monitors* en el servidor *Exchange*. El *Link Monitors* prueba el *path* de mensajería entre dos servidores o desde un servidor *Exchange* a otro sistema de mensajería, siempre probando la unión.

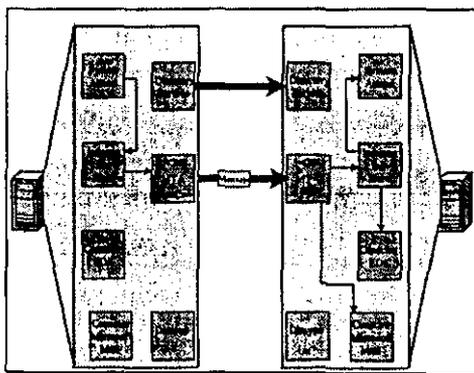


Fig. 6.11 *System Attend.*

El *System Attendant* genera un mensaje *e-mail* direccionado al correo del *System Attendant* en el lado remoto de la unión. Si el receptor es otro *System Attendant*, el mensaje es replicado. Si el receptor reside en un sistema de mensajería externo, un agente automáticamente puede ser configurado para replicar el mensaje, o si la dirección no es válida, un *NDR* es generado.

Conectores.

Los conectores (Fig. 6.12) transfieren información entre *sites*, servidores y otros sistemas de mensajería.

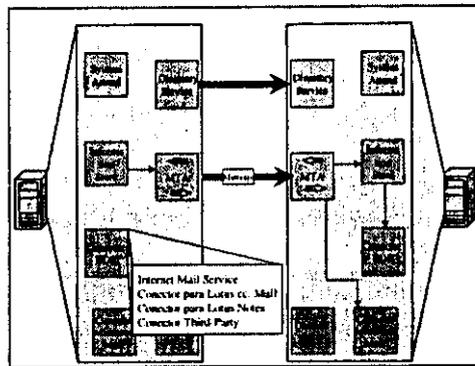


Fig. 6.12 Conectores.

Si éstos conectores son instalados en servidores múltiples, los mensajes deben ser transferidos entre el origen y el conector. Esto incluye transferencia de mensajes desde un usuario en el servidor *Exchange* u otro conector. Esta transferencia de mensajes es posible entre dos diferentes sistemas de mensajería a través de un servidor *Exchange*. El *MTA* puede transferir un mensaje destinado a un conector remoto basándose en la información de direcciones contenida dentro del mensaje.

Conectores *Microsoft Exchange Server Development Kit (EDK-based)*.

Los conectores *EDK-based* utilizan el *Information Store* para enviar mensajes en la misma forma que el *System Attendant* utiliza el *Information Store*. Cuando un mensaje sale a través de un conector *EDK-based* necesita ser enviado, y será enviado al *Information Store*.

El *Information Store* determina si el mensaje es local y lo procesa, pero si identifica que el mensaje es enviado a un usuario de un servidor remoto, transfiere el mensaje al *MTA*.

El usuario remoto puede ser un usuario en un servidor *Exchange* o un receptor con acceso a través de otro conector. A esta acción se le conoce como *backboning*.

El conector *EDK-based*, incluye lo siguiente :

- Servicio de correo *Internet*.
- Conector para *Lotus cc:Mail*.
- Conector *Lotus Notes*.
- Conectores *Third-Party*.

Conector de Correo *Microsoft*.

El conector de correo *Microsoft* envía mensajes directamente al *MTA* para transferirlo. Si el mensaje es destinado a un usuario en el mismo servidor, el *MTA* envía el mensaje al *Information Store* para mandarlo. Si el mensaje se intenta enviar a un usuario de un servidor remoto, el mensaje es transmitido directamente al *MTA* remoto para transferirlo. El conector de correo *Microsoft* es solamente conector para *Exchange* y no cumple con la norma *EDK*.

Otros Conectores.

En adición a los conectores precedentes, el servidor *Exchange* proporciona el conector *site* y el *X.400*. Éstos conectores no son componentes de *software* separados; en lugar de esto, son considerados como configuraciones del *MTA*.

Microsoft Mail Connector y Directory Synchronization.

La sincronización de directorio (*Dirsync*, Fig. 6.13) es responsable de dar mantenimiento a la información del directorio del correo de *Microsoft* para *PC* y a la red de *AppleTalk* con algún sistema que utilice el protocolo (*Dirsync*) de correo de *Microsoft* y de la red *AppleTalk*, incluyendo :

- Correo de *Microsoft* para redes *PC* (*MS Mail PC*).
- Correo de *Microsoft* para red *AppleTalk* (*MS Mail [AppleTalk]*).
- Sistemas Externos de Correo, como *PROFS*.

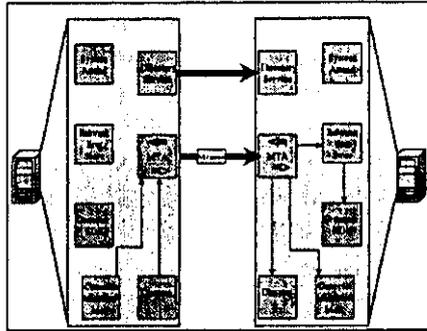


Fig. 6.13 Conector Microsoft Mail.

Si un conector de correo *Microsoft* participa con un *Dirsync* residente en un servidor remoto, *Dirsync* deberá comunicarse con el conector remoto a través de los servicios proporcionados por el *MTA*.

Componentes de Comunicación.

A continuación se muestra gráficamente (Fig. 6.14) los componentes de comunicación :

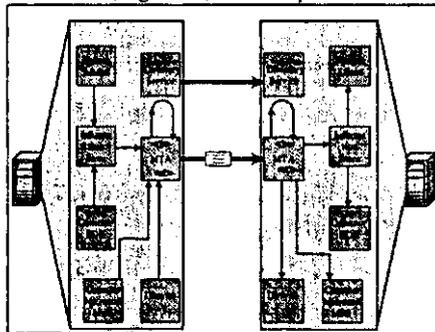


Fig. 6.14 Componentes de comunicación.

Los servicios para comunicarse con un *site*, mantienen la estructura de la organización y proporcionan mensajería funcional como se muestra en la siguiente tabla :

Servicio inicial	Servicio Receptor	A través	Razón
Private Information Store	Private Information Store	MTA	(IPM) Transfiere mensaje interpersonal
	Public Information Store	MTA	Transfiere IPM
	Cualquier conector	MTA	Transfiere IPM
Public Information Store	Public Information Store	MTA	Replicación de folder público
	Private Information Store	MTA	Transfiere IPM
	Cualquier conector	MTA	Transfiere IPM
System Attend	Public Information Store	MTA	Transfiere IPM
	Private Information Store	MTA	Transfiere IPM
	System Attend	MTA	Transfiere IPM (Link Monitor)
Dirsync	MS Mail(PC)	MTA	Mensajes Dirsync
	MS Mail(AppleTalk)	MTA	Mensajes Dirsync
Directory Service	Directory Service	Directo	Actualizaciones del Directorio

Adicionando Servidores a un *Site*.

Cuando un servidor es adicionado a un *site* (Fig. 6.15) se deberá considerar la información necesaria para establecer la unión, como el nombre del *site* y la cuenta de servicio con que fue configurado el primer servidor.

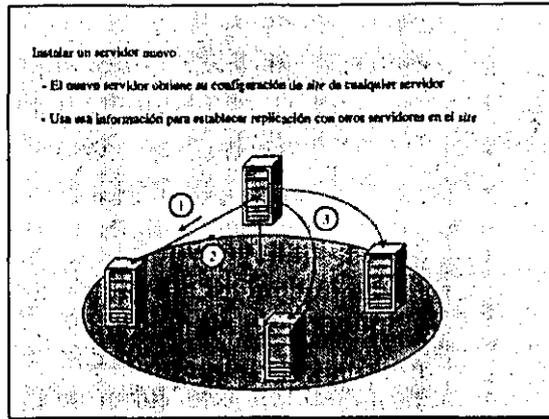


Fig. 6.15 Adicionando un servidor a un *site*.

Setup para el Nuevo Servidor.

Cuando se ejecuta el *Setup* para realizar la instalación de un servidor adicional a un *site* se realizan los siguientes pasos :

1. Se adiciona en el servidor remoto una réplica de la base de datos de directorios existente en el servidor instalado.
2. Todos los servidores adicionados al *Site* existente deberán ejecutar una copia *up-to-date* del directorio, que obtendrá la información desde el servidor remoto de todos los objetos dentro del *site*. Todo el contenido, con excepción del *Recipient Container*, son copiadas dentro del directorio local sobre el nuevo servidor.
3. Se determina a todos los demás servidores utilizar el mismo nombre de *site* para utilizar el *Stub Directory*, y se instruye a éstos para comenzar a replicar los datos del directorio.

Stub Directories.

Un *Stub Directory* es una replica de la información, esta es utilizada para ahorrar tiempo cuando un servidor es adicionado a un *site*. Si el directorio entero es copiado, el programa *Setup* deberá esperar cuando ocurra la transferencia de datos. Si el archivo es demasiado largo, por ejemplo, un *site* debe mantener una lista de 500,000 usuarios, el proceso podrá tomar algo de tiempo. Para copiar solamente el *Stub Directory*, el proceso de inicio del *Setup* es muy rápido. Cuando el *Stub Directory* es copiado en el nuevo servidor y el *Setup* es completado, el nuevo servidor puede participar en la replica de directorio de forma regular y transferir mensajes. El servidor podrá utilizar de forma regular la propiedad de replica y obtener las listas receptoras de servidor *Exchange*.

Estrategia del Corporativo.

El corporativo definió como servidor primario el servidor de México para proporcionar el servicio de correo al 70% de los usuarios de la afiliada y se eligió como servidor de respaldo o foráneo dentro del mismo *site* uno en la ciudad de Puebla para dar acceso al 30% de usuarios restantes.

Como parte de la estrategia del corporativo se definió que si una afiliada no contaba con los medios suficientes para implementar el servicio de correo en forma local, éste servicio se ofrecería desde otra afiliada, por lo que se realizaron pruebas de acceso desde diferentes filiales a la afiliada de México y se determinó que algunas ciudades de Centroamerica tomarían el servicio de nuestra filial.

El servicio de correo para la filial de México se considera crítico, ya que proporciona servicio no sólo a los usuarios locales sino también a algunas otras filiales en otro país.

Las características de los servidores adquiridos para instalar la aplicación de *Exchange* y sus componentes son :

- Servidor para México .- *IBM Netfinity 7000* con dos procesadores *pentium pro* a 200 Mhz, módulo de memoria de 500 Mb, 18 bahías de discos *Hot Swap*, tarjeta de red *Ethernet 10/100*, 9 discos de 4.5 Gb *Hot Swap* y tarjeta controladora de arreglos de discos. Se configuraron 2 discos para sistema operativo y 7 discos para un arreglo *Raid 5* para datos.
- Servidor de Puebla .- *IBM modelo 330* con dos procesadores *pentium II* a 300 Mhz, módulo de memoria de 256 Mb, 6 bahías de discos *Hot Swap*, tarjeta de red *Ethernet 10/100*, 6 discos de 4.5 Gb *Hot Swap* y tarjeta controladora de arreglos de discos. Se configuraron 2 discos para sistema operativo y 4 discos para un arreglo *Raid 5* para datos.

Ambos servidores se compraron con las licencias de *software* necesario para implementar *Exchange* y su sistema de respaldo en forma total.

El servidor de México fue adquirido de mayor capacidad para soportar la cantidad de usuarios destinados a México y preveer un crecimiento a un año del 30%, el servidor de Puebla también fue adquirido considerando un crecimiento del 40%.

El uso de un servidor en la ciudad de Puebla que esté unido al servidor de México, permite a los usuarios de Puebla tener un tiempo de respuesta de acceso a la información y de envío de mensajes locales más rápido que si tuvieran que acceder al servicio en la ciudad de México, el tiempo de acceso puede ser despreciable para la ciudad de Puebla, no así para las otras ciudades foráneas que toman el servicio de correo tanto del servidor de Puebla como del de México.

Adicionalmente, se pueden definir otros servidores foráneos en otras ciudades importantes del país y unirlos a todos en el mismo *site*, esto minimizaría el tiempo de acceso para aquellas ciudades foráneas que viajan a México o a Puebla por su correo, ya que éstas localidades normalmente dependen de los medios de comunicación existentes en el país.

ESTRUCTURA DE EXCHANGE PARA EL ALMACENAMIENTO DE INFORMACIÓN.

7.1.- Esquema de almacenamiento de *Exchange*

Actualmente, para muchas compañías, es sumamente importante la habilidad de comunicarse rápida y eficazmente por correo electrónico y de esta manera permanecer en un nivel alto de competencia, muchas compañías pueden ver afectada su operación diaria cuando no se cuenta con correo electrónico ya que es una herramienta importante para comunicarse con el personal dentro y fuera de la compañía. Por éste motivo, los administradores de correo tienen un trabajo importante, son responsables de mantener y administrar la recepción y envío del correo electrónico, procurando que no existan interrupciones, y uno de los principales aspectos a considerar es mantener la integridad y la seguridad de la base de datos para evitar la pérdida de información.

Exchange implemento una arquitectura de componentes para el envío de los correos electrónicos definidos por la *CCITT*, siendo sus componentes el *User Agent (UA)*, el Agente de Transmisión de Mensajes (*MTA*) y el *Information Store (IS)*, para construir una aplicación que se considera la primera en solucionar los problemas de mensajería en redes *LAN* que ofrece escalabilidad y crecimiento para muchas plataformas o ambientes de trabajo.

Arquitectura de la base de Datos de *Exchange*

Para entender como *Exchange* mantiene la información en el sistema, es importante entender, que la estructura de la base de datos (Fig. 7.1) trabaja en unión con los componentes de *Exchange*.

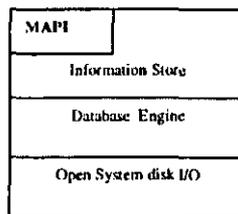


Fig. 7.1 Arquitectura de la Base de Datos

Information Store (IS)

El almacenamiento de la información es la clave principal para la administración de la base de datos de *Exchange*, éste componente es el responsable del almacenamiento de los datos. El almacenamiento de la información se realiza en dos bases separadas, una de ellas es la Base de Datos Privada, *Priv.edb*, la cual administra la información en los *mailboxes* de los usuarios, y la Base de Datos Pública, *Pub.edb*, la cual administra la información en los folders públicos.

El *IS* trabaja en conjunto con el *Messaging Application Programming Interface (MAPI)* y con el *engine* de la base de datos de *Exchange*, para asegurar que todos las cuentas de los usuarios han sido guardadas en disco en el servidor. Por ejemplo, cuando un usuario selecciona la opción de guardar, un mensaje de *Microsoft Outlook*, *MAPI* llama al *IS*, el cual a su vez hace un llamado al *engine* de la base de datos, para que esté guarde las modificaciones que se le hicieron a éste mensaje en el disco .

El *IS* provee un servidor basado en una estructura donde se almacena la información que es creada por los usuarios. Su amplia estructura de base de datos almacena información heterogénea como son mensajes de correo electrónicos, *attachments*, formas electrónicas, imágenes, mensajes de voz y provee un rápido acceso a la base de datos.

El servidor de *Microsoft Exchange* cuenta con un número de herramientas para administrar o manejar la información de la siguiente manera:

- Establece límites de almacenamiento para manejar la cantidad de espacio en disco utilizado en el servidor por folders privados y públicos.
- Fija fechas límite y las borra automáticamente del *IS* y todo lo que sobrepase los límites.
- Establece una seguridad granular o individual en los folders públicos y privados
- Fija horarios para el copiado de folders públicos.

La base del servidor del *IS* tiene dos bases de datos: una almacena folders privados para los usuarios del correo electrónico, y la otra almacena los folders públicos.

La facilidad en el poder de copiado le permite la distribución automática de la información almacenada en el folder público hacia varios lugares. Existe un tercer folder opcional de la base de datos el cual es un folder personal.

El *IS* copia los folders públicos, refuerza los límites de almacenamiento y envía mensajes a los usuarios del mismo servidor (envío local).

El mensaje originado en el servidor es almacenado en el *IS*, éste guarda el mensaje unido al correo de *Microsoft* para el servidor de *Exchange* y el *MTA*, éstos dos señalan el intercambio de correo de *Microsoft* que el mensaje esta esperando. El *Interchange* recoge el mensaje, y lo convierte a formato de correo *Microsoft* y lo envía a los conectores de la oficina de mail. El *MTA* recoge el mensaje y lo envía a su destino final.

Componentes de la Base de Datos

Al diseñar *Exchange* se trató de utilizar la tecnología estándar de las bases de datos, como pueden ser *WINS* y *DHCP*, al igual que la base de datos de *Microsoft SQL Server*.

El *engine* de la base de datos de *Exchange* deposita en la memoria 4KB de datos, llamados páginas, lo cual permite actualizar las páginas en la memoria y se tiene precaución de los nuevos escritos o de la actualización de páginas desde el disco (Fig. 7.2) el *engine* de la base de datos no envía la información para que se almacene en el disco, sólo lo envía a la memoria. Ello permite que el sistema sea eficiente por que al escribir en la memoria es más rápido que escribir en el disco duro. Cuando un usuario hace una petición, el *engine* de la base de datos empieza a dar respuesta a esa petición desde la memoria y marca esa página como sucia (Una página sucia es una página que la memoria reconoce como una página con información). Estas páginas sucias más tarde se almacenaran en el *IS* en el disco duro.

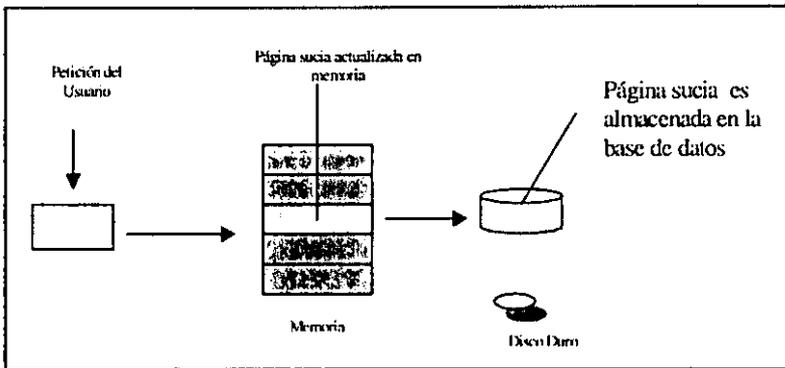


Fig. 7.2 Escribiendo Datos en el Disco

De esta forma, dejar los datos en memoria es la forma más rápida y eficiente de procesar la información, la última versión de la base de datos esta en memoria, y cualquier modificación o cambio que se lleve a cabo en la memoria, no se actualiza en el disco, ya que la base de datos y la memoria están fuera de sincronía. Si hay alguna página sucia en memoria, que pudiera ser transportada y escrita en éste momento en el disco, la base de datos se encuentra marcada y estaría inconsistente, aunque se escuche extraño, cuando normalmente se ejecuta *Exchange*, se considera técnicamente que la base de datos es inconsistente. El único momento en el que se considera que la base de datos de *Exchange* esta en un estado consistente, es cuando todas las páginas que contienen información en memoria fueron enviadas al disco duro por medio de un shutdown, en donde no ocurrió ningún error.

Si se perdiera el contenido de la memoria, antes que la información se escriba en el disco duro, tendríamos una base de datos inconsistente, por lo que *Exchange* necesita un proceso seguro para copiar todo lo que tiene en memoria y enviarlo al disco para su almacenamiento, ya que si se perdiera información, es complicado el poder recuperarla. *IS* es el responsable de dejar el correo a los usuarios en el mismo servidor de donde se envió, y de enviar el correo al *MTA* para verificar a los usuarios que son de otro servidor.

Estructura Pública del Almacenamiento de la Información

El almacenamiento público de la información es el primer mecanismo utilizado por los clientes *MAPI* para tener el acceso a los folders públicos. Aunque los folders públicos pueden localizarse en diferentes áreas de almacenamiento de información, la jerarquía del folder representa independientemente todos los folders y subfolders públicos, como se muestran en la siguiente gráfica.(Fig. 7.3).

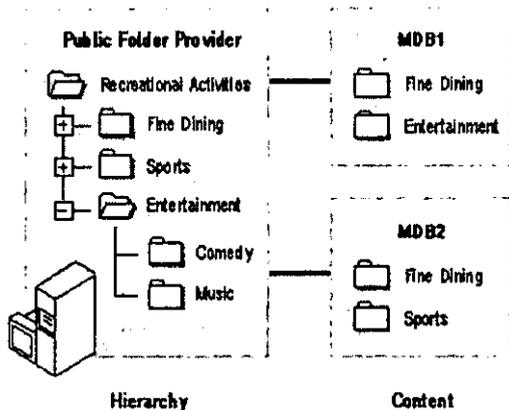


Fig. 7.3 Almacenamiento Público de la Información.

La jerarquía del folder público es almacenada en el *IS*. El utilizar el servidor de *Microsoft Exchange* permite a los usuarios el uso de un índice creado por el folder público de objetos para enlistar los folders principales y regresar al cliente *MAPI*. Cuando se utiliza una aplicación *MAPI* para ver los subfolders o los folders públicos principales, el proveedor se conecta al *IS* que mantiene por un instante todo lo que los folders contienen. Posteriormente, el proveedor va al *IS* para realizar todas las operaciones subsiguientes en ese folder.

Cualquier cambio en la jerarquía del folder público es ejecutada por la jerarquía del servidor.

Árbol de Información del Directorio del Servidor de *Microsoft Exchange* (DIT)

El DIT representa la topología del servidor de *Microsoft Exchange* e ilustra la relación entre la organización, *sites* y servidores. En la siguiente gráfica (Fig. 7.4.) se muestra la organización y la jerarquía del directorio raíz (root), el *site* esta por debajo de la organización y los servidores aparecerán debajo de los *sites*.

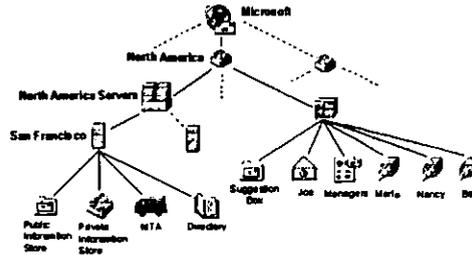


Fig. 7.4. Organización y Jerárquica del Directorio Raíz

Por ejemplo: *Microsoft* es el nombre de la organización, *North America* es el nombre del *site* de la organización y *North America Servers*, y *San Francisco* son los nombres de servidores que pertenecen al *site* *North America*.

Parte Interna del Servidor de *Microsoft Exchange*

El servidor de *Microsoft Exchange* es un sistema muy bien organizado y estructurado con todo lo que una compañía necesita para manejar las comunicaciones de la organización. Los componentes del servidor son:

- Servicio de Directorio (*Directory Service*).
- Almacén de Información (*Information Store, IS*).
- Conectores *MTA*.
- Asistente de Sistemas (*System Attendant*).

