UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN

"DISEÑO E IMPLEMENTACION DE UNA RED DE AREA LOCAL ADMINISTRADA BAJO EL SISTEMA OPERATIVO WINDOWS NT"

T E S I S

QUE PARA OBTENER EL TITULO DE

INGENIERO MECANICO ELECTRICISTA

P R E S E N T A :

OSCAR HERNANDEZ SANCHEZ

ASESOR: ING. JOSE JUAN CONTRERAS ESPINOSA

CUAUTITLAN IZCALLI, ESTADO DE MEXICO 2000

UNIDAD DE LA ADMINISTRACION ESCOLAR
DEPARTAMENTO DE EXAMENES PROFESIONALES

U. N. A. M.
FACULTAD DE ESTUDIOS SUPERIORES-CUAUTITLAN

ASUNTO: VOTOS APROBATORIOS

DEPARTAMENTO DE EXAMENES PROFESIONALES

DR. JUAN ANTONIO MONTARAZ CRESPO
DIRECTOR DE LA FES CUAUTITLAN
P R E S E N T E

ATN: Q. Ma. del Carmen García Mijares
Jefe del Departamento de Exámenes
Profesionales de la FES Cuautitlán

Con base en el art. 28 del Reglamento General de Exámenes, nos permitimos comunicar a usted que revisamos la TESIS:
"Diseño e Implementación de una Red de Area Local Administrada Bajo el Sistema Operativo Windows NT"

que presenta el pasante: Oscar Hernández Sánchez
con número de cuenta: 8457144-1 para obtener el título de :
Ingeniero Mecánico Electricista

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXAMEN PROFESIONAL correspondiente, otorgamos nuestro VOTO APROBATORIO.

A T E N T A M E N T E
"POR MI RAZA HABLARA EL ESPIRITU"
Cuautitlán Izcalli, Méx. a 3 de julio del 2000.

PRESIDENTE	Ing. José Juan Contreras Espinosa	
VOCAL	Ing. Armando Aguilar Márquez	
SECRETARIO	Ing. Rogelio Ramos Carranza	
PRIMER SUPLENTE	Ing. José Luz Hernández Castillo	
SEGUNDO SUPLENTE	Ing. Jorge Altamira Ibarra	

A MIS PADRES:

IGNACIO HERNANDEZ RANGEL

GUADALUPE SANCHEZ BAEZA†

Gracias por que me han enseñado a ser hombre. Me han enseñado que ante todos los problemas y adversidades teniéndolo todo para perder, el darse por vencido nunca es la solución.

Me han enseñado a arriesgar lo poco que se tiene en pos de conseguir algo mejor, dándome ejemplo de no pecar de soberbia si triunfo, y educando mi capacidad de afrontar frustraciones y derrotas sin quejas ni ira al ser vencido.

Me han enseñado que el ser humilde, es ir a darle la cara a una persona que acaba de humillarte y no devolverle el insulto, si no perdonarlo y dejarle las puertas abiertas.

Me han enseñado y corregido inteligentemente en mis momentos de desorientación, me han servido cuando el que debería del servirles soy yo.

Han estado presentes cuantas veces los he necesitado, en los momentos felices para alentarme y en los momentos de tristeza para consolarme y aconsejarme.

Y a veces me han indicado que yo solo debo resolver mis problemas.

Me han legado una personalidad de servicio y entrega, pues han dejado todas sus diversiones para darme incluso hasta lo que no han tenido.

Me han enseñado a tener sangre fría en los momentos de crisis y cautela y honor en los momentos grandes. Me han respetado mi individualidad y más aún, me han enseñado a no cometer sus errores invitándome a seguir su camino de aciertos.

Pero más que todo, me han enseñado a ser un hombre fiel, dedicado, responsable y justo. Que suerte tengo de haber sido bendecido por Dios con unos padres como ustedes, excelentes amigos, los mejores de todos.

A MIS HERMANOS:

CRISTINA,

GERARDO,

ANA

Y

YAZMIN.

Quienes han sido mis mas grandes amigosy guias, y que me han apoyado incondicionalmente toda mi vida.

