UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

CAMPUS
A R A G Ó N

"ADMINISTRACIÓN DE LOS RECURSOS DE UNA RED DE DATOS MEDIANTE WINDOWS NT. "

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A

ROBERTO PEREZ PEREZ.

ENEP ARAGON

MÉXICO, D.F. 1998.

ADMINISTRACION DE LOS RECURSOS DE UNA RED DE DATOS MEDIANTE WINDOWS NT.

INDICE

CAPITULO 2 INSTALACION DE UN SERVIDOR WINDOWS NT.

CAPITULO 3. ADMINISTRACION DE UNA RED WINDOWS NT.

ADMINISTRACION DE LOS RECURSOS DE UNA RED DE DATOS MEDIANTE WINDOWS NT.

Objetivo:

Determinar las ventajas que proporciona Windows NT para administrar una red de datos, mostrando su versatilidad, herramientas y facilidad de instalación y uso.

INTRODUCCION

La creciente necesidad de compartir recursos, obtener facilidad en el intercambio de información, así como la necesidad de mantener segura dicha información, son puntos relevantes dentro de las empresas. La complejidad de los sistemas y las configuraciones de cada empresa, obligan a utilizar recursos para lograr los objetivos de forma flexible para cada problema y cada necesidad.

En el complejo mundo del cómputo las instituciones y empresas de hoy requieren de un sistema operativo de red que proporcione facilidad de uso, operabilidad y servicios de comunicaciones integrados, ofreciendo al mismo tiempo, el mejor rendimiento. Por esto y más, es necesario realizar un análisis de los sistemas operativos que juegan en el mercado un papel principal, para adecuarlo a las necesidades propias.

La idea de implementar e instalar un servidor de comunicaciones surge de la necesidad de establecer la comunicación con otras redes, contar con accesos a la red Internet y proporcionar diferentes servicios para mantener a distintos usuarios en constante intercomunicación.

Debido a que Windows NT es uno de los sistemas operativos de red que satisface estas necesidades, está diseñado para trabajar con los sistemas que se tienen hoy en día, y la tecnología que requierá en un futuro. Además de las capacidades de comunicación optimizadas y funcionalidad, Windows NT le ayuda a mejorar la forma en que una institución pública o empresa se mantenga en contacto tanto interna como externamente, proporcionándole mayores

capacidades de compartir ideas e información a través de su funcionalidad para accesos a la red Internet. Windows NT mejora la facilidad de uso, instalación y administración, integrando una interfaz de usuarios más amigable.

Los administradores ahora pueden tener la misma interfaz de usuario en todas sus plataformas Windows de 32 bits, resultando esto en menores requerimientos de entrenamiento y facilidad de migración de usuarios dentro de la familia Windows de sistemas operativos. Como parte de su esfuerzo continuo de simplificación de las redes de cómputo Microsoft ha añadido varios asistentes para la Administración en NT. Estos asistentes, están diseñados principalmente para administradores menos experimentados, ya que proporcionan una guía completa e interactiva para realizar las tareas más comunes de administración.

En el área de la flexibilidad, Windows NT integra todas las características de escalabilidad, y seguridad que se requieren, sin sacrificar la velocidad o el tiempo de respuestas. Las mejoras en velocidad y rendimiento en compartición de impresoras y archivos, procesamiento de aplicaciones, Internet y acceso remoto, lo hacen una de las plataformas más poderosas y completas que existen.

La integración de la interfaz gráfica más amigable, proporciona un ambiente consistente tanto en estaciones de trabajo como en servidores. Eso redunda en menores necesidades de entrenamiento e implementación rápida de redes nuevas. En conjunto, esta integración y los asistentes para la administración, hacen muy fácil administrar la red sin problemas.

La administración cotidiana de los servidores de red, se facilita con herramientas como el Administrador de Tareas y el Monitor de Redes. El Administrador de Tareas proporcionando información detallada de cada aplicación y proceso que se esta ejecutando en el sistema. Con esta información, los administradores pueden tener acciones inmediatas para mejorar la confiabilidad y rendimiento del sistema.

Otra herramienta muy poderosa para diagnostico, es el monitor de Redes, examina el tráfico que entra y sale del servidor, incluso a nivel paquetes, y lo captura para el análisis posterior. De esta forma, es posible detectar y corregir fallas reales o potenciales en la red.

Por otra parte, Windows NT proporciona integración transparente y en una sola plataforma para su correo electrónico, servidor de archivos, bases de datos y comunicaciones. Trabaja con los sistemas tales como: NetWare, UNIX, y mainframes o minicomputadoras IBM. Además Windows NT soporta más de 5,000 plataformas de hardware, más que las soportadas por sus tres más cercanos competidores combinados Windows NT Server es compatible con todos los protocolos de red actuales, incluyendo: TCP/IP, IPX/SPX, NetBEUI, Apple Talk, DLC, HTTP, SNA, PPP, PPTP. Windows NT Server es el más flexible en soporte a una amplia variedad de clientes, incluyendo: Windows 3.x, Windows 95, Windows NT Workstation, IBM OS/2, y Macintosh.

El servicio de Directorio de Windows NT (NTDS) puede soportar más de 25,000 usuarios por dominio y. Literalmente, cientos de miles de usuarios por empresa. No importa que tan centralizado o distribuido sea una empresa, NTSD le permite crear un directorio que se ajuste exactamente a las

necesidades de la empresa además permite administrar todos los recursos, servicios y aplicaciones. Proporciona la plataforma más completa para Internet, NT es el único sistema operativo para redes con un servidor web integrado. Microsoft Internet (IIS). El que IIS esté incluido en NT significa que la instalación y administración del servidor web, es tan sólo parte del sistema operativo.

Así, empresas, escuelas, instituciones de investigación, oficinas remotas, trabajadores viajeros y otros usuarios, se conectan en red con Windows NT utilizando el Servicio de Acceso Remoto (RAS). Sin embargo, el realizar negocios por teléfono puede resultar costoso, especialmente a larga distancia. Para resolver este problema, Microsoft, en conjunto con otras corporaciones protocolo "Point-to Point Tuneling" (PPTP). PPTP permite que los usuarios remotos se conecten con un proveedor de servicio de Internet (ISP) local y utilizando un canal seguro, accesen su red tal y como si estuvieran en su escritorio. PPTP proporciona este nivel de seguridad ya que ofrece encapsulado de protocolos y encripción de información para las conexiones RAS. Esto significa que los usuarios pueden crear redes privadas virtuales utilizando redes públicas de datos como Internet.

Los desarrolladores pueden tomar ventaja de la infraestructura cliente/servidor única conocida como Distributed component Objet Model (DCOM), para construir aplicaciones de alto rendimiento, seguras y distribuidas a través de la Internet. DCOM extiende la arquitectura COM permitiendo a los componentes a interactuar a través de las redes mejorando la seguridad total del sistema operativo de red.

Además de presentar una alta estabilidad, proporciona el desarrollo de administración de forma sumamente fácil para el usuario, traduciéndose esto en una interface de fácil comprensión y manejo, ya que se pueden realizar tareas en paralelo y un manejo de usuarios con una seguridad verdaderamente eficiente. Una vez definida la seguridad con permisos se hace más fácil la administración. Este sistema operativo tienen la ventaja de trabajar con interoperabilidad, esto es, pueden comunicarse con otros sistemas operativos como novell realizando una compartición de recursos sencilla tanto de impresoras como de archivos y ambos usuarios que estén ya sea en la parte de NT como en la parte de Novell, pueden accesar a los recursos de ambos lados.

Para la comunicación entre dominios se emplea las relaciones de confianza las cuales se realizan en maquinas que son controladoras primarias y una vez estableció esta relación un usuario puede viajar en ambos dominios y accesar a los recursos sin ningún problema.

CAPITULO I. REDES DE DATOS.

Objetivo:

Definir las características principales de los distintos tipos de redes, sus topologias y su forma de intercambiar información.

CAPITULO I. REDES DE DATOS.

1.1. TRANSMISION DE DATOS.

Los datos que provienen de una computadora o un dispositivo periférico pueden ser transmitidos de diversas formas según sea la naturaleza de la señal enviada, el sincronismo entre el emisor y receptor, y la secuencia que llevan los bits en caso de una transmisión digital y la simultaneidad emisión-recepción.

La forma más sencilla de transmitir datos digitales, es enviarlos directamente a través de una línea de transmisión. Este modo de transmisión se denomina transmisión en banda base. Su inconveniente es la fuerte degradación que experimenta la señal con la distancia, por lo que generalmente se utiliza en distancias cortas. Por el contrario, existen diferentes formas de transmitir datos a larga distancia:

- Transmisión Analógica.- este tipo de transmisión maneja señales que pueden tener cualquier valor de forma continua y dentro de unos márgenes. Las señales analógicas utilizan medios que han sido diseñados para la transmisión de voz, siendo necesario el uso de adaptadores de líneas o módems. Las líneas de transmisión clásicas fueron creadas para la transmisión de señales analógicas de tipo telefónico, las cuales se adaptaron para la comunicación entre equipos informáticos.

- Transmisión Digital.- es aquella transmisión que maneja señales discretas, utilizando medios diseñados específicamente para este tipo de transmisión,

basados en tecnologías de alta escala de integración; así con esta modalidad se consigue una alta calidad y velocidad de transmisión.

En la transmisión de datos existe un proceso mediante el que un emisor informa un dispositivo receptor sobre los instantes en que va a transmitirse las correspondientes señales al que se le denomina *sincronización*. El proceso de sincronización se clasifica en dos tipos básicos:

- Transmisión *Asincrona.*- Consiste en acompañar a cada unidad de información de un bit de arranque y otro de parada. Esto se consigue de tal forma que en el primer cero es el bit de arranque y a continuación se transmiten los bits correspondientes al carácter, terminando la transmisión con un bit uno, cuya duración mínima sea entre uno y dos veces la de un bit. La línea se mantendrá en este nivel hasta el comienzo de la transmisión del siguiente carácter.

- Transmisión *Síncrona*- Es una técnica más eficiente que la anterior y consiste en el envío de una trama de datos que configura un bloque de información comenzando con un conjunto de bits de sincronismo y termina con otro conjunto de bits de final de bloque. En este caso, los bits de sincronismo tienen la función de sincronizar los relojes existentes tanto en el emisor como en el receptor de tal forma que estos controlan la duración de cada bit y carácter ahorrando con respecto al esquema anterior los bits de inicio y de parda de cada carácter.

1.1.1. MODELO O.S.I.

La necesidad de intercambiar información entre sistemas heterogéneos, es decir, entre sistemas cuyas tecnologías son muy diferentes entre sí, llevó a la ISO (International Standard Organization), actualmente llamada I.T.U. (International Telecommunication Union), a buscar la manera de regular dicho intercambio de información.

El modelo de referencia OSI (Open Systems Interconnection) surge en el año 1983 y es el resultado del trabajo de la ISO para la estandarización internacional de los protocolos de comunicación.

MODELO OSI.		
Nivel 7	Aplicación	Provee servicios generales relacionados con aplicaciones.
Nivel 6	Presentación	Otorga el formato de datos
Nivel 5	Sesión	Coordina la interacción en la sesión de los usuarios
Nivel 4	Transporte	Provee una transmisión de datos confiable punto a punto.
Nivel 3	Red	Enruta unidades de información
Nivel 2	Enlace de Datos	Provee intercambio de datos entre dispositivos en el mismo medio.
Nivel 1	Físico	Transmite un flujo de bits a través del medio físico.

Figura 1.1 Representación del modelo O.S.I.

Las funciones de las 7 capas del modelo OSI que se observan en la figura 1.1 se describen a continuación:

1.- Capa Física:

- Transmisión de flujo de bits a través del medio.
- Maneja voltajes y pulsos eléctricos.
- Especifica cables, conectores y componentes de interfaz con el medio de transmisión.

2.- Capa de Enlace de Datos:

- Estructura el lujo de bits bajo un formato predefinido llamado trama.
- Para formar una trama, el nivel de enlace agrega una secuencia especial de bits al principio y al final del flujo inicial de bits.
- Transfiere tramas de una forma confiable libre de errores.
- Provee control de flujo.

3.- Capa de Red:

- Divide los mensajes de la capa de transporte en paquetes y los ensambla al final.
- Utiliza el nivel de enlace para el envío de paquetes encapsulados en una trama.
- Enrutamiento de paquetes.

- Envía los paquetes de nodo a nodo usando ya sea un circuito virtual o como datagramas.
- Control de Congestión.

4.- Capa de Transporte:

- Establece conexiones punto a punto sin errores para el envío de mensajes.
- Permite multiplexar una conexión punto a punto entre diferentes procesos del usuario.
- Provee la función de difusión de mensajes a múltiples destinos (broadcast).
- Control de Flujo.

5.- Capa de Sesión:

- Permite a usuarios en diferentes máquinas establecer una sesión.
- Una sesión puede ser usada para efectuar un login a un sistema de tiempo compartido remoto, para transferir un archivo entre 2 máquinas, etc.
- Controla el diálogo (quien habla, cuándo, cuánto tiempo, half duplex o full duplex).
- Función de sincronización.

6.- Capa de Presentación:

- Establece una sintaxis y semántica de la información transmitida.
- Define los campos de un registro, como lo son: nombre, dirección, teléfono, etc.

- Comprensión de datos.

7.- Capa de Aplicación:

- Transferencia de archivos (ftp).
- Login remoto (rlogin, telnet).
- Correo electrónico (mail).
- Acceso a bases de datos, etc.

1.2. CANALES DE COMUNICACION EMPLEADOS EN REDES DE DATOS.

Cualquier medio físico que pueda transportar información en forma de señales electromagnéticas, se puede utilizar en redes locales como medio de transmisión. La selección del medio físico a utilizar, depende de:

- El tipo de ambiente en donde se va instalar
- El tipo de equipo a usar.
- El tipo de aplicación y requerimientos.
- La capacidad económica en relación costo/beneficio esperado.

Por lo que se deben tomar en cuenta los aspectos anteriores para elegir el medio de transmisión correcto de acuerdo a las necesidades.

1.2.1. CABLE COAXIAL.

En general, el cable coaxial es el medio ideal para el transporte de señales de radiofrecuencia entre 5 – 100 Hz. Es también un recurso relativamente barato con respecto a otros. Teniendo al cable coaxial dividido en dos tipos:

- Cable Coaxial de Banda Angosta: En el cable coaxial, la malla exterior tienen una doble función, es el conductor de retorno de transmisión y también es un blindaje para reducir la interferencia que el cable puede emitir o captar de exterior. Por su efectividad en esta última función intervienen dos factores, el cubrimiento que se tenga de la superficie del aislamiento y la conductividad eléctrica que tenga. Con la malla se pueden lograr cubrimientos superiores al 90- 95%. Una cinta aluminizada y con traslape logra el 100% de cubrimiento pero tienen muy poco metal y por lo tanto, menor conductividad que la malla.

- Cable Coaxial de Banda Ancha: Es el mismo que es utilizado en redes de televisión (CATV), teniendo la característica de utilizar FDM (Multiplexión por división combina voz, datos y vídeo, simultáneamente permitiendo voz y vídeo más. La señal en el cable es en modo analógico de radiofrecuencia (RF) y por lo tanto sus daños deben ser modulados antes de la transmisión, usando un módem RF. Se necesitan módems en cada terminal, lo que aumenta más su costo y las velocidades.

1.2.2. PAR TRENZADO.

Es el medio de transmisión más utilizado en la actualidad en las redes LAN. Existen dos tipos de trenzado.

1) Par trenzado sin blindaje UTP (Unshielded Twisted Pair), que es un tipo de cable con uno o más pares de conductores de cobre aislados y trenzados contenidos dentro de una sola envoltura de plástico sin blindaje.
2) Par trenzado con blindaje STP (Shielded Twisted Pair), similar al UTP sólo que con una trenza o lámina metálica entre los pares de cobre y el revestimiento de plástico. La norma ANSI/TIA/EIA-568-A, el estándar para el Cableado Comercial para Telecomunicaciones en Edificios (Commercial Building Telecomunications Cabling Standard), ha establecido tres categorías de cable par trenzado UTP de 100 ohms para utilizar en las LAN.

Categoría 1: Sus características de transmisión se especifican hasta 16 Mhz. Usando comúnmente en bajas velocidades de transmisión como transmisiones asíncronas y sistemas telefónicos y en velocidades medias como las que se presentan en aplicaciones de redes Token Ring (4Mbps) y Ethernet.

Categoría 2: Sus características de transmisión se especifican hasta 20 Mhz. Pudiendo soportar cualquier aplicación de la categoría 1.

Categoría 3: Sus características de transmisión se especifican hasta 100 Mhz. Es el medio estandarizado más popular usando transmisiones de datos a alta.

1.2.3. MICROONDAS.

Básicamente el uso que se les da a los enlaces vía microondas es en aquellos lugares donde sea difícil llevar el medio de comunicación físico como cable trenzado, fibra óptica, etc., así como en donde las distancias a cubrir son demasiado grandes. Entre las ventajas que se encuentran en los enlaces por microondas es que se tienen un ancho de banda grande, con cobertura para distancias grandes.

La principal desventaja que se tienen en este tipo de enlace es que son muy susceptibles a tormentas eléctricas, fenómenos meteorológicos y otras interferencias extremas por lo que la tasa de error es elevada en comparación con otros medios de comunicación.

1.2.4. FIBRA OPTICA.

La fibra óptica básicamente se compone de dos medios con índices de refracción diferentes, la parte central de la fibra es el núcleo generalmente de vidrio y en el viaja la mayor parte de la luz, alrededor del núcleo esta el revestimiento. La relación entre el índice de refracción entre ambos elementos produce el fenómeno de reflexión total interna. El cambio de índice de refracción entre la parte interior o el núcleo de la fibra y la parte envolvente, puede ser brusco o en etapas graduales. Existen dos tipos básicos de fibras

ópticas, fibra monomodo y fibra multimodo. En las fibras monomodo el haz de luz sigue una sola trayectoria a través del conductor de vidrio del núcleo, en las multimodo el haz de luz sufre diferentes difracciones siguiendo entonces trayectorias diferentes.

1.3. CLASIFICACION DE REDES.

Se emplea el concepto de red cuando se interconectan dos a más computadoras en un medio específico para compartir recursos. De esta forma, las funciones principales de una red son:

- Ser un medio para compartir comunicaciones.
- Ser un punto de interconexión para computadoras y terminales.
- Ser un recurso para compartir software.

Y dependiendo del área geográfica que comprenda la red, se va a clasificar en tres tipos básicos:

I. LAN (Local Area Network) Redes de Area Local.
II. WAN (Wide Area Network) Redes de Area Extendida.
III. MAN (Metropolitan Area Network) Redes de Area Metropolitana.

1.3.1. REDES DE AREA LOCAL.

Para definir el concepto de lo que es una Red de Area Local o LAN, se deben considerar tres aspectos importantes:

- Una LAN en una red de comunicaciones, lo que implica que debe conllevar facilidad en la transmisión de datos de un dispositivo a otro.
- Los dispositivos de comunicación de datos incluyendo todo dispositivo que se comunique sobre un medio de transmisión.
- El área geográfica que comprende una LAN es pequeña.

Tomando en cuenta lo anterior podemos definir a una LAN como una red de comunicaciones que provee interconexión con una variedad de dispositivos de comunicación de datos dentro de un área pequeña, la cual generalmente es comprendida.

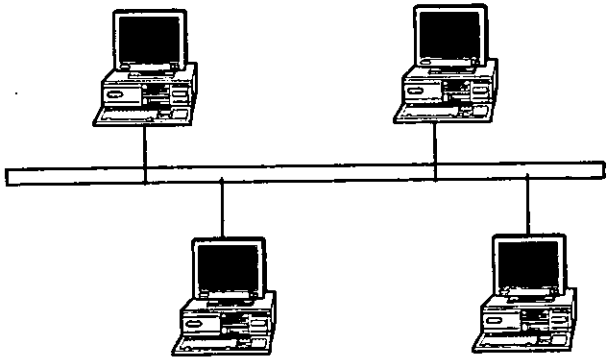

Figura 1.2 Representación Sencilla de una Red de Area Local

1.3.2. REDES DE AREA EXTENDIDA.

Cuando se interconectan diversas LAN entre sí, se pueden integrar en lo que se definen Redes de Area Metropolitana, o en Redes de Area Extensa, dependiendo de las características que posea la interconexión de redes LAN. Una WAN puede conectar computadoras entre distintos edificios o entre dos

continentes. Desde un punto de vista técnico, las WAN se conectan normalmente a través de servicios que no dependen de la distancia entre las computadoras, como son los recursos de telecomunicaciones públicas y privados, vía microondas y por medio de satélites.

1.3.3. REDES DE AREA METROPOLITANA

Un tipo de red que a menudo se confunde con una WAN son las MAN. Este tipo de red de computadoras es en realidad una conexión de MAN, regulada por consejos administrativos locales o estatales.

Los usuarios que necesiten comunicarse dentro de un área metropolitana que contenga derechos de uso público deben basarse en una serie de normas establecidas como las proporcionadas por la IEEE 802.6 para obtener conexiones de red de alta velocidad entre los edificios. Así, una MAN es en realidad una WAN que utiliza simplemente un conjunto de recursos de red específicos.

1.4. ARQUITECTURA Y TOPOLOGIAS DE RED

La configuración de una red suele conectarse como *topología* de la misma, en otras palabras, la topología es la forma en que se conecta la red. Para el caso de la arquitectura de red, se refiere al conjunto de niveles con sus servicios y protocolos existentes en una red y a la forma en que se va a integrar. Entre las topologías de red existen, las más comunes son: árbol o jerárquica, bus, en estrella, en anillo y en malla.

1.4.1. TOPOLOGÍA EN BUS.

Esta estructura es recuente en las redes de área local, por lo que resulta fácil controlar el tráfico entre las estaciones de trabajo. La limitante que existe con ésta topología reside en el hecho de que suele existir un solo canal de comunicación para todos los dispositivos de red. En consecuencia, si el canal de comunicaciones falla, toda la red deja de funcionar.

A pesar de sus inconvenientes, en la figura 1.3, podemos observar que este tipo de topología de red es de muy fácil integración motivo por el cual se utiliza con frecuencia.