Los componentes del servidor de *Microsoft Exchange* se ejecutan como los servicios de *Windows NT* y trabajan juntos:

Almacenan y mantienen toda la información acerca de la organización y cada uno de los *sites* en el directorio del servidor de *Microsoft Exchange*.

Controla quien puede acceder a la información del directorio y como puede ser utilizada ésta.

Provee de un Inbox universal que permite a los usuarios exponer, devolver o manejar información tal como mensajes electrónicos, documentos, faxes desde una sola dirección.

Recibe, entrega, transfiere, y manda mensajes a través y más allá de la organización.

Monitorea el estado de los servidores y de sus conexiones.

Se asegura que todos los servidores con y a través de los *sites* tengan la misma información del directorio.

Maneja horarios de replicación y conflictos con la replicación.

El administrador de Programas del *Microsoft Exchange* usa un administrador de los componentes del servidor. En la Fig. 7.5 se muestra como trabajan los componentes del servidor con el programa de administración del servidor de *Microsoft Exchange*.

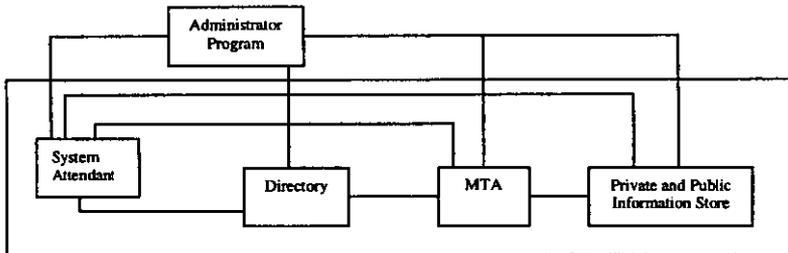


Fig. 7.5. Trabajan en conjunto los componentes del servidor de *Exchange* con el programa de administración del servidor.

El Programa de Administración

Una ventaja del servidor de *Microsoft Exchange* es su facilidad de manejo a través de grandes organizaciones dispersas geográficamente. Una aplicación gráfica del sistema de administración te permite manejar de forma centralizada todos los componentes del servidor, incluyendo receptores, conectores y servidores, a lo largo de toda la organización.

El programa de Administración que tiene el *Microsoft Exchange* despliega una estructura jerárquica de la organización lo cual permite un manejo y navegación de los elementos de cada nivel.

Se puede apreciar en la Fig. 7.6:

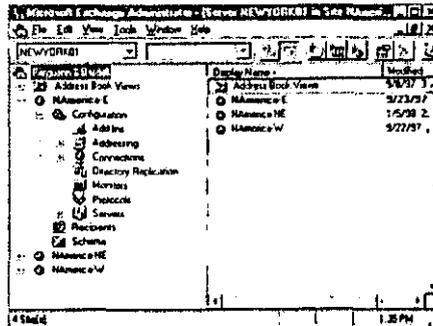


Fig.7.6. Un administrador puede visualizar todos los componentes del servidor con sólo hacer click en el servidor iluminado en la parte izquierda de la ventana.

7.2 BD Pública características

Folders Públicos

Estos son componentes claves del Servidor de *Microsoft Exchange*. Es su copiado lo que permite a los usuarios el compartir información.

Copiado de los folders públicos

Una característica de la fuerza del servidor de *Microsoft Exchange* es su habilidad para distribuir y sincronizar la información compartida a través del sistema de copiado del servidor. Esta habilidad se soporta teniendo múltiples copias sincronizadas de folders en diferentes lugares, es indiferente si se está conectado sobre un ambiente *LAN*, *WAN*, *Internet* ó *X.400*. En éste sentido, la información de copiado significa:

Las copias sincronizadas de un folder público pueden residir en múltiples servidores, distribuyendo el proceso de cargado y mejorando el tiempo de respuesta para los usuarios que tienen acceso dentro del folder.

Las copias sincronizadas de un folder público pueden residir en muchos sitios separados geográficamente, reduciendo de forma dramática la cantidad de tráfico de larga distancia *WAN* necesaria para tener acceso a la información.

Si un servidor que sostiene una copia de un folder público llega a estar no disponible, otros servidores cuentan con copias sincronizadas del mismo folder y una copia puede ser obtenida sin problema incrementando gradualmente la disponibilidad de la información para los usuarios, el resultado será un sistema altamente redituable.

El servidor de *Microsoft Exchange* ofrece a los usuarios un acceso único independiente de la información compartida. El manejo del copiado de los folders públicos es muy sencilla.

Esta basado en mensajes y utiliza la infraestructura tolerante a fallas.

El administrador sólo necesita seleccionar los servidores que recibirán réplicas de los folders públicos y el servidor de *Exchange* hará el resto.

Un folder público, se emplea para guardar información que se pretende compartir con un grupo de usuarios, Los folders públicos facilitan el intercambio de información y están localizados en el servidor.

Necesidades de los Folders Públicos.

Además de describir las necesidades de cada folder público para cada grupo de usuarios, también se deben decidir que políticas para la administración se implementarán tomando en cuenta solamente los folders públicos:

Los folders públicos necesitan que cada grupo pueda ser evaluado por un estudio de cada folder del grupo que será exclusivamente utilizado. Para cada folder se necesita estimar los siguientes detalles:

Volumen de la nueva información.

Cuantos mensajes o formas serán creados cada día y su tamaño promedio.

Tiempo estimado de duración de la información. Cuantos días puede guardarse esta información, Por ejemplo, un folder público con calendarios y anuncios semanales podría no necesitar salvar información por más de 2 semanas, pero una aplicación de un cliente podría requerir datos que se deban guardar indefinidamente.

Carga. ¿Cuántos usuarios tendrán acceso al folder público?, ¿Cuántas veces al día?, Los folders públicos no necesitan estar en el mismo servidor como el usuario. Si la carga de la red es suficientemente alta puede ocasionar problemas y será mejor colocar los folders públicos en el servidor o en otro segmento de la red.

El almacenamiento de la información en los folders públicos, es el primer sistema de almacenamiento con información importante para los usuarios e incluye:

Mensajes

- Un servidor basado en sus *mailboxes* y sus contenidos.
- Folders públicos y sus contenidos.
- Folder privado donde se almacena la información en el servidor, en lugar de la computadora del usuario.
- Documentos.
- Formas.
- Temas definidos por los usuarios.

Entre éstos temas, los folders públicos tienen un gran significado para los programadores por que son capaces de desarrollar poderosas aplicaciones que comparten información a través de empresas. Un folder público es semejante a un folder de mensaje privado *API (MAPI)* en el sentido de que almacena información, pero al contrario de los folders privados, los folders públicos pueden estar disponibles para los usuarios a través de una organización. Por ejemplo; un folder público puede almacenar una biblioteca completa de documentos incorporados de tal manera que todos en la compañía puedan tener acceso a la información en un servidor central y localizarlo de una manera sencilla, ello ofrece una simple y unificada visión de la información para todos en la empresa.

El almacén público puede verse como un tipo especial de *mailbox*, éste está formado por un grupo de folders públicos que son creados por el administrador, por usuarios o por aplicaciones.

Además los folders públicos comparten muchas de las mismas características que los folders privados, las principales diferencias son:

Son objetos que tienen una dirección. A cada folder público en el *IS* tiene su correspondiente objeto en el directorio de *Microsoft Exchange*.

Tienen propiedades adicionales para que se consulten los folders de acuerdo a los privilegios que estableció el administrador.

Tiene una propiedad adicional que especifica una o más reglas que se ejecutarán cuando ocurra un evento o mensaje determinado.

Ellos están en una jerarquía pero pueden ser distribuidos a múltiples almacenamientos de la información. Por ejemplo. Dos folders públicos tienen el mismo folder, pero físicamente están localizados en diferente *IS* o en diferente servidor.

Pueden ser replicados por toda la organización para incrementar la habilidad y el acceso rápido de los datos.

Administración Centralizada

Las herramientas gráficas de la administración se utilizan para configurar y mantener la organización, tanto los *sites* como los servidores se encuentran en un mismo lugar. Esta herramienta nos permite tener una representación gráfica de todos los objetos en el directorio.

El directorio es una estructura jerárquica de objeto que representa a cada componente de la organización, incluyendo folders públicos y usuarios de correo. El administrador de programas es utilizado para manejar todo en la organización en un *site*, aunque se haya manipulado la estructura de la jerarquía del directorio o cambiando las propiedades de objetos individuales.

7.3 BD Privada características

Los folders privados son depósitos de información que pertenecen a un individuo o individuos específicos. Solo éstos usuarios o sus ayudantes tienen permiso de obtener la información contenida en éstos folders.

Almacenamiento de Mensajes

Microsoft Exchange permite los folders de correo privados para ser almacenados en el servidor en el *IS* y en los almacenamientos de información personal (*Personal Information Stores, PST*) en las estaciones de trabajo. Los folders públicos generalmente se almacenan en el *IS*. Es posible establecer políticas en la administración para limitar el volumen del correo privado en el *IS*. Limitando el almacenamiento de mensajes privados en el *IS* mientras se permite el almacenamiento de mensajes personales, reduce las necesidades de almacenaje.

Se puede controlar el almacenamiento en el *IS* con políticas para el tamaño y límite de los mensajes que se envían y se reciben. El almacenaje de correo de *Microsoft Exchange* tiene una arquitectura llamada *single-copy*, por ejemplo; si un mensaje es enviado a 10 personas en un servidor, el correo de cada uno de ellos obtiene un pequeño indicador para la sencilla copia compartida del mensaje.

Si se deciden implementar límites de almacenamiento de los *mailboxes*, éste necesita ser diferente para cada grupo de usuarios.

Almacenamiento Público

Cada servidor de *Microsoft Exchange* tiene su propio *IS*. Como resultado, los *mailboxes*, folders públicos y folders privados pueden ser distribuidos entre éstos servidores de la forma más conveniente y según las necesidades de la organización y así hacer fácil el manejo de la información.

Para los clientes la aplicación *MAPI*, la estructura lógica del almacenamiento de la información aparece como un mensaje *MAPI* almacenado, éste está formado por los *mailboxes*, el folder raíz, y el folder de manejo internacional de programa (*IPM*), así como folders no *IPM*, *inbaskets*, *outbaskets*, *wastebasket*, folders de localización y más.

Sin embargo el servidor de *Microsoft Exchange*, va más allá de la definición básica de un almacén de mensajes *MAPI*, esto definiendo 2 tipos de almacén: privados y públicos. Los almacenes privados guardan temas que pertenecen a individuos y que no pueden ser compartidos por múltiples usuarios. Los almacenes privados pueden residir en una central de trabajo en un guardado personal o pueden residir en el servidor de *Microsoft Exchange*.

De forma contrastante, el almacén público reside siempre en un servidor y contiene folders y mensajes que pueden ser compartidos entre múltiples usuarios y aplicaciones.

Microsoft Exchange define exactamente un almacén público, el cual es independiente de cualquier almacén de información en la empresa. Un almacén público único es compartido por todos los usuarios a través de la organización, así el servidor múltiple de *Microsoft Exchange* es utilizado.

El almacén público es simplemente una colección de folders públicos. No existe distinción entre tipos de folder tales como el *IPM* o *inbasket* en el almacén privado.

Para la perspectiva de los desarrolladores, el acceso a los almacenes públicos es similar a acceder cualquier otro almacén *MAPI*.

7.4 Archivos de log transaccionales características

Exchange utiliza los archivos de *log* transaccionales, para procesar los mensajes y para que en caso de una falla del sistema, se pueda recuperar la información de forma rápida. Los archivos de *log* transaccionales son un respaldo, los cuáles permitirán en un momento dado la reconstrucción de la información.

En la siguiente gráfica (Fig. 7.7), podemos observar que se tienen los archivos *log* en discos separados del disco que almacena la base de datos y ello se hace para resguardar la información.

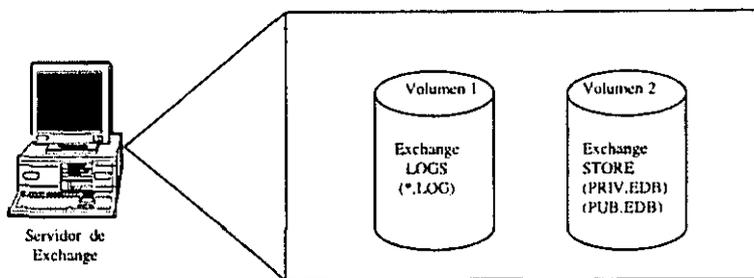


Fig. 7.7 Almacenamiento de los Archivos *Logs* Transaccionales.

La razón de esto es que los archivos *log* constantemente se están escribiendo en disco y es muy raro que se lean, y tanto la información de la base de datos como los archivos *log* necesitan estar escribiendo en disco. Todo esto depende de la cantidad de usuarios que tengamos.

Cuando se hace un cambio en el directorio de *Exchange* los primeros cambios se escriben en los archivos *logs* transaccionales (*.LOG), y el *engine* de la base de datos se encarga de copiar los cambios en el archivo de la base de datos actual que tiene la extensión (*.EDB) éste método proporciona las siguientes ventajas.

Desempeño: La información es almacenada en el archivo *log* transaccional en forma secuencial, siempre hasta el final del archivo. Cuando la información se almacena en el archivo de la base de datos, el *engine* de la base de datos accederá a la información de forma aleatoria, por que la información no se puede guardar de forma secuencial en la base de datos. Esto significa que es más rápido escribir la información en los archivos *log*, y hasta el final se copia a la base de datos.

Rehabilitación: Si la base de datos se dañara o destruyera, se pueden usar los archivos de *log* transaccionales para crear o recrear el archivo de la base de datos actual.

Estas dos características hacen que el almacenamiento de la información en los archivos *logs* sea eficiente. Y como se pudo observar en la figura anterior si se ponen los archivos *log* en un disco separado, ello permitirá que el *engine* de la base de datos pueda utilizar el otro disco para otros propósitos.

El tamaño de un archivo *log* es de 5MB. Si un archivo *log* tiene un tamaño mayor, ello nos indicará que ese archivo está dañado.

8.1 Procedimientos de Migración de Usuarios.

Para realizar el proceso de migración de los usuarios se evaluaron diferentes alternativas, algunas de ellas fueron:

- Eliminar el correo actual e iniciar de cero en el nuevo correo.
- Imprimir el correo actual y guardarlo en carpetas.
- Instalar el *software* llamado *Direct-to-1* en cada computadora para realizar la migración de los mensajes actuales hacia el nuevo sistema de correo.
- Realizar un *forward* de los mensajes más importantes en el correo actual hacia el nuevo sistema de correo.

Como parte de la estrategia de migración se seleccionó la opción de eliminar el correo actual e iniciar en cero y se propuso como alternativa para algunas personas la opción de dar un *forward* a los mensajes más importantes hacia el nuevo sistema de correo, esta opción fue comentada con los usuarios recomendándoles que no se intentara migrar todo el correo actual, ya que en el nuevo sistema de correo se configuró un límite de espacio para cada usuario y éste límite podría ser alcanzado durante el envío de sus mensajes a su nueva dirección de correo.

Antes de iniciar el proceso de migración se identificó una problemática que se podría presentar en todas las afiliadas, la actualización de las direcciones de correo en todo el mundo no era inmediata, por lo que algunas afiliadas estarían viendo la dirección anterior de correo de un usuario, aunque éste usuario ya hubiera sido migrado al nuevo sistema de correo y su dirección hubiera cambiado.

Esto podría provocar que algunos mensajes no llegarán a su destino y en un momento dado generar un problema de comunicación entre afiliadas.

Para evitar éste problema fue necesario configurar el *software* de correo anterior en todos los usuarios migrados para que identificaran como nueva dirección de correo la definida en el servidor de *Exchange*, esto funcionaba enviando los mensajes recibidos en el correo anterior hacia la nueva dirección del usuario, evitando así, que los usuarios tuvieran que consultar en ambos tipos de correo.

El procedimiento de configuración del correo anterior es el siguiente (Fig. 8.1):

1. Accesar *Team Links*, seleccionar las opciones *OPTIONS, SETUP..., MAIL PROFILE*.

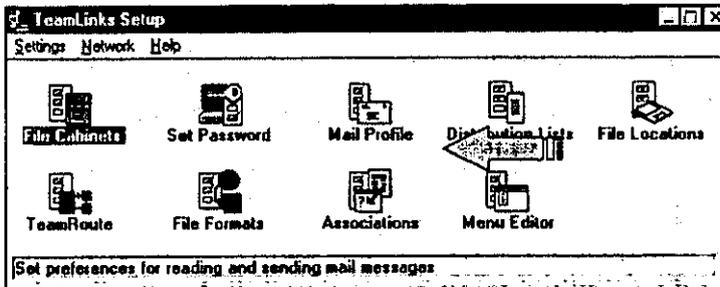


Fig. 8.1 Accesando a *Team Links*

2. Seleccionar la opción *RECEIVE OPTIONS*, teclear en el recuadro *FORWARDING ADDRESS*, el siguiente formato:

(Nombre.Apellido@XX.XXX@XX@XXXX)

Formato de envío de mensajes de *Teamlinks* a *Outlook*.

Dar un click al botón *OK* y salirse de *Team Links*.

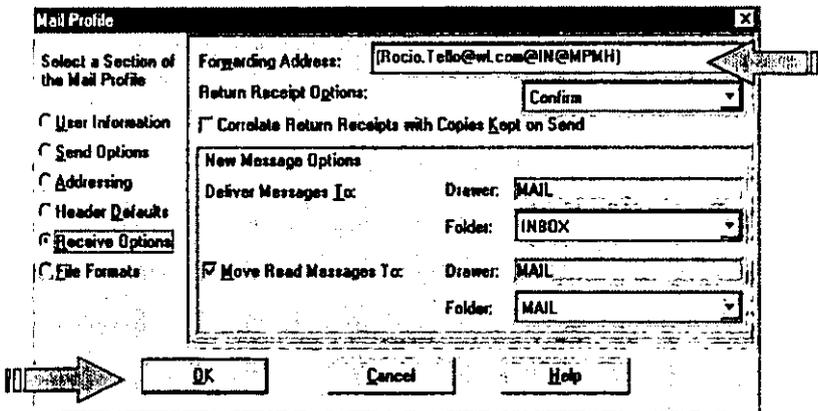


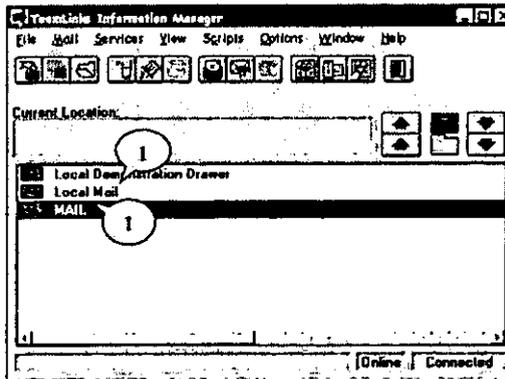
Fig. 8.2 Formato de envío de mensajes de *TeamLinks* a *Outlook*

Se proporcionó el siguiente instructivo para facilitar al usuario las herramientas propuestas para salvar sus mensajes o imprimirlos.

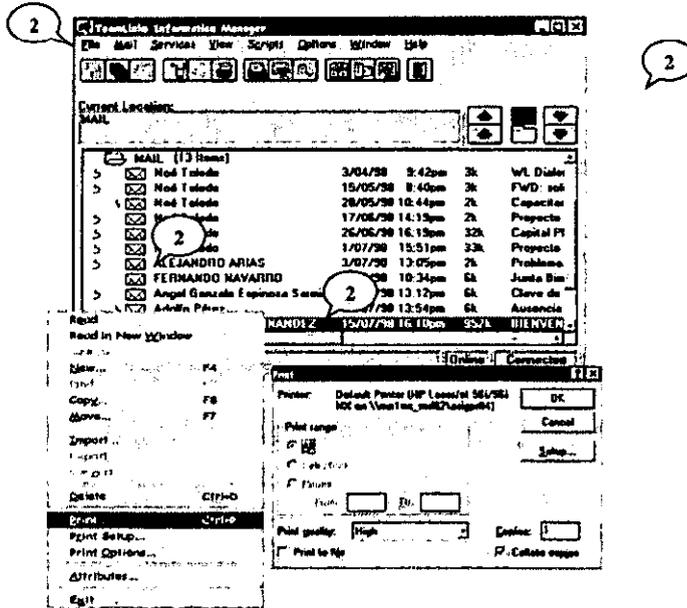
TEAM LINKS

Procedimiento para imprimir los mensajes en el correo anterior:

1. Posicionarse donde se encuentren almacenados los mensajes, ya sea en un Correo Local (*Local Mail*) o en el *Mail* principal.

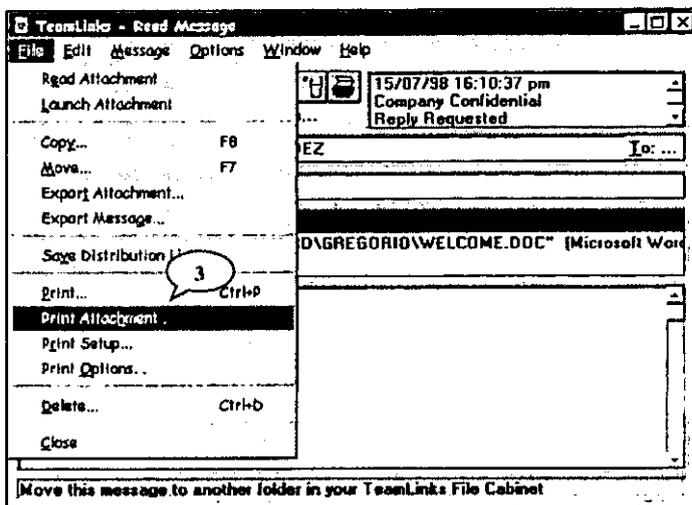


2. Posicionarse en el mensaje que se desea guardar, seleccionar las opciones del menú *FILE*, *PRINT* y oprimir el botón *OK*. Con ésta opción, se podrá imprimir todo el *mail*, desde el mensaje, las personas a las que va dirigido y los *attachments*.



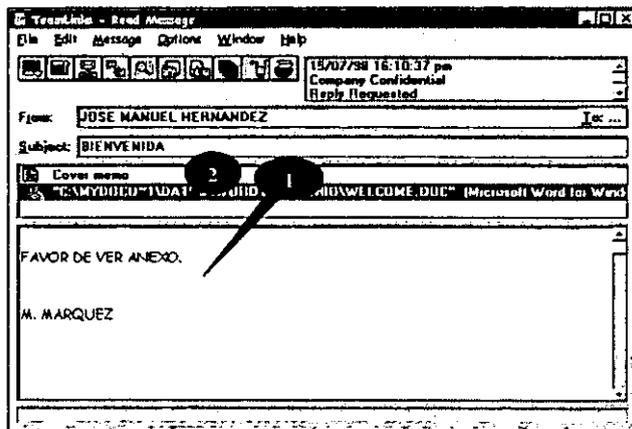
3. **NOTA:** Si únicamente se desea imprimir los *ATTACHMENTS*, se tendrá que abrir el mensaje, seleccionar la opción de *FILE, PRINT ATTACHMENT* y oprimir el botón de *OK*.