A MIS SOBRINOS:

ITZEL,

AARON

Y ALBERTO

A MIS AMIGOS:

"Un amigo es una persona que nunca duda de ti, pues la mayor injuria que se le puede hacer a un hombre es dudar de él.

Un amigo es un ser clarividente que tiene el valor de decirte, "haces mal".

Un amigo es un corazón grande que olvida y perdona.

Un amigo que se compromete ayudarte, es una perla del fondo del mar."

Henri Didon

A MIS PROFESORES:

Entre quienes tengo a muy grandes amigos.

Introducción

Las redes en general, consisten en "compartir recursos", y uno de sus objetivos es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a 1000 Km de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente.

Un segundo objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. Por ejemplo todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias. Además, la presencia de múltiples CPU significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encarqarse de su trabajo, aunque se tenga un rendimiento global menor.

Otro objetivo es el ahorro económico. Los ordenadores pequeños tienen una mejor relación costo / beneficio, comparada con la ofrecida por las máquinas grandes. Estas son, a grandes rasgos, diez veces más rápidas que él más rápido de los microprocesadores, pero su costo es miles de veces mayor. Este desequilibrio ha ocasionado que muchos diseñadores de sistemas construyan sistemas constituidos por poderosos ordenadores personales, uno por usuario, con los datos guardados una o más máquinas que funcionan como servidor de archivo compartido.

Este objetivo conduce al concepto de redes con varios ordenadores en el mismo edificio. A este tipo de red se le denomina LAN (red de área local), en contraste con lo extenso de una WAN (red de área extendida), a la que también se conoce como red de gran alcance.

Un punto muy relacionado es la capacidad para aumentar el rendimiento del sistema en forma gradual a medida que crece la carga, simplemente añadiendo mas procesadores. Con máquinas grandes, cuando el sistema esta lleno, deberá reemplazarse con uno más grande, operación que por lo normal genera un gran gasto y una perturbación inclusive mayor al trabajo de los usuarios.

Otro objetivo del establecimiento de una red de ordenadores, es que puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre sí. Con el ejemplo de una red es relativamente fácil para dos o más personas que viven en lugares separados, escribir informes juntos. Cuando un autor hace un cambio inmediato, en lugar de esperar varios días para recibirlos por carta. Esta rapidez hace que la cooperación entre grupos de individuos que se

encuentran alejados, y que anteriormente había sido imposible de establecer, pueda realizarse ahora.

Cada uno de los tres siglos pasados ha estado dominado por una sola tecnología. El siglo XVIII fue la etapa de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la época de la máquina de vapor. Durante el siglo XX, la tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, hemos asistido a la instalación de redes telefónicas en todo el mundo, a la invención de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de las computadoras (ordenadores), así como a la puesta en órbita de los satélites de comunicación.

A medida que avanzamos los últimos años del siglo XX y los primeros del siglo XXI, se ha dado una rápida convergencia de estas áreas, y también las diferencias entre la captura, transporte almacenamiento y procesamiento de información están desapareciendo con rapidez. Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, simplemente oprimiendo una tecla. A medida que crece nuestra habilidad para recolectar procesar y distribuir información, la demanda de mas sofisticados procesamientos de información crece todavía con mayor rapidez.

CAPITULO 1

La industria de ordenadores ha mostrado un progreso espectacular en un muy corto tiempo. El viejo modelo de tener un solo ordenador para satisfacer todas las necesidades de cálculo de una organización se está reemplazando con rapidez por otro que considera un número grande de ordenadores separados, pero interconectados, que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de redes de ordenadores. Estas nos dan a entender una colección interconectada de ordenadores autónomos. Se dice que los ordenadores están interconectados, si son capaces de intercambiar información. La conexión no necesita hacerse a través de un hilo de cobre, el uso de láser, microondas y satélites de comunicaciones. Al indicar que los ordenadores son autónomos, excluimos los sistemas en los que un ordenador pueda forzosamente arrancar, parar o controlar a otro, éstos no se consideran autónomos.

A mediados de los 70 diversos fabricantes desarrollaron sus propios sistemas de redes locales. Es en 1980 cuando Xerox, en cooperación con Digital Equipment Corporation e Intel, desarrolla y publica las especificaciones del primer sistema comercial de red denominado EtherNet. En 1986 IBM introdujo la red TokenRing. La mayor parte del mercado utiliza hoy día la tecnología del tipo EtherNet.