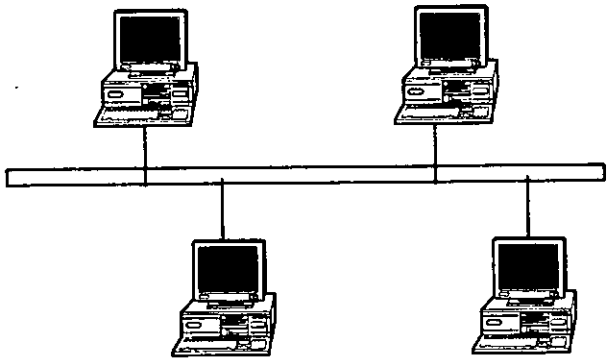

Figura 1.3. Topología en Bus.

1.4.2. TOPOLOGÍA EN ESTRELLA.

La topología en estrella es una de las más empleadas en los sistemas de comunicación de datos. Todo el tráfico emana del núcleo de la estrella, que es el nodo central.

El nodo por lo general es un servidor, el cual posee el control total de las estaciones de trabajo y si alguna estación falla la comunicación no es interrumpida.

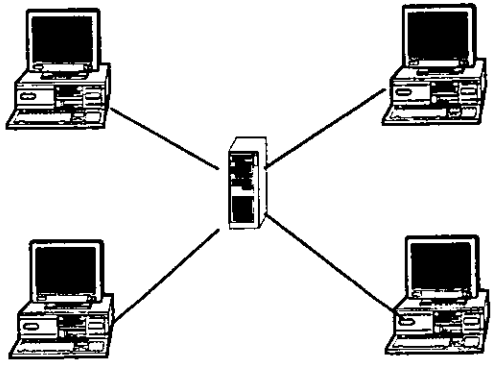

Figura 1.4. Topología tipo Estrella.

1.4.3. TOPOLOGÍA EN ANILLO.

La topología en anillo se llama así por el aspecto circular del flujo de datos. En la mayoría de los casos, los datos fluyen en una sola dirección, cada estación recibe la señal y la retransmite a la siguiente del anillo.

La organización en la topología de red en anillo resulta atractiva porque con ella son raros los embotellamientos, tan frecuentes en los sistemas en estrella o en árbol.

El problema más importante en esta topología es que todos los componentes del anillo están unidos por un mismo canal, así, falla el canal entre dos nodos toda la red se interrumpe.

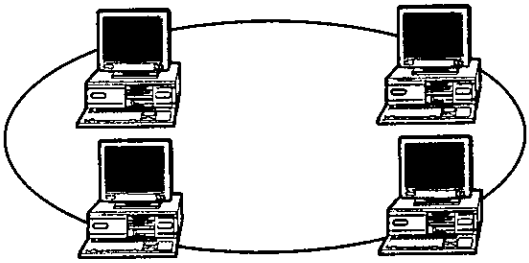

Figura 1.5. Topología en Anillo.

1.4.4. TOPOLOGÍA EN MALLA.

La topología en malla se ha venido empleando en los últimos años. Lo que la hace atractiva en su relativa inmunidad a los problemas de embotellamiento y averías. Gracias a la multiplicidad de caminos entre las estaciones de trabajo, es posible orientar el tráfico por trayectorias alternativas en caso de que algún nodo este averiado u ocupado.

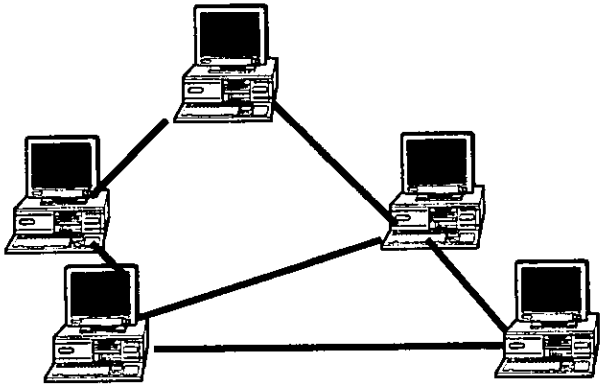

Figura 1.6. Topología en Malla.

1.5. ELEMENTOS DE RED

Cuando se pretende comunicar un sistema informático con otro a través de una red de comunicaciones, es necesario que exista un conjunto de elementos físicos y lógicos que permitan dicha comunicación. Debemos de entender por comunicación no solo la conexión entre los equipos si no todo el conjunto de elementos que permiten el entendimiento entre ambos, con independencia a sus características individuales.

El estado actual de la conectividad entre quipos de tan distinta naturaleza hace necesario el estudio de los elementos que coordinan las conexiones y transmisiones, por niveles bien definidos y separados de tal forma que el conjunto de todos ellos engloba todos los aspectos que pueden presentarse.

1.5.1. SERVIDOR.

Un servidor es un dispositivo que ofrece un servicio en una red, es decir que realiza una función específica de servicio para uno o varios clientes. En ciertas circunstancias, este término designará a una máquina, éste será el caso si dicha máquina está dedicada a un servicio particular, por ejemplo: servidores de impresión, servidor de archivos, servidor de correo electrónico, etc.

1.5.2. ESTACIÓN DE TRABAJO.

Una estación de trabajo es una computadora empleada como terminal bajo un sistema o plataforma (Windows NT, OS/DOS, UNIX, etc.), que puede

proporcionar potencia de cómputo local y agregarse a la capacidad de cómputo del sistema. Una estación de trabajo también de trabajo también puede usarse como un sistema único.

1.5.3. TERMINAL.

Una terminal, como su nombre lo sugiere, es el punto final de un sistema de cómputo, en donde las unidades que la componen son fundamentalmente una unidad de despliegue de vídeo y un teclado que conecta dispositivos de una red para intercambiar información mediante software.

1.5.4. PROTOCOLOS

Un protocolo es un conjunto de reglas y normas que permiten el intercambio de información entre dos dispositivos o elementos de red de un mismo nivel. Dentro de los protocolos más utilizados de forma más amplia se encuentran: TCP/IP, IPX/SPX, NETBEUI, X.25, X.75, etc.

Debido a la creciente popularidad de TCP/IP y a los servicios de comunicación que provee la Red Internet, ahora se encuentra uniendo miles de redes de área local, conectando millones de hosts o servidores. Así, podemos definir a TCP/IP como un conjunto de protocolos diseñados con una arquitectura en capas. Así, definiremos la estructura de TCP e IP.

- Transfer Comunication Protocol: El protocolo TCP provee un servidor confiable de entrega de paquetes Orientado – a – Conexión, o sea, TCP se

encarga de dar la ilusión de que la comunicación entre dos computadoras es de punto a punto con un flujo continuo de información, a diferencia de IP, donde se sabe que la información fluye en paquetes y que dicha información puede ser retransmitida varias veces antes de alcanzar su destino.

El concepto de conexión es muy importante porque le permite a un puerto local dar servicio a muchos puertos remotos concurrentemente. Esta es la base del modelo de aplicación cliente servidor que es usado en redes.

La comunicación punto a punto confiable indica que TCP acepta la responsabilidad de la secuencia de datos, validación y, si es necesario, retransmisión, la aplicación o proceso que use los servicios de TCP no necesita preocuparse de todo lo anterior, puede asumir que los datos que envía serán recibidos íntegros, en el orden exacto en el que fueron enviados. Otra de las responsabilidades de TCP es el Control de flujo, el cual es un mecanismo que previenen al transmisor de enviar datos más rápido de lo que el receptor puede manejar. TCP toma la información que se quiere transmitir,, la divide en pedazos y numera cada uno de estos, de tal manera que el receptor pueda verificar la llegada de los mismos y colocarlos en orden.

- Internet Protocol (IP): EL Protocolo de Internet (IP) es llamado la base tecnológica de TCP/IP. Las funciones que realiza IP son las siguientes:

a) Servicios de Entrega de Paquetes.- IP provee un servicio de entrega de datagramas, "Sin Conexión", llamado así porque no se lleva a cabo una coordinación entre el punto transmisor y el punto receptor. Cada paquete es tratado independientemente, los cuales pueden llegar en desorden y hasta

podrían no llegar. La entrega "Sin – Conexión" es similar a poner una carta en el buzón: se deposita (datagrama) y se olvida de ella. Se asume que el servicio postal (Red IP) entregará la carta (datagrama) a su destino. Este servicio "Sin – Conexión" es "No – Confiable" porque IP no puede garantizar la entrega, pero es llevado a cabo con el "Mejor- Esfuerzo", esto es, los datagramas no son descartados fácilmente (precisamente como el cartero no tira las cartas sin razón). Los datagramas pueden no ser entregados por la falla de recursos o por una falla en el hardware pueden no ser entregados por la falla de recursos o por una falla en el hardware de la red.

b) Servicios de Direccionamiento.- El servicio de direccionamiento de IP determina rápidamente si una dirección IP dada por la capa de transporte pertenece a la red local o a otra red. Las direcciones IP son números de 32 bits divididos en 4 octetos. Cada dirección es la combinación del identificador único de la red y el identificador único de la máquina. El problema inmediato con las direcciones IP es que son difíciles de memorizar. Por esta razón, las computadoras también pueden ser identificadas con nombres particulares.

Las capas permiten a los diseñadores del protocolo dividir en módulos las tareas y servicios que realizará e mismo. El diseño también especifica la manera en que un módulo interactúa con otros. La arquitectura en capas de los protocolos de más alto nivel interactúan con protocolos de niveles más bajos. El modelo de TCP/IP está formado por cuatro capas:

1. La capa de aplicaciones es la capa más alta de la pila; ésta provee servicios de alto nivel a los usuarios como transferencia de archivos, entrega de correo electrónico, y acceso a terminales remotas. Los programas de aplicación escogen entre diferentes protocolos de transporte dependiendo del tipo de servicio de transporte que requieran.

2. La principal tarea de la capa de transporte es proveer comunicación punto a punto entre las aplicaciones. Los protocolos de transporte usan el servicio de entrega de paquetes que provee la capa de Internet.

3. La capa de Internet provee el servicio de entrega de paquetes de una máquina a otra, por medio del protocolo de Internet (IP). La integridad de los datos se verifica en este nivel, por el mecanismo de verificación que es implementado en capas superiores (transporte o aplicación).

4. La capa de acceso al medio acepta datagramas de la capa de Internet y los envía físicamente. El "modulo" para el acceso al medio es con frecuencia un manejador de dispositivo (device driver) para una pieza particular de hardware, y la "capa" de acceso al medio puede consistir de múltiples módulos.

Para que la información fluya a través de las capas, ésta pasa por un proceso de encapsulamiento. Los mensajes o información recibida por la capa de TCP es encapsulada con un encabezado de TCP en un paquete llamado "segmento de TCP", este segmento de TCP es entregado a la capa de IP, en el que se agrega un encabezado de IP y el paquete llamado: "Datagrama de IP" es creado. El

paso final incluye el encapsulamiento del Datagrama de IP en paquetes creados para la capa de acceso al medio.

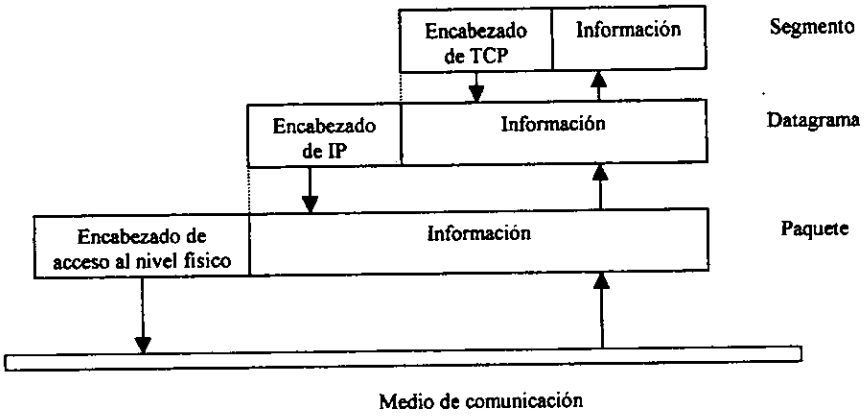

Figura 1.7. Modelo de Comunicación.

Una función de la capa de Internet es definir la "Unidad básica de Transferencia de Datos" usada en las redes TCP/IP: el Datagrama IP. Además, IP también es responsable de la selección del camino por el que viajan los datos, esto es llamado "Enrutamiento". El protocolo Internet también incluye un conjunto de reglas que define cómo se procesarán los paquetes, incluyendo cuándo generar mensajes de error y cuándo se descartan datagramas. Parte de este proceso incluye la "Fragmentación de Datos" y el "Reensamblado", aunque IP realiza esta función sólo cuando el hardware lo requiere.

El TCP/IP no distingue de una manera tan fina los niveles superiores de la pila de protocolo como lo hace OSI. Los tres niveles OSI superiores son casi equivalentes a los protocolos del proceso Internet. Algunos ejemplos de protocolos de proceso son:

- FTP: Protocolo que permite la transferencia de archivos entre sistemas.
- SMTP: Protocolo Simple de Transferencia de Correo. Se usa para transferir correo electrónico entre sistemas.
- NFS: Sistema de disco virtual en red que permite a una computadora cliente montar sistemas y directorios de archivos remotos. Lo desarrolló su origen Sun Microsystems.
- SNMP: Protocolo de administración simple de red el cual es usado para administrar dispositivos remotos relativa a su configuración, errores y alarmas.
- DNS: Es un servicio que proporciona una o más computadoras de la red para ayudar a localizar una ruta hacia un nodo deseado. Esto ahorra a cada sistema de la red el mantener una lista de todos los sistemas con los que quiere comunicarse. Lo usan las compuertas de correo.

El nivel de transporte del modelo OSI es el responsable de la entrega confiable de datos. En la pila del protocolo Internet, corresponde a los protocolos entre anfitriones, ejemplos de esto son: TCP y UDP. El TCP se usa para traducir mensajes de longitud variable de los protocolos de los niveles superiores y proporciona el acuse de recibido y el control de flujo orientado a la conexión entre sistemas remotos.

El Protocolo Internet (IP) es responsable de las comunicaciones entre sistemas. Se asigna al modelo OSI como parte del nivel de red. Este nivel del modelo OSI es responsable del movimiento de información por la red. Esto se logra al examinar la dirección del nivel de red. Esta dirección determina los sistemas y la ruta para enviar el mensaje.

IP proporciona la misma funcionalidad que el nivel de red y ayuda a obtener los mensajes entre sistemas, pero no garantiza la entrega de estos mensajes. IP también puede fragmentar los mensajes en bloques y luego reensamblarlos al llegar a su destino. Cada fragmento puede tomar una ruta de red diferente entre sistemas. Si los fragmentos llegan fuera de orden, IP reensambla los paquetes en la secuencia correcta en el destino.

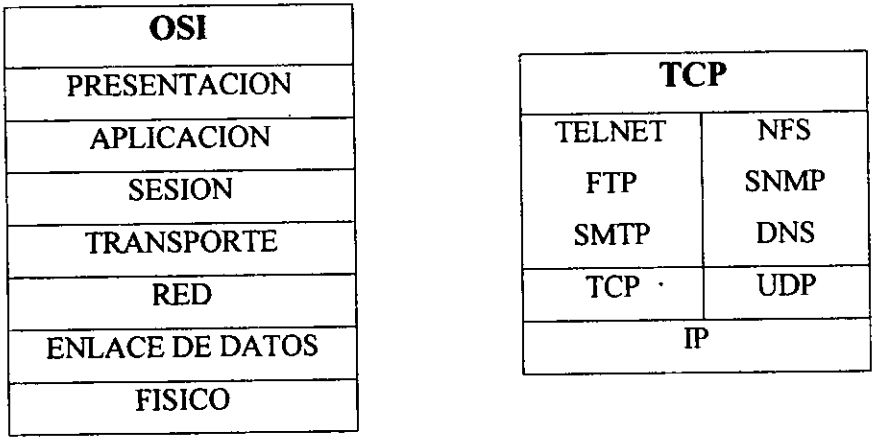

Figura 1.8. Compartición entre O.S.I. y T.C.P.

El Protocolo Internet requiere que se asigne una dirección a cada dispositivo de la red, ésta dirección se le conoce como dirección IP y está organizada como una serie de cuatro octetos. Cada uno de éstos, define una dirección única, una parte de la dirección representa una red y otra pare representa un nodo particular de la red.

CLASE	NODOS DISPONIBLES	BITS INICIALES	DIRECCION INICIAL
A	$2^{24} = 167772$	0XXX	0-127
B	$2^{16} = 65536$	10XX	128-191
C	$2^{8} = 256$	110XX	192-223
D		1110	224-239
E		1111	240-255

Figura 1.9. Clases de Direcciones IP.

Las direcciones IP se asignan a rangos llamados clases, conforme la aplicación y el tamaño de una organización. Las tres clases más comunes son A, B y C, las cuales representan la cantidad de bits asignables de manera local y que están disponibles para la red local.

En la figura 1.9 se muestran las relaciones entre las diferentes clases de direcciones, la cantidad de nodos disponibles y el ajuste de dirección inicial.

Las direcciones de clase A se utilizan en redes muy grandes o conjuntos de redes relacionadas. Todas las instalaciones educativas están agrupadas bajo las direcciones de clase A. Las direcciones de clase B se usan para redes grandes que tienen más de 256 nodos, pero menos de 65, 536 nodos. La mayoría de las organizaciones emplea las direcciones de clase C. Es recomendable que una organización tenga varias direcciones de clase C, porque la cantidad de direcciones de clase B es limitada, la clase D está reservada para el envío múltiple de mensajes en la red, y la clase E para experimentación y desarrollo.

Las direcciones Internet se administran mediante el Centro de información de red (NIC). Aparte de asignar direcciones, el NIC puede proporcionar otra información de valor. Este es un dispositivo de todos los documentos técnicos que se relacionan con Internet. Tiene una colección de documentos que describen todos los protocolos asociados, las metodologías de ruteo, los lineamientos para administrar la red y los métodos para usar diferentes tecnologías de red.

1.5.5. SUBREDES.

Hacer subredes es el proceso de dividir una red lógica grande en redes físicas más pequeñas. Entre las razones para dividir una red pueden estar las limitaciones eléctricas o la tecnología de redes; un deseo de segmentar para simplificar, al poner una ser separada en cada piso de un edificio y una necesidad de ubicaciones remotas conectadas con una línea de alta velocidad.

Las subredes más pequeñas se comunican con las otras por medio de compuertas y ruteadores las cuales resultan más fáciles de manejar. También, dentro de una organización puede haber varias subredes que estén en la misma subred. Con esto es posible dividir de modo lógico las funciones de la red en grupos de trabajo. Las subredes individuales son separadas. Para lograrlo, la dirección IP se ve en dos partes; red y anfitrión. La parte de red se convierte en la dirección IP asignada y en los bits de información de subred. En esencia, estos bits se eliminan en la parte del anfitrión.

La cantidad de bits asignados para una red de clase B es 16. La parte de subred agrega 6 bits y esto da un total de 22 para distinguir a la subred. Esta división

resulta en 64 redes con 1,024 nodos cada una. La parte de red puede ser más grande o más pequeña, según la cantidad de redes deseadas o el número de nodos por red.

1.5.6. SEGMENTACIÓN DE RED.

Por diversas necesidades de aplicación, las redes se dividen en segmentos. Algunas de estas razones están relacionadas con las tecnologías de red subyacentes; otras, responden a ubicaciones geográficas. Algunas de las mejores razones para aislar segmentos de red se basan en el uso específico que se le denomina a la red.

Si una gran cantidad del tráfico de una red sucede entre unos cuantos nodos, es mejor aislar estos. El aislamiento disminuye el uso y proporciona una red mejor respuesta para los demás usuarios de red.

Otras razones para la segmentación es el cambio de tecnología de red. Por ejemplo, en un área de oficina se puede ejecutar Token Ring y en el piso de ventas de la tienda es factible ejecutar Ethernet. En cada caso, hay una función distinta, la oficina puede requerir Token Ring para comunicarse AAS/499. Pero el piso de ventas puede tener Ethernet para que se comuniquen los controladores y las computadoras de ese departamento. Luego la información del mismo piso puede subirse a la red de la oficina para seguir los pedidos. Las tecnologías se conectan por lo general mediante ruteadores, que sólo pasan la información puede compartirse entre los nodos de las redes respectivas.

El uso excesivo de ruteadores en una red puede llegar a ser molesto para ésta y sobrepasar sus beneficios. Emplear un ruteador sirve de poco si todos los nodos de una red deben comunicarse con todos los nodos de otra red y viceversa. En esta instancia las ventajas del ruteo podrían disminuir por la sobrecarga de los protocolos de ruteo. En este tipo de situaciones, un puente (bridge) es la mejor alternativa.

Un puente permite compartir toda la información entre dos redes. El acceso es en el nivel físico y no en el nivel de red, por lo que no incurre en una sobrecarga de traducción de direcciones y ruteo. Un puente permite transmitir toda la información, incluso el sistema de emisión de mensajes. Si dos redes rara vez comparten información, el ruteador es la mejor alternativa y caso contrario, un puente es la selección adecuada.

1.6. SELECCIÓN DE UNA CONFIGURACION DE RED.

El medio físico que emplea las redes actualmente es muy diverso. El tráfico de red no esta limitado a Ethernet, ARCnet o Token Ring. Puede viajar por el RS232 asíncrono, las líneas E1 y la estructura de relevadores.

No hay que olvidar el ancho de banda que requiere una aplicación. Muchas aplicaciones necesitan la transferencia de megabytes de datos. Otra cosa por considerar es la ubicación física de la red. Si todos los nodos están en el mismo edificio, es posible usar una sola LAN. Sin embargo, si las redes se diseminan por toda ciudad, tal vez se necesite una conexión E1. Si los nodos están en posiciones geográficas diferentes, es factible usar una red de estructura de relevadores o de paquetes de intercambio.

En la disposición de una red, se debe tomar en cuenta el tipo de información que habrá de transmitirse por la red, la ubicación física y la carga de la red. Para determinar la capacidad de la red, examine el tipo de estaciones de trabajo, de servidores y aplicaciones. Si en la red se usan estaciones de trabajo sin disco, se pone una mayor carga en la red para cada nodo. La razón de esto es que cada estación remota requiere que todo nodo, con el código del sistema operativo, baje por la red. Como todas las aplicaciones utilerias y archivos de datos están guardados de modo remoto, cada acción de la estación de trabajo necesita tener acceso a la red.