La opción de únicamente *PRINT*, volvería a imprimir todo el *mail*, como se señala en el paso 2.

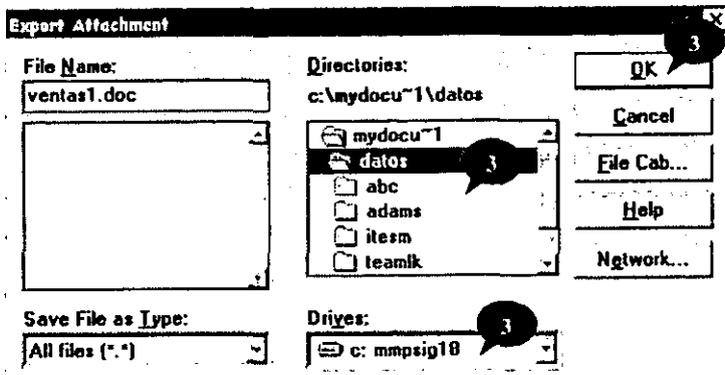


Para guardar los mensajes en archivos de texto, se deberán seguir los siguientes pasos:

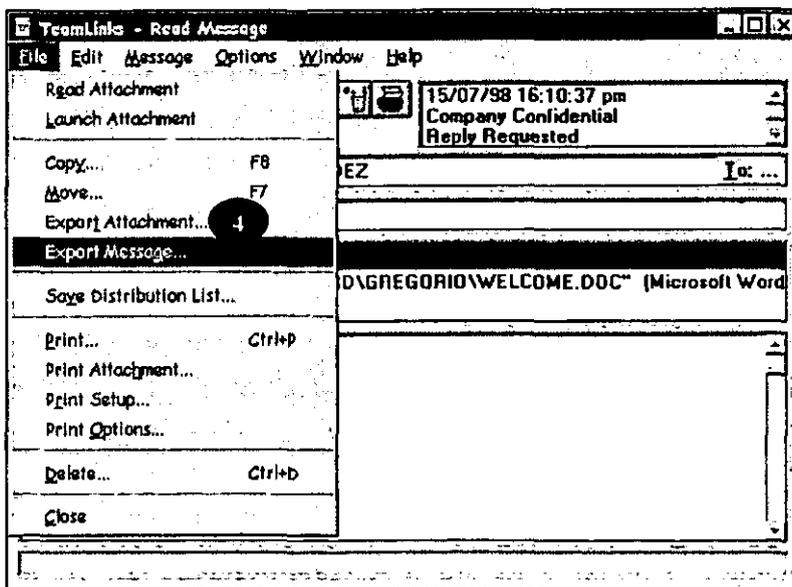
1. Abrir el mensaje a salvar, posicionarte en el *ATTACHMENT*. Verificando que realmente estés posicionado en éste, ya que dependiendo de donde te encuentres, será lo que va a salvar.
2. Seleccionar las opciones *FILE*, *EXPORT ATTACHMENT* y ...



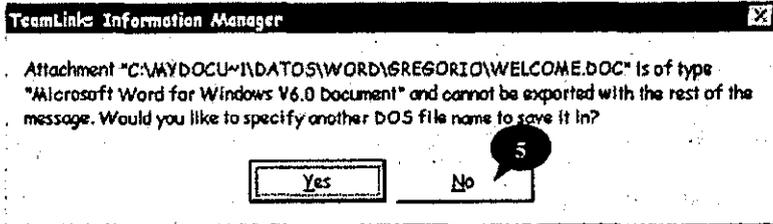
3. Cuando aparece la ventana donde se le tiene que asignar un nombre, seleccionar el lugar donde se desea guardar y oprimir el botón *OK*.



4. Si se desea guardar únicamente el mensaje, los pasos serán los mismos, pero ahora se tendrá que seleccionar **FILE, EXPORT MESSAGE**.



5. En caso de que el mensaje tuviera un **ATTACHMENT**, aparecerá una ventana la cual nos señalará que no lo podrá guardar con el resto del mensaje. En éste caso, favor de oprimir el botón **NO**.



Para visualizar los mensajes salvados de *Teamlinks* desde *Outlook* una vez que éstos se hayan transferidos, se deberán realizar los siguientes pasos:

Paso 1. Abre *Outlook*

Paso 2. De la barra de *Outlook* selecciona *Other* (En esta barra se encuentran *Outlook*, *Mail* y *Other*) Los iconos que se visualizarán son:

- *My Computer*
- *My Documents*
- *Favorites*
- *Public Folders*

Paso 3. Dependiendo de dónde salves tus archivos, selecciona el icono correspondiente para navegar y encontrarlos

Paso 4. Tus archivos tanto anexos como mensajes aparecerán como iconos con el nombre que tu les hayas elegido

Paso 5. Basta con dar doble click sobre ellos para abrirlos.

8.2 Campaña de Difusión del Nuevo Correo.

Como parte de la estrategia de difusión del nuevo producto se generó una lluvia de ideas que pudiera determinar cual sería la mejor estrategia de difusión, así como preparar a los usuarios para el futuro cambio y darles una visión sobre cual sería el impacto de éste movimiento.

Algunas de las estrategias propuestas para realizar la difusión fueron:

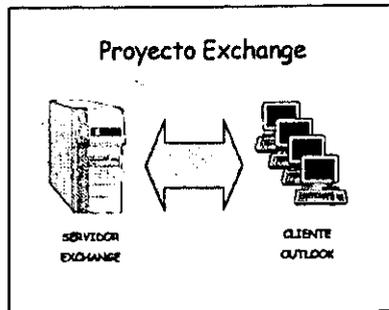
- Utilizar los tableros por piso.
- Diseñar Cartelones
- Utilizar la difusión de la Revista “Colega” de la compañía.
- Utilizar el Boletín *Board* para desplegarse cuando encendieran las máquinas.
- Generar una semana de difusión en todas las localidades, presentado un panorama general del cambio.

Como parte del programa de difusión se plantearon las siguientes actividades:

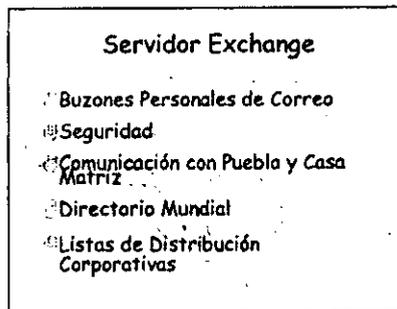
- Fecha para realizar la semana de difusión.
- Número de sesiones por día.
- Instructor por día.
- Cupo por sesión: 25
- Sesiones para foráneos.
- Reservar salas de capacitación.
- Realizar un programa de reservaciones automático.
- Diseñar mantas para poner a la entrada de las oficinas y del estacionamiento.
- Reservar artículos promocionales para las sesiones de difusión.
- Asegurar la difusión en las oficinas de Ventas foráneas.
- Proporcionar folletos sobre el producto.

Como parte de la difusión se programaron sesiones de 1 hora para explicar a los usuarios el cambio y su impacto, así como la importancia de una buena coordinación interdepartamental para enviar a toda la gente a capacitarse.

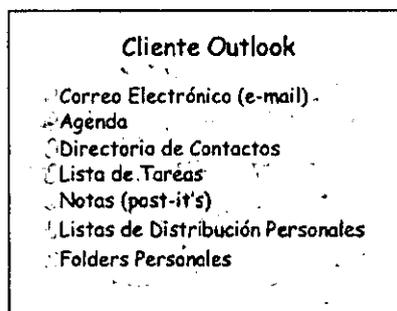
Cual es el *software* correspondiente a cada plataforma, para el servidor, el *Software* es *Exchange* y para los clientes con *Windows 95*, el *software* de correo es *Outlook*.



Cuáles son las características del servidor de *Exchange*.



Cuáles son las características del *software* de clientes.



Se mencionaron también las principales ventajas de migrar a éste nuevo correo.

Principales Facilidades

- Envío y recepción de mensajes con cualquier colega del corporativo.
- Envío y Recepción de Archivos en cualquier formato reconocido por Office.
- Envío y Recepción de mensajes y archivos con cualquier socio de negocios que tenga correo en Internet.

Principales Facilidades (Cont.)

- Respuesta automática de mensajes en caso de ausencia.
- Transferencia de mensajes en forma automática a otro usuario.
- Agenda Personal.
- Programación de juntas con otros usuarios desde la PC.
- Integración total con Office.

Se mencionó como se llevaría a cabo el proceso de migración, la implementación de los clientes, instalación del nuevo *software* y desinstalación del anterior, la migración de los mensajes que se encuentren en el correo anterior y el proceso de capacitación.

Implementación y Capacitación

- A los usuarios con el correo anterior.



- Un mes despues, a los nuevos usuarios.

La estrategia de capacitación se llevo a cabo de la siguiente manera:

Se planteó capacitar como primera instancia a todo el personal que contará con el correo anterior y el *software* de calendarización.

Durante el proceso de capacitación se llevaría simultáneamente la instalación del *software* nuevo en los clientes.

Una vez finalizados todos los usuarios con el *software* anterior, se inicia el proceso de capacitación de nuevos usuarios, así como la instalación del *software* en sus *PC*'s.

Capacitación

México:
Duración: 8 hrs.
Lugar: Sala de Capacitación

Foraneos:
Duración: Variable
Lugar: Instalaciones del Proveedor



Se explicó durante esta sesión la importancia de su asistencia a la capacitación, así como la estrategia para registrarse, el proceso de implementación estaba definido por una fecha límite propuesta por Casa Matriz para migrar a todos los usuarios del correo actual al nuevo sistema de correo.

Estrategia

- El registro para la capacitación se hará por medio de la aplicación "Capacitación Outlook" que se encontrará en "Folder México"
- El día del entrenamiento será instalado el nuevo sistema mientras los usuarios se capacitan.



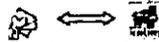
Se comentaron las consideraciones más importantes que se deberían tomar en cuenta durante el proceso de migración, algunas de las más importantes son:

- Convivencia entre los dos sistemas de correo en todo el corporativo.
- Migración de los mensajes existentes en el correo actual hacia el nuevo sistema de correo.
- Migración de las juntas calendarizadas del sistema de correo actual hacia el nuevo.
- Fecha de eliminación definitiva del correo actual.
- Proceso de eliminación definitivo.

Todas éstas consideraciones deberán ser tomadas en cuenta por todos los usuarios para estar listos para la migración.

Consideraciones

Durante la transición los usuarios de Outlook podrán intercambiar mensajes y archivos con los usuarios de Teamlinks.



El correo de Teamlinks y las citas de Calendar no serán migrados al nuevo ambiente.

Consideraciones (cont...)

Los mensajes se deberán imprimir o salvar en archivos de texto.

Las citas de Calendar deberán ser reprogramadas en la nueva agenda.

Existe una fecha límite para eliminar Teamlinks y Calendar de todas las PCs.

8.3 Capacitación.

Los procesos de capacitación, difusión e implementación fueron diferentes y planeados específicamente por cada filial.

Durante el proceso de capacitación a todos los usuarios de la compañía, se consideraron dos alternativas, la primera consistía en preparar a un grupo de personas del departamento para impartir sesiones de capacitación de 8 horas, la segunda alternativa era contratar un proveedor externo para que realizara la capacitación.

Se seleccionó como alternativa para México contratar a un proveedor externo que pudiera impartir la capacitación a todos los usuarios.

Como parte del proceso de capacitación se realizaron las siguientes actividades:

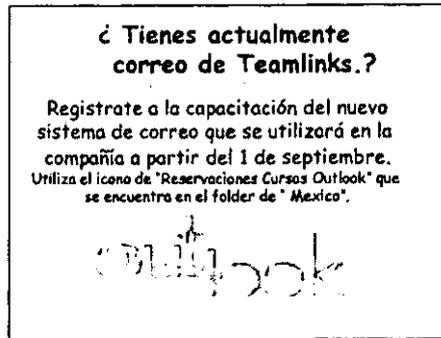
- Se generaron grupos de 10 usuarios y se programaron 60 días de capacitación, durante el proceso de capacitación que cada usuario selecciono, el equipo *PC* era preparado por personal del departamento para instalar el nuevo *software* y configurar el *software* anterior para que enviara los mensajes recibidos hacia el nuevo sistema de correo.
- El procedimiento para los foráneos no fue el mismo que para la Ciudad de México, debido a que el personal foráneo no puede desplazarse a México solo un día para tomar capacitación, por lo que se contrataron servicios específicos para cubrir las zonas foráneas.
- De igual forma la segunda ciudad más importante Puebla, tuvo que ser capacitada en sesiones de tres días por usuario por lapsos de 2 horas.

Para poder satisfacer las necesidades de registro de todo el personal a las sesiones de capacitación se generó una aplicación en *Visual Basic* y se dejó disponible para que todos los usuarios pudieran accederla desde cualquier *PC* conectada en red, esta aplicación fue diseñada para trabajar con una base de datos que nos permitiera registrar por medio del número de empleado que usuario se registraba y que sesión había seleccionado, además de diferenciar si era de México o foráneo.

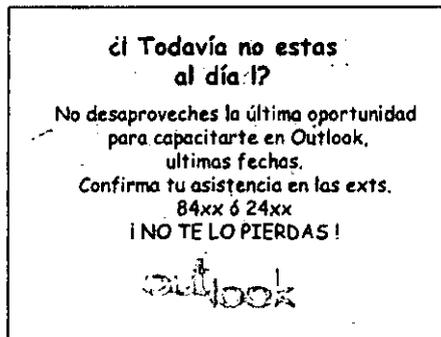
Adicionalmente nos permitía imprimir reportes de asistencia diaria y poder llevar un control de quien ya había sido capacitado y que usuarios faltaban.

Como parte del proceso de difusión de la capacitación se desplegaron las siguientes pantallas durante el encendido de las *PC's* con el fin de recordarle a los usuarios que el tiempo de capacitación era limitado y que todos los usuarios sin excepción deberían ser capacitados y migrados en una fecha límite.

Para iniciar con el proceso de capacitación se decidió iniciar la capacitación y migración de aquellos usuarios que ya tenían instalado el correo de *Teamlinks*, el cual sería eliminado en un tiempo específico.



Se emitió el siguiente mensaje cuando se considero que aún no se cubrían todos los usuarios y el tiempo de finalización estaba próximo.



Finalmente, se habían establecido como metas migrar al 100% de los usuarios que contarán con el *software* anterior, los cuáles eran aproximadamente 150 usuarios, esta meta se logró aproximadamente en 2 meses.

El número de usuarios restantes que fueron capacitados en el nuevo *software* y migrados fueron aproximadamente 400 usuarios en un tiempo de 3 meses.

8.4 Instalación en PC's.

Software seleccionado *Outlook 97* y *Outlook 98*.

La rápida migración de los usuarios se logra definiendo un proceso de instalación del *software* sencillo y eficiente, el cual se describe a continuación:

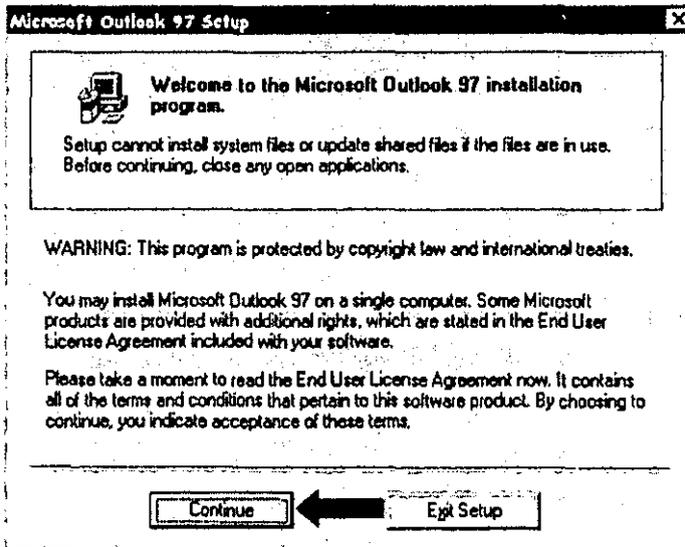
Antes de comenzar, verificar si el usuario tiene ya instalada la aplicación de *Outlook*; de ser así, favor de hacer un respaldo de los siguientes archivos: **.PST, *.FAV, VIEWS.DAT*.

Conectarse al drive `\\MSOUTLOOK\W\INSTAL`. Posicionarse en el folder *OUTLOOK.W32* y ejecutar la aplicación:



Setup.exe

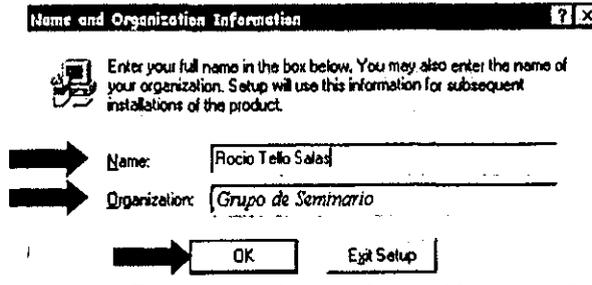
Aparecerá un asistente que nos informará que debemos de cerrar todas las aplicaciones que se tengan abiertas. Una vez cerradas, oprimir el botón *CONTINUE*.



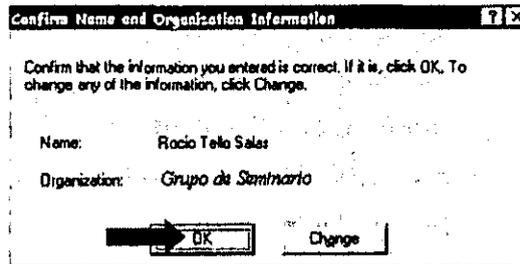
En la siguiente ventana favor de escribir:

Name nombre del usuario
Organization nombre de la organización

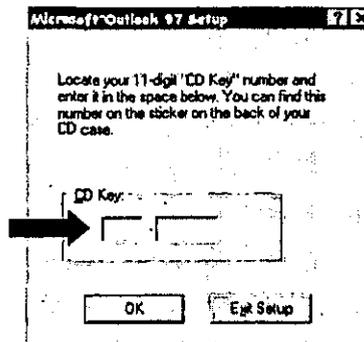
Oprimir el botón *OK*.



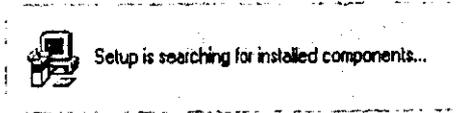
Saldrá una ventana para que confirmemos la información previamente capturada, dando un click al botón *OK* si está correcta o un click al botón *CHANGE*, en caso de que se tuviera que corregir.



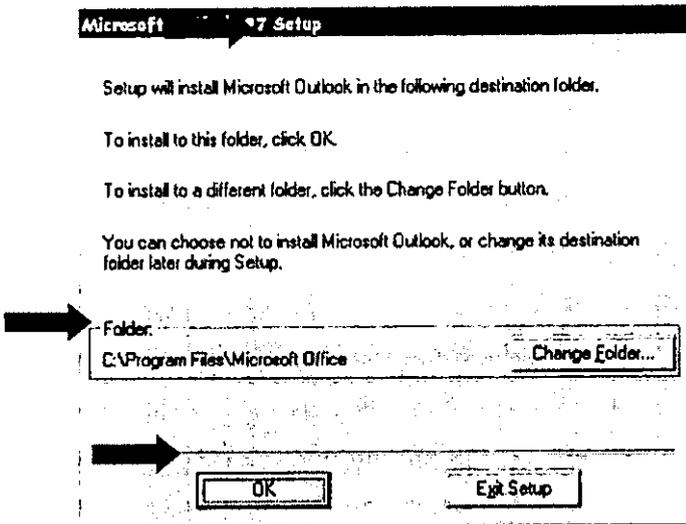
En la siguiente pantalla teclear el número "CD KEY" 4444-4444444 y oprimir el botón *OK*. Aparecerá el número de identificación del producto. Oprimir el botón *OK*.



Comenzará la instalación de los componentes.



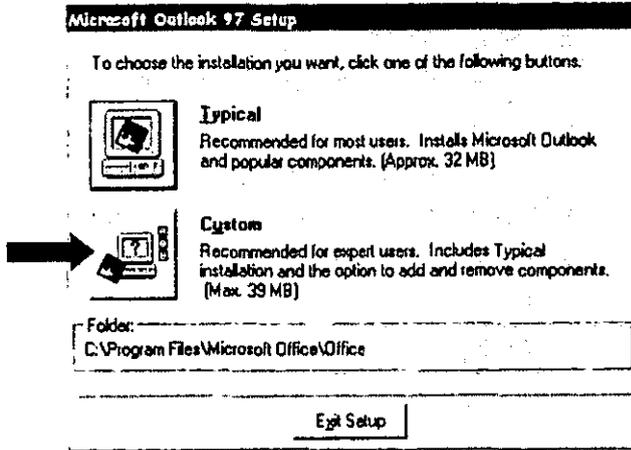
El folder de destino donde deberá ser instalado *OUTLOOK* es en *C:\PROGRAM FILES\MICROSOFT OFFICE*. Oprimir el botón *OK* en caso de que sea correcto.



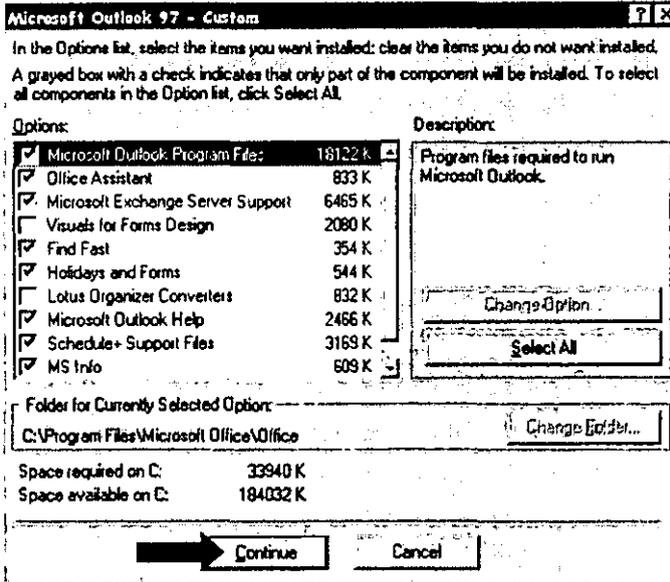
Seguirá con la instalación de los componentes.