En 1982 aparecen los ordenadores personales, siendo hoy una herramienta común de trabajo. Esta difusión del ordenador ha impuesto la necesidad de compartir información, programas, recursos, acceder a otros sistemas informáticos dentro de la empresa y conectarse con bases de datos situadas físicamente en otros ordenadores, etc. En la actualidad, una adecuada interconexión entre los usuarios y procesos de una empresa u organización, puede constituir una clara ventaja competitiva. La reducción de costes de periféricos, o la facilidad para compartir y transmitir información son los puntos claves en que se apoya la creciente utilización de redes.

Redes de área local (LAN):

Uno de los sucesos más críticos para la conexión en red lo constituye la aparición y la rápida difusión de la red de área local (LAN), como forma de normalizar las conexiones entre las máquinas que se utilizan como sistemas ofimáticos. Como su propio nombre indica, constituye una forma de

interconectar una serie de equipos informáticos. A su nivel más elemental, una LAN no es más que un medio compartido (como un cable coaxial al que se conectan todas las computadoras y las impresoras) junto con una serie de reglas que rigen el acceso a dicho medio. La LAN más difundida, la Ethernet, utiliza un mecanismo denominado Call Sense Multiple Access-Collision Detect (CSMS-CD). Esto significa que cada equipo conectado sólo puede utilizar el cable cuando ningún otro equipo lo está utilizando.

Ethernet y CSMA-CD son dos ejemplos de LAN. Hay tipologías muy diversas (bus, estrella, anillo) y diferentes protocolos de acceso. A pesar de esta diversidad, todas las LAN comparten la característica de poseer un alcance limitado (normalmente abarcan un edificio) y de tener una velocidad suficiente para que la red de conexión resulte invisible para los equipos que la utilizan.

Además de proporcionar un acceso compartido, las LAN modernas también proporcionan al usuario multitud de funciones avanzadas. Hay paquetes de *software* de gestión para controlar la configuración de los equipos en la LAN, la administración de los usuarios, y el control de los recursos de la red. Una estructura muy utilizada consiste en varios servidores a disposición de distintos (con frecuencia, muchos) usuarios.

Redes de área extensa (WAN):

Cuando se llega a un cierto punto deja de ser poco práctico seguir ampliando una LAN. A veces esto viene impuesto por limitaciones físicas, aunque suele haber formas más adecuadas o económicas de ampliar una red de computadoras. Dos de los componentes importantes de cualquier red son la red de teléfono y la de datos. Son enlaces para grandes distancias que amplían la LAN hasta convertirla en una red de área extensa (WAN). Casi todos los operadores de redes nacionales ofrecen servicios para interconectar redes de computadoras, que van desde los enlaces de datos sencillos y a baja velocidad, que funcionan basándose en la red pública de telefonía, hasta los complejos servicios de alta velocidad adecuados para la interconexión de las LAN. Estos servicios de datos a alta velocidad suelen denominarse conexiones de banda ancha. Se prevée que proporcionen los enlaces necesarios entre LAN para hacer posible lo que han dado en llamarse autopistas de la información.

Intranets

Una intranet es una versión reducida del Internet. Es usada principalmente por empleados de una compania que están distribuidos geográficamente por largas distancias y que pasan una gran cantidad de tiempo trabajando colaborativamente. Por usar los principios del Internet, tales como el correo electrónico, las corporaciones pueden garantizar el acceso a todos sus recursos de información a todos los usuarios de su organización.

La Intranet nació casi de la noche a la mañana, como una parte importante de los sistemas de información corporativos. Investigadores en el Boston Research Group estiman que a principios de 1994 tan poco como el 11 porciento de las grandes organizaciones comerciales tenían una Intranet. Para 1996 ese numero se había elevado por encima del 50 por ciento, y en tanto el numero de grandes corporaciones que adoptan una Intranet se eleva, firmas de un tamaño pequeño a mediano están encontrando en la Intranet los beneficios de poner al alcance de su gente la información en redes.