También se debe considerar la cantidad de tráfico NFS que se dará en la red, ya que, NFS proporciona servicios de disco virtual, remotos, por lo que la información recuperada y guardada en esos discos remotos se usa de manera constante sobre red.

Otros elementos por considerar son las imágenes gráficas grandes, los archivos de intercambio y paginas usadas por la memoria virtual, las aplicaciones de base de datos distribuidas, el tráfico de impresión y el tráfico de terminales. Todo esto se debe considerar en cualquier red, pero los diseñadores y usuarios de LAN de PC´s no tienen casi nunca que enfrentarse a ello.

Es por éstas razones que cuando una red se conecta a una comunidad de usuarios general, entran en juego todos los aspectos del ambiente de red.

CAPITULO II. INSTALACION DE UN SERVIDOR WINDOWS NT.

Objetivo:

Describir detalladamente la instalación de un servidor para una red Windows NT, su forma de operar y sus características principales.

CAPITULO 2 INSTALACION DE UN SERVIDOR WINDOWS NT.

2.1 SISTEMAS OPERATIVOS DE RED

Los sistemas operativos, básicamente se dividen en dos tipos:

1) PUNTO A PUNTO: Este es un tipo de sistema operativo que les permite a los usuarios compartir los recursos de sus computadoras y acceder a los recursos compartidos de otras. Según este esquema, se pueden compartir un directorio o una impresora de la computadora propia, de forma que otros usuarios puedan acceder a ellos, pudiendo hacer estos lo mismo son sus computadoras. El modo punto a punto implica que todas las computadoras poseen el mismo status en la red. Ningún sistema es "esclavo" de otro.

2) CON SERVIDOR DEDICADO: En un sistema operativo con servidor dedicado una o más computadoras se conservan como servidores de archivos, ni pudiendo utilizarse para otra actividad. Los usuarios accesan a los directorios y recursos de archivos dedicados, pero no a los de otros sistema. De ésta forma, se aumenta la seguridad y se evita reducir el rendimiento de las computadoras personales.

Además, los sistemas operativos de red ofrecen una amplia variedad de servicios, los que se describen a continuación:

- Nomenclatura global: un sistema de nomenclatura global permite a los usuarios ver y accesar a los recursos y a otros usuarios de cualquier punto de la red, sin tener que saber exactamente donde se encuentran.

- Servicio de archivos y directorios. En una red los usuarios accesan a programas y archivos que se encuentran en el servidor de archivos central debido a que los usuarios guardan sus archivos privados en este servidor, la seguridad e integridad de los datos es importante.

- Sistema tolerante a fallas: Un sistema tolerante a fallas ofrece un sistema para asegurar la supervivencia de la red en caso de que fallen los componentes.

- Seguridad en la conexión: Mediante esta posibilidad se puede restringir el acceso de usuarios al servidor sus directorios y archivos, mediante "passwords". También se puede evitar que algunos usuarios puedan conectarse desde estaciones de trabajo distintas de las que se les haya asignado. Además se pueden establecer restricciones del tiempo para las sesiones de trabajo de los usuarios.

- Herramientas de administración: Las herramientas de administración se hacen esenciales cuando crece el tamaño de las redes. Sin éstas, puede llegar a ser imposible el seguimiento de las actividades y el rendimiento de las MAN y las WAN. Una solución es agrupar los responsables y darles herramientas para gestionar de forma remota los servidores y las estaciones de trabajo.

Existen en el mercado diversos sistemas de red, pero dentro de esta gama algunos tienen la facilidad de operar en una PC y otros no. Dentro de los sistemas de red más populares y utilizados se encuentran:

- Windows NT
- Novell
- Unix

Windows NT: es un sistema operativo que incluye funciones multitarea, portabilidad y soporte para realizar tareas de multiproceso simétrico desarrollado por Microsoft. Usa un sistema de ficheros propio conocido como NTFS mediante el cual, entre otras cosas, puede aceptar hasta 256 caracteres para nombres de fichero, también dispone de un sistema siguiente de transacciones, es decir, si el sistema falla por alguna razón, al arrancar de nuevo Windows NT vuelve a poner los datos en el estado en que se encontraban. Este sistema ha sido diseñado con una estructura modular y portable. Básicamente consta de un núcleo kernel y varios subsistemas diferentes. hay subsistemas que pueden ejecutar programas que funcionan bajo OS/2 y un DOS virtual que permite ejecutar MS-DOS y aplicaciones Windows de 16 bits.

El código de NT ha sido escrito en su totalidad en lenguaje de programación C, de ahí su portabilidad. Como se puede apreciar, Windows NT cumple con las normas de nivel de seguridad C-2 definidas por el gobierno norteamericano para entornos en los que se exige una alta seguridad. Dispone de un modulo de control de accesos llamado Event Viewer (Visualizador de Eventos) que permite al administrador de la red disponer de la información contenida en un fichero de registro en el que se almacenan todos los errores e intentos de

violación que se han producido en la red, así como la fecha, hora tipo y lugar en donde se ha producido el intento y también el nombre del usuarios que los ha causado.

Además Windows NT dispone de un servicio que se conoce como servidor de acceso remoto llamado RAS que permite que otras estaciones de trabajo DOS, Windows y NT puedan marcar y entrar en una red NT y trabajar como si estuvieran conectados directamente a ella. Este servicio puede soportar un máximo de 64 conexiones, soporta también el protocolo X.25 y permite conectarse a través de la Red Digital de Servicios Integrados (RDSI o ISDN de sus siglas en inglés). Otra característica de Windows NT, es que se puede configurar un servidor SNA de NT puede conectarse con ordenadores Mainframe, soportando hasta 250 clientes en modo asíncrono.

UNIX: Este sistema operativo tienen grandes ventajas y características, de tal forma que lo han convertido en el sistema operativo estándar de los sistemas distribuidos,; es decir micro, mini y macro computadoras conectadas en red. El sistema UNIX tiene capacidades de multiprocesamiento de una manera más sencilla y versátil que muchos otros sistemas operativos, además que ha demostrado un gran capacidad para desarrollo de software bajo su plataforma. Existe una gran facilidad para ejecutar las tareas en cualquier arquitectura de computo: microcomputadoras, minicomputadoras, main frames, y demás; esto es gracias al lenguaje en el está desarrollo: el lenguaje C.

Además que la seguridad es un factor que caracteriza al sistema UNIX porque trabaja en modo protegido e incluye elementos de seguridad que lo hacen muy bueno para el trabajo de multiusuario. No obstante, algunas de sus

inconveniencias es el alto uso de comandos, los cuales el usuario o administrador que trabaja con UNIX debe de tener siempre en mente; y no trabaja en un ambiente cien por ciento gráfico, lo que resulta en un sistema operativo diseñado para usuarios más experimentados.

Novell: Esta compañía ha desarrollado a partir de los años sesentas una gran cantidad de productos para la administración de los sistemas de computo, lo que le ha permitido colocarse entre las compañías más importantes dedicadas a esta actividad. La línea de productos actual de sistemas operativos de Novell incluye Net Ware Lite, un sistema operativo punto apunto basado en el DOS. Net Ware es un sistema operativo de red e 32 bits que se ejecuta en procesadores Intel de 80386 y superiores. Este incorpora los servicios de directorios Net Ware (Net Ware Services NDS). Dentro de este sistema, cada usuario y recurso será denominado como un objeto en el sistema DNS y será registrado en una base de datos global de la red. Así los administradores de red y los usuarios pueden accesar fácilmente a los objetos del sistema sin importar en donde se encuentren en la red. Net Ware es un sistema operativo de 32 bits que usan un espacio de direccionamiento sin segmentación. Esto permite que los programas trabajen en un modo más eficiente. Puede manipular miles de interrupciones y procesar miles de peticiones de clientes por segundo. Net Ware es modular y expandible, además de que se pueden realizar modificaciones, actualizaciones y aplicaciones en la red. Dentro de los servicios que pueden ofrecer Net Ware están:

- Soporte para sistemas operativos distintos del DOS.
- Servicios de comunicaciones.
- Servicios de bases de datos.

- Servicios de mensajes.
- Servicio de almacenamiento y copias de seguridad.
- Servicio de administración de la red.

Con Novell la seguridad es ofrecida a varios niveles, los cuales se describen a continuación:

- Seguridad a nivel cuenta/clave de acceso: Los usuarios introducen la orden LOGIN par tener acceso al sistema de archivos y estos introducen su nombre de usuario seguido de una clave de acceso.

- Restricciones sobre las cuentas: bajo NetWare, cada usuario tiene una cuenta gestionada por el administrador de la red. Se pueden aplicar restricciones sobre las cuentas para controlar cuando pueden conectarse los usuarios, desde que estaciones pueden hacerlo y cuando expiran sus cuentas.

- Seguridad de objetos y archivos: El administrador de la red asigna a los usuarios privilegios (trustee rings) sobre objetos, directorios y archivos.

- Seguridad entre redes: Los servicios del sistema deben controlar todos los objetos en redes interconectadas, incluyendo objetos de usuario y sus derechos de acceso.

2.2. DISPOSITIVOS UTILIZADOS

Para poder llevar a cabo la instalación del Servidor de Comunicaciones, se utilizaron los siguientes dispositivos y recursos:

- Disponibilidad de ocho salidas habilitadas de comunicación de datos con una velocidad de transmisión de 64 Kb/seg para conectar en red al servidor.

- A estas salidas de datos se instalaron siete máquinas de tipo PC, las que fueron destinadas a servir como estaciones de trabajo con el software de Windows NT Workstation, con las siguientes características: procesador AMD 586/133MHz con 8 MB en memoria RAM y discos de 1 Gb.

- Una PC destinada a trabajar como servidor, en donde se instaló el software de Windows NT Server y aplicaciones específicas para su uso, teniendo el servidor las siguientes características: Procesador Pentium 120 Mhz con 32 MB RAM, H.D. de 2 Gb, una unidad lectora de CD-ROM de 8x.

- Las PC se conectaron a la R.I.T. por medio de tarjetas de red 3 COM Etherlink III e interfaces RJ45 hacia las rosetas de datos.

- Disponibilidad de una impresora Láser 4 HP para aplicaciones en red.

2.3. CUALIDADES DE WINDOWS NT.

A continuación se describen las cualidades principales de Windows NT con las que se baso la propuesta de utilizarlo tanto en las estaciones de trabajo como en el servidor:

- El sistema operativo de red Windows NT es el más apropiado para la operación y administración de una red LAN porque presenta una alta estabilidad de comportamiento para administrar un número pequeño de estaciones de trabajo, aproximadamente de 1 a 350.

- Es un sistema operativo de red Centralizado, es decir, todas las cuentas y políticas de seguridad pueden ser administradas desde un punto de computadora a computadora y de usuario a usuario. Esto es, las herramientas de administración de red de Windows NT permiten administrar cualquier computadora que corra bajo Windows 3. X, Windows for Workgroups 3.x, Windows NT Workstation y Windows NT Server.

- Deriva una mayor y mejor administración en la asignación de recursos compartidos que otros sistemas operativos de red.

- Posee un alto grado de interoperabilidad con otros sistemas de red como lo son Netware de Novell y Unix.

- Incluye el servicio RAS (Remote Access Service) Servicio de Acceso Remoto, el cual proporciona la facilidad de 256 conexiones simultáneas de forma remota.

- Contienen una facilidad de integración, tanto de software como de hardware.

- Posee soporte múltiple de plataformas: Intel 80386 y posteriores, Power Pc, MIPS R4x00, DEC Alpha AXP y múltiples procesadores simétricos o sencillos.

- Contiene software integrado para utilizar diferentes protocolos: TCP/IP, IPX/SPX, NetBEUI, AFP, DLC, además de utilizar el servicio de Ras con X.25, ISDN y líneas publicas estandarizadas.

- El usuario y administrador no necesita ser una persona experta, debido a su facilidad de instalación y manejo, así como el ambiente gráfico en el que se desenvuelve. El empleo de este sistema operativo de red se puede describir como "amigable" debido a su facilidad de uso y la gran ayuda de operación disponible en pantalla.

- Trabaja con las aplicaciones que corren bajo Windows 3x. y Windows 95.

- Contiene un sistema de tolerancia a fallas, el cual aisla una aplicación o recurso con falla permitiendo terminar la ejecución sin necesidad de cerrar aplicaciones y servicios, con la ventaja de no necesitar reiniciar el sistema.

- La tendencia comercial gira hacia el entorno de NT, debido a las características propias que lo constituyen.

- La empresa Microsoft ofrece un respaldo de soporte con sus licencias, así como descuentos en futuras actualizaciones. Esto se traduce en que Windows NT resulta una opción costeable para una empresa, negocio, o lugar donde se requiera una red LAN.

2.4.INSTALACION DEL SERVIDOR DE COMUNICACIONES

En ésta sección intentamos brindar de forma global, un apoyo para la instalación del Servidor con Windows NT. La finalidad no es otorgar una guía paso a paso para su instalación, si no más bien la descripción de los recursos que se deben utilizar, así como los parámetros más importantes a definir dentro de éste entorno. Así, la instalación del Servidor se inicia copiando los archivos de inicialización desde discos flexibles o desde un CD-ROM (Según el recurso) al disco duro del servidor.

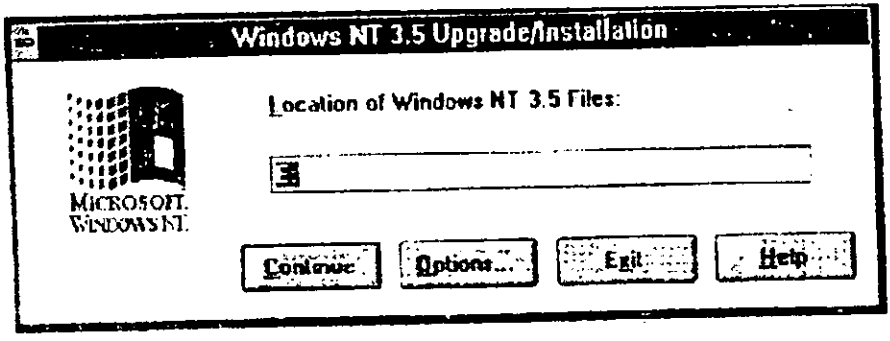

Figura 2.1 Ventana de Inicialización.

Lo primero a definir, será el tipo de partición a utilizar, en donde recomendamos utilizar el formato NTFS, para poder hacer uso de sus propiedades dentro de NT:

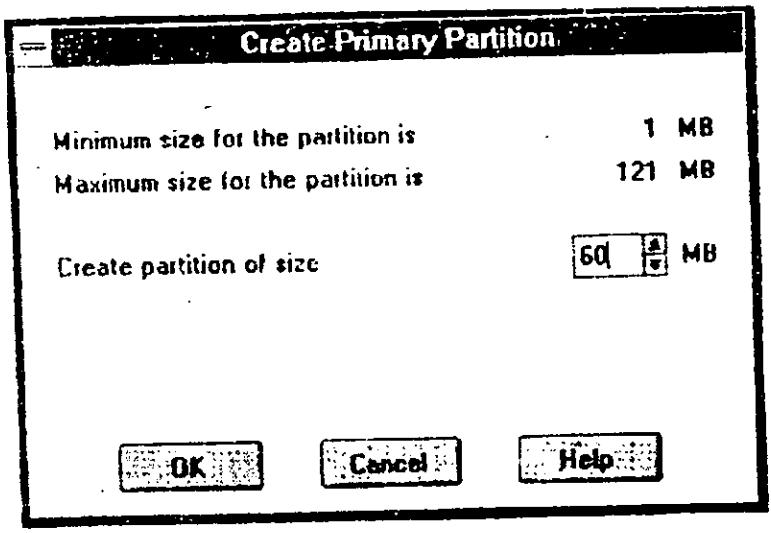

Figura 2.2 Ventana de Opciones para Particionar el HD.

Posteriormente se instalarán los archivos de ejecución y se validarán los dispositivos que se tengan instalados, esto es, detectará el tipo de disco duro instalado, la cantidad de memoria RAM, el tipo de procesador, y si los dispositivos de red existentes.

Aquí es donde Windows NT muestra sus cualidades de integración, ya que reconoce los dispositivos y además selecciona automáticamente sus parámetros bajo la supervisión del usuario, es decir, permite modificarlos, aún, que el mismo los optimiza:

Por ejemplo, una vez que se reconoce la tarjeta de red se configuran sus parámetros, teniendo la opción de verificar que no existan conflictos en las interrupciones (IRQ), en los DMA, o con cualquier otro dispositivo:

Después detecta el tipo de protocolo de acuerdo a los dispositivos de red instalados y conectados, en donde encontraremos la siguiente ventana de configuración:

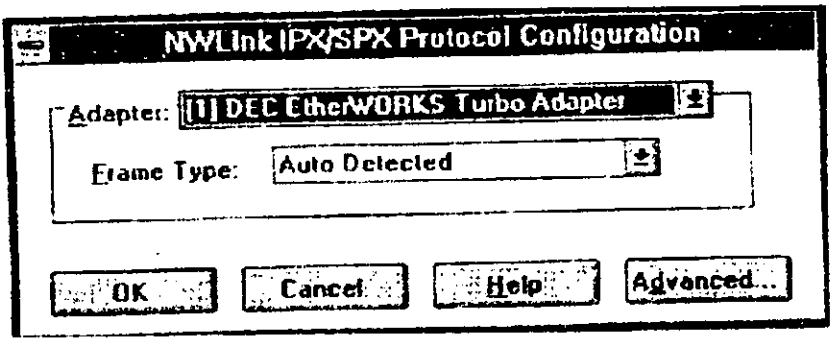

Figura 2.3. Detección de Protocolo de cuerdo a los Dispositivos de Red Instalados.

De acuerdo con lo realizado anteriormente, se definen los parámetros de al red; este punto es de suma importancia porque aquí es donde se define el Dominio y el Nombre de la máquina con el que se identificara como servidor:

Pasando al menú de configuración de protocolo, podremos adicionar ó quitar los protocolos que sean necesarios para la comunicación de la red como TCP/IP, NetBEUI, etc., para poder establecer la comunicación dentro y fuera de la red.

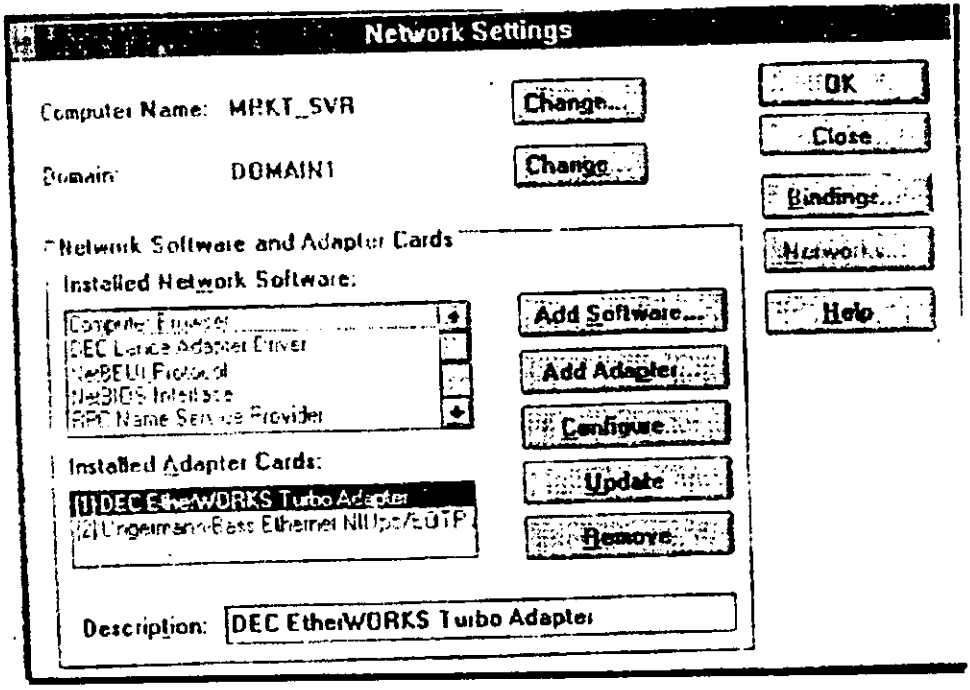

Figura 2.4. Configuración de los Parámetros de Red

Después se define el Servidor de Nombres de Dominio (DNS), el cuál nos muestra la dirección con la cual puede ser localizado nuestro Servidor de Comunicaciones de acuerdo al dominio al que pertenece; teniendo la característica de asignar un nombre a cada una de las direcciones a utilizar.

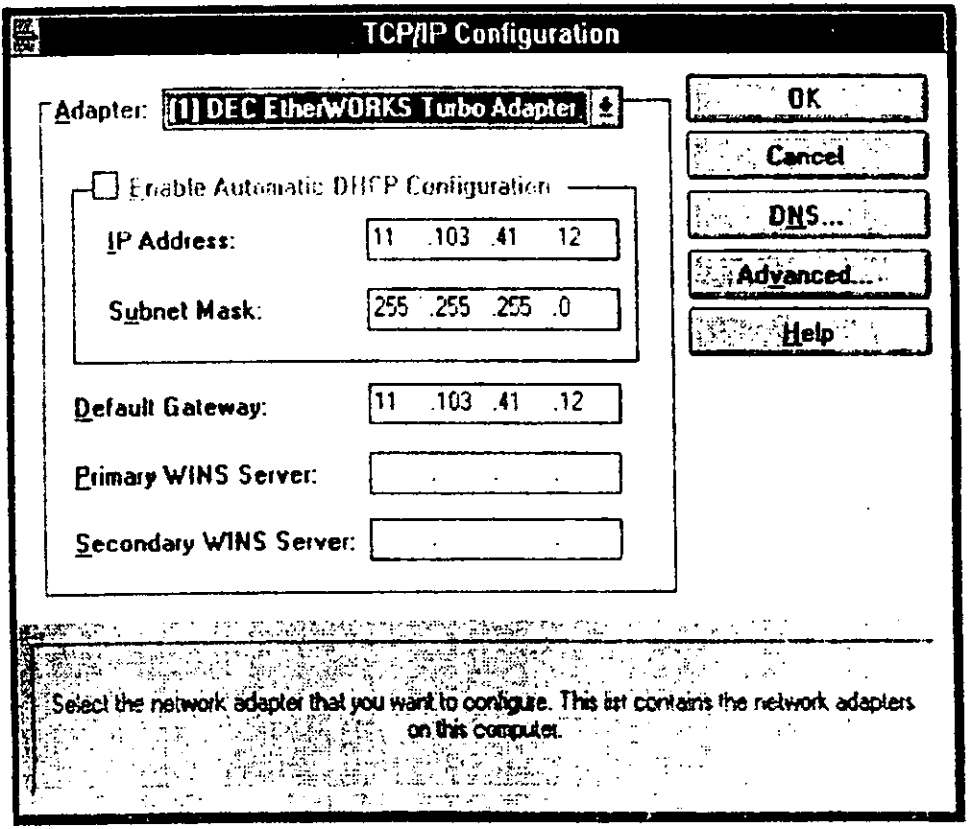

Figura 2.5. Configuración para TCP/IP.