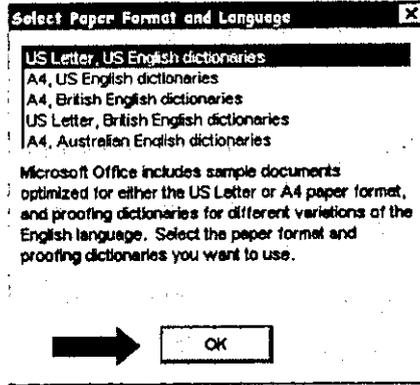
El tipo de instalación a seleccionar es *CUSTOM*.



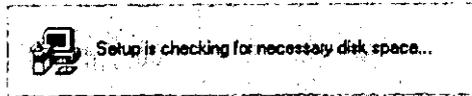
Sin cambiar ninguna opción, dar un click al botón *CONTINUE*.



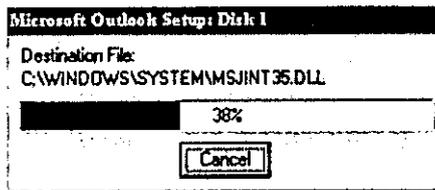
NOTA: Si apareciera la siguiente pantalla, favor de escoger para el tipo de papel y el lenguaje la opción de *US LETTER, US ENGLISH DICTIONARIES*. Oprimir el botón *OK*.



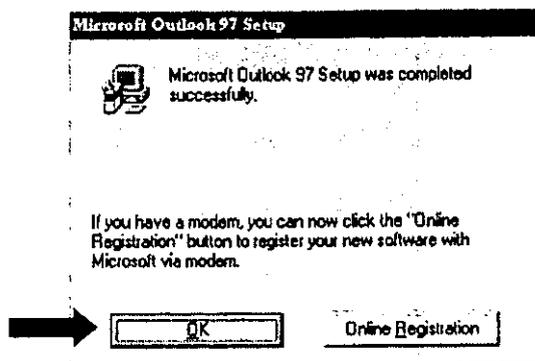
Se checará que se tenga el espacio necesario para la instalación.



Comenzará con la instalación.



Aparecerá una opción para el modem. Oprimir el botón *OK*.



Con esto concluirá la instalación de *Outlook*. En caso que durante la aplicación se generará el siguiente icono en el *desktop*, favor de borrarlo.



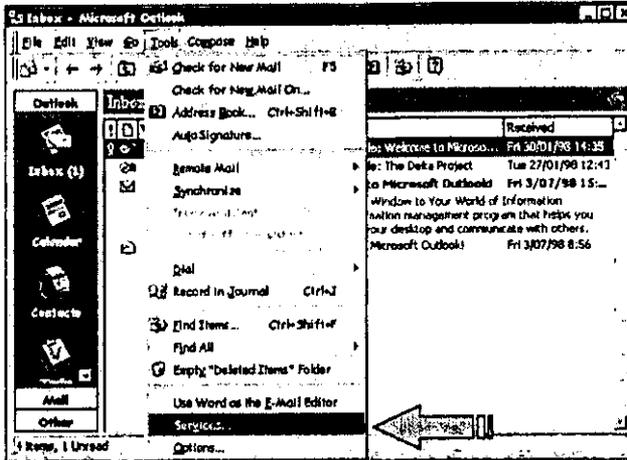
Setup for Microsoft Internet Explorer 3.02.lnk

NOTA:

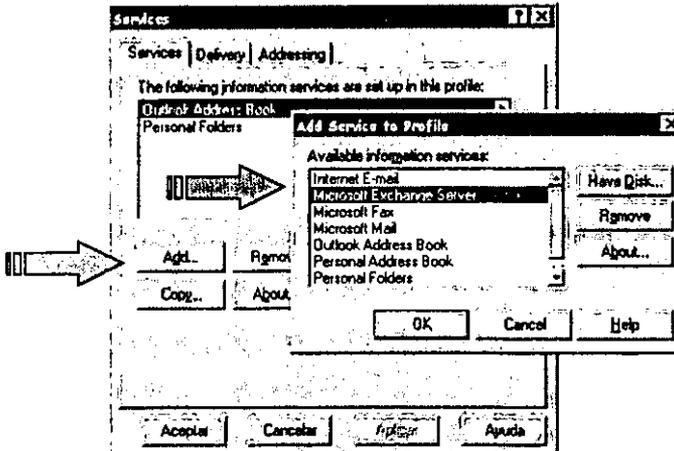
Por último, los archivos que fueron previamente respaldados (**.PST*, **.FAV*, *VIEWS.DAT*), hay que volverlos a copiar a donde corresponda.

Configuración:

Una vez instalado *OUTLOOK*, favor de acceder a la aplicación y posicionarse en las opciones *TOOLS, SERVICES*.



Oprimir el botón *ADD*, seleccionar *MICROSOFT EXCHANGE SERVER* y oprimir el botón *OK*.

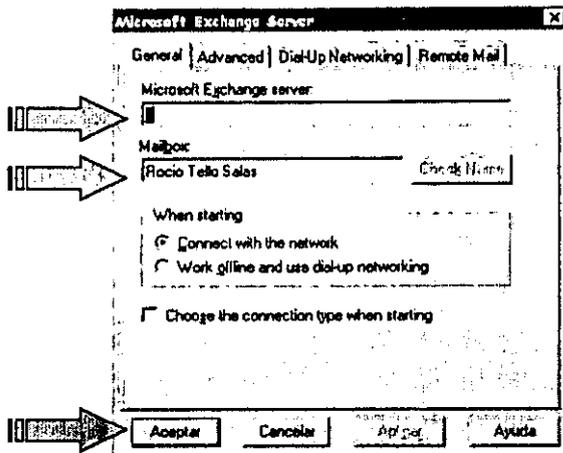


En la siguiente ventana favor de escribir la información:

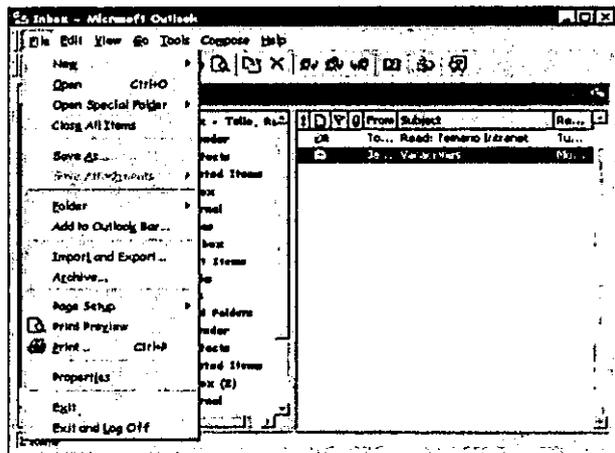
Microsoft Exchange Server: *SERMEXPR* (para usuarios de México)
SERPUEPR (para usuarios de Puebla)

Mailbox: teclear el apellido del usuario, oprimir el botón *CHECK NAME* y escoger al usuario.

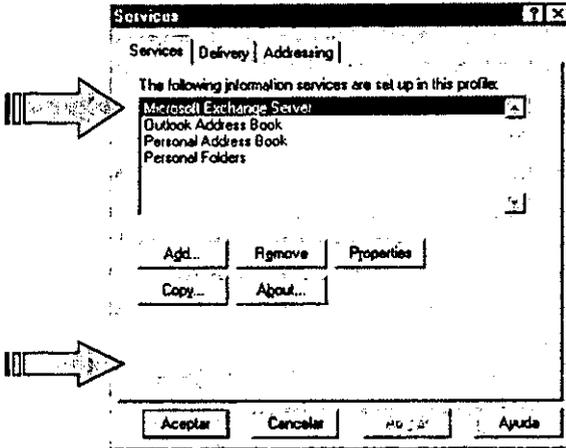
Oprimir el botón *ACEPTAR*.



Una vez ingresado los datos, tendremos que salir con las opciones de *FILE* y *EXIT AND LOG OFF*, para que los cambios sean actualizados.

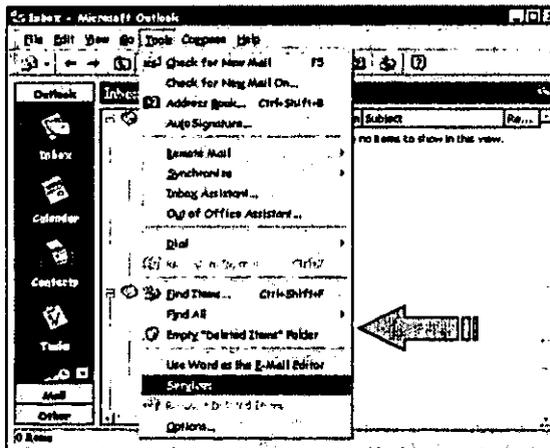


Se deberá verificar que se tengan los siguientes servicios, de lo contrario, será necesario agregarlos.

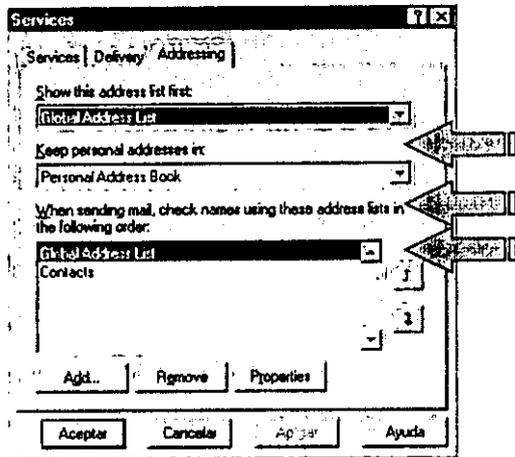


a) Definición de la lista GLOBAL ADDRESS LIST.

Seleccionar las opciones **TOOLS**, **SERVICES**, **ADDRESSING**, buscar en el primer recuadro la lista **GLOBAL ADDRESS LIST** y seleccionarla. Aplicar la misma lista en el tercer recuadro, posicionándola como la primera opción donde se verifiquen los nombres, de los destinatarios de los mensajes que se envíen. Oprimir los botones **APLICAR** y **ACEPTAR**.

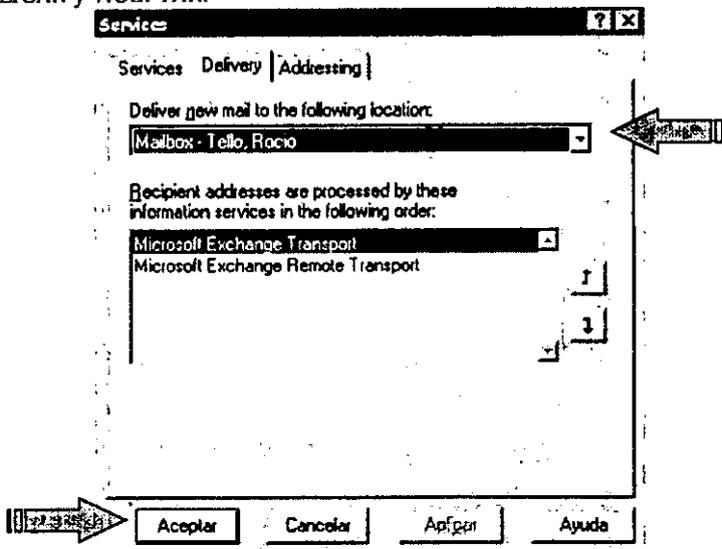


Continuación de la definición de *Global Address List*.....



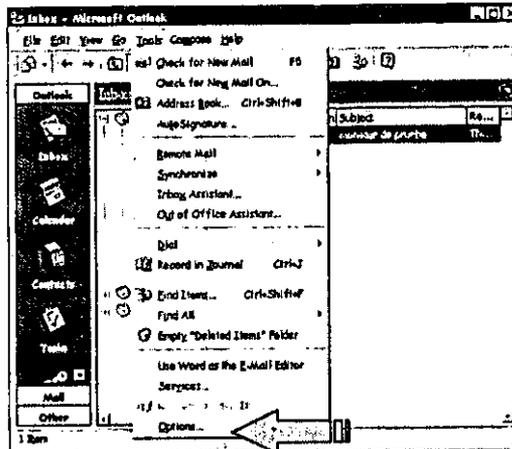
b) *Definición del MAILBOX como localidad para recibir los mensajes.*

Para configurar la localidad donde van llegar los mensajes, posicionarse en las opciones *TOOLS, SERVICES, DELIVERY*, seleccionar en el primer recuadro el *MAILBOX* del usuario. Oprimir los botones *APLICAR* y *ACEPTAR*.

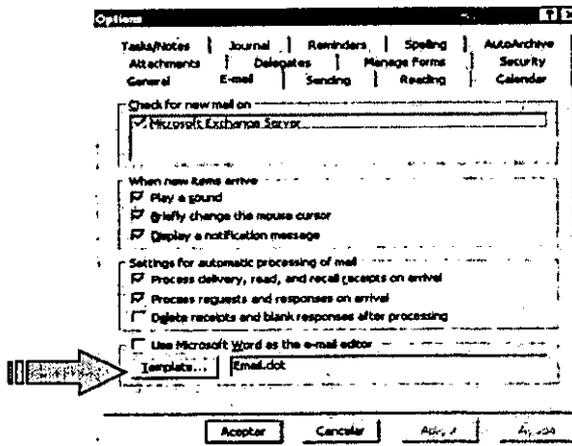


c) *Deshabilitación de WORD como el editor de OUTLOOK.*

Seleccionar las opciones *TOOLS, OPTIONS*.

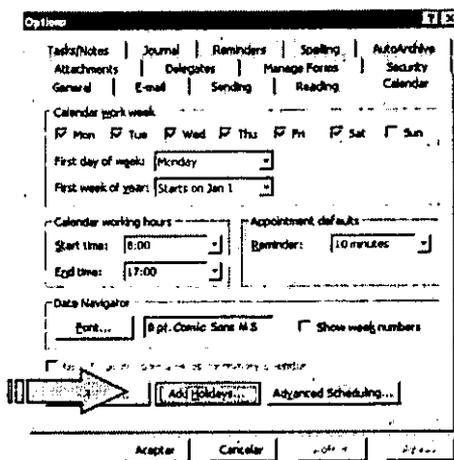


Dentro de las opciones, posicionarse en *E-MAIL* y desmarcar *USE MICROSOFT WORD AS THE E-MAIL EDITOR*, si es que estuviera Seleccionada.

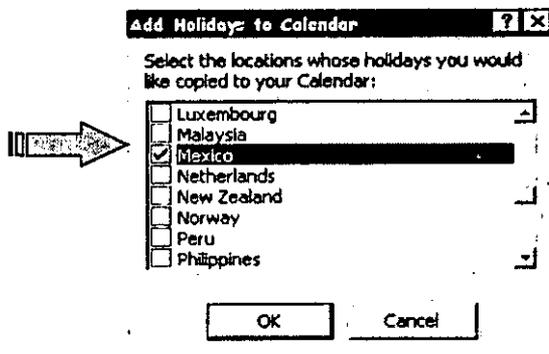


d) Agregar días festivos.

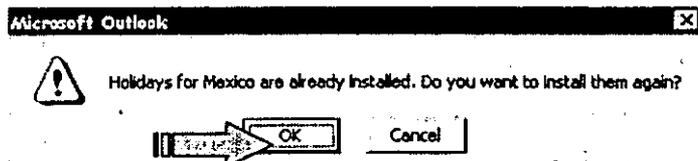
Seleccionar las opciones *TOOLS*, *OPTIONS*, *CALENDAR* y oprimir el botón de *ADD HOLIDAYS...*



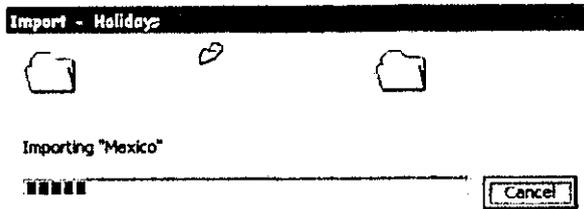
Aparecerá una lista de los países de donde se desea instalar los días festivos en el *CALENDAR*, verificar que solamente quede marcado *MÉXICO* y oprimir el botón *OK*.



NOTA: Si apareciera la siguiente pantalla, favor de darle un click al botón *OK*.

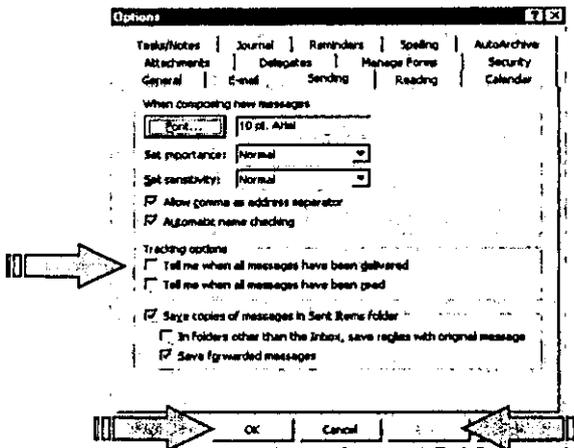


Se llevará acabo la importación de los días festivos de *MÉXICO* en el *CALENDAR*.



Deshabilitar el notificador de los mensajes cuando llegan a su destino.

Seleccionar las opciones *TOOLS, OPTIONS, SENDING* y marcar las opciones "Tell me when all messages have been delivered" y "Tell me when all messages have been read". Oprimir los botones *APPLY* y *OK*.



NOTAS:

Los folders que deben aparecer en cada sección son los siguientes:

Sección del *Mailbox*: *Calendar, Contacts, Deleted Items, Inbox, Outbox, Sent Items*.

Sección Personal *Folders*: *Contacts, Deleted Items, Inbox, Journal, Notes, Outbox, Sent Items, Tasks*.

Verificar que *TIME ZONE* sea *CENTRAL TIME (US & CANADA)*, desde *REGIONAL SETTINGS* en *CONTROL PANEL*.

8.5 Alta de Cuentas en el Correo.

8.5.1 Administración de *Windows NT*.

Administrar *Windows NT* involucra tareas diarias y después de la instalación, requeridas por *Windows NT Workstation* y *Windows NT Server*. La administración de éstas tareas se puede agrupar en cinco categorías generales.

1.- Administración de usuarios y grupos de cuentas

Esta categoría incluye la planificación, creación y mantenimiento a usuarios y grupos de cuentas para asegurar que cada usuario puede entrar a la red y acceder a los recursos necesarios.

2.-Administración de Impresión

Instalar impresoras locales o en red y resolver problemas comunes de impresión. Esto asegura que los usuarios puedan conectarse y usar los recursos de impresión fácilmente.

3.-Administración de la Seguridad

Planificar, implementar y poner en práctica políticas de seguridad para proteger los datos y recursos compartidos de la red, incluso folders, archivos, e impresoras.

4.- Monitorear eventos y recursos de la red

Planificar y llevar a cabo una política para rastrear infracciones de seguridad, y supervisar y controlar el uso de los recursos.

5.- Respalidar y restaurar datos

Planificar, programar *backups* regularmente para proteger los datos más importantes. Tener un buen plan del *backup* para asegurar su localización rápidamente y restaurar los datos críticos.

Herramientas administrativas de *Windows NT*

La siguiente tabla describe las herramientas utilizadas por *Windows NT* para la administración de la red.

<i>Windows NT Server</i>	Propósito
<i>Administrative Wizards</i>	Pasos para realizar tareas administrativas, tal como crear cuentas de usuario, crear y modificar cuentas de grupo, establecer permisos en archivos y folders, e instalar impresoras de red.
<i>Server Manager</i>	Visualizar y manejar dominios y computadoras.
<i>User Manager for Domains</i>	Maneja la seguridad para dominios, servidores miembro, y <i>workstations</i> . Si la computadora no se configuro como un controlador del dominio, se instala el <i>User Manager</i> .

<i>Windows NT Workstation</i>	Propósito
<i>User Manager</i>	Maneja la seguridad para computadoras en las cuáles se ejecuta <i>Windows NT Workstation</i> .

<i>Ambos Sistemas</i>	Propósito
<i>Backup</i>	Apoya a los datos para protegerlo de pérdidas accidentales o de hardware y fracasos de los medios de comunicación.
<i>Event Viewer</i>	Monitorea los eventos en una computadora. El <i>Event Viewer</i> proporciona información acerca de errores, advertencias, y éxito o fracaso de una tarea, tal como los esfuerzos del usuario al tratar de entrar a la red.
<i>Windows NT Diagnostics</i>	Visualiza e imprime información de la configuración del sistema, tal como información sobre la memoria, controladores y los servicios.
<i>Help</i>	Despliega información sobre temas de <i>Windows NT</i> . La ayuda se puede acceder desde el menú <i>Start</i> o presionando F1.

8.5.1.1 Alta de usuarios.

Una cuenta de usuario se define con características únicas y tiene autoridad para habilitar el *log* sobre el dominio para poder acceder a los recursos de la red.

Cada persona que regularmente utilice la red, deberá contar con una cuenta. Se puede utilizar la cuenta de usuario para el control de los accesos de usuarios al dominio o a la computadora. Por ejemplo, se puede limitar el número de horas a un usuario para poder firmarse al dominio.

Tipos de Cuentas de usuario

Existen tres tipos de cuentas de usuario, éstas son creadas cuando las cuentas se dan de alta. La siguiente tabla describe los tipos de cuentas de usuario:

Cuenta de Usuario	Descripción
Cuenta para usuario	Esta cuenta habilita al usuario a firmarse sobre la red y, con los permisos apropiados, acceder a los recursos de la red. Éstas cuentas contienen información acerca del usuario, incluyendo el <i>Username</i> y el <i>password</i> .
Cuenta <i>Guest</i>	La construcción de la cuenta <i>Guest</i> es utilizada para tener usuarios ocasionales que se firman y accesan los recursos desde una computadora local. Por ejemplo, un empleado necesita acceder a la computadora por un corto tiempo, para esto puede utilizar la cuenta <i>Guest</i> . La cuenta <i>Guest</i> es deshabilitada por <i>default</i> .
Cuenta de Administrador	La construcción de la cuenta de Administrador es utilizada para manejar todas las computadoras y la configuración del dominio. Esta cuenta es utilizada para ejecutar todas las tareas; como son: crear o modificar cuentas de usuarios o grupos de cuentas; manejar la seguridad, crear configuraciones de impresión y asignar permisos y derechos para el acceso de recursos.

Nombres Convencionales

Los nombres convencionales establecen como los usuarios se identifican sobre la red. Una convención consistente de nombres permitirá a los usuarios recordar sus *usernames* y localizarlos en las listas.