Proceso distribuido:

Parece lógico suponer que las computadoras podrán trabajar en conjunto cuando dispongan de la conexión de banda ancha. ¿Cómo conseguir, sin embargo, que computadoras de diferentes fabricantes en distintos países funcionen en común a través de todo el mundo? Hasta hace poco, la mayoría de las computadoras disponían de sus propias interfaces y presentaban su estructura particular. Un equipo podía comunicarse con otro de su misma familia, pero tenía grandes dificultades para hacerlo con un extraño. Sólo los más privilegiados disponían del tiempo, conocimientos y equipos necesarios para extraer de diferentes recursos informáticos aquello que necesitaban.

En los años noventa, el nivel de concordancia entre las diferentes computadoras alcanzó el punto en que podían interconectarse de forma eficaz, lo que le permite a cualquiera sacar provecho de un equipo remoto.

Conexiones de red:

Una red tiene dos tipos de conexiones: conexiones físicas —que permiten a los ordenadores transmitir y recibir señales directamente— y conexiones lógicas, o virtuales, que permiten intercambiar información a las aplicaciones informáticas, por ejemplo a un procesador de textos. Las

conexiones físicas están definidas por el medio empleado para transmitir la señal, por la disposición geométrica de los ordenadores (topología) y por el método usado para compartir información. Las conexiones lógicas son creadas por los protocolos de red y permiten compartir datos a través de la red entre aplicaciones correspondientes a ordenadores de distinto tipo, como un Apple Macintosh y un PC de IBM. Algunas conexiones lógicas emplean *software* de tipo cliente-servidor y están destinadas principalmente a compartir archivos e impresoras.

Protocolos de intercambio:

En informática, como en las relaciones humanas, el protocolo de intercambio es la señal mediante la cual se reconoce que puede tener lugar la comunicación o la transferencia de información. Los protocolos de intercambio se pueden controlar tanto con *hardware* como con *software*. Un protocolo de intercambio de *hardware*, como el existente entre un ordenador o computadora con una impresora o con un módem, es un intercambio de señales, a través de cables específicos, en el que cada dispositivo señala su disposición para enviar o recibir datos. Un protocolo de *software*, normalmente el que se intercambia durante las comunicaciones del tipo módem a módem, consiste en una determinada información transmitida entre los dispositivos de envío y de recepción. Un protocolo de intercambio de *software* establece un acuerdo entre los dispositivos sobre los protocolos que ambos utilizarán al comunicarse. Un protocolo de intercambio de *hardware* es por tanto similar a dos personas que físicamente estrechan sus manos, mientras que un protocolo de intercambio de *software* es más parecido a dos grupos que deciden conversar en un lenguaje particular.

El protocolo de comunicaciones podría definirse como el conjunto de reglas para determinar qué sistema debe emitir la información y cuál debe recibirla. Normalmente se engloban aquí las señales que se emplean en los conductores y las reglas de interpretación de los bits de control y datos. Un protocolo puede descomponerse en niveles lógicos o capas denominados layers.

El comité 802 del IEEE (Institute of Electrical and Electronic Engineers) desarrolla protocolos estándares divididos en capas que se corresponden con el modelo de 7 niveles de la ISO (International Standards Organization).

Para ilustrar la necesidad de un protocolo puede pensarse en el siguiente ejemplo, tomado de un campo totalmente distinto al de las redes de ordenadores, pero con problemas afines de transporte:

Supóngase que se quiere trasladar los restos de un arco románico desde un monte hasta otro país. Con este fin se numeran las piezas, se desmonta en orden, según unas normas; las piezas se agrupan en contenedores numerados. Se realiza un primer transporte hasta un puerto de mar en contenedores (containers). En el puerto, los containers se agrupan y otra empresa de transportes los envía por vía marítima al país de destino. Puede suceder que los containers se envíen en distintos barcos, con escalas distintas... En el puerto de destino la compañía naviera reagrupará los containers y los traspasará a la empresa de transporte terrestre, que los entregará al arquitecto en el lugar de emplazamiento. Allí en un orden inverso al empleado en el lugar de origen sé desagruparán las piezas y se montará el arco.