Una vez seleccionado nuestro protocolo de comunicación, si seleccionamos la opción de propiedades, la siguiente ventana que aparezca nos mostrara la dirección IP a la cual esta direccionada la computadora, la mascara de red, y la compuerta (gateway). Todas las especificaciones se pueden modificar posteriormente para posibles actualizaciones y cambios:

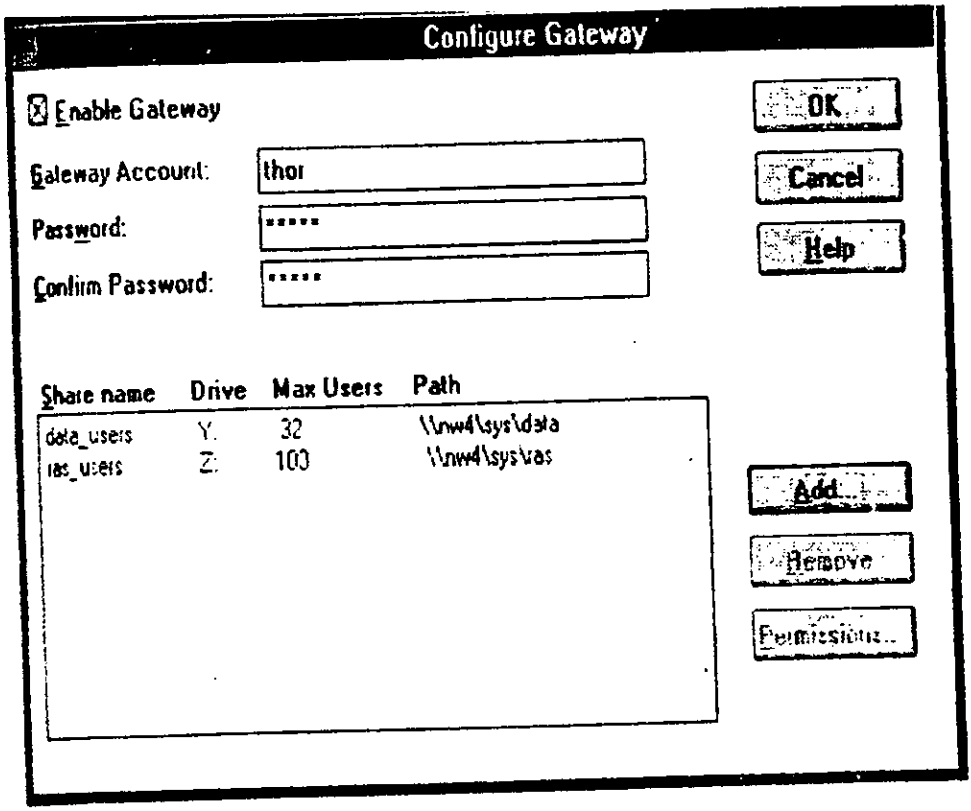

Figura 2.6 Configuración de la Compuerta (Gateway).

Después de definir a TCP/IP como protocolo a utilizar, se configura la seguridad de acceso con el SNMP (Simple Network Managment Protocol) Protocolo de Administración de Red Simple, el cuál permite administrar vía remota a aquellas computadoras que trabaje sobre ambiente NT, por medio de herramientas de administración como Sun Net Manager o HP Open View:

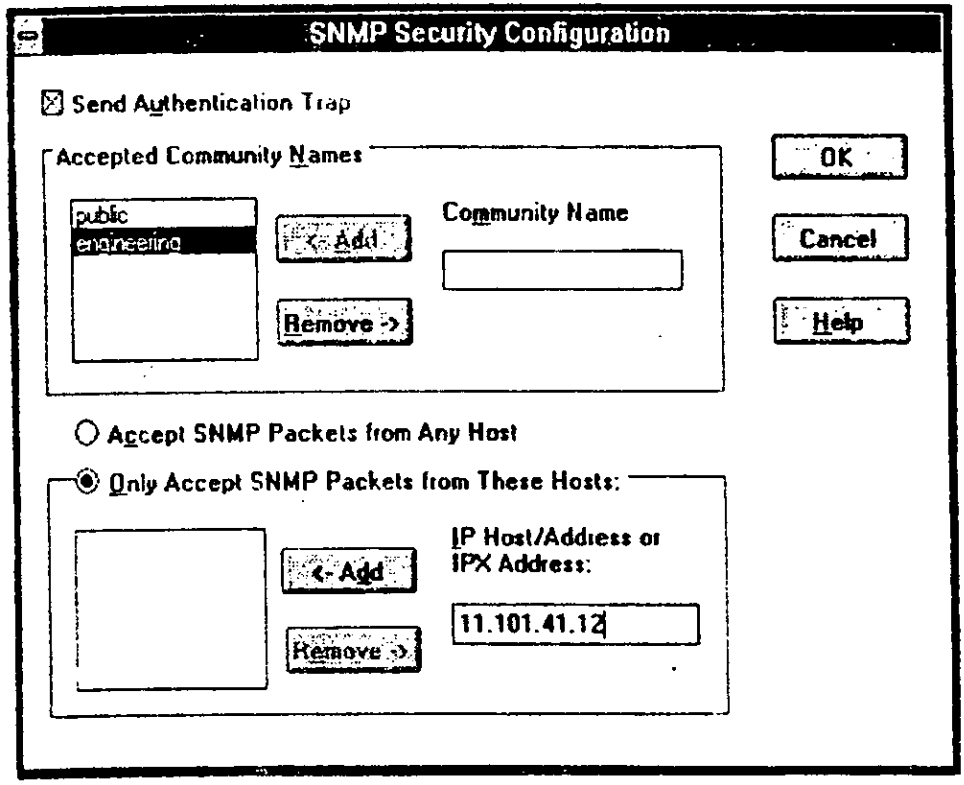

Figura 2.7. Configuración de la Seguridad con SNMP.

Una vez configurado el SNMP, se puede utilizar el Agente SNMP para administrar los accesos de información con la herramienta de administración disponible:

Ahora, si se tienen acceso remoto a la red vía módem (en nuestro caso utilizamos tarjetas de red) se adiciona el DHCP (Dynamic Host Configuration Protocol) el cuál es un Protocolo de Host Dinámico, que es un servicio utilizado para configuración de forma automática TCP/IP a las computadoras

que trabajen con NT, y para accesar a impresoras de otra red con TCP/IP e inclusive en otras plataformas como Novell o UNIX.

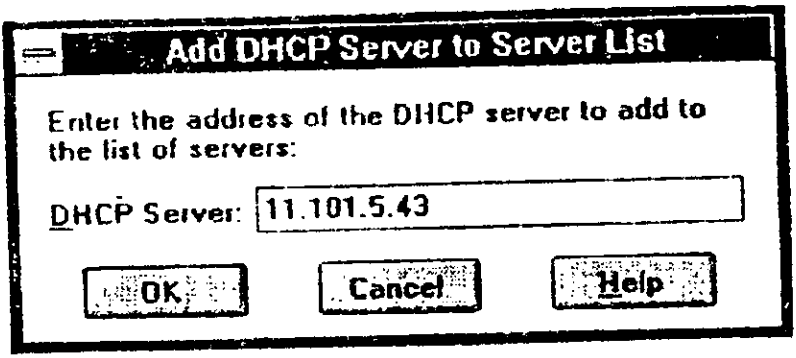

Figura 2.8 Configuración del Protocolo de Host Dinámico (DHCP).

Posteriormente, se puede configurar la forma en que se conectara a la red y se visualizaran que otros están conectados a este dominio, así como sus características:

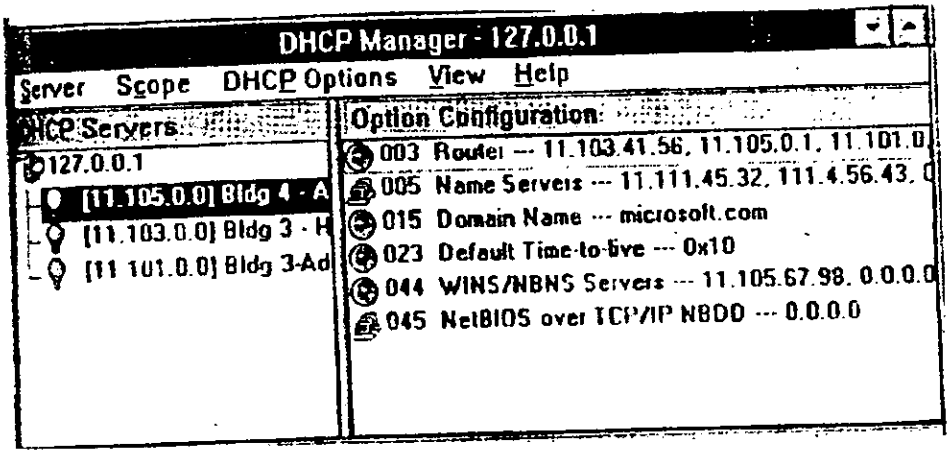

Figura 2.9 Administración del DHCP.

Ahora, para instalar aplicaciones, NT primero verifica si hay algunas existentes (ésta opción es más utilizada cuando se instala NT como actualización):

Una vez que encuentran aplicaciones existentes se puede decidir si se desean instalarlas o quitar algunas de las existentes:

Una vez establecida la forma en que el Servidor NT operara en la red, se definen los dispositivos instalados en éste de forma similar que en cualquier Windows 3.x.

Por ejemplo, si se desea cambiar el tipo de tarjeta de vídeo se accesa al panel de control y se selecciona la tarjeta indicada o se define por medio de su respectivo driver.

De esta forma, si Windows NT no reconoció todos los dispositivos instalados o no los asocio con uno similar, se tienen la facilidad de emplear el driver del dispositivo respectivo.

Por último, se cargan todos los archivos de instalación, se reinicia automáticamente el servidor y Windows NT se iniciará. En donde se observará su entorno característico:

2.5 CARACTERISTICAS DE WINDOWS NT

Un punto que hay que tener muy presente es el hecho de que Windows NT, puede aprovechar al máximo las capacidades de procesadores de 32 bits o mayores, además, NT corre actualmente sobre microprocesadores Intel 80386 o

mayores, sobre procesadores RISC ALPHA de Digital Equipment Corporation y sobre computadoras con arquitecturas multiprocesadores, tales como Compaq y NCR.

Windows es una familia Extensible, que abarca diferentes tipos de necesidades, pero conservando siempre la compatibilidad y la facilidad de uso, sin importar la complejidad del sistema y poder del procesamiento que exista tras la interfaz amigable.

Windows NT esta basado en una serie de modelos básicos. Una vez que se ha comprendido los principios que fundamentan estos modelos es mucho más fácil de comprender el funcionamiento interno del sistema operativo.

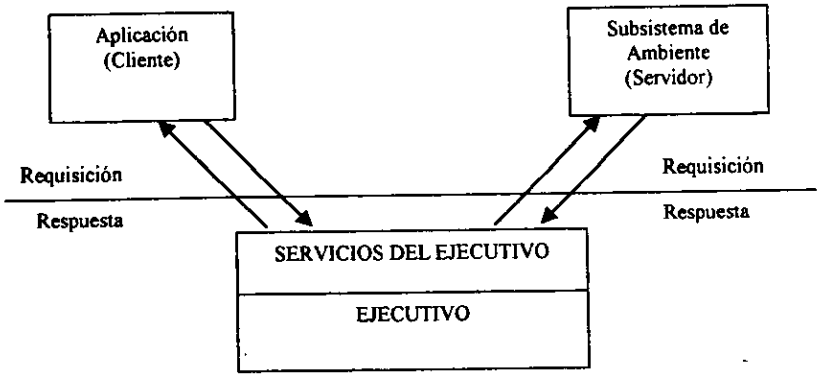

Figura 2.10 Arquitectura Cliente- Servidor

* Modelo Cliente – servidor. Este modelo es tradicionalmente asociado a redes de comunicaciones en las cuales existen computadoras o nodos que son clientes y computadoras o nodos que son servidores. Un mismo nodo puede en ocasiones realizar ambas funciones al mismo tiempo. El principio es idéntico

cuando hablamos de un sistema operativo. En este caso existen procesos clientes y procesos servidores.

En la gráfica anterior, la aplicación es el Cliente y el Subsistema de ambiente es el servidor. Ambos se comunican entre sí utilizando LPC (Local Process Communication), que son una serie de servicios de comunicación que proporciona el Ejecutivo NT, que es el núcleo del sistema.

El proceso Cliente envía una requisición al proceso Servidor, a través del Ejecutivo; el Servidor recibe la requisición, la atiende y envía la repuesta. Un subsistema ambiente, para establecer un paralelo, es como una "vista" de datos. Es decir es el proceso que construye y presenta un interfaz al usuario a través de la cual este obtienen acceso a los servicios del sistema. Ejemplos de subsistemas de ambiente que están disponibles la primera versión de Windows NT son Windows 3.1, Windows 3.11 (32 bits), POSIX y OS/2 (modo carácter). Explicando esto de otra forma podemos decir que cada subsistema de Ambiente presenta una visión o una realidad Virtual del sistema. Dicha visión cambia un poco dependiendo de la idiosicrasia propia del sistema operativo que la originó, y es compaginada con la realidad del Ejecutivo NT a través de los servicios que el mismo proporciona a cada subsistema.

Cabe mencionar el hecho de que una de las consecuencias del uso de este tipo de arquitectura, en el caso de Windows NT, ha sido que el sistema operativo esta estructurado por capas en forma completamente modular. Como en el caso del modelo OSI en comunicaciones, cada módulo es completamente independiente de los demás. Por lo que es necesario definir muy cuidadosamente las interfaces de comunicación entre módulos y será posible en

un momento dado el "sacar" un módulo y reemplazarlo por otro nuevo sin afectar al resto del sistema operativo.

Como se aprecia en la gráfica de la figura 2.18, la capa del Ejecutivo corre en modo privilegiado y tanto la aplicación como el subsistema de Ambiente, corren en modo usuario. Correr en modo privilegiado significa que las aplicaciones no tienen acceso directo a los procesos del Ejecutivo, más que a través de una serie de servicios que llamamos servicios del Ejecutivo y que son el único mecanismo que poseen las aplicaciones que corren en Windows NT para obtener el acceso a los recursos del sistema. Las implicaciones del uso de este modelo son enormes. Cada subsistema de ambiente corre en un ambiente completamente aislado de las demás, en un modo usuario y completamente aislado de sus aplicaciones, lo que significa que cuando una aplicación falla no puede detener al sistema tampoco al subsistema de ambiente.

Si el subsistema de Ambiente falla no puede a su vez detener al sistema. Esto quiere decir que si una aplicación falla, lo único que se vera afectado será sus propias instancias de ejecución. El resto de las aplicaciones y subsistemas de ambiente seguirán corriendo de forma normal. Otro resultado derivado del uso de este modelo es el hecho de que cada subsistema de ambiente corre en realidad en modo nativo, no es una emulación. Hecho que garantiza buen rendimiento al correr aplicaciones.

Finalmente, un sistema operativo de este tipo se presta muy fácilmente a la integración de sistemas de cómputo distribuido. Ya que estos operan esencialmente siguiendo un modelo Cliente- Servidor, con lo cual la red de

comunicaciones se convierte en una extensión natural del sistema operativo, en este caso de Windows NT.

- Modelo de Multiprocesamiento Simétrico: En un intento por incrementar el poder de cómputo al servicio de los usuarios, se ha buscado otros caminos, caminos diferentes al de la computación de más y más componentes en una pastilla semiconductora.

Uno de estos caminos ha llevado al desarrollo de la tecnología RISC y otro ha sido el desarrollo de computadoras con múltiples procesadores, no siendo excluyentes uno de otro. La creación de sistemas de procesadores múltiples presenta problemas interesantes para los desarrolladores de sistemas operativos. Y no resulta ninguna exageración el señalar que cualquier sistema operativo que busque jugar un papel importante dentro de la industria de cómputo en los primeros años, deberá ser capaz de operar en este tipo de ambiente. Así, otro de los modelos sobre los cuales esta basado Windows NT, es el modelo de Multiprocesamiento Simétrico (SMP por sus siglas en inglés, Symmetric MultiProcessing).

En general existen dos formas de operar un sistema de cómputo con procesadores múltiples. La primera consiste en utilizar un modelo asimétrico en el cual por ejemplo un procesador corre los procesos, propios del sistema operativo y otro las aplicaciones. Se proporciona algún mecanismo de comunicación entre procesos para que pueda fluir la información entre el sistema operativo y las aplicaciones, generalmente a través de memoria compartida por todos los procesadores.

Este modelo presenta el inconveniente de que si no hay mucha carga para el sistema operativo por ejemplo, un CPU estará siendo desaprovechado, mientras que probablemente existan aplicaciones que puedan necesitar de ese poder de procesamiento.

Windows NT utiliza el modelo de procesamiento asimétrico, es decir que no existen procesadores destinados a tareas específicas, como seria el correr el sistema operativo, o atender solo requisiciones de dispositivos de Entrada/Salida.

Cada proceso en Windows NT puede poseer varias instancias de ejecución. Estas instancias de ejecución se llaman threads. Y para situarlas aun mejor podemos compararlas con procesos ligeros. Es decir, al momento de correr un programa en cualquier sistema operativo, se genera una instancia de Ejecución del código de ese programa. Dicha instancia de ejecución se instala en una región de memoria, crea sus variables de ambiente y estructuras de datos, conforme se le va proporcionando tiempo de CPU va realizando una serie de tareas par las cuales el programa fue concebido y realizado.

A esta primera instancia de ejecución de un programa se le conoce como proceso y en sistemas operativos multitareas como es el caso de Windows NT. UNIX, OS/2, cada proceso puede generar instancias de ejecución. Lo que significa que la relación entre la instancia de ejecución original y las que se hayan generadas después, se mantendrán de alguna manera.

Tenemos entonces que tanto el Ejecutivo, el kernel, las aplicaciones, los subsistemas de ambiente corren en forma de procesos y cada uno de ellos

tienen una o varias instancias de ejecución, llamadas threads. Ahora bien, en un sistema multiprocesadores, sobre todo si es de procesamiento simétrico, uno de los retos es repartir el trabajo equitativamente. El objetivo ideal es que todos los procesadores se aprovechen todo el tiempo, al cien por ciento de su capacidad y para que esto sea posible, no pueden existir procesadores de propósito específico. Es decir que todos los procesadores deben ser capaces en un momento dado de correr cualquier tipo de proceso, sea este un proceso de sistema operativo, una aplicación o una operación de entrada salida. Windows NT emplea exactamente este modelo, calendarizado threads, no procesos y haciéndolo en base a prioridades claramente definidas.

Existen 32 colas de ejecución dentro del sistema operativo, en estas se van depositando los threads que esperan ejecución y cada cola corresponde a una prioridad diferente, algunas de las prioridades son de tiempo real. Con excepción de los threads del kernel, cualquier threads puede ser forzado en un momento dado por el sistema operativo a abandonar su uso de CPU en beneficio de un threads que tenga que realizar alguna operación crítica. El proceso de Calendarización de threads (llamado calendarizador en la, gráfica), parte integral del Kernel, asigna threads a los diferentes procesadores conforme estos se van ocupando, en base a las prioridades de las colas con prioridad de tiempo real y luego el resto. la prioridad de un thread determinado va aumentando conforme se incrementa el espacio de tiempo transcurrido sin que haya recibido atención de alguno de los procesares del sistema. El kernel mismo se hace cargo de sincronizar a los diferentes procesadores entre sí.

- Modelo de Manejo Interno de Objetos: Este tercer modelo nos indica que Windows NT maneja internamente aquellos recursos que pueden ser

compartidos por dos o más threads, tratándolos como objetos. Esto quiere decir que los threads solo tienen acceso a los recursos del sistema mediante la solicitud de servicios al ejecutivo (Servicio del Ejecutivo) en el caso general y a los servicios internos del kernel, en el caso de los threads del mismo kernel cada recurso y cada objeto tienen sus propios atributos y características que proporcionan uno o varios servicios propios. Absolutamente todo aquello que puede ser aprovechado por dos o más threads es manejado internamente como un proceso – objeto.

Esto significa que tanto procesos como threads ven a los recursos del sistema como una serie de identificadores de acceso, pero desconocen completamente como son o como funcionan estos recursos.

Para los threads en ejecución es lo mismo escribir a un disco duro que hacerlo a un WORM, aun cuando la estructura del sistema de archivos de ambos sea completamente diferente. Esto es algo parecido al uso de una red telefónica solo conoce números telefónicos, pero no sabe no se preocupa por saber si su línea es analógica o digital, o de a través de cuantas centrales o conmutadores tiene que pasar antes de que una llamada llegue a su destino.

Las consecuencias importantes de la utilización de este modelo son dos:

- La primera radica en el hecho de que el funcionamiento del sistema operativo, aplicaciones y demás software que corre, es completamente independiente de la estructura y características propias de cada recurso como un objeto, la estructura interna del mismo puede cambiar, pero siempre presentara la misma interfaz.

- La segunda es también muy importante y consiste en que todos los recursos son administrados y proporcionados por el sistema operativo mediante el recurso de creación y asignación de objetos, el esquema de seguridad interno del mismo sistema operativo. No puede ser pasado por alto. Cada vez que se crea o solicita acceso a un objeto, el sistema de seguridad del sistema operativo autoriza o no el acceso al objeto en cuestión.