Para determinar el nombre convencional, se requiere considerar los siguientes puntos:

- Los *usernames* deben ser únicos. El dominio de la cuenta de usuario debe ser único para el dominio. Las cuentas de usuario locales deben ser únicas para la computadora local.
- Los *usernames* pueden contener 20 caracteres (entre mayúsculas y minúsculas) exceptuando los siguientes caracteres: “ / \ [] : , + * ? < > . Se puede utilizar una combinación de caracteres especiales y alfanuméricos en el nombre convencional para ayudar a identificar usuarios.
- Si se tiene un gran número de usuarios, los nombres convencionales deberán considerar nombres duplicados. Por ejemplo, dos usuarios se llaman Pedro. Algunas sugerencias para manejar nombres duplicados son:
 - 1) Utilizar el primer nombre hasta la última inicial, y entonces adicionar letras del apellido para hacer los nombres duplicados únicos. Por ejemplo, para Pedro Pérez, uno sería PedroP y el otro PedroPe.
 - 2) Otro caso sería adicionando números, por ejemplo: Arturo7A, Arturo8A.
- En grandes organizaciones, se requiere identificar usuarios temporales por su cuenta de usuario. Por ejemplo, para identificar usuarios temporales, se puede utilizar una ‘T’ y seguido el identificador del usuario. Por ejemplo, T-Arturo8A.

Passwords

Para protección de un dominio o una computadora, todas las cuentas de usuario requieren de un *password*. Se deben considerar las siguientes líneas como guía para asignar passwords:

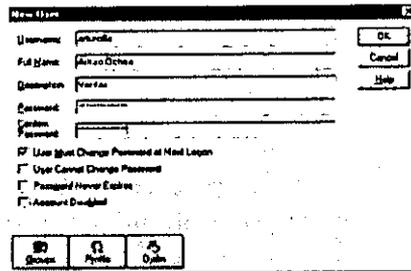
- Asignar siempre el *password* a la cuenta del Administrador para prevenir el intento de acceso a usuarios no autorizados.
- Determinar quién llevara el control del *password*. Se pueden asignar *passwords* únicos a usuarios para prevenir que otros usuarios los cambien, o se puede permitir autoridad a usuarios para acceder otros *passwords* la primera vez que sé accesen. En la mayoría de las redes, los usuarios son los que controlan sus *passwords*.
- Determinar la expiración de estos. Se deberá contemplar éste punto, especialmente, para las cuentas de usuarios de empleados temporales para expirar los *passwords* a la finalización de su contratación.
- Educar a usuarios sobre la forma de proteger sus *passwords*:
 - 1) Evitar el uso de asociaciones obvias como por ejemplo: nombres de la novia (Ej. SUCMGEY).
 - 2) Utilizar *passwords* largos. Éstos pueden tener 14 caracteres de longitud.
 - 3) Utilizar mayúsculas y minúsculas intercambiadas. Esto hace al *password* único. Por ejemplo, el *password* SeCret es diferente a secret.

Horarios de Acceso y Restricciones de Trabajo

Si se requiere determinar el tiempo de acceso de un usuario a la red y el horario en que se pueda firmar, se puede determinar el horario de acceso y las restricciones de trabajo consideradas en los siguientes puntos:

- Los horarios de acceso deben ser aplicados a usuarios que sólo requieran accesos en períodos de tiempo específicos. Por ejemplo, sólo se permite el acceso a usuarios nocturnos en ese tiempo.
- A usuarios que requieran firmarse hacia otras computadoras cuando existen datos importantes en estas.

Creación de Cuentas de Usuario



Para crear una cuenta de usuario se debe seguir el siguiente procedimiento:

- 1.- Iniciar el *User Manager for Domains* (o el *User Manager en Windows NT Workstation*).
- 2.- Sobre el menú de *User*, dar click a *New User*.

3.- Configurar las siguientes opciones:

<i>Username</i>	Es un nombre único basado en el nombre convencional. Es un elemento requerido.
<i>Full name</i>	Es el nombre completo del usuario y sirve para identificar que persona es la dueña de la cuenta. Es un elemento opcional.
<i>Description</i>	Es la descripción del ambiente o área del usuario. Esto puede ser una clasificación de trabajo, departamento o una ubicación de la oficina. Es opcional.
<i>Password</i>	Es el <i>password</i> para tener seguridad, pero solo si se debe controlar este. No se debe tener asignado un <i>password</i> a una cuenta; sin embargo, para mayor seguridad se deberá, siempre, realizar las modificaciones al <i>password</i> cuando es el primer acceso. Nota que el <i>password</i> no es desplegado. Se representa por una serie de 14 asteriscos para introducir el <i>password</i> , correspondiendo a la longitud del mismo.
<i>Confirm Password</i>	Aquí se tecléa el <i>password</i> por segunda vez para determinar que este se introdujo correctamente. Esto es requerido cuando se asigna un <i>password</i> .

4.- Teclee *Add* y la cuenta de usuario es creada. Después de presionar *Add*, todo lo que se escribió en la pantalla desaparece. Esto permite que se pueda volver a crear otra nueva cuenta.

8.5.2 Administración en Exchange.

Existen diversos métodos para administrar un servidor de *Microsoft Exchange*, algunas de éstas herramientas son las mismas que utiliza el *Windows NT*.

Programa de Administración

El programa de administración de *Microsoft Exchange* (*Admin.exe*) es una aplicación que se ejecuta sobre *Windows NT* y permite que el administrador pueda hacer lo siguiente:

- Configurar la organización entera, incluyendo los *sites* y todos los servicios.
- Monitorear toda la organización.
- Realizar una administración *single-seat*.
- Establecer los permisos para todos los usuarios.

Los componentes del servidor de *Microsoft Exchange* se ejecutan como los servicios de *Windows NT*, a continuación mencionamos algunas de las herramientas que usa tanto *Windows NT* como el *Microsoft Exchange* para administrar sus recursos:

- Servicios/ Panel de Control.
- Visualizador de Eventos (*Event Viewer*).
- Administrador del Servidor (*Server Manager*).
- Monitor de rendimiento (*Performance Monitor*).
- Administrador de Tareas (*Task Manager*).
- Editor de Registros (*Registry Editor*).

Servicios/ Panel de Control

El administrador puede utilizar esta opción, para verificar el estado de los servicios de servidor, así como, activar, detener o poner en pausa cualquier servicio.

Visualizador de Eventos

Monitorea los eventos en una computadora. Proporciona información acerca de errores, advertencias, éxitos o fracasos de tareas.

Administrador del Servidor

Sólo el administrador puede hacer:

- Administrar los dominios.
- Ve las propiedades y administra los servidores, viendo cuáles son los directorios y recursos compartidos, tanto en servidores locales como remotos.
- Ve y administra los directorios compartidos en los servidores locales y remotos.
- Permite enviar mensajes a los usuarios desde esta opción, como un mensaje del administrador de *Exchange*.
- Permite iniciar o detener servicios de forma remota.

Monitor de Rendimiento

Permite visualizar la actividad del procesador al realizar algunas tareas, y el estatus de los servicios.

Administrador de Tareas

Se usa como un monitor y control de programas de los procesos que se ejecutan en la computadora, muestra cuanta memoria esta usando el CPU, los procesos que se están ejecutando, entre otros.

Editor de Registro

Se utiliza para verificar o modificar la configuración de la información almacenada en un registro, muestra la información en tres formas y pueden ser modificadas por el administrador.

Microsoft Exchange tiene una ventana, a la cual se le llama ventana de administración, donde se pueden apreciar los servidores que componen a la organización, sus *sites* y las configuraciones que tienen.

Esta ventana nos muestra la organización jerárquica, puede mostrarnos muchas ventanas de administración, pero es una por cada servidor. Cuando un servidor es seleccionado, el nombre del servidor se despliega en la barra de título de la ventana.

La ventana de administración tiene dos partes principales, como se aprecia en la siguiente (Fig.8.3).

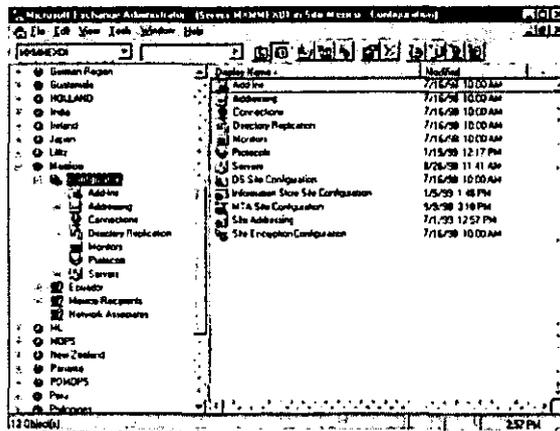


Fig. 8.3 Ventana de Administración.

- *Container panel* .- El panel izquierdo despliega el contenido de los objetos que están abiertos.
- *Contents panel*.- En el lado derecho de la ventana se despliegan los objetos que están en cada contenedor.

Tipos de Objetos

Tanto los *sites* como los servidores se muestran en la ventana de administración como objetos:

- Contenedores de objetos .- éste puede contener otros objetos y su uso es para varios grupos.
- Objetos hoja.- éstos objetos no contienen otros objetos y generalmente son los *mailboxes* o los conectores

El programa de Administración puede ser utilizado por el usuario y que sea conveniente a las necesidades de organizaciones particulares. La colocación para las vistas y columnas están determinadas en las bases para usuarios. El resto de las colocaciones son universales.

Opciones para los Usuarios

El siguiente cuadro muestra las opciones del contorno personalizado que aporta el Programa de Administración

Opciones	Propósito
Vistas	Para seleccionar el tipo de objetos dentro de un destinatario que serán vistos, tales como <i>mailboxes</i> , listas de distribución (<i>DLs</i>), recipiente de usuarios, folders públicos y recipientes ocultos.
Columnas	Especifica la columna que debe observarse y el orden en que debe hacerlo. Permite la clasificación de los datos mostrados. No todas las columnas pueden ser seleccionadas. El sub menú <i>Sort By</i> (en la vista de menús) enlista que columna puede ser seleccionada.
Auto-nombrarse	Especifica como mostrar los nombres o los alias de forma automática cuando se crea un nuevo <i>mailbox</i> . Las opciones incluyen: ninguno, último primero, último, primeras últimas iniciales y usuario. La colocación por default para los alias es primer nombre y última inicial.
Permiso de Colocación	Especifica la colocación de las vistas de permisos de colocación para los objetos
Colocación de cuenta de los dominios	Especifica que dominio <i>Windows NT</i> será utilizado cuando inicie la información de <i>Windows NT</i> en las páginas apropiadas.
<i>mailbox</i>	Para borrar una cuenta primaria de <i>Windows NT</i> cuando se borra un del servidor de <i>Microsoft Exchange</i> . Para buscar cuentas <i>Windows NT</i> ya registradas al momento de crear un <i>mailbox</i> del servidor de <i>Microsoft Exchange</i> .

Personalizar la Barra de Herramientas.

Una de las nuevas características del programa de Administración es la adición de una barra de herramientas que puede ser personalizada. Algo mejor que tener que navegar a través de varios menús con diferentes términos para los comandos utilizando frecuentemente por el administrador, éstos comandos pueden adicionarse directamente desde la barra de herramientas con sólo oprimir la tecla adecuada.

Vistas de las Libretas de Direcciones.

Las vistas de las libretas de direcciones son contenedores virtuales que permiten al administrador tener agrupadas las carpetas de objetos y organizadas de manera lógica basándose en un directorio que presenta las mismas características.

8.5.2.1 Alta de Cuentas

El administrador es el encargado de crear y manejar los *mailboxes*, las listas de distribución, las carpetas de los usuarios, y los folders públicos.

Mailboxes

Es un espacio en el servidor de *Microsoft Exchange* en el cual se entrega el correo electrónico. El administrador crea un *mailbox* para cada usuario.

Listas de Distribución (*DL's*)

Las *DL's* es una lista de recipientes creados para acelerar el correo de una gran cantidad de mensajes y otra información.

Carpetas de los Usuarios

Una carpeta de usuario es un indicador de una lista foránea o carpetas que se encuentran fuera de los mensajes de la organización, tales como las carpetas de *Internet*, con el *SMTP*, las direcciones personalizadas de los usuarios, son de gran ayuda en la identificación de carpetas y tienen direcciones de correo alfanuméricas y que no son fácilmente reconocidas, esta es una característica muy importante, ya que las direcciones de *e-mail* inusuales, procedentes de fuentes externas, aparecen regularmente en ambientes de negocios.

Folders Públicos

Este tipo de folder es un depósito para diferentes tipos de información tales como los mensajes de correo o los archivos, que pueden ser compartidos por una gran cantidad de usuarios, los folders públicos forman las bases para todo tipo de aplicaciones del usuario tales como; pizarras de boletines, foros de discusión, sistemas de seguimiento de los usuarios y más.

Creando y Configurando *Mailboxes*

El servidor de *Microsoft Exchange* presenta herramientas y características que son utilizadas para crear y configurar *mailboxes*, con el *Microsoft Windows NT User Manager*, un *mailbox* puede ser creado al mismo tiempo que una cuenta de *Windows NT*, de esta manera si una *mailbox* es creada a partir del Programa de Administración de *Microsoft Exchange* o a partir de *Windows NT* Manejador de Dominios, la interface es la misma, el programa de Administración de *Microsoft Exchange*, incluye extractos e importantes características de usuarios migrantes ya existentes como lo son *Novell Netware*, *LAN Manager* y *Windows NT Networks*.

Creación de *Mailboxes* utilizando el *User Manager* de *Windows NT*

Antes de que el servidor de *Microsoft Exchange* pueda ser utilizado por clientes, el administrador debe de crear los *mailboxes* que estarán asociados con las cuentas de los usuarios de *Windows NT* y de forma opcional deberá de configurar para cada usuario los *mailboxes* con sus respectivos atributos, como el poder mostrar el nombre, los permisos y opciones como el tamaño de los mensajes y el tamaño máximo de almacenamiento de cada usuario.

La herramienta del Manejador de Dominios es el que administra la seguridad de las cuentas en la base de datos en los dominios de *Windows NT*.

Cuando se instala el programa de administración de *Microsoft Exchange*, se instala el Manejador de Dominios el cual tiene la extensión, *Mailumx.dll*, ésta librería dinámica proporciona la liga entre el Manejador de Dominios y las características de la página del *mailbox* del programa de Administración del *Microsoft Exchange*.

Creación y Configuración de *Mailboxes* usando el Programa de Administración

El programa de administración de *Microsoft Exchange* (*Admin.exe*) es una aplicación basada en *Windows NT* lo cual permite al administrador configurar, manejar y monitorear a la organización de *Microsoft Exchange*.

Para crear un *mailbox*, se necesita usar el Programa de administración de *Microsoft Exchange* (Fig. 8.4) se selecciona de la barra de menús, Archivo, y se da un click donde dice Nuevo *Mailbox*.

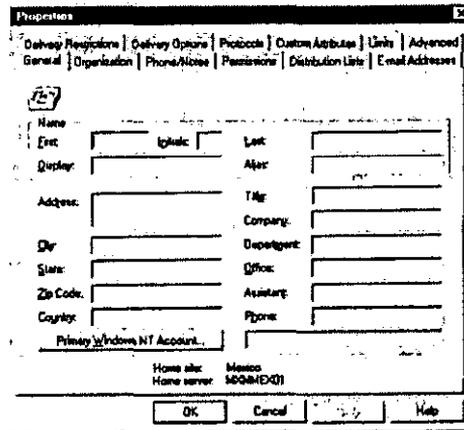


Fig. 8.4 Creando y configurando *Mailboxes* usando el programa de administración.

Configuración del *Mailbox* y Características de las Páginas

Para la configuración del *mailbox* se requiere personalizar las páginas. En la siguiente lista se describen las propiedades de las páginas.

Propiedad de la Página	Propósito
General	Almacena la información básica como es el nombre, dirección, compañía, sería la cuenta del usuario en <i>Windows NT</i> .
Organización	Almacena la información del dueño de la cuenta y recibe los reportes directos. Esta información forma parte de la libreta de direcciones
Avanzados	Deja a un lado el nombre del directorio, fija el tamaño que ocupará el <i>mailbox</i> , fija los niveles del directorio de replicación, y determina cualquiera de los <i>mailbox</i> que aparecerán en la libreta de direcciones.

Creación de Tareas del *Mailbox*

Especificando el Servidor Local (*Home Server*)

El servidor local es aquel que contiene los *mailboxes* de los usuarios, éste servidor se especifica cuando el *mailbox* se crea haciendo clic en *Home Server*. Si el servidor *home* no se ha especificado, el programa de administración, asume que el servidor *home* para esa nueva cuenta será el servidor donde se esta ejecutando el programa de administración.

Asociando un *Mailbox* con las Cuentas de *Windows NT*

Cada *mailbox* deberá estar asociado con un usuario o grupo de usuarios o cuentas de *Windows NT*. Un usuario de *Windows NT* o grupo de usuarios pueden estar asociados con uno o varios *mailboxes*. Cuando se crea un *mailbox*, el programa de administración buscará en el dominio de *Windows NT* la cuenta con el mismo nombre, si se llegará a encontrar, el administrador asociará esta cuenta con el *mailbox*.

Seleccionando *Advanced Settings*

Las características de esta propiedad *Advanced*, le presenta al administrador una variedad de grandes opciones, a continuación se listan, las más utilizadas

Propiedad	Propósito
<i>Message Size</i>	Limita el tamaño de los mensajes que se envían entre usuarios
<i>Storage Limit</i>	Deja a un lado las configuraciones de <i>default</i> en el almacenamiento de información para la información privada, o restringe el almacenamiento de la información privada usando el <i>mailbox</i> .
<i>Hide Mailbox</i>	Se encarga de que éste <i>mailbox</i> se oculte en la lista global de direcciones.
<i>Trust Level</i>	Especifica que recipientes están usando el correo de <i>Microsoft 3.x</i> durante la sincronización de directorios con sistemas de correos foráneos.

Creación y Configuración de las Listas de Distribución

El administrador crea las listas de distribución (Fig. 8.5) para habilitar a los usuarios para enviar correos para los diferentes grupos, el crear las listas de distribución implica varias tareas.

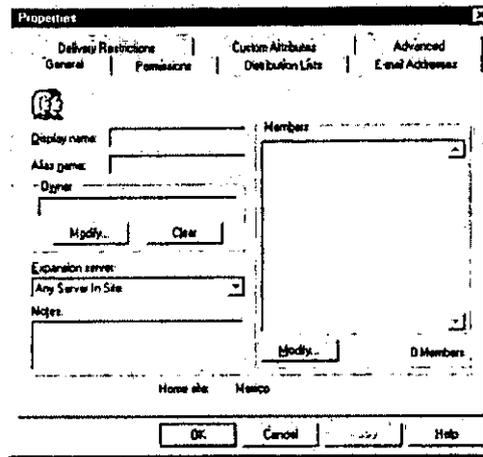


Fig. 8.5 Configuración de las Listas de Distribución (DL's).

Designación y Expansiones del Servidor

Cuando un usuario del *site* envía un mensaje a las listas de distribución, el servidor de *Microsoft Exchange* expande la lista, resuelve el nombre de los recipientes en la lista, y determina la ruta más eficiente para hacer llegar el mensaje.

Especificando la Lista de Distribución Propia

En la creación de una lista de distribución por default se le asigna a un dueño. Éste dueño puede modificar a los miembros que usan el *Microsoft Exchange* o el cliente de *Microsoft Outlook*, teniendo todos los permisos del administrador del *Microsoft Exchange*.

Seleccionando Características Avanzadas de las Listas de Distribución

Propiedad	Propósito
<i>Message Size</i>	Limita el tamaño del mensaje que se enviará a las listas de distribución.
<i>Allow Out of Office Messages to Originator</i>	Auto envía los mensajes de salida
<i>Hidden Distribution List</i>	Oculto las listas de distribución para que no aparezcan en la libreta de direcciones
<i>Trust Levels</i>	Determina cualquier información de la lista de distribución que deba replicarse, a otros sistemas de correo durante la sincronización del directorio.
<i>Hide Membership</i>	Oculto a los miembros de la lista de distribución

Creando y Configurando los Recipientes de los Clientes

Es un recipiente fuera del *site* de envío o de la organización y *Microsoft Exchange* (Fig. 8.6) la representa como la lista global de direcciones.

The screenshot shows the 'Propiedades' dialog box with the 'Listas' tab selected. The fields are as follows:

- Name:** First, Last, Display, Alias
- Address:** Address, City, State, Zip Code, Country
- Other fields:** Title, Company, Department, Office, Assistant, Phone
- Primary Windows NT Account:** [Empty]
- Home site:** Mexico
- Home server:** M00MEX01

Fig.8.6 Configurando los recipientes de los clientes.

Especificando el tipo de Recipiente

Cuando se crea un nuevo recipiente para un cliente, se especifica el tipo de la dirección de correo electrónico, éste aparece en una lista global de direcciones y puede ser direccionada o añadida a una lista de distribución. Se utiliza el Programa de Administración para crear un recipiente para clientes desde otros sistemas de mensajes.

Configurando características avanzadas en los recipientes de clientes

Propiedad	Propósito
<i>Message Size</i>	Limita el tamaño del mensaje enviado a un recipiente de un cliente en particular.
<i>Allow Rich Text</i>	Permite manejar formatos como poner negrillas, color. Permite enviar archivos (<i>attachments</i>)
<i>Hide Recipient</i>	Oculta el recipiente del cliente para que no aparezca en la libreta de direcciones.

Propiedades de la página en un recipiente de un objeto común.

Listas de Distribución.

Se usa la propiedad *Distribution List* para especificar las *DL's* con su respectivo recipiente. Cuando el recipiente pertenece a una lista de distribución, el recipiente recibirá todos los mensajes de la lista de distribución.

Direcciones de Correo Electrónico.

Se usa la propiedad *E-mail Addresses* para crear o modificar claves de correo electrónico de los objetos. Si el alias es cambiado por el usuario, la dirección de correo no se podrá actualizar automáticamente, y se deberá hacer en forma manual.

Restricciones de Entrega.

Se usa la propiedad *Delivery Restrictions* para restringir los mensajes entregados en todos los recipientes:

Accept Messages From.- Crea una lista de todos aquellos a los que acepta sus mensajes.

Reject Messages From.- Crea una lista de todos aquellos que no aceptan sus mensajes.

Atributos del Cliente

Es una característica particular la cual esta asociada con el objeto del recipiente. Por ejemplo, las páginas de propiedades contienen atributos predefinidos como el *mailbox*, nombre, dirección, ciudad, estado y código postal.

Se pueden definir 10 atributos adicionales en el objeto contenedor del *site* y asignar éstos objetos a los recipientes individuales, éstos atributos proporcionarán mayor información acerca de los objetos de ese recipiente que se especificará en la organización, podría ser un número de identificación de los usuarios.

Manejo de los Recipientes de Objetos

Empleo de Plantillas para la creación de *Mailboxes*:

Una plantilla es un *mailbox* que se crea para ser usada de modelo para nuevos *mailboxes*. Su configuración puede ser copiada a unos nuevos, o se puede crear utilizando el *Migration Wizard* a través del comando *Directory Import* o el comando *Duplicate*, duplicar una plantilla de *mailbox* puede crear un *mailbox* sencillo o un gran número de *mailboxes* con propiedades preconfiguradas.

Encontrando un Recipiente

Para encontrar un recipiente particular, se utiliza el comando *Find Recipients* (Fig. 8.6) de la opción de *Tools* en el programa de administración, éste comando puede localizar recipientes de cualquier parte de la organización basados en una variedad de criterios diversos como pueden ser por el nombre, apellido, *site*, etc.