Al estudiar este ejemplo, se encuentra un paralelismo con otro ejemplo como puede ser el envío de una información entre usuarios de ordenadores en un hospital:

Supóngase -por ejemplo- que quiere enviar una imagen de rayos X, o el texto correspondiente a un historial clínico, de un departamento de un hospital a otro departamento.

Los datos que componen la imagen o el historial deben dividirse puesto que por su tamaño no puede emplearse un único datagrama. Además, esta información debe circular por una red con distintos soportes físicos y velocidades (coaxial, fibra óptica, etc.) y luego, por fin, recomponerla en el otro ordenador. Estos procesos plantean las siguientes cuestiones:

1. ¿Qué criterio se sigue para numerar las piezas originales?

2. ¿Con qué criterio se agrupan en las unidades de transporte (containers)?

3. ¿Cómo se ha decidido el tamaño de esas unidades de transporte en cada uno de los medios físicos?

4. ¿Qué criterio se emplea para reagrupar la información al llegar a un nuevo puerto (tipo de red)? : hay que tener en cuenta que los envíos pueden ir por distintos caminos, y llegar primero, los que salieron más tarde.

5. ¿Qué criterio se sigue para desagrupar la información?

Los protocolos establecen todas las reglas correspondientes al transporte en sus distintos niveles. Cada nivel de abstracción corresponde a un layer.

En un nivel se trabaja con la aplicación que maneja la información que se desea transportar; en otro se carga la información en los datagramas; otro nivel controla el acceso al medio. En el ordenador que recibe la información, los layers trabajan de forma análoga a él que envía, pero en sentido inverso: Controla el acceso al medio, lee los datagramas, reagrupa la información, y pasa los datos a la aplicación.

Algunos protocolos conocidos son:

NetBEUI.

Es el protocolo utilizado por las antiguas redes basadas en Microsoft LAN Manager. Es muy rápido en pequeñas redes que no lleguen a la decena de equipos y que no muevan ficheros de gran tamaño, a partir de ahí es mejor buscar otra opción y lo desinstalarlo de los clientes y servidores, esto último siempre que no se tenga ningún equipo que utilice LAN Manager.

IPX/SPX.

Este protocolo, implementado por Novell, ha demostrado sobradamente su valía en redes de área local, es rápido, fácil de configurar y requiere pocas atenciones. Es el protocolo que Microsoft recomienda para redes de área local basadas en DOS, Windows 3.x, Windows 95 y Windows NT.

El principal inconveniente que presenta para redes medianas y grandes es que no se puede enrutar o sea que no puede pasar de una subred a otra si entre ambas hay un encaminador (router), por lo que no puede usarse en redes WAN. Otro inconveniente que presenta en redes con un cierto

número de equipos es que puede llegar a saturar la red con los broadcast que lanzan los equipos para anunciarse en la red.

TCP/IP.

Este protocolo juega aquí con sobrada ventaja pues se trata de un favorito por los constructores del internet por lo que se hace imprescindible si se está conectado a Internet o si se quiere crear una Intranet.

La capacidad de TCP/IP para mover información en una red, por grande que sea, sin perder datos, su sistema de nombres y direcciones, y su facilidad para saltar de una red a otra lo convierten en el candidato ideal para cualquier red de ordenadores dispuesta a no quedar aislada de otros sistemas de redes, o sea del resto del mundo.

Protocolo usado por Internet

El conjunto de Protocolos de Control de Transmisión y Protocolo de Internet (TCP/IP, siglas en inglés), desarrollado originalmente por el Departamento de Defensa estadounidense, es el conjunto de conexiones lógicas empleado por Internet, la red de redes planetaria. El TCP/IP, basado en *software* de aplicación de igual a igual, crea una conexión entre dos computadoras cualesquiera.