2.5.1 ESTRUCTURA DE WINDOWS NT.

Conociendo ya los modelos arquitectónicos ahora se analizan las principales capas que constituyen a Windows NT.:

- Capa de Abstracción de Hardware: HAL (Hardware Abstracción Layer por sus siglas en inglés) es básicamente una capa cuya función principal consiste en aislar al Ejecutivo y al Kernel de las diferencias que puedan existir entre diferentes plataformas de Hardware. Actualmente, todas las plataformas de hardware a las cuales ha sido portado a Windows NT (Intel 80X86, MIPS y ALPHA) poseen arquitectura Little Endian lo que significa que almacenar un dato de 16 bits colocan el byte más significativo en la primera dirección de memoria y el menos significativo en la segunda dirección de memoria. Es decir, que el dato 346H, almacenaría el 03 en la dirección 0001. Otras plataformas (SPARC, RIOS y HP-PA por ejemplo), tienen arquitectura Big Endian, es decir que almacenan los datos invirtiendo el orden que utiliza Little Endian. Al momento de portar Windows NT a una plataforma Big Endian. HAL será capa responsable de hacer que esta sea desconocida para Windows NT.

- El Microkernel: El concepto de Microkernel en sí, no es nuevo. Diferentes sistemas operativos experimentales han empleado el concepto. En esencia, el Microkernel es el corazón del sistema operativo. Se hace cargo de realizar funciones básicas necesarias para que pueda operar el sistema. En el caso de Windows NT, el kernel se ocupa de la calendarización de threads, manejo y despacho de excepciones, sincronización de múltiples procesadores y en general proporciona al Ejecutivo una serie de Servicios Internos que este utiliza para poder realizar sus funciones.

- Manejadores de Dispositivos: los manejadores o drivers de dispositivos son bien conocidos. En general se llama drivers aquellos módulos de software que se encargan de "hablar" directamente con los dispositivos de Entrada/Salida de la computadora, o en general con el hardware de la misma, ya sea directamente a través de HAL, para luego pasar la información resultante al Ejecutivo o al Kernel.

- Sistema de E/S: La función que realiza el sistema de Entrada/Salida es comunicarse con los Manejadores de Dispositivos. Aislando al resto del Sistema Operativo de las particularidades de cada tipo de dispositivos. Este sistema es en gran medida responsable del hecho de que Windows NT sea completamente independiente de los dispositivos de salida. Por ejemplo, el mecanismo de vídeo, de disco duro, de impresora; será exactamente el mismo, lo cual simplifica considerablemente la labor de los desarrolladores de software. El sistema de E/S se hace cargo también del manejo de memoria caché y de la estructuración, manejo y presentación al usuarios de la información contenida en los sistemas de archivos.

Los sistemas de archivos que maneja Windows NT en su versión inicial es FAT (File Allocation Table), el sistema de archivos tradicional de DOS, HPFS (High Performance File System de OS/2), acceso a red mediante un sistema de archivos llamado Redirector y un nuevo sistema de archivos NTFS (NT File System).

Las características generales de NTFS son:

- Manejo de volúmenes de hasta 18 Gbytes.
- Manejo de nombres universales.
- Permite la existencia de archivos de solo ejecución.
- Un solo sistema de archivos abarca varios dispositivos físicos y un solo archivo ambiente.
- Manejo del método de Fiule system Recovery, lo que permite al sistema de archivos recuperarse rápidamente por ejemplo después de una interrupción de energía eléctrica.
- Cumple con las especificaciones POSIX 1003.1, lo que significa que es sensible al uso de mayúsculas, mantienen la hora de última modificación realizada sobre un archivo determinado, e incorpora hard links.

Una característica interesante del sistema de E/S de Windows NT consiste en que permite cargar y descargar dinámicamente sistemas de archivos y drives o manejadores.

- El Ejecutivo: Es probablemente el módulo más complejo de todo el sistema operativo, sus funciones abarcan una porción enorme de lo que es el trabajo

del sistema operativo. Así mismo es su responsabilidad ofrecer a los procesos, en modo usuario, los servicios del Ejecutivo que éstos necesitan para poder tener acceso a los recursos del sistema. El ejecutivo ofrecer procesamiento multitareas, administración de recursos de memoria incluyendo el manejo de memoria virtual, acceso a dispositivos de E/S, creación de procesos y threads, creación y manejo de objetos, administración de los sistemas de seguridad y auditoria, ofrece mecanismos de comunicación entre procesos tales como memoria compartida y LPC (Local Process Comunication. Equivalente en funcionalidad a los mecanismos de IPC de UNIX).

En general, podemos decir que las llamadas a los servicios del Ejecutivo guardan similitud con lasa llamadas al sistema en un UNIX. Y resulta importante subrayar el hecho de que ningún componente del Ejecutivo, ni el ejecutivo mismo, son procesos que corran continuamente en la memoria de la computadora. El esquema de funcionamiento consiste en que cuando un proceso cualquiera realiza una llamada a los servicios del Ejecutivo, siguiendo el modelo de la arquitectura Cliente- Servidor, el proceso pasa un mensaje que es tomado por el sistema y entregado al componente del Ejecutivo que proporciona el servicio solicitado y que corre en modo privilegiado. Este componente toma control del thread en cuestión, corriendo siempre en modo privilegiado y realiza la función necesaria. Una vez que ha terminado devuelve el control para que la aplicación o el subsistema protegido, según sea el caso, siga corriendo.

Otro de los componentes del Ejecutivo es el Administrador de memoria Virtual que puede ser asignado a cada proceso es de 4 GB. Siempre y cuando estos

existan claro esta, ya sea en memoria principal (RAM) o en memoria secundaria. Este VMM (Virtual Memory Manager) es el responsable del proceso de Paginación, que consiste en trasladar paginas de RAM poco utilizadas a memoria secundaria y traerlas a RAM cuando estas son necesarias; así, los objetos de estructura de datos del sistema operativo, no residen en memoria paginable.

- Manejo Estructurado de Excepciones. El manejo de excepciones es un componente del sistema operativo que se hace cargo del control de interrupciones u otros eventos que interrumpen la ejecución normal de procesos para destinar tiempo de CPU a alguna tarea importante, como control de errores o control de dispositivos de E/S (entrada/salida). Esto le permite tener control sobre eventos y errores, y manejarlos de la manera más conveniente, siempre dentro del contexto de su aplicación.

- Subsistemas Protegidos: Finalmente, los componentes de la capa superior de Windows NT son los subsistemas protegidos se dividen en dos tipos, los subsistemas de Ambiente, los cuales se muestran en la gráfica titulada Estructura de Windows NT y corren un modo usuario y los Subsistemas Integrales, que corren en modo privilegiado. Los subsistemas de Ambiente son básicamente los ambientes operativos que proporciona Windows NT. Cada Subsistema de Ambiente es responsable de sus propios API's y una misma aplicación No puede utilizar APIs de diferentes subsistemas de Ambiente. Sin embargo, un subsistema de Ambiente, puede proporcionar servicios sobre cualquier proceso, siempre y cuando se cumplan dos condiciones, que es proporcione el identificador de proceso y que el usuario tenga los permisos apropiados.

Cada Subsistema de Ambiente ve una "vista" diferente del espacio de memoria del sistema. Cada vista adecua las características del espacio de memoria a la ideosincracia particular del subsistema de ambiente en cuestión. Debajo de todo esto, el Ejecutivo se hace cargo del manejo de memoria para todo el sistema. Los servicios que proporcionan estos subsistemas a través de sus API's se conocen como Servicios Nativos.

Desde este punto, el usuario puede correr cualquier aplicación que desee. El subsistema de Ambiente Windows ejecuta la aplicación, si es Win 32 lo ejecuta sin ningún problema. Si se trata de una aplicación Posix u OS/2, el subsistema Win 32 identificará el subsistema correcto y lo llamara, pasándole el control de la aplicación y abriendo para una ventana que recibe el nombre de consola. El control de vídeo de las diferentes sesiones de los sistemas de ambiente es mantenido por Win 32 en todo momento. Una excepción ocurre al ejecutar aplicaciones DOS o Windows de 16 bits. El subsistema de ambiente Win 32 ejecuta entonces una aplicación llamada (Virtual DOS Machine), misma que crea una consola para la aplicación de Win 32 y es responsable entre otras cosas de pasar las llamadas de estas aplicaciones al subsistema de ambiente Win 32.

Por lo que se refiere a lo subsistemas integrales, tales como ya mencionamos, corren en modo privilegiado, su labor consiste en realizar funciones tales como el manejo de sesiones, manejo y administración del esquema de seguridad de usuarios, manejo y administración de cuentas de usuarios y el más noble de todos ellos, el subsistema Integral de Red. Este subsistema proporciona servicios básicos LAN Manager, es decir, comparte archivos y recursos de impresión bajo un esquema de seguridad a nivel recurso. Las capacidades para

manejo de seguridad a nivel usuario, las capacidades de administración a través de red, tales como el manejo de dominios, servicios de réplica automática, utilerias de respaldo a través de red y lo servicios de tolerancia a fallas (manejo de discos en espejo y discos duplexados), están disponibles bajo el nombre de LAN Manager para Windows NT.

Incluidos también en Windows NT como servicios Nativos Subsistemas de red como los servicios de ARPA, interfaz prográmatica de Sockets de Berkeley, los protocolos TCP/IP, AP_Is de LAN Manager (Named Pipes con capacidad punto a punto y Mailslots), APIs para desarrollo de aplicaciones de administración remota y RPC's (Remote Procdure Cails) siguiendo los estándares del DCE (Ambiente de Cómputo distribuido de OSF), lo que permite desarrollar aplicaciones distribuidas en una red de comunicaciones. De hecho, LPC el mecanismo de comunicación entre procesos a nivel local, es un subconjunto de los RPC's de DCE. Win 32 es por así decirlo el ambiente nativo de Windows NT, su interfaz gráfica es idéntica a la de Windows 3.x para DOS. Un usuario común no notará la diferencia a primera vista. Las diferencias entre los hermanos de la familia Windows son enormes sin embargo, tal y como se ha podido apreciar en las secciones anteriores. Windows NT es un sistema operativo multitareas, que ofrece Multiprocesamiento simétrico y características de seguridad e integridad propias de un sistema operativo de misión crítica.

Puntos importantes a señalar son el hecho de que Windows NT es probablemente el sistema operativo más fácil de portar a nuevas plataformas. Solo el dos por ciento del código esta escrito en ensamblador, el resto esta en C y C++. Las aplicaciones son completamente compatibles a nivel código fuente

entre plataformas de hardware diferente y la ya popular interfaz programática e Windows 16 ha sido extendida, no completamente modificada, para conservar al máximo la inversión en código ya desarrollado. En total 735 APIs han sido conservadas casi intactas, solamente extendiendo sus argumentos a 32 bits. Además de esto, se proporcionan 414 nuevos API´s para las nuevas funciones. En general, se ha eliminado totalmente las funciones para manejo de memoria expandida, funciones que llamen a interrupciones o que asumen la existencia de memoria segmentada. Win 32 muestra a los desarrolladores un espacio plano de memorias de 32 bits, sin importar la plataforma de hardware.

El subsistema de Ambiente de Win 32 incluye funcionalidad OLE, para manejo de objetos, capacidades para manejo de multimedia. Cumple con los requisitos de seguridad para un sistema de computo nivel C2.

Y por lo que se refiere al manejo de sistemas de caracteres multinacionales, maneja Unicode. Código de representación de caracteres de 16 bits, considerando un estándar en la comunidad de naciones Europeas. Mediante Scripts Unicode, que son subconjunto de este código, es posible obtener todos los caracteres que requiere un idioma específico para ser representado por escrito, inclusive lenguas orientales.

2.6 IMPLEMENTACION DE RED

Después de haber descrito los recursos empleados y haber instalado el software de Windows NT, se procedió a implementar el Servidor de Comunicaciones bajo la siguiente jerarquía:

- Se proporciono a las máquinas con sus respectivas direcciones IP y se hicieron pruebas de salida, esto es, se realizaron pruebas con el comando Ping y Telnet con la finalidad de verificar el buen funcionamiento de las tarjetas de red y que realmente existe conexión al exterior, en este caso hacia la R.I.T.

- Posteriormente se llevo a cabo la validación del dominio de red que direcciona las estaciones de trabajo hacia el Servidor con la ayuda de Windows Nt Server.

- Una vez establecido lo anterior, se procedió a realizar la administración de red bajo el entorno de Windows NT, esto es, se establecieron las relaciones de confianza habilitando los grupos de trabajo a compartir, los miembros de grupos, las respectivas cuentas de usuario y sus derechos, así como la implementación de las aplicaciones a utilizar y la forma de organizar el monitoreo y la seguridad de la red.

- Este seguimiento se detalla en consecuencia en éste y los siguientes capítulos.

2.7 CONCEPTO DE DOMINIOS.

La unidad básica de la administración centralizada y la seguridad en Windows NT es el dominio. Un dominio es un grupo de servidores que se ejecutan en Windows NT y en cierto modo, funcionan como un único sistema. Todos los servidores con Windows NT de un dominio utilizan el mismo conjunto de cuentas de usuario, por lo que la información de una cuenta de usuario solo necesita escribirse una vez para todos los servidores del dominio que reconocen dicha cuenta. La agrupación de computadoras en dominios proporciona dos grandes ventajas a los usuarios y administradores de la red. Lo que es más importante, los servidores de un dominio constituyen una unidad administrativa única que comparte la información de seguridad y de cuentas de usuario. Cada dominio posee una base de datos que contiene las cuentas de los usuarios y grupos, y las configuraciones del plan de seguridad. Todos lo servidores que ejecuten Windows NT en dominio mantendrán una copia de esta base de datos. Ello significa que los administradores solo necesitaran administrar una cuenta para cada usuario y que cada usuario solo tendrá que utilizar una cuenta. La segunda ventaja de los dominios es la comodidad que brindan al usuario: cuando un usuario examine la red para buscar recursos disponibles, observara que esta agrupada en dominios, en lugar de ver los servidores e impresoras de toda la red al mismo tiempo.

Las relaciones de confianza son vínculos entre dominios, que permiten realizar una identificación transparente, en virtud de la cual un usuario solo poseerá una cuenta de usuario en un dominio pero podrá acceder a toda la red. Si se organizan adecuadamente los dominios y relaciones de confianza de la red, todas las computadoras con Windows NT reconocerán a todas las cuentas de

usuario, por lo que el usuario solo tendrá que iniciar una versión y facilitar una contraseña solo una vez para accesar a cualquier servidor de la red.

2.8 RELACIONES DE CONFIANZA

Estableciendo relaciones de confianza entre los dominios de la red, podrá permitir que determinadas cuentas de usuario y grupos globales pueden utilizarse en dominios distintos del que estén situadas dichas cuentas. Ello facilita en gran medida la administración, ya que cada cuenta de usuario tiene que crearse una sola vez para toda la red. Además, ofrece la posibilidad de accesar a cualquier computadora de la red y no únicamente a las computadoras de uno de los dominios.

A partir de esto, el dominio que confía reconocerá a todos lo usuarios y cuentas de grupos globales del dominio en el cual se confía. Estas cuentas podrán utilizarse como se desee dentro del dominio que confía, podrán iniciar sesiones en estaciones de trabajo situadas en el dominio que confía, integrarse en grupos locales dentro de dicho dominio, y recibir permisos y derechos dentro de este dominio. Las relaciones de confianza pueden ser unidireccionales o bidireccionales. Una relación de confianza bidireccional es simplemente un par de relaciones unidireccionales, en virtud del cual cada dominio confía en el otro.

En la siguiente figura (2.11), los dominios Finanzas y Envío confían mutuamente y las cuentas de cada uno de estos dominios pueden utilizarse en el otro. Sin embargo, puesto que producción confía en ventas, pero ventas no

confía en producción, las cuentas de producción podrán utilizarse en el dominio ventas, pero las cuentas de ventas no podrán emplearse en producción.

La confianza entre dominios no es una operación transitiva. Por ejemplo, si ventas confía en producción y producción confía en finanzas, ventas no confiara automáticamente en finanzas. Si desea que ventas confíe en finanzas deberá establecerse una relación de confianza adicional directamente entre estos dominios. Para establecer la relación de confianza, se debe tener la siguiente consideración:

a) Se necesita al menos dos dominios para poder realizar la relación de confianza.
b) Definir cual será el dominio que confía (el dominio que va a compartir los recursos).
c) Definir cual dominio será confiado (es el dominio que ingresara a otro dominio y empleara los recursos).

Una vez definido lo anterior se procederá a establecer la relación de confianza, dentro de la ventana herramientas administrativas, ejecutar el icono Manejador de usuarios del dominio, en donde ejecutaremos la relación de confianza, la pantalla es la siguiente:

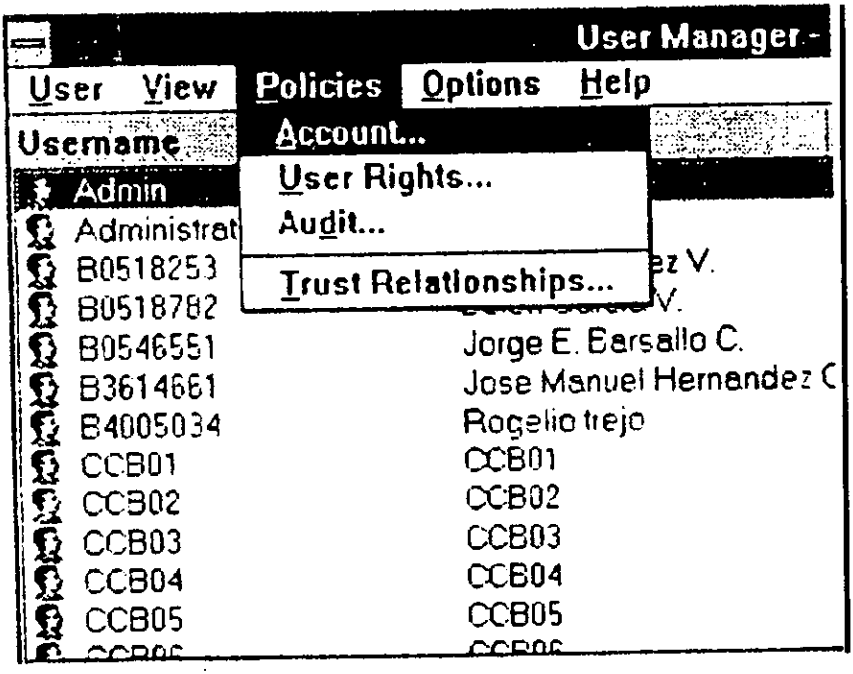

Figura 2.11 Ventana de Acceso a las Relaciones de Confianza.

Una vez estando dentro, accionar el menú policies en donde se deberá seleccionar "Trust Relationships". Posteriormente encontraremos la ventana donde se deben definir como se van a realizar éstas relaciones de confianza.

En donde, si es el dominio que confía (que comparte sus recursos), se tendrá que poner el nombre del otro dominio en la parte con la Leyenda "Trusted Domains". (Dominio en el que confió). Y si es el dominio que ocupara los recursos del otro dominio, deberá poner el nombre del dominio que confía en la parte con la leyenda "Permitted to Trust this Domain" (Permita que confíen en mi). Con esto se establece la relación de confianza.

Cabe hacer mención que las relaciones de confianza, no son necesariamente reciprocas.

2.9 GRUPOS DE TRABAJO

Un grupo de trabajo esta compuesto por varias personas que utilizan la red con regularidad deben disponer de una cuenta de usuario en algún dominio de la misma. La cuenta de usuario contienen datos diversos sobre el usuario, como su nombre, contraseña y limitaciones de uso de la red.

2.9.1 TIPOS DE GRUPOS.

Dentro de una red existen dos diferentes grupos de trabajo, los cuales se definen como grupos locales y grupos globales, los grupos simplifican la concesión de derechos y permisos de uso de recursos, ya que basta con conceder a un grupo un determinado derecho o permiso, para que tal derecho o permiso quede concedido automáticamente a todos los miembros presentes y futuros de ese grupo.

Grupos Locales.

Un grupo local es un conjunto de usuarios y grupos globales procedentes de uno o varios dominios, que se reúnen bajo un solo nombre de grupo. Aunque un grupo local de un dominio podrá contener usuarios y grupos globales de ese dominio, así como de cualquier otro de su confianza, sólo está permitido conceder a un grupo local derechos y permisos sobre los recursos situados en el mismo dominio donde ese grupo local haya sido definido.

El empleo de ese grupo sólo podrá realizarse localmente en los servidores de su dominio. Un grupo local puede contener usuarios y grupos globales, pero no puede contener a otros locales. La forma de representar a los grupos locales, se muestra a continuación en la figura 2.12.

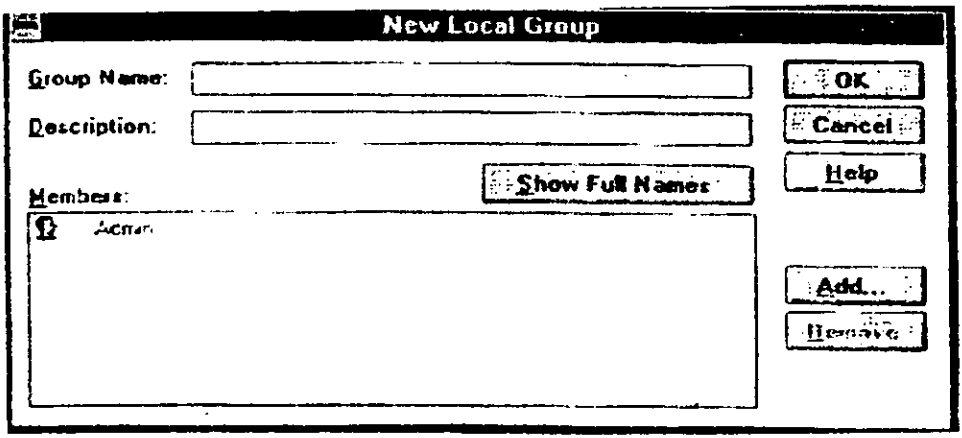

Figura 2.12 Representación de un Grupo Local.