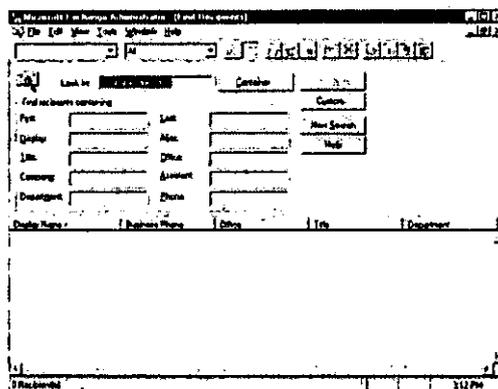


Fig. 8.6 Utilizando el comando *Find Recipients*.

Moviendo y limpiando un Mailbox

Con sólo dar un click en la pantalla de contenidos y en la opción *Tools* de la barra de menús, seleccionando *Move Mailbox* (Fig. 8.7) un *mailbox* puede ser movido a otro servidor o dentro de un mismo *site*, en cualquier momento, el usuario es movido, el perfil del cliente es automáticamente actualizado y se localiza en el servidor correcto.

Cuando los *mailboxes* se mueven a un servidor nuevo, el tamaño del contenido del *mailbox*, en el servidor destino podría incrementarse por que las copias individuales de los mensajes simples son creadas para cada *mailbox* que se ha movido en el almacén de información privada, en el servidor destino. Los *mailboxes* también pueden ser movidos utilizando el *Home Server* en la propiedad *Advanced* en el *mailbox* del usuario.

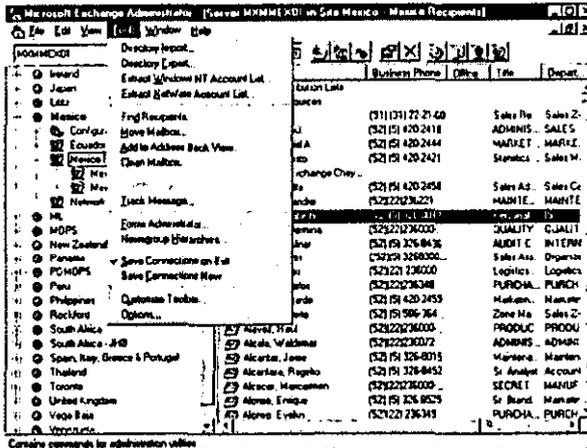


Fig. 8.7 Utilizando la opción *Move Mailbox*.

Como se muestra en la figura anterior, para limpiar un *mailbox*, primero se debe dar un click en el menú *Tools* de la barra de herramientas y seleccionar *Clean Mailbox*, se desplegará una ventana de verificación solicitando la confirmación ya que todo el correo y los datos existentes en el *Mailbox* serán borrados.

8.6 Desinstalación del software de correo anterior.

8.6.1. Administración de Windows NT.

Administración del ambiente de trabajo de usuarios.

User Profile

Cuando un usuario se firma por primera vez a *Windows NT* - basado en clientes, un *User Profile* es creado por *default* para éste usuario. El *User Profile* define la apariencia de un ambiente de usuario de escritorio y los usuarios de red y conexiones de impresora. Un *User Profile* también puede ser actualizado para restringir que interface vean los usuarios y que tienen disponible usar cuando ellos se firman en la red. Por ejemplo, un administrador puede remover la carpeta de herramientas administrativas para prevenir que cualquier usuario modifique la configuración

El *User Profile* contiene todos los elementos de definición de un usuario para el entorno de trabajo de la computadora corriendo bajo *Windows NT*. Todos los elementos para especificaciones de usuarios se guardan automáticamente en la carpeta *Profiles* (C:\Winnt\Profiles).

8.6.1.1 Definiciones de Logon Script

Logon Scripts

Estos se utilizan para usuarios que necesitan firmarse desde un ambiente que no es *Windows NT*-basado en clientes (*LAN Manager*, *MS-DOS*, *Windows for Workgroups* y *Windows 3.x*), un *Logon Scripts* puede ser utilizado para configurar a los usuarios de la red y las conexiones de impresión. No puede ser utilizado para definir la apariencia del ambiente de escritorio de los usuarios o configurar *hardware*, como por ejemplo la resolución de la pantalla de video.

Un *Logon Script* es un proceso *batch* (.bat o .cmd) o un archivo ejecutable (.exe), el cual se ejecuta automáticamente cuando el usuario se firma en la red.

Roaming User Profiles

Roaming User Profiles proporcionan al usuario el mismo ambiente de trabajo, no importa en que *Windows NT* para computadora entre con su cuenta. Éste es almacenado centralmente sobre el servidor de la red. Es posible especificar un *Roaming User Profile* para una cuenta de usuario.

Se puede especificar uno de los dos siguientes *Roaming User Profiles*:

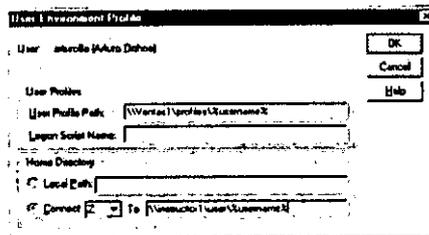
- *Roaming Mandatory User Profile*.- éste es un *User Profile* preconfigurado que el usuario no puede modificar y puede ser asignado a varios usuarios. Esto principalmente es para que, cambiando un sólo *Profile*, el administrador pueda realizar un cambio radical al ambiente de computadoras cliente.

Se puede utilizar éste tipo de *Profile* para asignar características comunes a todos los usuarios que requieren idéntica configuración de su escritorio.

- *Roaming Personal User Profile*.- éste es un *User Profile* que el usuario puede modificar; esto principalmente sucede cuando el usuario termina su sesión, el *User Profile* es actualizado para incluir algunas modificaciones realizadas por el usuario. Cuando el mismo usuario vuelve a firmarse, el *Profile* se carga como se guardo la última vez. Si se utiliza el *Roaming Personal User Profile*, cada usuario deberá ser asignado a un *Profile*.

Definir un ambiente de usuario

Usa la caja de dialogo *User Environment Profile* para introducir las rutas para el *User Profile*, *logon script*, y el *home folder*. Debes seguir los siguientes pasos:



1.- En la caja de dialogo de *New User* (o *User Properties*), da click al botón *Profile*.

2.- En la caja de dialogo *User Environment Profile*, se debe configurar las siguientes opciones.

User Profile Path La ruta para la carpeta del *User Profile*: Para *User Profiles* personales, teclear:

`\\server_name\profile_share\%username%`

Para *mandatory user profiles*, teclear

`\\server_name\profile_share\profile_share`

Logon Script Name El nombre del *Logon script*. Puedes usar la ruta de usuarios de computadoras locales o una ruta *UNC* para compartir folders en un servidor de red.

Home Directory La ruta del *home folder*. Puedes usar la ruta de usuarios de computadoras locales. Por ejemplo:

`\\server_name\script_share\script_name`

Para especificar una ruta de red, se selecciona **Connect** y una letra para la unidad de disco. En la caja **To**, teclear un ruta. Un *UNC* comienza con dos dígitos con dos diagonales invertidas seguidas por el nombre del servidor y después el nombre de la carpeta compartida. Por ejemplo:

`\\server_name\users\%username%`

Antes de poder especificar una locación de red, debe existir una carpeta sobre el servidor de red compartida.

8.6.2 Procedimientos Automáticos de Desinstalación.

Una vez finalizado el proceso de instalación se dio un tiempo de espera a los usuarios mientras se definía la estrategia de desinstalación del *software* anterior en las *PC's*, éste tiempo de espera se considero para darle tiempo a los últimos usuarios migrados de revisar sus mensajes y determinar el procedimiento de migración hacia el nuevo sistema de correo o eliminarlos.

Se realizó la instalación del *software* de *Outlook* en todos los equipos *PC* y *Laptop* de la compañía incluyendo foráneos en el tiempo límite.

Debido a que todos los usuarios en el momento de firmarse a la red ejecutan su *logon script*, se genero un procedimiento automático *bat*, que verificara en todos los equipos la existencia del *software* de correo anterior y una vez identificado lo eliminara totalmente.

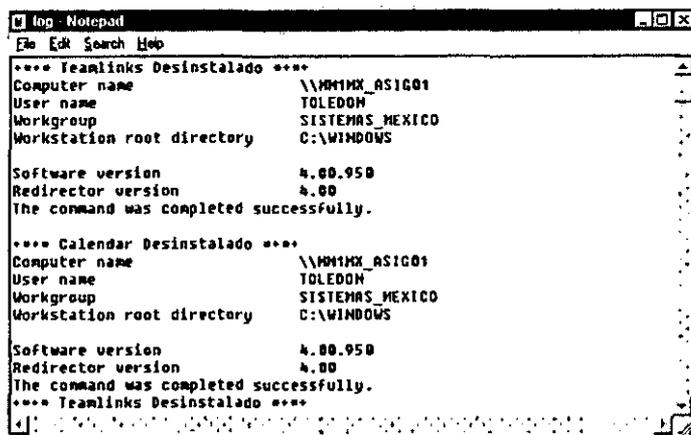
Antes de ejecutar éste procedimiento en el *logon script* se le notificó a todos los usuarios para que considerarán que una vez ejecutado, desaparecería todo su correo anterior.

Para realizar el proceso de desinstalación se generó un archivo *bat* con la información necesaria para identificar los directorios de *TeamLinks* y *Calendar Manager*, los cuáles debían ser desinstalados.

Se configuro el *Logon script* de los usuarios para ejecutar éste procedimiento en un día específico y eliminar en forma masiva el *software*.

El procedimiento de desinstalación utilizado es el siguiente archivo *Bat* (Fig. 8.8) el cual se encargaba de verificar si el *software* se encontraba instalado en la *PC* o ya había sido eliminado con anterioridad, el procedimiento trabajaba con banderas de control que permitían identificar si el procedimiento ya se había ejecutado en alguna *PC*.

El archivo de *log* generado (Fig. 8.9) muestra información de la desinstalación, los puntos más importantes a considerar eran que incluía el nombre de la computadora donde se ejecutó el procedimiento, la clave del usuario firmado a la red y el *Workgroup* al que pertenece el usuario, además de adicionar la leyenda "****Desinstalado****".



```
log - Notepad
File Edit Search Help
**** Teamlinks Desinstalado ****
Computer name      \\MM1MX_ASIG01
User name          TOLEDDN
Workgroup          SISTEMAS_MEXICO
WorkStation root directory C:\WINDOWS

Software version   4.00.950
Redirector version  4.00
The command was completed successfully.

**** Calendar Desinstalado ****
Computer name      \\MM1MX_ASIG01
User name          TOLEDDN
Workgroup          SISTEMAS_MEXICO
WorkStation root directory C:\WINDOWS

Software version   4.00.950
Redirector version  4.00
The command was completed successfully.
**** Teamlinks Desinstalado ****
```

Fig.8.9 Archivo *log* generado, en el cual muestra información de la desinstalación.

ESQUEMA DE RESPALDO Y RESTAURACIÓN DE INFORMACIÓN

Para poder realizar un *backup* o recuperación de las bases de datos de *Exchange*, es necesario entender dónde se encuentran, cómo pueden ser respaldadas y cómo pueden ser restauradas.

Se deben respaldar dos tipos de datos:

Datos Estáticos.

- El Sistema Operativo, que en éste caso es *Windows NT* con sus respectivos parches o *service packs*.
- El paquete de *Exchange (Software)*
- El *software* de soporte adicional que se encuentre instalado en el servidor, como *software* de *backup*, administración o monitoreo.
- El *software* de aplicaciones que se encuentre instalado en la máquina, como *Mailbox Agents*, o *software* de *Workflow*.

Datos Dinámicos.

- Bases de datos de *Exchange* y Archivos de soporte, como Bases de datos de Directorios e *Information Store*, Archivos de *log* Transaccionales y archivos apuntadores.
- La base de datos de *MTA*.
- Los archivos de *log* de monitoreo de mensajes (Track).

Particiones de un servidor dedicado para *Exchange Server*.

Se especifican tres áreas de disco.

- El Disco del Sistema .– Soporta *Windows NT*, Archivos de *SWAP*, otros *software* de Aplicación, algunas veces, archivos dinámicos de *Exchange* como áreas de trabajo o bases de datos de *MTA*:

Ejemplo: C:\<System Disk>

- El Disco de Archivos de *Log* Transaccionales .– Bases de datos de archivos de *log* de transacciones. Éste disco es pieza fundamental del *performance*:

Ejemplo: D:\<Transaction Logs>

- Una partición extendida para Bases de Datos .- Frecuentemente trabaja sobre un arreglo de tolerancia a fallas *RAID 5* para proveer la continuidad del servicio:

Ejemplo: E:\<Exchange Databases>

La distribución de algunos de los principales componentes a través de éstos directorios es:

DESCRIPCIÓN	UBICACIÓN	ARCHIVOS
Base de Datos de Directorios	E:\EXCHSRVDSADATA	DIR.EDB
Base de Datos del <i>Information Store</i>	E:\EXCHSRVMDATABASE	PRIV.EDB, PUB.EDB

Otros componentes.

El *backup* y el *restore* de un servidor de *Exchange* es un proceso complejo que involucra una serie de componentes que deben trabajar en forma conjunta.

Particionar un servidor de *Exchange* es normalmente benéfico para incrementar el *performance* y realizar la recuperación de archivos. Con los sistemas de *backup* apropiados y la estructura de directorios adecuada se pueden recuperar los datos de usuario aún perdiendo una partición.

- Si el disco de sistema es dañado, los archivos de *log* transaccionales podrían recuperar la información de usuarios dado que éstos se encuentran en otro disco.
- Si el disco donde se encuentran los archivos de *log* transaccionales es dañado, no se pierde información de los usuarios a menos que se dañe la base de datos que se encuentra en otro disco.
- Si la base de datos es dañada, se tendría que restaurar de un respaldo y dado que los archivos de *log* están en otro disco, automáticamente se regeneraría la información de usuarios.

Los puntos explicados anteriormente incrementan la seguridad de la información, pero es necesario entender la relación entre ellos.

Métodos para Realizar un *Backup Online* y *Offline*.

Backup Online.

Para realizar un *backup Online* se requiere que los servicios *Information Store* y *Directory Service* de *Exchange* se encuentren corriendo.

Backup Offline.

Para realizar un *backup Offline* se requiere que todos los servicios de *Exchange* sean detenidos antes de lanzar el respaldo. Todos los archivos de *Exchange* son copiados al drive especificado incluyendo el *Windows NT Registry*.

Exchange instala una versión de *NTBACKUP* que permite realizar el respaldo de las bases de datos de *Exchange* en forma *Online* y restaurarlas desde cinta. Se encuentran también disponibles por otros vendedores algunos módulos (agentes) que permiten realizar esta función de respaldo en línea.

- *Cheyenne ARCserve*
- *Seagate BackupExec*
- *Legato Networker*.

Ventajas de utilizar *software* de terceros para realizar *backups* de *Exchange*.

- *Administración y manejo* – Algunos *software* de terceros permiten realizar los *backups* desde un lugar centralizado y proporcionan grandes ventajas para el manejo de las cintas y su calendarización.
- *Performance* – Existen grandes diferencias en tiempo de respaldo entre un *software* de terceros y el *software NTBACKUP* de *Windows NT*.
 - PE. Usando *NTBACKUP*: 6 GB por hora.
 - Usando *ARCserve* o *BackupExec*: cerca de 30 GB por hora.

9.1 Respaldo fuera de línea.

Offline Backup.

Copia todos los archivos del disco a los medios especificados sin verificar por corrupción. Todos los archivos son respaldados estando los servicios de *Exchange* fuera de línea. Los archivos de *Log* transaccionales no se eliminan después de cada respaldo, por lo que en un momento dado puede saturar el disco donde se encuentran almacenados.

Este punto debe ser verificado constantemente, ya que cuando el sistema autodetecta insuficiente espacio para trabajar, automáticamente da de baja los servicios de *Exchange*.

9.2 Respaldo en línea.

Tipos de respaldo *Online*.

Full Backup.

Este backup respalda toda la base de directorios y del *Information Stores*. Se respaldan los archivos de *log* transaccionales y posteriormente son borrados.

Copy.

Copia todos los archivos y no elimina los archivos de *log* respaldados.

Incremental.

Se realiza el respaldo de los últimos cambios generados en las bases de datos del *Directory e Information Store* desde el último *backup* completo (Full), respaldando también los archivos de *log* y borrándolos siempre y cuando hayan sido copiados a cinta.

Diferencial.

Se realiza el respaldo de los cambios generados en la base de datos de *Information Store* y *Directory* desde el último respaldo completo (Full). Un *backup* diferencial respalda los archivos de *log* pero no los elimina del disco.

Ventajas y Desventajas de los respaldos en Línea y Fuera de Línea.

En línea.

- El servicio se mantiene activo durante el tiempo de respaldo.
- La transferencia de mensajes continúa durante el proceso de respaldo.
- Es posible recuperar todos los mensajes después de una caída del equipo, ya que existen archivos de *Log* Transaccionales y existe un respaldo en línea.
- Es rápido.

Fuera de línea.

- El servicio de correo esta interrumpido durante el tiempo que dure el respaldo.
- No hay envío ni recepción de mensajes.
- No es posible recuperar todos los mensajes. Si el servidor se daña, sólo se podrían recuperar los mensajes hasta el último respaldo realizado.

Estrategia del Corporativo.

Actualmente el servidor de correo da servicio a casi 1000 cuentas de usuarios incluyendo al personal de las oficinas, al personal de la planta y al personal foráneo.

El uso del correo se ha vuelto crítico para toda la compañía, por lo que el servicio se considera de alta disponibilidad y no debe ser dado de baja por ningún motivo.

Este servicio permanece activo 7x24 y sólo es dado de baja para mantenimientos programados o problemas de producción que se presenten.

El sistema de respaldo con el que cuenta éste servidor es *Online*, diariamente se realiza el respaldo en la noche pero manteniendo el servicio activo, ya que el corporativo cuenta con servicio en tres turnos. El *software* utilizado para realizar el *backup* es *ARCserve* con el agente de respaldo de *Exchange*.

El resguardo de las cintas se lleva a cabo en una bóveda de seguridad, por lo que los respaldos realizados en la noche a todos los servidores de producción son enviados a primera hora a una bóveda donde permanecen hasta el día siguiente y luego son regresados a la oficina.

Las cintas no son utilizadas hasta que ha pasado una semana de antigüedad para cada día con excepción del viernes que se realiza un respaldo semanal y es resguardado para mantener respaldos semanales y finalmente el último día del mes se realiza un respaldo mensual que también es guardado.

Diariamente se respaldan todas las bases de datos *online*, los archivos de *log* transaccionales y todos los *mailboxes* independientes de cada usuario. El respaldo de los *mailboxes* es selectivo para cada afiliada, y como afiliada mexicana hemos detectado la facilidad de poder ofrecer a nuestros usuarios la posibilidad de recuperar correo que ya ha sido eliminado.

CAPÍTULO 10

HERRAMIENTAS DE OPTIMIZACIÓN Y MONITOREO.

10.1 Funciones del Procedimiento *Performance Optimizer*.

El *Performance Optimizer* es una herramienta que provee *Microsoft Exchange Server*, la cual debe ejecutarse cuando ha finalizado la instalación del servidor *Exchange Server*, esta nos da la facilidad de configurar de manera eficiente los recursos del *Exchange* así como el *hardware* donde reside este. Además de cuando se instala el *software* de *Microsoft Exchange* es recomendable ejecutar el *Optimizer* cuando:

- La función del servidor donde reside el *Exchange* cambie (se le asignen nuevas tareas o conectores).
- El número de *mailboxes* en el servidor u organización del *site* se incrementen o decrementen considerablemente.
- Se hagan cambios en el servidor del *Exchange Server*, tales como aumento de *memoria RAM*, Disco o cambie la configuración del disco duro.

Los dos tipos de ayuda que provee el *Optimizer* están definidas por las siguientes características:

- Analiza y recomienda la optima distribución de los directorios de datos del *Exchange Server*.
- Analiza y configura en el *registry* tanto la memoria como otros recursos del sistema.

Ejecución del *Performance Optimizer*.

Al ejecutar el *Performance Optimizer* éste presenta una pantalla en la cual se advierte que los servicios del *Microsoft Exchange Server* dejarán de funcionar, esto significa que se detendrán todas las entregas de *mails* así como los accesos de los clientes; hasta que la configuración del *Optimizer* finalice.

En la Fig. 10.1 se muestran los tres tipos de información que se requieren:

- Cuantos *mailboxes* serán configurados
- Que tipo de servicio se usara
- Cuantos usuarios formarán parte de la organización.

Microsoft Exchange Performance Optimizer

In order to effectively evaluate some system parameters, Microsoft Exchange Performance Optimizer needs some information from you. Please indicate your answers to the following questions.

How many users do you expect to host on this server?	For what type of server will this computer be configured? (Check all that apply)	How many users will be in your organization?
Users on this server: <input checked="" type="radio"/> 1 - 25 <input type="radio"/> 26 - 50 <input type="radio"/> 51 - 100 <input type="radio"/> 101 - 250 <input type="radio"/> 251 - 500 <input type="radio"/> More than 500	Type of server: <input checked="" type="checkbox"/> Private Store <input checked="" type="checkbox"/> Public Store <input checked="" type="checkbox"/> Connector/Directory Import <input checked="" type="checkbox"/> Mailserver <input type="checkbox"/> POP3 only	Users in organization: <input checked="" type="radio"/> Less than 100 <input type="radio"/> 100 - 999 <input type="radio"/> 1,000 - 9,999 <input type="radio"/> 10,000 - 99,999 <input type="radio"/> 100,000 or more

Memory Usage

Limit memory usage to MB

< Back Next > Cancel Help

Fig. 10.1 Pantalla de información del *Optimizer*

Adicionalmente se podrá definir el límite de memoria total a usar. El *Optimizer* detecta el total de memoria *RAM* instalada en el servidor la cuál será la base para definir éste límite; nunca podrá ser mayor al total detectado.

Después de que se definió el número de usuarios y la función de estos, el *Optimizer* hace un análisis del disco y presenta la propuesta de distribución de los componentes de datos del *Exchange*, como se muestra en la Fig. 10.2:

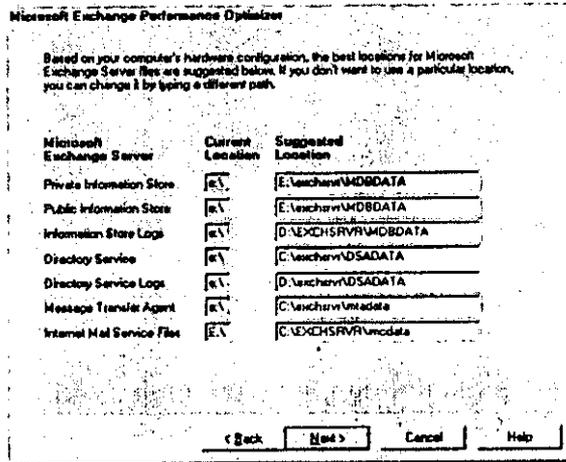


Fig. 10.2 Pantalla de direccionamiento de datos.