Componentes Fisicos de la Red

Los servicios en la mayoría de las LAN son muy potentes. La mayoría de las organizaciones no desean encontrarse con núcleos aislados de utilidades informáticas. Por lo general prefieren difundir dichos servicios por una zona más amplia, de manera que los grupos puedan trabajar independientemente de su ubicación. Los *routers* y los *bridges* son equipos especiales que permiten conectar dos o más LAN. El *bridge* es el equipo más elemental y sólo permite conectar varias LAN de un mismo tipo. El *router* es un elemento más inteligente y posibilita la interconexión de diferentes tipos de redes de ordenadores. El hecho de que sean redes distintas quiere decir que tienen distinto medio de transmisión, distinta estructura de la información que transmiten, distintas velocidades. Además, como puede intuirse con los ejemplos de transporte mencionados al hablar de protocolos, puede haber problemas de encaminamiento cuando la información pasa de una red a otra: dependiendo del tráfico, los paquetes de información pueden enviarse por caminos alternativos.

Hubs (concentradores)

Son un punto central de conexión para nodos de red que están dispuestos de acuerdo a una topología física de estrella. Son dispositivos que se encuentran físicamente separados de cualquier nodo de la red, aunque algunos Hubs se enchufan aun puerto de expansión en un nodo de red.

El hub tiene varios puertos a los que se conecta el cable de otros nodos de red.

Pueden conectarse varios Hubs para permitir la conexión de nodos adicionales

La mayoría de los Hubs tienen un conector BNC además de los conectores normales Rj-45. El conector BNC permite que se enlacen Hubs por medio de un cable coaxial thin. Al disponer del conector BNC, no se tiene que desperdiciar un puerto RJ-45 en cada Hubs para la conexión con otro hub. Por el contrario, ese puerto puede conectarse a un nodo de red. Además los Hubs conectados con cable thin, también se pueden instalar nodos de red con adaptadores thin en el mismo segmento de cable.

Repeaters (repetidores)

Es un dispositivo que permite extender la longitud de la red, amplifica y retransmite la señal.

Los repetidores multipuertos permiten conectar más de dos segmentos de cable de red. Es importante no olvidar que aunque el repetidor multipuertos permite crear una topología física de estrella basada en varias topologías físicas de bus, el propósito principal de un repetidor es extender la longitud máxima permitida del cable de la red.

Bridge (puente)

Es un dispositivo que conecta dos LAN separadas para crear lo que aparenta ser una sola LAN. Los puentes revisan la dirección asociada con cada paquete de información. Luego si la dirección es correspondiente a un nodo del segmento de red actual, no pasara el paquete a otro lado. La función del puente es transmitir la información enviada por un nodo de una red al destino pretendido en la otra red.

Opera en la capa de acceso al medio (capa 2)

Los puentes también se emplean para reducir la cantidad de trafico en un segmento de red. Mediante la división de un solo segmento de red en dos segmentos y conectándolos por medio de un puente se reduce él trafico general de la red. El puente mantendrá aislada la actividad de la red en cada segmento a menos que el nodo de un segmento envíe información al nodo de otro segmento en cuyo caso el puente pasaría la información.

Pueden ser programados para que sepan que direcciones se encuentran de que lado del puente o pueden identificarlo simplemente observando los paquetes y viendo de donde vienen y a donde van.

Routers (Ruteadores)

Son similares a los puentes, solo que operan a un nivel diferente. Requieren por lo general que cada red tenga el mismo Sistema Operativo de Red (Network Operating System=NOS). Con un NOS común el ruteador puede ejecutar funciones más avanzadas de las que podría permitir un puente, como conectar redes basadas en topologías lógicas completamente diferentes como ETHERNET Y TOKEN RING. También determinan la ruta más eficiente para el envío de datos en casos de haber más de una ruta.

Son mucho más complejos que los puentes. Entienden el protocolo de los paquetes y traducen entre protocolos distintos. Si se quisiera conectar una LAN ETHERNET que maneja un protocolo con otra LAN ETHERNET que maneja otro protocolo diferente, necesitara un ruteador.

También sirve para enviar paquetes a través de rutas distintas cuando se conectan varias redes. Esto significa que los Ruteadores pueden enviarse por la ruta más rápida, más barata, la más confiable etc. dependiendo del criterio que resulte más importante.

Existen dos clases:

1. Los estáticos: difíciles de mantener, ya que el administrador de red tiene que proporcionarles información sobre como seleccionar rutas para los paquetes.
2. Los dinámicos: Mucho más inteligentes que los estáticos. Observan todas sus interfaces y construyen tablas que identifican las rutas optimas. Si una ruta falla y hay una conexión alterna disponible, un ruteador dinámico puede asegurar que el sistema de interredes soporte las fallas.