Para crear un Grupo Local se debe, dentro de la ventana herramientas administrativas, ejecutar el icono de "manejo de usuarios" del dominio deseado:

Se definirá el nombre de grupo local, una breve descripción, y se adicionan a los usuarios y grupos globales:

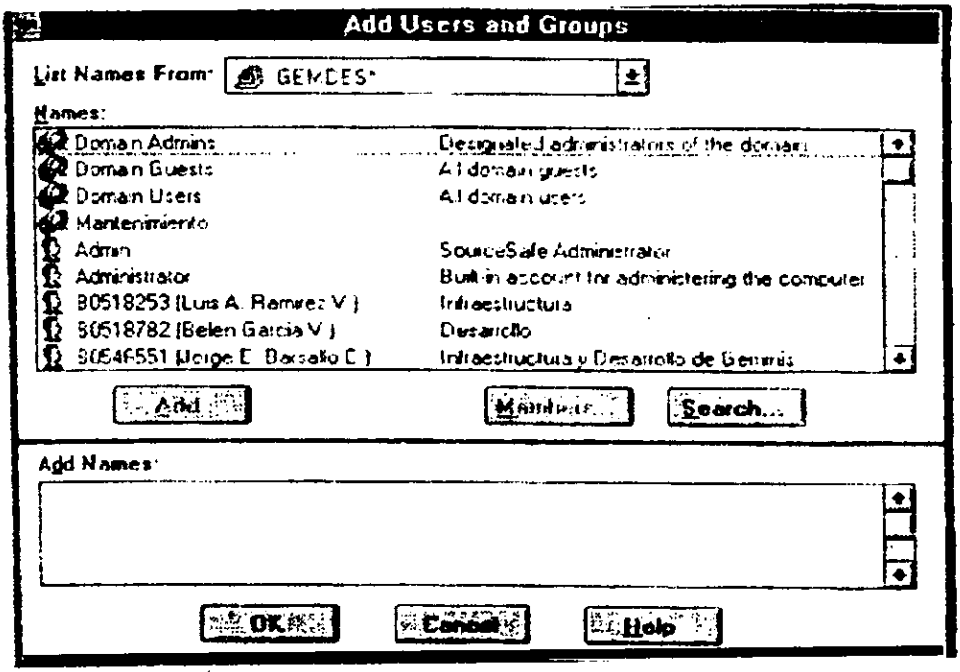

Figura 2.13. Creación de un Grupo Local.

Miembros de Grupos Locales.

Los miembros que pueden contener un grupo global son cuentas de usuarios del dominio en donde ha sido creado, un grupo global después de creado esta listo en cualquier punto y un grupo global, no puede contener grupos locales o globales.

Grupos Globales

El termino "global en los grupos globales viene de hecho de que un grupo global puede ser usado globalmente. Un grupo global reside sobre los

controladores de dominio, y contienen las cuentas de usuarios de sus dominio. Sin embargo, el uso de un grupo global no esta restringido a la base de datos en la cual esta reside. Un grupo global puede ser adicionado como un miembro de cualquier grupo local definido en cualquier lugar de su dominio, los grupos locales es un mecanismo para recolectar cuentas de usuario dentro de grupos que pueden ser usados en todo el dominio.

En lugar de la asignación de permisos a cada grupo global, el administrador asigna permisos al grupo local para el cual los grupos globales ha sido adicionados. El administrador simplemente adiciona a los nuevos usuarios al grupo global apropiado que es parte de un grupo local.

Por omisión cuando una cuenta de usuario es creada en un dominio, esta es automáticamente asignada a los usuarios del dominio del grupo global. Los grupos globales y locales no pueden usar el mismo nombre, los nombres de grupos deben ser únicos dentro de la base de datos.

La creación de un grupo global se realiza de la siguiente manera. De la ventana "Herramientas Administrativas", ejecutar el icono "Manejo de Usuarios" del dominio en donde se desea agregar ese grupo global, en donde aparecerá la siguiente pantalla:

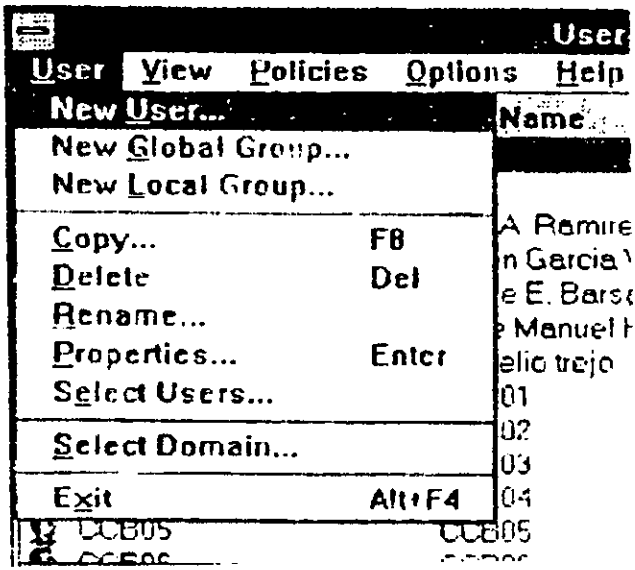

Figura 2.14 Creación de un Grupo Global

Del menú "user", seleccionar "New Global Group", adicional a los miembros que formarán parte de ese grupo global, nombrarlo y darle una descripción para identificarlo.

De ésta forma, se integra un grupo global, seleccionado, e inclusive, se pueden adicionar futuros miembros a éste u otro grupo previamente creado.

Miembros de Grupos Globales.

Los grupos globales pueden contener cuentas de usuarios como miembros. Ellos no pueden contener grupos locales u otros grupos globales, porque los grupos globales están limitados a donde reside las cuentas. Es recomendable colocar a los usuarios dentro de grupos locales y a los grupos locales dentro de

grupos globales para minimizar la administración en estaciones de trabajo y servidores que trabajen con Windows NT.

Los grupos globales no tienen la misma autoridad para llevar a cabo funciones de red como los grupos locales lo hacen. Para llevar las tareas administrativas los grupos globales deben ser adicionados al grupo local.

Estrategias de Grupos.

Para facilitar la administración y el mantenimiento de la red, conviene que tenga en cuenta varias estrategias de utilización de grupo globales y grupos locales. Como un ejemplo; si los dominios están divididos de tal modo que cada uno de ellos corresponde a una división o departamento de la empresa, puede considerar como grupo local a un grupo de usuarios pertenecientes a un mismo departamento.

Este grupo de dominios puede recibir permisos y derechos en otros dominios, por lo que el concepto de grupo global constituye un medio para exportar este grupo de usuarios, como una misma unidad, a otros dominios. Cuando un administrador observe que el nombre del grupo aparece precedido por el nombre del dominio, sabrá tanto el tipo de personas que representan dicho grupo, como el origen o ubicación de mismo.

Un grupo local es un grupo que puede incluir usuarios y grupo globales procedentes de otros dominios, por lo que se trata de un modo de importar de una sola vez un conjunto de usuarios y grupos globales de otros dominios, para su utilización en el dominio local.

Como ejemplo de su aplicación, supongamos que el dominio ingeniería posee un servidor en el cual existe un directorio compartido, las personas de otros dominios están interesados en consultar estos documentos.

Los administradores de la red podrán permitir esta posibilidad del siguiente modo:

1. Creando grupos globales en los dominios que quieren accesar al directorio.
2. Creando un grupo local llamado "información lista" en el dominio Ingeniería.
3. Incorporando los grupos globales al grupo local "información lista".
4. Concediendo al grupo globales al grupo local "información lista".

Como puede observarse, un grupo local es una forma de reunir grupo globales y asignarles permisos a todos una sola vez. De este modo, si algún otro grupo global necesita más adelante los mismo permisos de algún grupo global existente, bastará con agregar el nuevo grupo global al correspondiente grupo local, con lo cual dispondrá de todos los permisos que necesite.

Crear un Grupo con la Finalidad de:	Utilizando	Comentarios
Agrupar usuarios de este dominio en una misma unidad, para utilizarla en otros dominios.	Grupo global	El grupo global podrá incluirse en grupo locales o recibir permisos y derechos directamente en otros.
Recibir permisos y derechos en un solo dominio.	Grupo local	El grupo local puede contener usuarios y grupos globales de otros dominios.
Recibir permisos en estaciones de trabajo con Windows NT.	Grupo global	Los grupos globales de un dominio podrán rescindir permisos en estaciones de trabajo con Windows NT, pero no los grupos locales de un dominio.
Contener otros grupos.	Grupo local	El grupo local solo puede contener grupos globales y usuarios; sin embargo, ningún grupo puede contener otros grupos locales.
Incluir usuarios de varios dominios.	Grupo local	El grupo local solo podrá utilizarse en el dominio en el cual haya sido creado.

Tabla 2.1 Propósito de los Grupos Locales.

Es recomendable utilizar la construcción de grupos locales y globales donde sea posible.

El método recomendado para implementar grupos en un dominio es:

- Dentro de dominios: Crear usuarios y adicionarlos a grupos globales creados recientemente o que ya existen para accesar de recursos de amplio dominio.

- Adicionar grupos globales a grupos locales: Asignar el grupo local a los usuarios correctos y permisos a los recursos.

Esta estrategia requiere mantenimiento mínimo cuando tu equipo de trabajo cambia, todos los cambios son realizados a los miembros del grupo global en el controlador de dominio. Nada cambiara en el grupo local con respecto a los permisos y derechos asignados a esos grupos locales.

El controlador de dominio del servidor de Windows NT realiza esta estrategia por omisión, por ejemplo:

- Cuando una cuenta de usuarios es creada, automáticamente es adicionado un miembro de los usuarios de dominio del grupo global.
- Los usuarios del dominio son miembros de los usuarios del grupo local. Por lo tanto, el usuario creado nuevamente es un miembro del grupo local.

Utilidad de los Grupos.

La integración de usuarios en grupo permite conceder a varios usuarios el acceso a un recurso de una forma más fácil y rápida. Para conceder un permiso o derecho a todos los usuarios de un grupo, bastará con otorgar al derecho o permiso al propio grupo. Otra ventaja de los grupos es cuando algún nuevo usuario se afilia a la red. En un dominio con Windows NT o en una estación de trabajo con Windows NT, los grupos locales ofrecen además un método para clasificar usuarios y asignarles rápidamente conjuntos de derechos y permisos. Por ejemplo, para convertir una cuenta en operador de impresión de un dominio, bastará con incorporar dicha cuenta al grupo local "operadores de

impresión" del dominio, con ello, la cuenta adquirirá todos los derechos y facultades de un operador de impresión.

2.9.2. DIFERENCIA ENTRE GRUPOS GLOBALES Y LOCALES

Aunque los grupos globales y locales desempeñan funciones similares, para su creación y utilización se aplican reglas diferentes, así, dependiendo del tipo de grupo en el cual se han creado se clasifican de la siguiente forma:

Un grupo global creado en el domino de ventanas.

- Solo puede contener usuarios del domino ventanas.
- Puede utilizarse en cualquier dominio que confie en el dominio ventas.

Un grupo local creado en el domino ventas.

- Puede contener usuarios y grupos globales de dominio ventas y de cualquier dominio de confianza del dominio ventas.
- Sólo puede utilizarse en servidores del dominio ventas.

Obsérvese que los grupos locales de un dominio no pueden ser utilizados en las estaciones de trabajo con Windows NT pertenecientes a ese mismo dominio, ya que los grupos locales de un dominio son locales a los servidores del mismo. Los términos "grupo global" y "grupo local" no se refiere al contenido del grupo, sino a los lugares donde el grupo puede recibir derechos y permisos.

CAPITULO III. ADMINISTRACION DE UNA RED WINDOWS NT.

Objetivo:

Describir detalladamente los procedimientos de administración de una red Windows NT, ventajas, herramientas disponibles y niveles de seguridad.

CAPITULO 3. ADMINISTRACION DE UNA RED WINDOWS NT.

3.1. CREACION DE DOMINIOS

Con el sistema operativo de red Windows NT se incorporan diversos métodos y políticas de Administración y Seguridad. Estos métodos proporcionan numerosas formas de controlar la actividad de los usuarios, sin por ello impedir el acceso discrecional, lo que significa que es posible permitir a determinados usuarios accesar a un recurso o realizar una determinada acción, y al mismo tiempo impedírselo a otros usuarios. Dentro de la administración y seguridad de la red se establecen ciertas normas y grupos para el funcionamiento adecuado de dicha red a través de los siguientes métodos:

- Creación de dominios
- Tipos de grupos
- Tipos de cuentas
- Tipos de usuarios
- Derechos de usuarios

Un dominio utiliza el mismo conjunto de cuentas de usuario, por lo que la información de una cuenta de usuario solo necesita escribirse una vez para todos los servidores del dominio que reconocen dicha cuenta. El requisito mínimo de un dominio es un servidor que actúe como controlador de dominio y que almacene la copia principal de la base de datos de grupos y usuarios de dominio. Dentro de un dominio se puede incluir también otros servidores

adicionales que funcionen bajo otras plataformas tales como Lan Manager 2.x. Netware Novell o estaciones de trabajo con MS-DOS o Windows para grupos 3.x, etc., para esto se requiere de un controlador de dominio.

3.1.1.TIPOS DE MODELOS DE DOMINIOS

Existen cuatro tipos de modelos de dominios. A continuación se mencionan cada uno de ellos y sus diferentes características ya que el método que se utilice para planificar y organizar los dominios de una red es decisivo.

Si se configuran de tal modo que todas las cuentas de usuario y grupos globales sean validos en todos los dominios, podrá simplificar extraordinariamente la administración de la red y garantizar al mismo tiempo que todos los usuarios puedan acceder a todos los servicios de la red.

- Modelo de dominio único
- Modelo de dominio maestro
- Modelo de dominio maestro múltiple
- Modelo de dominio de confianza total

Modelo de Dominio Unico

Si una red no tiene demasiados usuarios y no necesita dividirla con fines de organización, se puede utilizar este modelo. Con este modelo, la red esta formada por un solo dominio, en donde sus características principales son:

- Naturalmente, todos los usuarios y grupos globales serán creados en el único dominio existente.
- No será necesario establecer relaciones y grupos globales serán creados en el único dominio existente.
- No será necesario establecer relaciones de confianza, ya que solo existirá un dominio en toda la red.
- Una red podrá utilizar el modelo de dominio único si no tiene más de 10.000 usuarios.
- Además, la existencia de un solo domino significa que los administradores de la red podrán administrar en cualquier momento todos los servidores de la misma, ya que la facultad de administrar servidores esta asociada al nivel de dominio.

Ventajas	Desventajas
Es el más indicado para empresas con pocos usuarios y recursos	No se puede utilizar en empresas que tengan más de 10,000 usuarios.
Administración centralizada de las cuentas de usuario.	No permite conectar los usuarios.
No es necesario administrar relaciones de confianza.	No permite agrupar recursos.
Los grupos locales solo tienen que definirse una vez.	El examen de la red resulta más lento si el dominio incorpora un gran número de grupos locales.

Tabla 3.1 Ventajas y Desventajas del Modelo de Dominio Unico.

Modelo de Dominio Maestro

El modelo de dominio maestro es una de las opciones más adecuadas para aquellas empresas o compañías en las cuales sea necesario dividir la red en

varios dominios con fines de organización pero cuya red no tenga más de 10,000 usuarios y grupos. Este modelo proporciona las ventajas de organización y administración centralizada que posee dominios múltiples. Un dominio maestro puede considerarse como un dominio de cuenta cuyo propósito principal es administrar las cuentas de usuario de la red. Los demás dominios de la red serán dominios de recursos, ya que en ellos no se almacenara no administrara ninguna cuenta de usuario, sino que su única finalidad será proporcionar recursos a la red.

Ventajas	Desventajas
En la opción más indicada para empresas que tengan menos de 10,000 usuarios y necesiten que los recursos compartidos se dividan en grupos.	No se puede utilizar en empresas que tengan más de 10,000 usuarios.
Administración centralizada de las cuentas de usuario, además de que los recursos se agrupan de una manera física	Obligan a definir grupos locales en los dominios donde vengan a utilizarse.
Los dominios de los distintos departamentos pueden tener sus propios administradores que se encargan de controlar los recursos del departamento	
Sólo se definen los grupos globales una vez.	

Tabla 3.2 Ventajas y Desventajas del Modelo de Dominio Maestro.

Modelo de Dominio Maestro Múltiple.

En empresas de gran tamaño que deseen disponer de administración centralizada, el modelo de dominio maestro múltiple es la opción más indicada, ya que es el que ofrece mayores posibilidades de ampliación, teniendo como principales características:

- En este modelo existe un número reducido de dominios maestros.
- Toda cuenta de usuario de la red será cruzada en algunos de estos dominios maestros.
- La administración del sistema de la empresa podrá administrar los dominios maestros.
- Podrán existir dominios departamentales que proporcionan recursos.
- Los dominios departamentales serán administrados por miembros de la administración del sistema.
- Existen relaciones de confianza entre diferentes dominios.

Ventajas	Desventajas
En la opción más adecuada para empresas que tengan menos de 10,000 usuarios de sistema de Administración Centralizada	Obliga a administrar un mayor número de relaciones de confianza.
Puede aplicarse hasta obtener redes con cualquier número de usuarios.	Puede ser necesario crear un número elevado de grupos locales como de grupos globales.
Los dominios departamentales pueden tener sus propios administradores, de administrar los recursos de sus respectivos departamentos.	
Los recursos se agrupan de una forma lógica	

Tabla 3.3 Ventajas y Desventajas del Modelo de Dominio Maestro Múltiple.

Modelo de Dominio de Confianza Total.

Con este modelo todos los dominios de red confiaran en todos los demás dominios, de éste modo, cada departamento podrá administrar su propio dominio y definir sus propios usuarios y grupos globales, los cuales podrán utilizarse desde los demás dominios de red. Así, se tienen como principales características: el gran número de relaciones de confianza hace que resulte impráctico para empresas de gran tamaño y que siempre existen relaciones de confianza.

Ventajas	Desventajas
Es el más adecuado para empresas sin departamento de sistemas de administración de información	Puesto que no existe una administración de usuarios centralizada, éste modelo no resulta práctico para empresas que cuenten con departamentos de administración de información centralizados.
Puede ampliarse hasta configurar redes con cualquier número de usuarios.	Cada departamento debe confiar en que los otros departamentos no van a agregar usuarios inadecuados a sus grupos globales.
Cada departamento tienen un control absoluto sobre sus recursos y cuentas de usuario.	
Tanto los recursos como las cuentas de usuario quedan agrupadas en unidades departamentales.	

Tabla 3.4 Ventajas y Desventajas del modelo de Confianza Total.

3.2 CUENTAS

Dentro de las políticas de administración y seguridad en Windows NT se otorgan ciertos derechos y permisos para hacer usos de los recursos de la red, estas facultades se controlan a través de una cuenta. Cualquier persona que utilice la red con regularidad debe disponer de una "Cuenta de Usuario" en algún dominio de la misma. La cuenta de usuario contienen datos diversos sobre el usuario tale como: su nombre, contraseña y limitaciones de uso de la red. Dentro de Windows NT existen dos tipos de cuentas:

1. Cuentas de grupo local de administradores: Este tipo de cuentas disponen de la autoridad necesaria para hacer prácticamente todo lo que deseen en los servidores con Windows NT o en estaciones de trabajo. Entre estas posibilidades se incluye la creación, eliminación y administración y grupos globales y grupos locales, la posibilidad de compartir directorios e impresoras, la concesión de permisos y derechos de uso de recursos a los usuarios y la instalación de programas y archivos de sistemas operativos.

2. Cuentas del grupo local usuarios: Estas cuentas son las de los usuarios habituales de la red, es decir las que la utilizan para su trabajo.

La creación de una nueva cuenta, se realiza con el siguiente procedimiento:

Dentro de la ventana "Herramientas Administrativas" ejecutar el icono Manejador de Usuarios del Dominio. Ahora, el menú "User" seleccionar New, donde aparecerá lo siguiente:

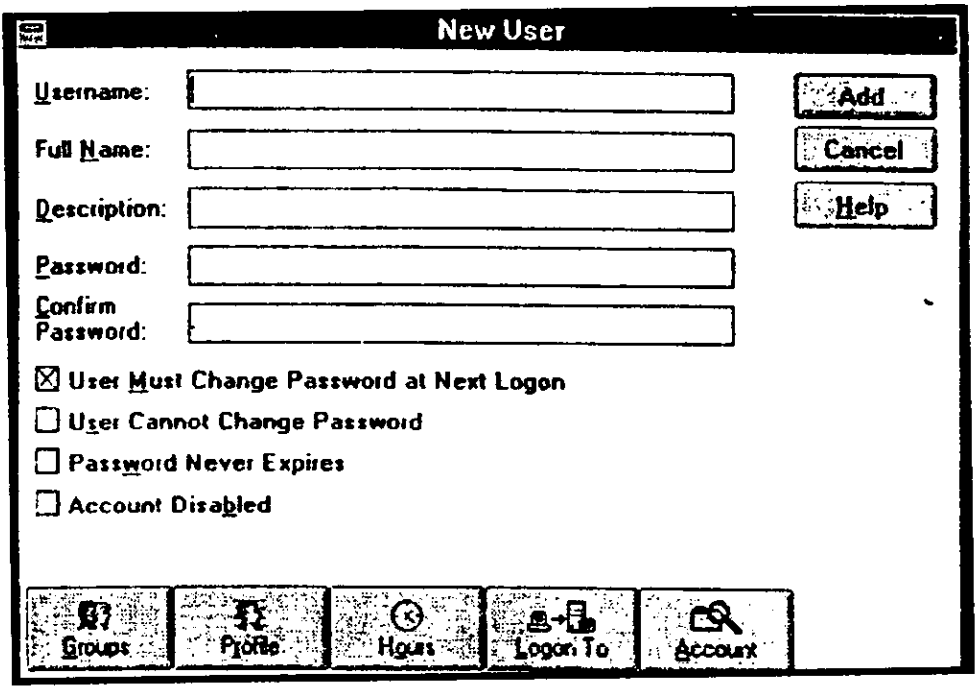

Figura 3.1. Ejemplo de la Creación de una Cuenta de Usuario

En donde se definirá su cuenta de usuario en la red, nombre del usuario, una descripción, el password, y las siguientes condiciones:

- User Must Change Password at Next Logon: Para que el usuario una descripción, el password en el segundo intento de ingresar a la red.
- User Cannot Change Password: El usuario nunca podrá cambiar su password.
- Password Never Expire: que el password nunca expire, que tenga siempre vigencia.
- Account Disable: La cuenta se desactive, ningún usuario podrá utilizar esa cuenta.

- Boton Group: A que grupos pertenece esa cuenta.
- Boton Profile: Con que tipo de escritorio podrá trabajar(colores dentro de windows, protectores de pantalla, etc.).
- Boton Hours: Se puede definir el tiempo que esta cuenta pueda trabajar durante la semana.