Realizada la distribución de los datos el *Performance Optimizer* habilita la opción de mover los archivos de datos automáticamente como lo muestra la Fig. 10.3.

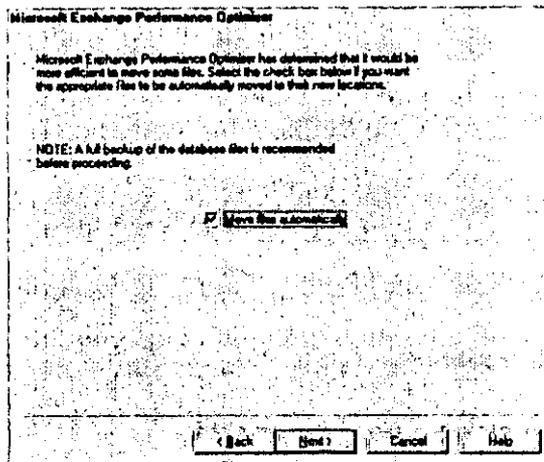


Fig. 10.3 Opción para mover archivos automáticamente.

El permitir mover los archivos de datos tiene importantes implicaciones en la recuperación de datos, ya que habilita el replicado del *log* de transacciones hacia las bases de datos del *Exchange Server*. Los archivos de *log* de transacciones registran los cambios de información en el *Exchange* y permiten deshacer una transacción cuando esta no termina adecuadamente

Optimización del Disco Duro.

Para comprender como el *Exchange Server* almacena sus archivos de datos en los distintos *drives*, es necesario entender como almacena la información. Cuando un mensaje es enviado el *Exchange Server* automáticamente escribe en el disco un archivo *log* de transacciones el cual es de 5 MB, éste archivo normalmente se llama EDB.LOG, cuando éste se llena se renombra como EDBNNNNN.LOG, donde; NNNNN es un número hexadecimal consecutivo al último almacenado; de tal manera, que el último archivo puede ser EDB0005B.LOG y el anterior EDB0005A.LOG. La escritura de éstos archivos es rápida y sencilla dado que la alta de nueva información se realiza en forma secuencial permitiendo que la administración de la información resulte eficiente y de fácil acceso en caso de que sea necesario restablecer la integridad de la base de datos de *Exchange* por alguna inconsistencia.

Para determinar la mejor distribución de las bases de datos en todos los dispositivos de almacenamiento, el *Optimizer* realiza una prueba en la cual crea archivos de 4MB con los cuáles simula el flujo de información de datos en el *Exchange*.

El *benchmark* del análisis del disco es desplegado en una tabla similar a la siguiente:

```
Found fixed logical disk C:
Found fixed logical disk D:
Found fixed logical disk E:
Found fixed logical disk F:
Performance Results
(Smaller values better)
Disk  RA(ms)    Seq(ms)
-----
C:    26195     176266
D:    51671     175844
E:    70077     176437
F:    24367     175563
```

Optimización de los Recursos del Sistema.

El *Performance Optimizer* balancea automáticamente los recursos del sistema, analizando la configuración del *hardware* (velocidad del procesador, *memoria RAM*, etcétera) y tomando como base, el número de usuarios en el servidor, las funciones que realiza y el número total de usuarios de la organización.

10.2 Verificación de la consistencia de las bases de datos

10.2.1 Comandos

Los comandos para la verificación de la consistencia son los siguientes:

EDBUTIL

En el modo de operación para consistencia, éste comando verifica la consistencia de una base de datos. Su sintaxis es la siguiente:

EDBUTIL/c <nombre de la base de datos> [opciones]

Parámetros : <nombre de la base de datos> - Nombre del archivo de la base de datos a verificar, o uno de /ispriv, /ispub, o /ds(ver notas).

Opciones : Ninguna, una o más de las siguientes opciones, separadas por un espacio:

/a - Verifica todos los nodos, incluyendo los anulados.

/k - Genera estadísticas del uso de claves.

/p - Genera información del uso de paginas.

/t<name> - Ejecuta una verificación solamente en la tabla especificada (por default: checa todas las tablas en la base de datos).

/o - Suprime el logotipo.

Notas: El *DS/IS*, verificador de la consistencia (reemplazado por el ajustador de la consistencia *DS/IS* en *Exchange 5.5*) no lleva a cabo ninguna restauración, y siempre asume que la base de datos está en un estado consistente, regresa un error si éste no es el caso.

Los parámetros especiales /ispriv, /ispub, y /ds utilizan el registro fijo automáticamente al nombre de la base de datos para el apropiado almacenamiento *Exchange*.

ESEUTIL

En el modo de operación para la integridad, éste comando verifica la integridad de una base de datos. Su sintaxis es la siguiente:

ESEUTIL /g <nombre de la base de datos> [opciones]

Parámetros : <nombre de la base de datos> - Nombre del archivo de la base de datos a verificar, o uno de */ispriv*, */ispub*, o */ds*(ver notas).

Opciones : Ninguna, una o más de las siguientes opciones, separadas por un espacio:

/t<nombre del archivo> - Nombre fijo temporal de la base de datos (por default: INTEG.EDB).

/v - Muestra resultados.

/x - Da detalle de los mensajes de error.

/o - Suprime el logotipo de *Exchange Server*.

Notas: El *DS/IS*, ajustador de la consistencia no lleva a cabo ninguna restauración, y siempre asume que la base de datos está en un estado consistente, regresa un error si éste no es el caso.

Los parámetros especiales */ispriv*, */ispub*, y */ds* utilizan el registro fijo automáticamente al nombre de la base de datos para el apropiado almacenamiento *Exchange*.

10.2.2 Technet

Esta herramienta proporciona ayuda técnica acerca de temas relacionados con los productos de *Microsoft*. En relación a nuestro tema tenemos las siguientes recomendaciones para verificar la consistencia de la base de datos.

- Una de las características importantes de un *log* de transacciones de un servidor *Exchange*, es su longitud, esta puede estar vacía o llena y deberá ser siempre de tamaño fijo de 5 MB. Sin embargo, si se detecta que el archivo de *log* es de otro tamaño, se puede asumir que dicho archivo es inconsistente. El *log* de transacciones se llama siempre EDB.LOG; cuando éste está lleno, es renombrado como EDB0001.LOG, EDB0002.LOG y así sucesivamente, después el nuevo archivo EDB.LOG es creado. En suma, cada archivo *log* de transacciones contiene una señal, la cual deberá coincidir con la señal del correspondiente archivo de base de datos. Si dicha señal no coincide, el correspondiente servicio falla sobre el *Startup* y refleja en el *log* de eventos un mensaje de error Jet-level, indicando una señal de *log* inválido o una señal de base de datos inválida.

- El archivo de checkpoint es una optimización, habilita un servicio para que las transacciones ejecuten o no un *commit* a las bases de datos. Éste archivo es llamado *EDB.CHK*, y es para el *Directory Service*, éste reside en el directorio *DSADATA*. Para el *Store service*, el cual reside en el directorio *MDBDATA*, si se ejecuta una optimización de ejecución, la locación de éste archivo debe variar. Algunas veces, cuando se ejecuta un *commit* de una transacción al archivo de base de datos, el checkpoint es actualizado.
- Facilidades de como los archivos de *log* de transacciones y los archivos de trabajo Checkpoint funcionan en casos de recuperación. Con todas las transacciones en un archivo de *log* de transacciones y el archivo de Checkpoint indicando que transacciones tienen *commit* sobre la base de datos, el *service scans* en el archivo Checkpoint busca la última transacción con *commit* a la base de datos. Entonces el *service scans* busca en el *log* de transacciones las transacciones que no han dado *commit* y las escribe sobre el archivo. Éste proceso se efectúa automáticamente cuando se inicia el servicio o cuando se restaura algún respaldo en línea.
- ¿Se necesita nuevamente iniciar el *DS/IS* ajustador de la consistencia antes de iniciar una restauración?

No usualmente. Éste se debe ejecutar sólo cuando se puede restaurar el *Information Store*. El ajustador de la consistencia *DS/IS* examina el *Information Store* y asegura que un objeto del directorio existe por cada objeto *Information Store* (crea un objeto del directorio si uno no existe).

También examina el directorio y se asegura que hay un correspondiente objeto *Information Store*

por cada objeto del directorio (elimina el objeto del directorio si uno no existe). Además verifica el

access control list (ACL) por cada objeto y quita cualquier entrada inválida. Si se restaura el *Information Store* hacia un servidor que ha sido adicionado recientemente a un site *Exchange*, se

debe esperar hasta que la réplica se complete. El nuevo servidor debe estar informado de todo los

servidores y *sites* en la organización y registrarse en lista global de direcciones. Después que la

réplica se ha completado, se ejecuta el *DS/IS* ajustador de la consistencia, si éste se ejecuta antes

de que se complete la réplica, los folders públicos son reubicados a éste nuevo servidor y se perderán los permisos de estos.

- ¿Cuándo se debe evitar ejecutar el *DS/IS* ajustador de la consistencia?

Hay dos situaciones las que se debe tener cuidado cuando se ejecuta el *DS/IS*:

- Si se ha roto temporalmente un conector de réplica del directorio entre dos *sites*, no se debe ejecutar el *DS/IS*, si se planea volver a conectar los *sites*. Si se ejecuta el *DS/IS* cuando se rompe el conector de réplica del directorio, cualquier ubicación de los folders públicos en

los servidores que no están en el *site* presente son reubicados al servidor local y cualquier correo que corresponda a otros *sites* se eliminan de la lista de permisos de los folders públicos. Cuando se adiciona nuevamente el conector de réplica del directorio, todos los cambios hechos a los folders públicos en el *site* presente se reproducen en toda la organización, los folders públicos son reubicados, y se pierden los permisos.

- Si se ha restaurado el *Information Store* hacia un servidor que se adiciono recientemente a un *Exchange site*, no se debe ejecutar el *DS/IS* hasta que el nuevo servidor se replique con el resto del *site* y está informado de los otros servidores y *sites* en la organización.
- ¿Cuál es la diferencia entre compactación, defragmentación y mantenimiento del *Information Store*?

El mantenimiento al *Information Store* debe realizarse entre 1:00 y 6:00 A.M., esto incluye compresión *tombstone*, envejecimiento de columnas, envejecimiento de índices, limpieza por lectura de usuarios y expiración de mensajes. Se pueden cambiar los períodos del mantenimiento del *Information Store* evitando colisiones con el proceso de respaldo, para reducir la carga en el servidor. La compactación es una defragmentación fuera de línea y petición de espacio al disco. Esta reorganización de eventos, consolida los datos y libera espacio. Defragmentación es la petición de espacio en disco en línea y defragmentación de la base de datos.

10.3 Verificación de la regeneración de las bases de datos

10.3.1 Comandos

Los siguientes comandos nos permiten verificar la regeneración de la base de datos:

EDBUTIL

En el modo de operación para restauración, éste comando ejecuta la recuperación, trae toda la base de datos a un estado consistente. Su sintaxis es la siguiente :

EDBUTIL /r [opciones]

Opciones : Ninguna, una o más de las siguientes opciones, separadas por un espacio:

/is o */ds* - (ver notas).

/l<ruta> - Ubicación de archivos *log* (por default: el directorio activo)

/s<ruta> - Ubicación de archivos del sistema, (por ejemplo, el archivo checkpoint; por default: el directorio activo).

/o - Suprime el logotipo.

Notas: Los parámetros especiales /is y /ds utilizan el registro fijo automáticamente a la ruta del archivo *log* y a la ruta del archivo raíz para los apropiados almacenamientos *Exchange*.

ESEUTIL

En el modo de operación para restauración, éste comando ejecuta la recuperación, trae toda la base de datos a un estado consistente. Su sintaxis es la siguiente:

ESEUTIL/r [opciones]

Opciones : Ninguna, una o más de las siguientes opciones, separadas por un espacio:

/is o /ds - (ver notas).

/l<ruta> - Ubicación de archivos *log* (por default: el directorio activo)

/s<ruta> - Ubicación de archivos del sistema, (por ejemplo, el archivo checkpoint; por default: el directorio activo).

/o - Suprime el logotipo de *Exchange Server*.

Notas: Los parámetros especiales /is y /ds utilizan el registro fijo automáticamente a la ruta del archivo *log* y a la ruta del archivo del sistema para los apropiados almacenamientos *Exchange*.

En el modo de Reparación. Éste comando repara alteraciones o daños de la base de datos. Su sintaxis es la siguiente:

ESEUTIL/p <nombre de la base de datos> [opciones]

Parámetros : <nombre de la base de datos> - Nombre del archivo de la base de datos a compactar, o uno de /ispriv, /ispub, o /ds(ve notas).

Opciones : Ninguna, uno o más de las siguientes opciones, separadas por un espacio:

/t<nombre del archivo> - Nombre fijo temporal de la base de datos (por default: REPAIR.EDB).

/d - Reparación de la base de datos, solo examina los errores.

/v - Muestra resultados .

/x - Da detalle de los mensajes de error.

/o - Suprime el logotipo.

Notas: Los parámetros especiales /ispriv, /ispub, y /ds utilizan el registro fijo automáticamente al nombre de la base de datos para el apropiado almacenamiento *Exchange*.

10.3.2 Technet

En relación a la verificación de la regeneración de la base de datos tenemos las siguientes recomendaciones.

- La manera de restaurar datos depende si el respaldo será implementado en línea o fuera de línea, un respaldo en línea es más fácil de ejecutar que uno fuera de línea. En un respaldo normal diario, se puede restaurar simplemente el último respaldo normal e iniciar el servicio. En un respaldo normal incremental se puede restaurar el último respaldo normal, todos los sets de incremento y comenzar el servicio, *Exchange* se manejará entre los archivos *log*. En un respaldo normal-plus-differential, se restaura el último respaldo normal, se restaura el último respaldo diferencial y se inicia el servicio.
- En un respaldo fuera de línea se debe seguir un procedimiento para la restauración del *Directory Service* y otro para el *Information Store*. Para el *Directory Service*, se restaura en los directorios *DSADATA* sobre diferentes unidades de disco, y entonces se inicia el servicio. Para el *Information Store*, la restauración se hace en los directorios *MDBDATA* (cuando las ubicaciones también son mostradas en el registro) y entonces ejecuta un programa llamado *ISINTEG:EXE* ubicado en el directorio *BIN* sobre el Servidor de *Microsoft Exchange* y proporciona a éste programa el comando de línea " - patch ". Después el servicio se desactiva y se necesita iniciarlo nuevamente.
- Para restaurar el registro de *Windows NT*, se ejecuta *NT.EXE* y revisa la caja del llamado "Restore Local Registry". Para restaurar el servicio del servidor *key-management*, se deberá desactivar el servicio, restaurar el directorio correspondiente, restaurar el disco de arranque e iniciar el servicio.
- El *Circular logging* es un importante concepto en cuestión de recuperación por desastre. Cuando un *Circular Logging* es activado, éste salva un almacenamiento para prevenir continuas reconstrucciones de los archivos del *log* de transacciones sobre la unidad de discos. El downside correcto, es con el *Circular logging*, con respaldos de forma incremental o diferencial cuando éstos no han ocurrido, sin embargo, éstos no son habilitados en caso de desastre. El *Circular Logging* es activado por default en *Exchange*; si no se requiriera de esto; se puede deshabilitar por medio del programa administrador. La ventaja de deshabilitarlo es proporcionar recuperabilidad adicional porque el *non-circular logging* mantiene una historia del *log* de transacciones para todas las transacciones. Éste archivo de *log* es depurado sólo cuando un respaldo en línea total o incremental da *commit* a todas las transacciones de la base de datos y la respalda.
- Se necesita un respaldo del *Directory Service* en cada computadora para poder restaurar un servidor?

No importa que tan antiguo sea el respaldo, el *Directory Service* se reconstruye sobre una computadora y, después de restaurarse, obtiene la información de otros directorios en el *site*.

- Para restaurar un servidor en un *site*, se debe de tener un respaldo del directorio (*DIR.EDB*) para el servidor. No es posible obtener la información del directorio desde una replica en otro servidor en el *site*, esto por que cada directorio es único. Si se tiene el respaldo original del directorio éste se puede restaurar y entonces obtener los cambios desde otro servidor en el mismo *site*, pero se debe tener el respaldo del directorio.
- Cuando se debe usar *edbutil /d /r* o *eseutil/p*. Éste es un último recurso y puede eliminar datos; se debe usar para reparar bases de datos sólo cuando no se puede restaurar y ninguna otra opción está disponible. Antes de ejecutar *edbutil /d /r* (para *Exchange 4.0* y *5.0*) o *eseutil /p* (*Exchange 5.5*), se debe asegurar :
 - Respaldar los archivos de la base de datos que se intentarán reparar.
 - Tener suficiente espacio libre en disco. *EDBUTIL* requiere espacio libre igual a 110 por ciento (25 por ciento para *ESEUTIL*) del tamaño del archivo a reparar.
 - Usar la opción de comando de línea / t (con una utilería) para indicar una unidad de disco que contenga el espacio libre requerido.
 - Ejecutar *isinteg- fix* después de que haya sido ejecutada la utilería.
- Cuando el Servidor *Exchange* está en un *PDC* y por alguna razón falla o se necesita actualizar a una nueva computadora, en éste caso, se promueve uno de los *BDCs* de los dominios a *PDC*, para después iniciar con la restauración .
- Restaurar el servidor completamente a un diferente equipo físico, ¿requiere una configuración como *BDC* o *PDC*?

No necesariamente, el paso importante es borrar la cuenta de la computadora, entonces se adiciona nuevamente al dominio de producción de manera que el equipo de restauración pueda hacer un nuevo *SID* utilizando el mismo nombre del servidor original de producción.

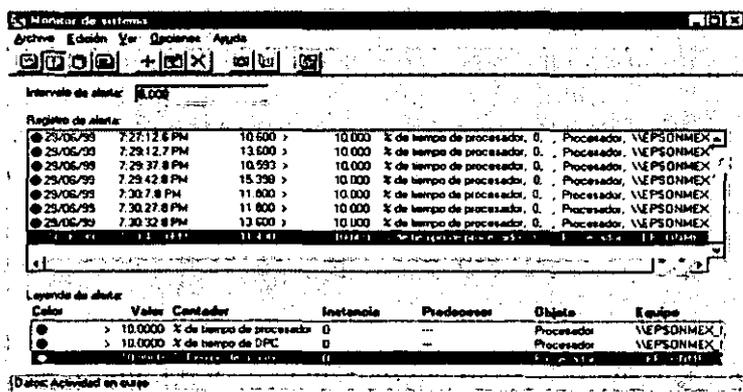
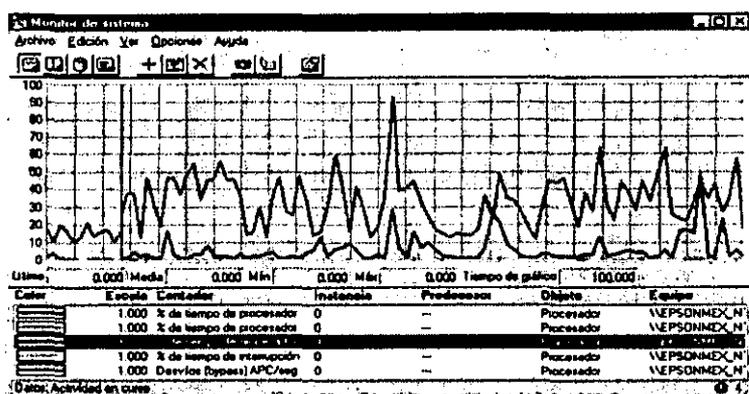
- Porqué no se pueden iniciar servicios entre restaurar una forma de respaldo completa y una diferencial, o una cinta incremental o una secuencial a ser restaurada?

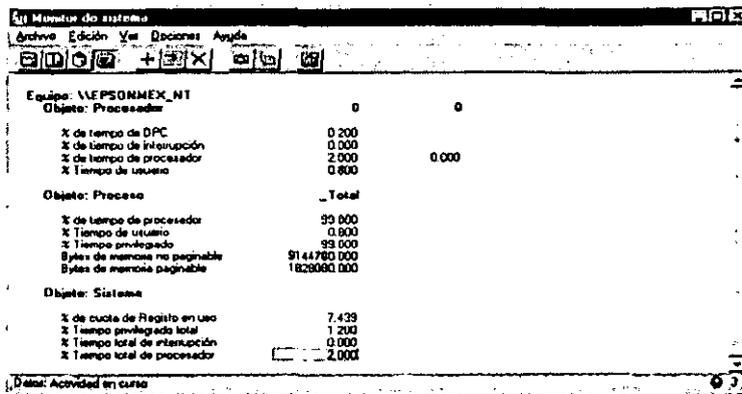
Por que para dar fin a una restauración, *Exchange* toma todos los *logs* en orden secuencial y entonces la base de datos retoma un nuevo estado.

10.4 Performance Monitor.

Windows NT incluye varias herramientas que permiten obtener fácilmente estadísticas e información del sistema, una de éstas herramientas es el *Performance Monitor*.

El *Performance Monitor* utiliza una serie de contadores que hacen el seguimiento de los datos, como por ejemplo el número de procesos que esperan tiempo de disco, el número de paquetes de red transmitidos por segundo y el porcentaje de utilización del procesador. Con éstos datos se pueden crear gráficos, establecer alertas y dar formato a informes que le permitan controlar y ajustar el rendimiento del sistema. Los datos se pueden mostrar al mismo tiempo que se recopilan, almacenan en registros para su uso y posterior comparación, o ambas opciones; tal y como se muestra en las Fig's. 10.4:





Fig's. 10.4 Performance Monitor

Con el Performance Monitor de sistema se puede:

- Ver simultáneamente los datos de cualquier número de equipos.
- Recibir una respuesta inmediata sobre cómo afectan al sistema los cambios que realiza.
- Ver y cambiar dinámicamente los gráficos que reflejan los valores de los contadores de la actividad actual.
- Exportar datos desde gráficos, registros de alertas e informes a programas de hojas de cálculo o de bases de datos para manipularlos e imprimirlos posteriormente.
- Crear un registro de alertas que enumere (y, opcionalmente, notifique) cuándo se ha sobrepasado el valor de un contador o un umbral configurado por el usuario.
- Crear archivos de registro que contengan datos acerca de diversos objetos de equipos distintos, de forma que pueda ver la información recopilada a lo largo del tiempo. Éstos archivos de registro se pueden utilizar para grabar la utilización normal de un recurso, observar tendencias y proyectar requisitos de *hardware* (diseño de capacidad).
- Agregar a un archivo determinadas secciones de otros archivos de registro existentes para crear un archivo de un período de tiempo más grande.
- Ver los informes de la actividad actual o crear informes de archivos de registro existentes.
- Guardar las configuraciones individuales de gráficos, alertas, registros o informes, o toda la configuración completa del entorno de trabajo y reutilizarlas cuando las necesite.