Sin embargo un ruteador básico solo conecta redes cuyos protocolos pueda entender.

Un ruteador esta diseñado de manera que si no puede canalizar los paquetes actúa como puente.

Gateways (compuertas)

Permite que los nodos de una red se comuniquen con tipos diferentes de red o con otros dispositivos. Este tipo de compuertas también permite que se compartan impresoras entre las dos redes.

Una vez que se pasa a funciones tales como encontrar datos en un registro, o archivo, es necesario construir toda clase de controles, verificaciones y protocolos para establecer, verificar, mantener y usar los servicios. Aquí es donde se hace necesario un método para traducir una manera de solicitar y usar servicios de otra.

Las compuertas cubren este papel de traducción. Se colocan entre dos sistemas y convierten las solicitudes del emisor a un formato que puede ser entendido por el receptor.

Transceiver

Este dispositivo permite conectarse a los cables coaxiales de la red, ya sea para implementar una nueva rama de la red o una simple derivación para un solo computador. Este aparato tiene un dispositivo tipo tornillo que penetra el interior del cable coaxial y hace contacto con el conductor central, sin necesidad de cortarlo; la parte exterior del tornillo hace contacto con el conductor

exterior para garantizar de esta manera una buena conexión eléctrica. Normalmente estos dispositivos pueden tener un conector AUI para hacer conexión con un computador o con un hub, y uno tipo coaxial para conectarse al cable principal de red o simplemente generar otra rama de la misma.

El transceiver tiene internamente un circuito electrónico que le permite transmitir y recibir los datos a través del cable y proteger el cable principal contra fallas que se presenten en el computador o la rama que está derivada de él. El cable que va del transceiver al computador tiene 5 pares de cable trenzado: uno para alimentar los circuitos del transceiver, dos para enviar y recibir datos y los otros dos para realizar funciones de control. Este cable tiene en cada extremo un conector AUI.

Tarjeta adaptadora de red

El papel de una tarjeta adaptadora de red es actuar como interfaz física o de conexión entre el computador y el cable de red.

Funciones:

- Preparar datos desde el computador para el cable de red. Antes de que los datos puedan ser enviados para la red, la tarjeta adapta la señal para que pueda viajar. El camino por el que viajan los datos en el computador es el bus. Los primeros buses de 8 bits fueron de IBM, IBM PC/AT usó bus de 16 bits, algunos computadores usan buses de 32 bits. En el bus los bits viajan en paralelo, mientras que en el cable de red viajan en serie.

  La tarjeta adaptadora de red toma los datos que viajan en paralelo, los agrupa y envía en serie por el cable de red, traduce las señales digitales del computador en señales ópticas y eléctricas para que puedan viajar por el cable. El componente responsable de esto es el transceiver.

- Asignar Direcciones de red. La tarjeta de red indica la localización o la dirección del resto de la red para distinguir todas las otras tarjetas.

  Las direcciones en la red son determinadas por la IEEE. Cada tarjeta tiene una dirección única quemada.

  En las tarjetas que utilizan DMA(Acceso Directo a Memoria) el computador asigna algo del espacio de la memoria para la tarjeta, solicita datos al computador, en el bus mueve datos de la memoria a la tarjeta, almacena en RAM mientras transmite o recibe cuando los datos viajan más rápido de lo que puede manejar.

- Enviar y controlar datos. La tarjeta transmisora y la receptora se ponen de acuerdo antes de enviar los datos en:

  - Tamaño máximo del grupo de datos a enviar.
  - Cantidad de datos que se envían antes de la transmisión (Confirmación).
  - Intervalo de tiempo entre cada trozo de datos enviado.
  - Tiempo de espera antes que la confirmación sea enviada
  - Cantidad de datos que cada tarjeta puede retener antes de un sobreflujo
  - Velocidad de la transmisión

- Controlar el flujo de datos entre los computadores y el sistema de cableado.

- Recibir los datos entrantes del cable y traducir en bytes para que la CPU las pueda entender.