3.2.1 CUENTAS DE USUARIO

Las cuentas de usuario están divididas en dos tipos: en Cuentas de Usuarios Globales y Cuentas de Usuarios Locales, en donde las cuentas de usuario y de grupo son creadas y administradas por el administrador de usuarios.

Si en una red existen servidores con sistemas operativos de Red distintos de Windows NT, como LAN Manager 2.X, Novel Netware o IBM LAN Server, podrá utilizar cuentas de usuarios locales para facilitar en cierta medida el acceso a través de la red a los distintos usuarios que dispongan de cuentas en un dominio que ejecuta Windows NT Server. Una cuenta local es una cuenta de usuario cuyo comportamiento es distinto de las cuentas de usuarios normales (globales).

Las cuentas locales no pueden utilizarse para iniciar una sesión de forma interactiva en una estación de trabajo con Windows NT Advanced Server es decir están limitados a un solo dominio. En las cuentas de usuarios se encuentran:

- Nombre de usuarios

- Contraseña
- Horas de inicio de sesión
- Estaciones de trabajo para inicio de sesión
- Directorio de base de datos
- Archivo de comandos de inicio de sesión
- Tipo de cuenta

3.2.2 TIPOS DE CUENTAS

Básicamente, existen dos tipos de cuentas: las cuentas de grupo local de administradores y las cuentas de grupo local de usuarios.

Cuentas de Grupo Local Administradores.- Las cuentas del grupo local Administradores disponen de la autoridad necesaria para hacer prácticamente todo lo que deseen en los servidores o en estaciones de trabajo con Windows NT. Entre estas posibilidades se incluye la creación, eliminación y administración y grupos globales y grupos locales, la posibilidad de compartir directorios e impresoras, la concesión de permisos y derechos de uso de recursos a los usuarios y la instalación de programas y archivos de sistemas operativos.

Cuentas del Grupo Local Usuarios.- Son las cuentas de usuarios habituales de la red, es decir que se utilizan para el trabajo diario.

3.3 ADMINISTRACION DE ENTORNOS DE USUARIOS

En una red de Windows NT existen diversos procedimientos para definir y optimizar los entornos de las estaciones de trabajo de los usuarios. Es posible definir las conexiones de red, las aplicaciones disponibles, los grupos de programas y el aspecto del escritorio de Windows. Incluso, si lo desea, se puede impedir que los usuarios de las estaciones de trabajo con Windows NT cambien de configuración del escritorio que se haya creado.

El método más potente para administrar los entornos de los usuarios es la asignación de *perfiles de usuario* a los usuarios de las estaciones de trabajo con Windows NT. Un perfil es un archivo que actúa como una instantánea del entorno del escritorio del usuario, definiendo los grupos del Administrador de Programas y los elementos de programa contenidos en dichos grupos, las conexiones de impresora, el tamaño y la posición de las ventanas, y los colores de la pantalla. Los perfiles permiten también limitar a los usuarios que modifiquen estas características en sus propias estaciones de trabajo.

Otra forma de mejorar los entornos de los usuarios consiste en asignarles *archivos de comandos de inicio de sesión*. Si un usuario tiene uno de estos archivos, éste se ejecutará cada vez que inicie una sesión en cualquier tipo de estación de trabajo de la red. Este archivo de comandos de inicio de sesión puede ser un archivo por lotes que incluye comandos del sistema operativo o un programa ejecutable.

También se puede optar por proporcionar a cada usuario un *directorio base* en un servidor o estación de trabajo. El directorio base de un usuario

proporcionará a dicho usuario un espacio de almacenamiento privado. Cada usuario tendrá control sobre el contenido y el acceso a su directorio base. Además, es posible establecer las *variables de entorno* de cada estación de trabajo. Las variables de entorno especifican la ruta de búsqueda de la estación de trabajo, el directorio donde se almacenan los archivos temporales, además de otra información similar.

3.3.1 FUNCIONAMIENTO DE LOS PERFILES DE USUARIO

Los perfiles de usuario contienen las características del entorno Windows NT de cada usuario. Los perfiles de usuario solamente resultan útiles para aquellos usuarios que trabajen en estaciones de trabajo con Windows NT. No tienen ningún efecto sobre los usuarios que utilicen estaciones de trabajo con MS-DOS.

Las estaciones de trabajo con Windows NT incorporan algunos aspectos de los perfiles de usuario, existen muchas maneras de aumentar la utilidad de los perfiles. Sin embargo, antes de aprender a hacerlo, conviene conocer perfectamente el modo en que los perfiles de usuario funcionan en las estaciones de trabajo con Windows NT.

La tabla 3.5 muestra exactamente lo que se ha guardado en un perfil:

Características que se Guardan en un Perfil de Usuario	
Origen	***Parámetros guardados***
Administrador de programas	Todas las opciones del Administrador de programas definidas por el usuario, como los grupos de programas personales y sus propiedades, los elementos de programa y sus propiedades, y todas las opciones que se guardan al elegir los comandos Guardar configuración al salir o Guardar configuración ahora.
Administrador de archivos	Todas las opciones del administrador de archivos definidas por el usuario, entre las cuales se incluyen las conexiones de red y todas las características que se guardan cuando está seleccionado el comando Guardar configuración al salir.
Interfaz de comandos	Todas las opciones de la interfaz de comandos definidas por el usuario, como las fuentes, los colores, las características de tamaño de búffer de pantalla y la posición de la ventana.
Administrador de impresión	Las conexiones de impresoras de red y todas las opciones que se guardan cuando se está seleccionando el comando guardar configuración al salir.
Opciones del panel de control	Todas las opciones de color, Mouse, escritorio, Cursor, Teclado, Internacional y sonido. Para la opción "Sistema, solamente se guardarán los datos del cuadro "Variables de entorno de usuario". Las demás opciones del panel de control no contienen ninguna característica específica del usuario.
Accesorios	Todas las opciones de cada aplicación específicas del usuario, que afectan a su entorno Windows NT. Entre las aplicaciones de accesorios se encuentran: Calculadora, Fichero, Reloj, Portafolio, Paintbrush y Terminal.
Aplicaciones para Windows NT de otros fabricantes	Cualquier aplicación que haya sido desarrollada específicamente para Windows NT podrá diseñarse de tal modo que mantenga las características de la aplicación para cada usuario. Si existe esta información, se guardará en el perfil de usuario.
Marca-texto de la Ayuda en pantalla	Cualquier marca-texto que se haya introducido en el sistema de Ayuda de Windows NT.

Tabla 3.5 Característica del Perfil de Usuario.

3.3.2 PERFILES LOCALES

Los perfiles locales son creados siempre por Windows NT de forma automática, sin que el administrador debe encargarse expresamente de ello. Cada vez que un usuario (excepto aquellos usuarios que no puedan mantener perfiles locales), al iniciar una sesión y posteriormente al cerrarla, en la estación de trabajo con Windows NT, se guardará en un perfil local las opciones que se hayan seleccionado (en este caso el usuario).

Entre estas características se incluyen las conexiones de red, los grupos y elementos de programas, el tamaño y la posición de la ventana, y el aspecto de la pantalla. Cuando el usuario vuelva a iniciar una sesión en una estación de trabajo, esta reconocerá al usuario y cargará el perfil que se creó la última vez que el usuario cerró una sesión en esta estación de trabajo.

Los perfiles garantizan que todo usuario pueda disponer de sus preferencias cada vez que inicie una sesión. En las estaciones de trabajo que son utilizadas por distintas personas, los perfiles permiten a cada usuario configurar un entorno personalizado. El entorno de usuario puede ser distinto del que utilicen los demás usuarios de esa estación de trabajo, pero se mantendrá cada uno de los entornos y se cargará el apropiado cuando un usuario inicie una sesión.

Los perfiles locales dependen de la computadora: las opciones que seleccione un usuario en una estación de trabajo no estarán a su disposición cuando dicho usuario inicie una sesión en otra estación de trabajo diferente.

En las redes con dominios y Windows NT, es posible crear perfiles para aquellos usuarios que dispongan de cuentas de dominio y almacenar dichos perfiles en los servidores, por lo que esta posibilidad aumenta la utilidad de los perfiles en tres aspectos:

- Cada usuario puede tener un perfil individual, con una configuración que se cargará cada vez que inicie una sesión en cualquier estación de trabajo con Windows NT.

- Es posible utilizar el perfil para limitar la posibilidad de acceso del usuario a su estación de trabajo, impidiéndole que modifique determinados aspectos de su configuración.

- Si muchos usuarios utilizan un mismo perfil, es posible otorgar a todos ellos el acceso a una nueva aplicación o servidor, con sólo editar ese perfil.

Las dos primeras ventajas se consiguen gracias a ambos tipos de perfiles de servidor: *perfiles personales y perfiles obligatorios*. La tercera ventaja sólo se consigue con los perfiles obligatorios.

3.3.3 DIFERENCIAS ENTRE LOS PERFILES PERSONALES Y OBLIGATORIOS

Tanto los perfiles personales como los obligatorios se almacenan en los servidores. En ambos casos es posible asignar un perfil a un usuario especificando en su cuenta de usuario la ubicación y el nombre de archivo del

perfil. Cada usuario sólo puede tener asignado un perfil. Las extensiones del nombre de archivo de los perfiles personales deben ser. USR. Los perfiles obligatorios deben tener extensión MAN. Los usuarios de perfiles personales pueden modificar de manera permanente sus perfiles. Aunque el usuario no será consciente de que está modificado su perfil, cada vez que cierre una sesión en una estación de trabajo, se guardarán los cambios que haya introducido en las características específicas del usuario. Cuando posteriormente dicho usuario vuelva a iniciar una sesión, se restablecerá el entorno que existiera la última vez que cerró una sesión.

Los usuarios de perfiles obligatorios no pueden introducir modificaciones de manera permanente en sus perfiles. Aunque un usuario que disponga de un perfil obligatorio puede modificar las características específicas del usuario a lo largo de la sesión, dichos cambios no se transferirán al perfil del usuario cuando éste cierre la sesión. Cuando el usuario vuelva a iniciar una sesión, se restablecerán las características originales del perfil, que no incluirá ninguno de los cambios realizados.

La principal aplicación de los perfiles personales consiste en permitir que las preferencias y opciones de cada usuario lo acompañen de una estación de trabajo a otra. Esto resulta claramente útil en aquellas redes en las cuales los usuarios utilicen a menudo distintas estaciones de trabajo. Sin embargo, también puede ser útil en otras situaciones. Por ejemplo, cuando la computadora de un usuario sea sustituida por otra más potente, la existencia de un perfil personal garantizará que las preferencias del usuario estén accesibles inmediatamente en la nueva computadora.

Los perfiles obligatorios de usuario permiten a un usuario tener un mismo entorno de escritorio en cualquier estación de trabajo, del mismo modo que los perfiles personales. Si se utilizan perfiles obligatorios, es posible también impedir que los usuarios puedan modificar sus propios perfiles. Ningún cambio en el entorno que realice un usuario a lo largo de una sesión se guardará en el perfil obligatorio del usuario. Cuando el usuario cierre la sesión y vuelva a iniciarla, se restablecerá el entorno original especificado en el perfil. Por este motivo, los perfiles obligatorios resultan de mayor utilidad cuando se desea limitar las posibilidades del usuario en sus propias estaciones de trabajo.

Puesto que a menudo un mismo perfil obligatorio se asigna a muchos usuarios, otra de sus ventajas es la posibilidad de actualizar fácilmente los entornos de numerosos usuarios a la vez. Por ejemplo, si necesita incorporar un nuevo elemento de programa para varios usuarios, bastará con que lo agregue a su perfil obligatorio.

Si se utilizan perfiles personales en lugar de obligatorios, no resultará práctico otorgar a los usuarios el acceso a nuevos servidores editando sus perfiles, ya que habría que cambiar individualmente el perfil de cada uno de los usuarios.

3.3.4 USO DE PERFILES PARA INICIAR APLICACIONES AUTOMÁTICAS.

Es posible utilizar un perfil para especificar las aplicaciones que se ejecutarán automáticamente cuando el usuario de un perfil inicie una sesión. Para ello, deberá colocar un icono para esta aplicación en un grupo de inicio de usuario.

La mejor forma de crear un grupo de inicio en el perfil de usuario es por medio del editor de perfiles de usuario. Esta herramienta permite designar como grupo de inicio cualquiera de los grupos de programa del usuario. Obsérvese que cuando se designa un grupo de inicio de esta manera, no es necesario que dicho grupo tenga el nombre de Inicio.

Cuando un usuario inicie una sesión en una estación de trabajo, puede que se ejecute automáticamente las aplicaciones de hasta dos grupos de programas. Si en la estación de trabajo existe un grupo de programas común llamado Inicio, se ejecutarán las aplicaciones de ese grupo. Si el usuario tiene un perfil basado en servidor y se ha utilizado el Editor de perfiles de usuario para designar como grupo de inicio alguno de los grupos de programas del usuario, se iniciarán las aplicaciones de ese grupo. Si el usuario no tienen ningún perfil, o si su perfil no tienen designado ningún grupo de inicio. Windows NT comprobará si el usuario posee algún grupo personal llamado Inicio. Si es así, se ejecutará las aplicaciones de ese grupo.

Observése que el grupo personal Inicio de un usuario sólo funcionará sin ningún administrador ha designado como grupo de inicio a alguno de los otros grupos de programas del usuario. Si algún administrador lo ha hecho, se desactivará el grupo personal del usuario llamado Inicio.

3.3.5 CREACIÓN DE PERFILES DE USUARIO

Se puede crear un perfil basado en servidor, de dos diferentes maneras, dependiendo si desea establecer configuraciones iniciales en el perfil.

Si no necesita establecer configuraciones en el perfil, puede especificar un nombre de archivo de perfil persona (Con la extensión USR), en cada cuenta de usuario. No debe existir ningún archivo con el mismo nombre de archivo, de esta manera la próxima vez que el usuario inicie una sesión, Windows NT verificará que no existe actualmente un perfil basado en servidor para el usuario. Cuando el usuario cierra la sesión, Windows NT crea un archivo con el nombre de archivo que especifico y guarda todas las configuraciones de cada usuario en el archivo que éste tuviese.

Este será el perfil que se cargará la próxima vez que inicie una sesión. Esta es una manera excelente de compartir las ventajas de un perfil basado en servidor con muchos usuarios, aunque estos ya tengan cuentas de usuarios. Asegúrese de especificar un nombre de archivo de perfil diferente para cada usuario, de manera que las modificaciones realizadas por usuarios no afecten a los demás.

Si desea establecer configuraciones en los perfiles de usuario, puede crear el perfil utilizado en el Editor de perfil de usuario y seguir los tres pasos siguientes:

1. Estar el una estación de trabajo con Windows NT y configurarla de la manera deseada.

2. Utilizar el administrador de programas para crear elementos y grupos de programas, establecer las conexiones de red, defina el tamaño y la posición de la ventana, y especifique el aspecto de la pantalla.

3. Utilice el Editor de perfiles de usuario para especificar otras opciones del usuario y, si lo desea, restringir las acciones que el usuario podrá realizar en esa estación de trabajo.

Se utiliza el Editor de perfiles de usuario para conceder a un usuario o grupo los permisos necesarios para utilizar ese perfil, luego guarde el perfil. De este modo se guardarán tanto las opciones seleccionadas mediante el editor de perfiles de usuario como la configuración general que se creó con el paso 1.

Cuando se guarde un perfil de usuario, se podrá almacenar como perfil personal o como perfil obligatorio normal, o bien como el perfil predeterminado de sistema o perfil predeterminado de la estación de trabajo.

Ahora, se utilizan los directorios base, que son directorios que pueden servir como áreas de almacenamiento privado para los usuarios. Normalmente, los usuarios utilizarán sus directorios base para almacenare datos privados. Por lo general, un usuario también podrá controlar el acceso a su directorio base y restringir o conceder el acceso al mismo por otros usuarios.

Si en las estaciones de trabajo de la red hay poco espacio libre en disco duro, puede asignar a cada usuario un directorio base situado en un servidor. También es posible asignar a los usuarios directorios base situados en sus propias estaciones de trabajo; por ejemplo, se puede realizar si en la estación de trabajo de un usuario existe espacio suficiente en disco duro para almacenar los datos del usuario, pero no desea que dicho usuario pueda acceder a los demás archivos y directorios de la estación de trabajo.

En este caso, probablemente lo que habrá que hacer es configurar la estación de trabajo del usuario de tal modo que su directorio base, así como los subdirectorios que contiene, sean los únicos para los cuales el usuario disponga de permisos superiores. Si un usuario posee un directorio base en una computadora distinta de la suya, se establecerá automáticamente una conexión con el directorio base cada vez que dicho usuario inicie una sesión.

Cada vez que un usuario inicie una interfaz de comandos, se seleccionará como directorio predeterminada el directorio base de ese usuario. Este directorio base del usuario también quedará seleccionado como directorio de trabajo en todas las aplicaciones que inicie el usuario, excepto en aquellas para las cuales exista un elemento de programa que especifique un directorio de trabajo distinto.

En Windows NT se proporcionan tres parámetros reemplazables, que pueden sustituirse para utilizarlos con los directorios base:

a) % HOMEPATH%. Representa el nombre de la ruta de acceso del directorio base del usuario.
b) %HOMEDRIVE%. Es la letra de la unidad local necesaria para la conexión de red con el directorio no esté situado en la propia estación de trabajo del usuario.
c) %HOMESHARE%. Es el nombre según UNC (Conversión de Nomenclatura Universal) del directorio compartido que contiene el directorio base del usuario. Puede utilizar estas variables cuando se instalen archivos de comandos de inicio de sesión u otros archivos por lotes, o desde el Administrador de programas; por ejemplo, cuando especifique rutas de acceso de aplicaciones o directorios de trabajo.

3.4 ADMINISTRACION DE ARCHIVOS

Uno de los usos más importantes de los servidores, en la mayoría de las redes, es compartir archivos y directorios con otros usuarios de la red. Cuando un directorio está compartido, los usuarios pueden conectarse a él desde sus propias estaciones de trabajo y acceder desde ellas a los archivos que contenga el directorio. El directorio compartido funciona como si fuera otro disco duro que pueden utilizar los usuarios.

El sistema operativo Windows NT ofrece un rendimiento excelente, fiabilidad y seguridad para compartir archivos, en especial cuando se utiliza el sistema de archivos de Windows NT (NTFS).

Se pueden establecer permisos de archivos en los directorios y en los archivos de los volúmenes NTFS, de manera que únicamente puedan acceder a ellos los usuarios que sean especificados.

Con los permisos de archivos en NTFS, pueden establecer una seguridad diferente para cada archivo y cada directorio. Para cada uno de ellos se pueden especificar exactamente qué grupos y qué usuarios podrán acceder a los archivos, y el nivel de acceso que tiene permitido cada grupo o cada usuario.

Los permisos de archivos en NTFS se aplican a los usuarios que trabajan en la computadora que contiene los archivos y a los usuarios que accedan a ellos a través de la red (si están compartidos).

3.4.1. COMPARTIR ARCHIVOS CON USUARIOS DE RED.

Cuando se comparte un directorio del servidor, los usuarios pueden teóricamente acceder a ese directorio y a los archivos que contenga, a todos sus subdirectorios y a los archivos que contengan. Todo punto del árbol de directorios situado debajo del directorio compartido puede estar disponible para los usuarios de la red.

Sin embargo, si el directorio compartido está en una partición NTFS, podrá bloquear el acceso a algunos de los directorios de un árbol de directorios compartido y a la vez, permitir el acceso a otros directorios, estableciendo permisos para los distintos directorios.

Cuando comparte un directorio, debe asignarle un nombre compartido, es decir, un nombre que deberá utilizar de la red para referirse a ese directorio. Los usuarios de Windows verán el nombre compartido cuando utilicen el Administrador de archivos para examinar la red y los usuarios de MS-DOS podrán ver el nombre compartido cuando utilicen el comando net view. Un nombre compartido puede ser el mismo que el nombre real del directorio, aunque también puede ser distinto.

Los usuarios verán el nombre compartido agregado al nombre de la computadora del servidor. Por ejemplo si se comparte un directorio en el servidor "Producción" y asigna al directorio el nombre compartido "Datos", los usuarios verán el recurso compartido como Producción/Datos. Un recurso que se comparte se denomina recurso compartido.

3.4.2. CONEXIÓN DE LOS USUARIOS.

Los usuarios de la red generalmente se conectan con los directorios compartidos asignando una letra de unidad a dichos directorios en su estación de trabajo. Después realizan esa letra de unidad para hacher referencia al directorio con el que estén conectados. Por ejemplo, supongamos que un usuario se ha conectado al directorio la letra F, este usuario verá el contenido del directorio Aplicaciones del servidor como si fuera el contenido de su unidad F. Para él, el subdirectorio HERRAMIENTAS será F:/HERRAMIENTAS.

Cuando un usuario de Windows se conecte a un directorio, podrá ver la letra de unidad que haya asignado al directorio y aparecerá un icono en la barra de unidades del Administrador de archivos.

Los usuarios de computadoras con MS-DOS que estén ejecutando software de estaciones de trabajo con LAN Manager (pero sin Windows) deberán utilizar el comando net use para conectarse a través de la red. El comando siguiente conecta la letra de unidad F: del usuario al directorio HERRAMIENTAS, del servidor PRODUCCIÓN.

Los usuarios de Windows NT, Windows para trabajo en grupo y Windows 3.1 utilizan el administrador de archivos para efectuar conexiones a través de la red, usando un cuadro de diálogo similar al siguiente (el cuadro de diálogo exacto dependerá del sistema que está ejecutando el usuario):

Los usuarios de estaciones de trabajo con MS-DOS (con y sin Windows 3.1 o Windows para trabajo en grupo) tienen restricciones adicionales sobre la manera de ver y acceder a los directorios compartidos, como se describe a continuación.

Cuando se asignen nombres a los directorios compartidos, hay que tener en cuenta si deben acceder a ellos usuarios de MS-DOS (incluyendo usuarios de Windows 3.1 y de Windows para trabajo en grupo). En este caso hay que asignar un nombre que cumpla la convención de nombres que tengan como máximo 8 caracteres (para los casos de usuarios de MS-DOS), si no se toma en cuenta esto los usuarios de MS-DOS no podrán ver ni accesar a los directorios compartidos cuyos nombres no cumplan esta convención.