El *Performance Monitor* puede ser configurado para proveer información acerca de cualquier computadora en la cual corra *Microsoft Exchange Server*, la siguiente tabla muestra algunas de las estadísticas que pueden ser accedidas:

Directory	MTA	MTA Connections	Information Store Access Permission Errors
Access Permission Errors	Messages /sec	Associations	Browse Operations /sec
Reads /sec	MMI Connections	Bytes Received /sec	Reads /sec
Replication Updates /sec	Work Queue Size	Messages Received /sec	Replication Updates /sec
Threads in Use	Connectors	Queue Size	Threads in Use
Writes /sec	Clients		Writes /sec

Con el *Performance Monitor* se puede ver el número de errores que se han generado en los permisos de acceso al sistema, operaciones de consulta y el número de lecturas y escrituras a los directorios de *Microsoft Exchange* y de *Microsoft Exchange Information Storage*. Con esta información fácilmente se puede determinar la carga y la actividad de los usuarios en la consulta y actualización de información en los directorios.

El *Performance Monitor* también provee estadísticas de los mensajes enviados así como las conexiones entre servidores, lo cual permite a los administradores observar las cargas de accesos de los directorios, el *MTA* y el *Information Storage*. Con esta información las organizaciones identifican probables cuellos de botella en el *performance* del sistema eliminándolos antes de que ocurran, además de esta manera los administradores pueden realizar una planeación efectiva para futuras expansiones.

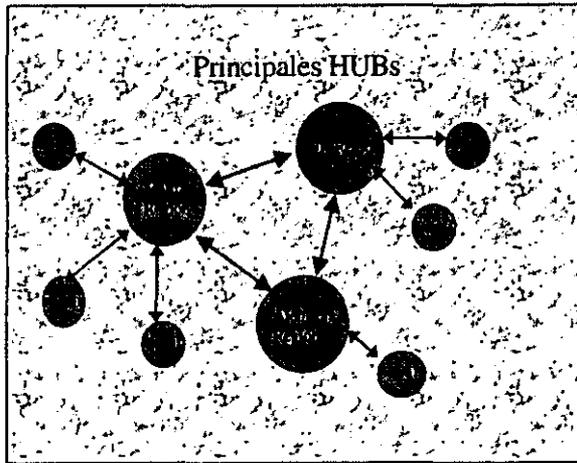
CONCLUSIONES

Podemos concluir que el *software* de *Microsoft Exchange Server* como sistema de mensajería es una herramienta poderosa respaldada por *Microsoft* a nivel mundial, ofrece un alto nivel de seguridad en el intercambio de información considerando además *Internet*, por lo que cualquier organización sin importar el tamaño puede contar con un sistema como éste, que ofrezca soluciones cliente/servidor y puedan ser accedidas en cualquier parte del mundo, su crecimiento es ilimitado y sólo es dependiente del *hardware* con que se cuente, éste fue uno de los factores fundamentales que se consideraron, ya que nuestra finalidad fue enlazar aproximadamente a 40 mil usuarios; la plataforma seleccionada para implementar esta solución en todo el corporativo fue *Intel* con *Microsoft Windows NT*. Esta tecnología es manejada por todo el corporativo y nos permitió que su implementación se realizara de una forma fácil para todas las afiliadas. Se definió el uso de arreglos redundante a fallas para garantizar la seguridad de la información y una fácil recuperación en caso de ser necesario.

Además de ser un *software* fácil de manejar y administrar, cuenta con diagnósticos integrados, acceso remoto y con una estructura de directorios flexible.

Las herramientas de administración de *Windows NT*, el *Performance Monitor* y el *Event Log* son herramientas integradas en *Exchange Server*, permitiendo a los administradores usar las mismas herramientas tanto para la administración de su sistema operativo de *Windows NT* como para los servidores de mensajería y colaboración.

Se utilizó la arquitectura *hub- and-spoke* para implementar *Microsoft Exchange* en toda la organización, ya que proporciona una administración eficiente, direccionamiento y solución de problemas desde una región soportada a otra región soportada. El uso de esta arquitectura permitió dividir en tres nodos principales toda la organización, minimizando así cuellos de botella con el *Hub* central y garantizando que al menos dos terceras partes de la compañía estuvieran comunicadas en caso de presentarse algún problema en el *Hub* central.



Para llevar a cabo la migración de correo en los usuarios se implementó una campaña de difusión que nos permitiera explicar a los usuarios el cambio de plataforma de correo y el impacto.

Para realizar el procedimiento de migración de usuarios fue necesario configurar el *software* de correo anterior en todos los usuarios migrados para que identificaran como nueva dirección de correo la definida en el servidor de *Exchange*, esto funcionó durante el proceso de migración, permitiendo que los usuarios identificaran ambas direcciones de correo y direccionando el correo anterior al nuevo.

El proceso de capacitación, difusión e implementación fueron diferentes y se planearon de forma específica para cada filial.

En la afiliada de México y sus zonas foráneas se seleccionó contratar a un proveedor externo que pudiera impartir la capacitación a todos los usuarios.

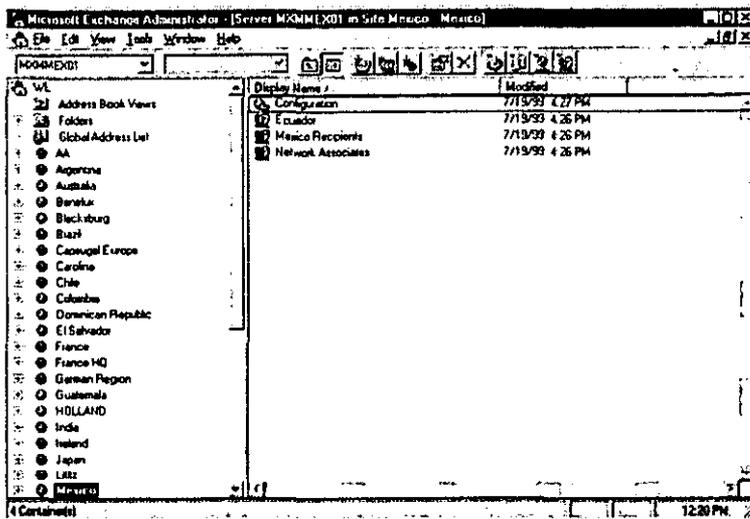
Durante el proceso de capacitación de usuarios se llevó a cabo en forma simultánea el proceso de instalación del *software* de *Outlook* en todos los equipos PC y laptop de la compañía.

Para realizar el proceso de desinstalación del *software* anterior (*TeamLinks* y *Calendar Manager*) se utilizaron herramientas propias de *Windows NT* como el manejo de *Logones Script*, los cuáles permitieron que todos los usuarios en el momento de firmarse a la red ejecutan un procedimiento automático **.bat*, que verificará en todos los equipos la existencia del *software* de correo anterior y una vez identificado lo eliminará totalmente.

Se configuró el *logon script* de los usuarios para ejecutar éste procedimiento en un día específico y eliminar en forma masiva el *software*.

Se generaron archivos de *log*, donde se pudo identificar posteriormente que el proceso se hubiera ejecutado correctamente y hubiera borrado toda la información antes mencionada.

Para el mes de Julio de 1999 se tienen definidos aproximadamente 40 *sites* dentro de la organización con un total de 34 mil cuentas.



El proceso de migración aún no ha concluido, y día a día se incluyen nuevos *sites* dentro de la organización. Países como México que proporcionan servicio de correo a la afiliada de Ecuador existen dentro de la organización, en algunos casos se pretende eliminar esta dependencia sobre todo cuando los medios de comunicación no son lo suficientemente eficientes para permitir esta conexión WAN, en otros cuando las afiliadas crecen lo suficiente para justificar la creación de un *site* local, entonces se implementa localmente.

Como parte del proceso de globalización se han definido en el corporativo algunos países como cabeza de una región, actualmente se está analizando si éstos países serán responsables de la implementación local o remota de los países que conformen la región completa.

El interés principal del corporativo sin importar que país sea la cabeza de región será siempre proporcionar a los usuarios las herramientas necesarias para realizar en forma eficiente su trabajo, en el caso de México, la ciudad de Ecuador no pertenece a nuestra región, Ecuador pertenece a la región Andina con cabeza de región en Colombia, pero debido al estudio y pruebas

realizadas de enlace y tiempo de respuesta en acceso se seleccionó a la ciudad de México para dar éste servicio.

El modelo seleccionado para implementar *Microsoft Exchange* ha permitido a la organización mantener un nivel de comunicación eficiente y rápido, incrementando el nivel de productividad y apoyando la toma de decisiones dentro del corporativo.

El uso de un correo eficiente y estable es fundamental para cualquier empresa líder ya que la comunicación y el acceso a la información es la clave de cualquier negocio.

GLOSARIO DE TÉRMINOS

ADSI: (Soporte a Active Directory Service Interface) Herramienta utilizada para construir aplicaciones basadas en Exchange que pueden ser integradas con Microsoft Windows 2000.

ANSI: (American National Standards Institute).

API: (Application Programming Interface) Interfaz de programación de aplicaciones mediante la que los programas invocan servicios del sistema operativo.

* **Archivo de Swap:** Es un archivo generado en algún espacio físico de la máquina y que se encarga de apoyar el proceso de la máquina para incrementar el performance.

ARP: (Address Resolution Protocol) Protocolo de Resolución de Direcciones. Protocolo usado en la conversión de direcciones IP.

ASP: (Active Server Page) Herramienta que provee la facilidad de crear aplicaciones Web proporcionando acceso a los datos de Exchange Server.

ATM: Modo de Transferencia Asíncrona.

Backbone: Dispositivo central utilizado para conectar las redes LAN dentro de una organización, se considera la columna vertebral de una red.

BDC: Backup Domain Controller, definido como controlador del dominio de un ambiente de Windows NT.

Bridge: Conmutador inteligente en una red que distribuye los datos a una subred y que pasa los datos de la subred a la red de área extensa (WAN).

CCITT: Comité de Consulta Internacional de Telefonía y Telegrafía para los estándares de comunicación.

CDDI: (Copper Distributed Data Interface).

CDO: (Collaboration Data Object). Herramienta que permite crear aplicaciones ASP con interface para Outlook Web Access.

Cheyenne ARCserve: Software de Respaldo comercializado por Computer Associate.

Cluster: Ambiente definido para trabajar con dos servidores redundantes a fallas conectados como uno solo con alta disponibilidad de servicio.

CSU / DSU: (Channel Service Unit / Data Service Unit). Dispositivo que convierte señales digitales estándares generados por un computador en un tipo de señales digitales de ambiente sincrónico.

DDS: (Digital Data Service). Líneas que proporcionan comunicaciones sincrónicas punto a punto.

Debugger: Es un programa especial utilizado para encontrar errores en otros programas.

DEC All-in-One: Software de correo utilizado por DEC en plataforma Alpha.

Decnet: Arquitectura de red de propiedad exclusiva de Digital Equipment Corporation, utiliza metodología de igual a igual para todas las máquinas de la compañía.

DecMailworks: Software de correo utilizado por DEC en plataforma Alpha, versión posterior a All-in-one.

Design Time Controls and Wizards: Herramienta que permite crear en forma fácil aplicaciones ASP.

DQDB: Bus de cola distribuida dual.

DTE/DCE: (Data Terminal Equipment / Data Communications Equipment).

E-Mail: Correo electrónico.

ECSA: (Exchange Carriers Standards Association).

EDBUTIL: Comando utilizado por Microsoft Exchange para optimizar la base de datos de directorios o de information store.

Exchange Hubs: Servidores principalmente de conexión y distribución en un ambiente de correo grande.

Exchange Server 5.5: Software de correo de Microsoft Corporation.

Ethernet: Estándar de red inicialmente desarrollado por Xerox y refinado por DEC e Intel. Ethernet interconecta computadoras personales y transmite a 10 Mgb por segundo. Utiliza una configuración de bus que puede conectar hasta 1024 computadoras personales y estaciones de trabajo. Está codificado con el estándar IEEE 802.3.

Fast Backups: Respaldos rápidos.

FDDI: (Fibre Distributed Data Interchange) Intercambio de Datos Distribuido por Fibra, potente intercambio de datos en redes de fibra óptica con topología de anillo. Tasas de transferencia de datos de hasta 100 Mbit/s.

FT-1: (Fractional T-1) T1 Fraccionado.

FTP: File Transport Protocol, Protocolo de Transferencia de archivos, servicio que transfiere archivos ASCII y binarios entre sistemas locales y no locales.

Full-duplex : Duplicación completa de cualquier servicio de proceso de datos.

HAL: (Hardware Abstraction Layer) Capa de abstracción de hardware, parte del sistema operativo Windows NT que se ocupa de trabajar con el hardware.

Header: Es una unidad de información que va al inicio de un grupo de datos.

Host-based: Se refiere a cualquier dispositivo que se encuentre instalado en la computadora host.

HTML: (Hypertext Markup Lenguaje) Lenguaje de etiquedo de hipertexto, lenguaje de descripción de documentos de las paginas WWW.

Hub: Dispositivo para reenviar datos de una computadora a otra dentro de una red.

ILS: (Internet Locator Server).

IMAP: (Internet Message Access Protocol).

Internet: 1) Cualquier red grande formada de redes más pequeñas. 2) La red internacional que conecta lugares de estudio, ciencia y comercio.

Intranet: Red local basada en TCP/IP.

ITU: (International Telecommunications Union).

KMS: (Microsoft Exchange Key Managment Server) Utileria que maneja firmas digitales o cifrado de mensajes individuales.

LAN: (Local Area Network) Red de Area Local, denominación para redes locales que actualmente se realizan mediante topología Ethernet o Twisted Paid.

LADP: (Lightweigh Directory Access Protocol) Protocolo a nivel de enlace, diseñado para conexiones de la ISDN.

Link Monitor: Utileria para monitorear el status de las conexiones entre los servidores del mismo site.

Lotus Notes: Sistema de correo propietario de IBM.

MAN: Redes de Area Metropolitana.

Message Tracker: Utilería para monitorear el status de un mensaje en cualquier parte de la red local, internacional o dentro de Internet.

MIME: (Encapsulation of Aggregate HTML Documents) Método de cifrado para transferir archivos cuálesquiera mediante el estándar de correo electrónico, solo permite archivos de texto de siete bits.

Microsoft BackOffice: Conjunto de productos diseñado para apoyar a las organizaciones a tomar decisiones y poder ofrecer soluciones cliente servidor de una manera precisa.

Microsoft Cluster Server: Grupo de servidores interconectados entre si manejados como un solo equipo.

Microsoft Exchange: Sistema de mensajería cliente/servidor que integra en un mismo sistema diferentes funciones como: el sistema de correo, calendarización de eventos en forma individual o en grupos, manejo de formas electrónicas ,usos de contactos y tareas, trabajo en grupo y sincronización online con correo offline en el momento de la conexión.

Microsoft SNA Server: Herramienta de enlace entre plataformas IBM AS/400

Microsoft SQL Server: Manejador de Bases de Datos.

Microsoft Visual InterDev: Herramienta de desarrollo de visual utilizadas para crear formas HTML.

MTA: (Message Transfer Agent) Utilería que determina si un mensaje pertenece al mismo nodo local o debe ser dirigido a otra localidad.

Multiplexing: Combina señales múltiples (analógicas o digitales)

NTBACKUP: Sistema de respaldo de archivos propietario de Windows NT.

OSI: (Open System Interconnection) Sistema de Interconexión Abiertos. Modelo para la interconexión de sistemas abiertos, el cual define la estructura de una red como una jerarquía de siete niveles.

Outlook 97 y Outlook 98: Software de correo electrónico para cliente.

Outlook Form: Paquete de herramientas para escribir y debugear VB Script.

PAD : (Packed Assembler/Disassembler): Dispositivo de acceso a paquetes. Una interfaz entre un terminal o computador y una red conmutada por paquetes.

PDN: Red Pública de Datos. Red de datos por paquetes. Una red establecida y operada por una PTT, compañía telefónica pública o privada, para el fin específico de proporcionar servicios de comunicación de datos al público. Puede ser una red conmutada por paquetes o una red digital como DDS.

Performance Monitor: Aplicación de Windows NT que muestra el desempeño de los componentes del servidor.

RPC: (Remote Procedure Call) Herramienta que permite ejecutar llamadas a procedimientos remotos.

Service Pack: Correcciones a versiones de sistemas ya liberados.

Server Monitor: Utilería que monitorea el comportamiento del equipo y realiza acciones

SMDS: (Switched Multimegabit Data Service).

SMS: (Microsoft System Management Server) Herramienta que permite que los clientes de Exchange y Outlook sean monitoreados y actualizados en forma remota.

Site: Región de intercambio que contienen cierto número de servidores

SMS: (Microsoft Systems Management Server).

SMTP Smart-Host : Protocolo simple de transporte de correo. Subprotocolo de correo electrónico de los TCP/IP.

SNMP: (Simple Network Management Protocol).

TCP/IP: (Transmission Control Protocol/Internet Protocol) Protocolo de control de transmisión/Protocolo Internet. Protocolo para controlar en flujo de datos en redes de área local y área extensa. La información se subdivide en paquetes, se direccionan, envían y se vuelven a componer en el orden correcto en su lugar de destino. Es el protocolo estándar de Internet

BIBLIOGRAFÍA

Advances in integrated services digital networks (ISDN) and broadband ISDN / William Stallings; ISBN 0-8186-2797-2, Editorial Los Alamitos, Calif. : IEEE Computer Society Press, 1992, 255 págs.

A guide to fractional T1 / James Trulove., ISBN 0-89006-524-1, Editorial Boston, Mass. ; London : Artech House.; 1992, 111 págs.

ATM switching systems / Thomas M. Chen, Stephen S. Liu; ISBN 0-89006-682-5, Editorial Boston : Artech House; 1995, 261 págs.

Comunicaciones y redes de procesamiento de datos. Nestor González Sainz; rev. Técnica Alberto Jaime. ISBN 968-422-147-9, Editorial McGraw-Hill, México, 1987, 396 pág.

DNS on Windows NT .Paul Albitz. Editorial O Reilly, 1998, ISBN 1-565-92511-4

El libro de las comunicaciones de Pc, José Antonio Carballar , Grupo Editorial Alfaomega, México 1997.

Enterprise networking : fractional T1 to SONET, frame relay to B-ISDN / Daniel Minoli. ISBN 0-89006-621-3, Editorial Boston ; London : Artech House, 1993, 734 págs.

FDDI and FDDI-II : architecture, protocols, and performance/ Bernhard Albert, Anura P. Jayasumana; ISBN 0-89006-633-7, Editorial Boston ; London : Artech House, 1994, 399 págs.

FDDI technology report / John F. Mazzaferro, Alexa A. Dell' Acqua; ISBN 0-9276957-0-7, Editorial Charleston, S.C. : Computer Technology Research Corp., 1a edición, 1991, 114 págs.

Guide to integrating digital services : T1, DDS, and voice integrated network architecture / Robert L. Dayton., ISBN 0-07-016188-7, Editorial New York : Intertext Publications, McGraw-Hill, 1989, 290 págs.

Inside Windows NT Server 4 Administrators Resource Edition; Drew Heywood, Darin Camp, Michel Hayes; Ed. New Riders Publishing 1997.

Internetworking : a guide to network communications : LAN to LAN, LAN to WAN / Mark A. Miller, ISBN 1-558-51143-1, Editorial San Mateo, Ca. : M&T Books; 1991, 425 págs.

Introduction to fast and oils technology / edited by Peter J. Wan; ISBN 0-9353153-5-7, Editorial Champaign, Ill. : American Oil Chemists' Society, 1991, 330 págs.

Introduction to T1/T3 networking / Regis J. Bates; ISBN 0-89006-624-8, Editorial Boston ; London : Artech House; 1992, 192 págs.

ISDN : the integrated services digital network : concept, methods, systems / Peter Bocker ; in coloboration with G. Arndt...[et al.]; ISBN 0-387-54819-X, 2a edición, 1993, 258 págs.

LAN, ATM, and LAN emulation technologies / Daniel Minoli ; Anthony Alles, ISBN 0-89006-916-6, Editorial Boston ; London : Artech House, 1996, 309 págs.

LAN/WAN optimization techniques / Harrell J. Van Norman., ISBN 0-89006-617-5, Editorial Boston : Artech House, 1992, 338 págs.

Managing and Maintaining Microsoft Exchange Server 5.5, Published by Microsoft, Press 1998, E.U.

Microsoft Education and Certification, Core Tecchonogies of Microsoft, Exchange Server 5.0, Student Workbook, Course Number: 771.

**Microsoft Exchange 5.0 Field Guide, Stephen L. Nelson 192 páginas
ISBN 1-57231-705-1**

Microsoft Exchange Server, Survival Guide, Greg Todd, et al, SAMS Publishing.

Principles of signaling for cell relay and frame relay /Daniel Minoli, George Dobrowski.
ISBN 0-89006-708-2, Editorial Boston ; London : Artech House, 1995, 305 págs.

Redes de computadoras : protocolos, normas e interfaces. Uyless Black; tr. Ra-Ma editorial.
ISBN 970-604-016-1, Editorial Macrobot, México, 1990, 421 pág.

Redes de datos : aspectos específicos en redes de computadoras. Editorial Fundación Arturo
Rosenblueth, Mexico, 1982, 200 Pág.

Redes de Ordenadores, Andrew S. Tanenbaum, 2ª. Edición, Editorial Prentice Hall

Redes locales y TCP/IP, José Luis Raya, Grupo Editorial Alfaomega, México 1997

Runnig Microsoft Windows NT Server 4.0, Sharon Crawford, Charlie Russell, 640 páginas,
ISBN 1-57231-333-1

Transmission networking SONET and the synchronous digital hierarchy / Mike Sexton, Andy
Reid; ISBN 0-89006-551-9, Editorial Boston ; London : Artech House, 1992,
360 Págs.

Teleinformatica y redes de computadores / coord. Antonio Alabau Munoz.
ISBN 968-86103-3-X, Editorial Marcombo, 2 edición, 1987, 351 pág.

Teletraffic technologies in ATM networks / Hiroshi Saito; ISBN 0-89006-622-1, Editorial
Boston ; London : Artech House; 1994, 174 págs.

Windows NT 4 Server al AL DESCUBIERTO; Jason Garms et al; Prentice Hall 1998.

Windows NT 4 ; Bernd Kretschmer; Alfaomega Grupo Editor, 1996.

Windows NT Server 4.0, Enterprise, Steve Kaezmarck., 1997.

Windows NT simple network management protocol . James D. Murray. Editorial Cambridge :
O'Reilly, 1a ed., 1998, Pág. 446, ISBN 1-565-92338-3