Si en un directorio compartido únicamente van accesar usuarios de Windows NT, se podrá utilizar un estilo diferente para los nombres compartidos, que podrán tener hasta 12 caracteres.

En los volúmenes NFTS se pueden asignar nombre de archivos de hasta 255 caracteres. No obstante, no necesita preocuparse de si estos nombres serán vistos por usuarios de MS-DOS.

El sistema NTFS proporciona mapeados de nombres, donde cada archivo o cada directorio cuyo nombre no cumpla la norma 8.3 de MS.DOS recibe automáticamente un nombre que sí la cumple. Los usuarios de MS-DOS que accedan al archivo o al directorio a través de la red verán el nombre en el formato 8.3; pero, los usuarios de Windows NT seguirán viendo el nombre largo. Hay que tener en cuenta que el sistema NTFS solamente crea nombres

cortos para los archivos y directorios que tengan nombres largos. No genera nombres cortos para los nombres compartidos que no cumplan con las normas de asignación de nombres de MS-DOS. Cuando se cree un nombre largo, Windows NT utilizará las siguientes reglas para generar un nombre corto:

a) Los espacios en blanco se eliminan.
b) Los caracteres que no están permitidos en los nombres de MS-DOS se cambian por signos de subrayado (-)
c) El nombre se trunca detrás del sexto carácter (o delante del primer punto del nombre largo si está entre los seis primeros caracteres); después se agrega un guión y un número a estos caracteres.
d) El número para el primer nombre corto creado para un conjunto de seis caracteres en un 1. Si se crean más nombres empleando estos seis caracteres, el siguiente nombre corto utilizará un 2, etc.
e) Si se crea un décimo nombre, sólo se utilizarán cinco caracteres del nombre largo y se agregará un 10 a continuación del guión.
f) Si el nombre largo contiene algún punto seguido por otros caracteres, el último de los puntos y los 3 primeros caracteres que le sigan se utilizarán como la extensión del nombre corto.

Si utiliza Windows NT en un entorno en el que no siempre se admiten los nombres largos, podría ser conveniente seguir utilizando las convenciones de MS-DOS para los 6 primeros caracteres de los nombres y utilizar puntos únicamente para separar los nombres de las extensiones. Por ejemplo, podría dar a un archivo el nombre AGOVEN Agosto 1997 Informe de VENTAS. XLS. El nombre corto correspondiente sería AGOVEN 1.XLS.

3.4.3 PERMISOS EN RECURSOS COMPARTIDOS.

Antes de compartir un directorio, se deberá definir los permisos del directorio, y de sus archivos y subdirectorios.

Cuando se comparte realmente el directorio, se tendrá la oportunidad de definir permisos de recursos compartidos. Estos son adicionales a los permisos individuales de los archivos y directorios. Los permisos de recursos compartidos cumplen la función de un conjunto máximo de permisos para cualquier archivo o subdirectorios del directorio compartido. Por ejemplo, supongamos que Juan tiene el permiso "Control Total" para el directorio APLICACIONES y su subdirectorio HERRAMIENTAS.

Después, se comparte el directorio y se concede a Juan el permiso de "Lectura" de archivos/directorios. Cuando Juan accese a través de la red, únicamente podrá leer los archivos. Las restricciones establecidas por los permisos de recursos compartidos impiden a Juan el "Control Total", a pesar de que tiene este permiso para los mismos directorios.

CAPITULO IV. SERVICIOS DE RED CON WINDOWS NT.

Objetivo:

Enumerar detalladamente las ventajas en cuanto a servicios que proporciona Windows NT al administrar una Red de datos.

CAPITULO 4. SERVICIOS DE RED CON WINDOWS NT

4.1 SERVICIOS QUE PROPORCIONA EL SERVIDOR

Los servicios que proporciona el Servidor de Comunicaciones no se limitan a los que se describen a continuación, ya que debido a la facilidad de integración de software y hardware este planeado para futuras expansiones. Así tenemos como servicios habilitados:

- Servidor de Impresión
- Servidor de Paquetería
- Servidor de Acceso a Internet
- Servidor de FTP.

4.1.1 SERVIDOR DE IMPRESIÓN.

Dentro de los servicios proporcionados por el Servidor de Comunicaciones, se encuentra el servicio de impresión en red. A continuación tenemos un esquema de como esta posicionada una impresora en red y como se da de alta dicha impresora para que actúe como una impresora compartida para toda la red.

En Windows NT, una impresora si no esta dada de alta en el servidor tendrá su funcionamiento únicamente como impresora local. Si se desea convertir una impresora local a una impresora de red, se deben realizar los siguientes pasos:

Dentro de la ventana Main accionar el icono Print manager, una vez estando en esta pantalla se seleciona Create Printer, en donde se darán los siguientes datos:

1) El nombre de la impresora: Debe ser único ya que de lo contrario no se podrá terminar la instalación de dicha impresora.

2) Driver: Definir el dispositivo adecuado al modelo de la impresora, para un buen funcionamiento de la impresora (Que no mande caracteres raros).

3) Descripción: Poner una breve característica de la impresora o de que departamento pertenece.

4) Impresión a: Se define el modelo de la tarjeta de red que tenga la impresora.

5) Compartir la impresora en la red: Al seleccioanr este cubo cualquier usuario que este trabajando en la red puede mandar su impresión, aunque este en otro segmento de red.

6) Nombre compartido: Es el nombre que va a tener dentro de la red, ya que por medio de este se podrá monitorear o buscar para conectarse.

7) Localización: Poner una breve descripción de donde se encuentra fisicamente.

4.1.2 SERVIDOR DE PAQUETERÍA.

Como su nombre lo indica, el Servidor de Paquetería es el que contiene toda la paquetería que utilizan los usuarios de la red, y como en el servidor se encuentran los paquetes instalados en forma administrativa, al instalar se pueden tener diferentes opciones. Por ejemplo, si se desea instalar office 4.2, se ejecuta el software de instalación desde el servidor y se configura y personaliza según las necesidades.

Con lo que se refiere al acceso es aquí donde se decide que grupos entran al subdirectorio y que grupos no accesan. Para instalar un paquete en forma administrativa solo hay que adicionarle al final del archivo que ejecuta la instalción lo siguiente/A que significa una instalación del modo administrativa. Ejemplo: Setup/A o Instalar /A.

Una vez que se termina de instalar la paquetería en forma administrativa se realiza el siguiente procedimiento para la asignación de permisos y la validación del software:

- Se selecciona el subdirectorio donde quedo la paquetería, posteriormente del menú Seguridad, seleccionar Permisos.

- Ahora se visualizarán los grupos por default, para adicionar un grupo, seleccionar el botón ADD.

- Seleccionar el grupo a adicionar, para hacerlo sombreamos el grupo y seleccionamos el botón Add, el nombre del grupo se colocara

automáticamente en nombres adicionados, una vez hecho esto seleccionaremos el tipo de acceso a ese subdirectorio, en donde los tipos de acceso son los siguientes:

A) No Acceso: El grupo no puede entrar al subdirectorio.

B) Lectura: Entra a los archivos pero solo los puede leer.

C) Adicionar y Leer: Entra a los archivos solo para agregar información.

D) Cambios: Entra a los archivos para modificar toda la información.

E) Control total: Puede realizar cualquier cosa a cualquier archivo, inclusive borrarlo.

Una vez que se configura el subdirectorio, aparecerá en la lista el grupo que estamos adicionando y por último seleccionar el recuadro Remplazar los permisos en el subdirectorio y dar OK. Así, tendremos un subdirectorio compartido.

4.1.3 SERVIDOR DE ACCESO A INTERNET.

Para la implementación del Servidor de Internet se analizarán cada uno de los términos involucrados en el establecimiento del servidor, además, explicaremos como está integrada la arquitectura de Windows NT y retomando nuevamente el modelo OSI se realiza una comparación de los protocolos que utiliza Windows NT y otras plataformas de red bajo el modelo Cliente-Servidor.

La Red Internet es una red global de computadoras interconcectadas entre sí, las cuales se comunican a través de un lenguaje común, llamados protocolos de transmisión de datos. Internet apareció a partir de un programa de investigación de la agencia de proyectos de investigación avanzados de la Defensa de Estados Unidos (DARPA),que es centro en las formas de enlazar diversas redes de computadoras. El resultado fue ARPANET, que se inició en 1969. En 1971, estaban conectadas cerca de 40 computadoras o anfitriones a ARPANET, y los investigadores, trabajaban para desarrollar la capacidad de enviar correo electrónico mediante las redes ARPANET, continuó creciendo a lo largo de los años setenta y también empezaron a conectarse a otras redes de computadoras.

A través del Servidor de Internet, se puede tener acceso a una gran cantidad de información ya que se utiliza un recurso llamado "web". El web es un sistema Hipermedia interactivo que conecta al usuario a la Red Internet. Para poder accesar a Internet se puede hacer de diferentes maneras, ya sea por un FTP, por Gopher, o por medio de un explorador gráfico (browser), como son los navegadores:

- Netscape, que es un programa de archivo, el cual es proporcionado por NSAPI (Net Scape Aplication Program Interface)

- Internet Explorer, que es un interfaz gráfica proporcionado por Microsoft.

La mayoría de las páginas están escritas en formato o lenguaje HTML, es decir en Lenguaje de Marcado de Hipertexto, pero actualmente con los adelantos en la programación se tiene una gran variedad de formatos como los GIF,

PostSCript, los documentos escritos en JAVA, ETC. Además del URL es necesario un protocolo de transporte de Hipertexto HTTP.

Para tener acceso a los recursos del Web se utiliza un URL. Un URL es una dirección descriptiva conocida como "Localizador Uniforme de Recursos"

Para comprender como se establecen este tipo de conexiones, se debe tomar en cuenta que en los sistemas Windows 3.x corren aplicaciones de 16 bits, y que dentro de la arquitectura de Windows NT, éste módulo ha sido reemplazado por una interfaz de aplicación de 32 bits.

El Módulo de Interfaz de red con aplicaciones de 32 Bits (32-bit API) contiene programas para aplicaciones de red con interfaz de 32 bits. Dentro de este módulo se encuentran presentes los archivos que hacen posible la conexión a red como son NETAPI.DLL y NETAPI.32DLL, estos dos archivos son básicamente los principales, pero también cuenta con dos archivos secundarios, que en un momento dado son básicos para el sistema, estos son NETBIOS.DLL y WINSOCK.DLL, las cuales son utilizadas para otras aplicaciones de red.

Por ejemplo el archivo WINSOCK.DLL es utilizado por el sistema para conectarse con sistemas que corren aplicaciones de 16 bits como Windows 3.x y Windows 3.11 para grupos de trabajo.

Básicamente, la estructura de un servidor para conexión a Internet consta de los siguientes elementos:

- Proveedor de Enrutamiento Múltiple (MPR, Múltiple Provider Router MPR). Dentro de una red normalmente se utilizan varios protocolos, o la combinación de dos protocolos, para ciertas aplicaciones Windows NT cuenta con un módulo llamado MPR el cual contiene archivos que se encargan de la verificación del tipo de protocolo que se esté utilizando para la conexión del sistema con otros sistemas remotos además cuenta con archivos de seguridad y modo protegido. El MPR se encuentra presente dentro de Windows NT en un folder llamado SYSTEM32 con el nombre de MPR.DLL, este archivo es cargado al sistema por el archivo ejecutable MPNOTIFY.EXE en el momento de la instalación.

El MPR contiene un archivo intermediario llamado MRPUI el cual proporciona una interfaz de usuario. Este archivo muestra mensajes de diálogo cuando no se ejecuta correctamente una aplicación o se desea terminar con una tarea.

Además, cuenta también con el archivo de seguridad: NETLOGON.DLL, el cual se encarga de verificar su permiso de usuario o cuenta local y ejecuta otra actividades relacionadas con la seguridad, cuenta además con el archivo ADVAPI32.DLL el cual se encarga de inspeccionar los contenidos de los registros para determinar que tipo de NPS utilizar.

- Proveedor de Red (NP, Network Provider). El proveedor de red ejecuta todas las funciones del protocolo específico, que requiera una aplicación. Establece o inhabilita una conexión, retorna un nivel de información y proporciona una interfaz consistente para ser usado por el MPR. El RMP siempre requiere de NP's, para saber que aplicación utilizar. Por otro lado el

NP permite que Windows NT soporte más de un protocolo, además el NP guarda datos sobre IFS del estado de la conexión.

- Administrador del Sistema de Archivos de Red (IFS Manager). Cuando el administrador de sistemas de archivos obtiene un nuevo estado de información, este llama al Controlador de Sistemas de Archivos de Red (FSD) para tomar el dato y otros recursos de información.

Por ejemplo cuando el proveedor de red le dice al administrador de sistemas de archivos que se ha conectado a una nueva unidad, el administrador de sistemas de archivos , llama inmediatamente al FSD para que liste un directorio. Además de estas funciones el IFS Manager ejecuta otras tareas normales como la apertura de archivos y hace solicitudes al sistema. En este módulo el MRP no se hace presente, sólo cuando se hace una petición especifica de red.

- Controlador del Sistema de Archivos de Red (Network File System Driver FSD). Cada servidor sobre la red puede utilizar un sistema único de archivo. Por ejemplo si se hace una conexión a un servidor de OS/2 se requiere el acceso al controlador HPFS.Novell y otros sistemas de red que utiliza el modelo cliente servidor utilizan un sistema especial que el proveedor ofrece para ampliar el sistema, seguridad, rehabilitación y capacidad de almacenamiento.

Aunque Windows NT conoce todo acerca de los HPFS, esté no podrá saber acerca del sistema especial de almacenamiento. Para accesar a esos sistemas de archivos, NT necesita un traductor especial para tener acceso a dichos archivos, el traductor hace un llamado a toda la red. El Controlador del sistema de

archivos de red ejecuta estas tareas. Un traductor interpreta archivos externos de Windows NT para que esté los pueda entender.

Un Controlador del sistema de archivos de red consta de un archivo llamado controlador de sistema especifico y del archivo VREDIR.VXD. El archivo VREDIR.VXD hace la interpretación de los archivos de sistemas específicos. Normalmente aquí hay sólo uno FSD para cada Proveedor de Red.

. Transporte de Red (Network transport NT). El número de piezas en un NT esta determinado por la complexión del Setup y de los requerimientos del protocolo. Existen cuatro elementos dentro de Windows NT:

a) Interfaz Controlador de Interfaz (TDI).
b) El Protocolo de Transporte.
c) La Especificación de Interfaces de Dispositivos de Red (NDIS).
D) Controlador del NIC.

Lo mínimo que constituye a un Transporte de Red (NT) son cuatro controladores, por ejemplo, se puede crear un NT para el protocolo NetBEUI usando los siguientes archivos: NETBIO.SYS (el TDI), NBF.SYS (NetBEUI Protocolo de Transporte), NDIS.SYS (NDIS Interface), y NE200.SDYS (Contolador NIS).

NETBIOS.SYS.- Hace un acceso virtual para el protocolo. Esta es la razón por la cual más de una máquina corre sobre el sistema y puede tener acceso a los controladores al mismo tiempo.

NBS.SYS.- Ejecuta tareas de llamado con el NDIS, hace solicitudes al protocolo específico y traduce las preguntas estandarizadas más pequeñas de la red.

NDIS.SYS.- Traduce cada solicitud especifica dentro de Windows NT y hace un llamado para que el NIC Pueda interpretarlo.

EL NIC.- Es un controlador de interface de red que convierte las solicitudes de sistema en una señal eléctrica para presentarlas sobre la red.

El transporte de red requiere de otros archivos como por ejemplo el NDIS30.DLL el cual suministra un soporte actual de Interface de protocolo de Aplicación (API) para NDIS.SYS. Se podría encontrar que NETBIOS.DLL ejecuta la misma función para NETBIOS.SYS.

En esencia se tienen muchos módulos diferentes para crear un transporte. La razón para que todos estos sean bastante fácil de entender, es por ejemplo si se quiere usar un NIC diferente, todo lo que se necesita hacer es hacer un cambio del controlador del NIC y no todos los archivos del protocolo específico.

- Tarjeta de Interface de Red (Network Interface Card NIC). Aquí hay que hacer una mención especial de esta parte por una razón. Este controlador en lo particular es un hardware específico, el cual se comunica con el NIC sobre un nivel fisico que puede entender. Este es el primer problema al tratar de encontrar un controlador que suministre una interfaz estandarizada y que se comunique con el NIC instalado en la máquina. El segundo problema es que sólo se puede colocar un controlador.

- Interfaz de Usuario para Compartir Microsoft (MSSHRUI). Este módulo responde solicitudes de información externa de usuarios para los recursos de configuración de la red, Además cada vez que sé accesa a un recurso el MSSHRUI le dice al NT que debe compartir un recurso, este módulo cuenta con un módulo de protección en el cual se regsitra su permiso de usuario (password). Cuenta con una interfaz para comunicarse con el MPR y el archivo ADVAPI32.DLL que permite al MSSHRU colocar las entradas apropiadàs en el registro, este archivo se localiza en el folder SYSTEM32 llamado NTSHRUI.DLL dentro de Windows NT.

- Servidor Virtual (VSERVER). El punto central de toda actividad para el servidor es el controlador virtual, SVR.SYS, el cual se encuentra en el folder SYSTEM32. Este componente suministra acceso directo a todos los recursos para las solicitudes a través del transporte de red. Trabaja con el administrador de IFS y los módulos de control de acceso para limitar el acceso a los recursos compartidos del sistema y asegura que todos los accesos sean ejecutados apropiadamente. Cada acceso comparte los recursos del sistema manteniendo una línea separada. Esto significa que el acceso a una aplicación no interfiere con ninguna otra.

- Sistema de Poleo (Spooler). El sistema de poleo es el encargado de verificar la conexión de cada uno de los dispositivos en el sistema de Windows NT (impresoras,tarjetas de red, unidades de cd-room etc). Dentro de Windows NT se encuentran tres archivos de poleo en el folder SYSTEM32: SPOOLSS.DLL, SPOOLSS.EXE y WINSPOOL.DRV.

- Control de Acceso (Access Control). Windows NT usa este módulo para una variedad de propósitos, que no exactamente para el control de la red. Por ejemplo Windows NT llama este modulo para verificar su password inicial. Dentro de Windows NT existen dos archivos NETAPI. DLL (de 16 bits) y el NETAPI32 (de 32 bits) dentro del folder SYSTEM32.

- Proveedor de Seguridad (Security provider). Windows NT suminiestra seguridad centralizada a través del archivo SECURITY.DDL que se encuentra ubicado dentro del folder SISTEM32. Obviamente que otros archivos se encuentran asociados a este tales como: el archivo DCESE.DLL el cual suministra seguridad al intercambio de datos de comunicación (DCE) cuando es llamado por el archivo de seguridad SECURITY.DLL

- NTFS (New Technology File System o Windows NT File System). NTFS proporciona seguridad y control de acceso a todos los archivos de datos dentro del sistema de Widows a través del archivo File Manager, por medio de esté archivo administra los recursos del servidor por medio de cuentas locales y globales.

Así lo anterior se integra en la explicación de la estructura de un servidor NT:

CONCLUSIONES

Se ha contemplado que las Comunicaciones es una de las ramas de la Ingeniería que se va actualizando y evolucionando día con día. Con el presente trabajo se manifiesta la necesidad de administrar, configurar y sobre todo, de comprender que en una red, un Servidor de Comunicaciones es la herramienta que hace posible el intercambio de información. Se han descrito los motivos por los cuales elegir a windows NT como un Sistema Operativo de red a utilizar, dadas sus características de operación e integración y su facilidad de manejo, para consolidarlo en un Servidor de Comunicaciones.

Se ha analizado el beneficio de administrar un Servidor con Windows NT, ya que emplea recursos propios como lo son los Dominios, los que nos facilitan la tarea de administrar usuarios y las Relaciones de Confianza. Estas cualidades son procedentes del hecho de que al trabajar con NT tenemos una administración centralizada, en la cual, la base de datos de los usuarios se encuentra físicamente en un sólo lugar, teniendo así una cuenta para cada usuario y el usuario con una sola cuente, puede accesar a distintos dominios de la misma red e inclusive de otras redes.

Con lo que respecta a la administración del Servidor de Comunicaciones, se han dado las bases para agrupar a los usuarios en grupos ya que así se pueden definir derechos sobre los archivos a los grupos y no a cada usuario, también facilita la definición de derechos, y una vez definidos en los grupos, solo basta integrar al, el, o los usuarios en el grupo para que hereden los permisos dados en el grupo y trabajen con esas restricciones.

Hablando de la seguridad, Windows NT implementa vía software arreglos llamados espejeo de discos, en los cuales la información se duplica. Esta facilidad permite que en una contingencia, se pueda cambiar el disco dañado sin perder toda la información, necesitando emplear para este arreglo dos discos duros. Además se puede asegurar que definiendo los permisos de forma adecuada, se logra un grado de seguridad eficiente en donde no se podrá burlar y no habrá perdida de información y desequilibrio en la consistencia de información.

Se contemplo la necesidad de utilizar las relaciones de confianza dentro del servidor para manejar la comunicación entre dominios, y una vez establecido la relación de confianza, compartir los recursos entre los usuarios para poder trabajar de un dominio a otro.

Se propusieron algunas alternativas para la utilización del servidor de Comunicaciones con NT, en donde se describió la forma de implementar servicios de impresión, paquetería, de acceso a Internet y de FTP. Pero los servicios que se pueden ofrecer no se limitan a los que se han descrito, la facilidad de integración y de operación son las propuestas que quedan libres para adecuar los servicios a las necesidades especificas de cada red y en su caso, de los usuarios que la componen.

BIBLIOGRAFIA

INTRODUCCION A WINDOWS NT
KEVIN C. DINFORD.
GRIJALBO, 1996

SUPPORTING MICROSOFT WINDOWS NT 3.51
MICROSOFT EDUCATION AND CERTIFICATION
STUDENT WORKBOOK, 1996

MICROSOFT WINDOWS NT VER. 4.0
MICROSOFT EDUCATION AND CERTIFICATION
STUDENT BOOK 1997

FUNDAMENTOS DEADMINISTRACION Y SISTEMAS OPERATIVOS DE RED.
JESUS BRAVO
ALFA, 1995.

INGENIERIA DE COMUNICACIONES
WILLIAN LITELL EVERITT
MARCOMBO, 1996.