Las tarjetas necesitan igual velocidad para transmitir. Algunas tarjetas tienen circuitos que permiten que se ajusten a la velocidad de otras tarjetas más lentas. Cuando todos los detalles de la comunicación han sido determinados, las dos tarjetas comienzan a transmitir y recibir datos.

Contiene hardware y firmware programado que implementa el control lógico de enlace (Logical Link Control) y las funciones de control de acceso al medio (Media Access Control).

Los adaptadores de computadores para cables son conocidos como NICs ("Network Interface Cards"). Estos conectan el computador físicamente al tipo particular de cable que ha sido seleccionado, traducen entre señales bus de PCs locales de bajo poder y señales de medios de red de alto poder para larga distancia más fuertes, y corren programas en su ROM que formatean las señales enviadas por cable. Es importante notar que ciertos tipos de NICs pueden enviar y recibir datos mucho más rápidamente que otros: hay token ring NICs de 4 mbps y de 16 mbps. , Ethernet NICs de 10 mbps. y de 100 mbps, NICs FDDI de 100 mbps, etc. Con las crecientes necesidades de rapidez en las redes locales, regionales y globales, la elección de NICs apropiados para servidores y clientes, es un elemento importante en el diseño de una red.

Hay muchos tipos de NICs de diferentes fabricantes para los sistemas de comunicación más populares como ARCnet, Ethernet y Token Ring. Casi cualquier PC equipado con una tarjeta cualquiera puede comunicarse con otro PC que tenga una tarjeta de un fabricante diferente. Para fibra óptica se restringe el uso de tarjetas a las de un solo fabricante.

Existen muchos parámetros y opciones diferentes que deben configurarse en los diferentes tipos de tarjetas. En las tarjetas más recientes la configuración puede realizarse totalmente por medio de software.

Configuración de opciones y montaje

- Algunas tarjetas se pueden configurar por software o por jumpers
- Interrupciones (IRQ. Interrupt Request). A través de IRQ los dispositivos hacen peticiones de servicios al microprocesador.
- Las IRQ son construidas dentro del hardware interno del computador y tienen asignados diferentes niveles de prioridad que el microprocesador puede determinar.

Cuando la tarjeta adaptadora de red envía un requerimiento (Request) para el computador, este usa una interrupción (Interrupt) que es una señal eléctrica enviada a la CPU del computador. Cada mecanismo del computador puede usar diferentes IRQ. Esta se especifica cuando el componente es instalado. (Configurado)

Los recomendados para instalar la tarjeta son el IRQ 3 o IRQ 5

Puerto base I/O. El puerto base de entrada/salida especifica un canal por el que fluye la información entre el hardware del computador y la CPU. El puerto se le muestra a al CPU como una dirección.

Cada componente de hardware en un sistema debe tener un número diferente de puerto base I/O.

Dirección de memoria Base. Identifica una localización en la memoria RAM del computador. Esta localización es usada por la tarjeta adaptadora de red como un área de buffer para almacenar los frames de datos entrantes y salientes , esto es llamado algunas veces la dirección RAM de arranque.

Frecuentemente la dirección de memoria Base para la tarjeta de red es D8000. Es necesario asignar una dirección de memoria base que no la este usando otro dispositivo.

Compatibilidad de tarjetas adaptadoras

La tarjeta debe:

- Encajar en la estructura interna del computador
- Tener el correcto tipo de conector de cable.

- Las topología anillo requieren tarjetas físicamente diferentes de las usadas por BUS y APPLE usa un tipo diferente de método de comunicación de red.

Arquitectura data bus

Hay cuatro tipos de arquitecturas de bus de datos:

1. ISA: (Industry Standard Architecture) Usada en computadores IBM PC XT y AT Hay para slot de 8 y 16 bits. La de 8 bits se puede colocar en un slot de 16 bits, pero la de 16 no se puede colocar en una de 8 bits. Es el standard de Arquitectura COMPAQ

2. EISA: (Extended Industry Standard Architecture) Es utilizada por AST, COMPAQ, EPSON, HEWLETT - PACKARD, NEC, OLIVETTI, TANDY WYSE, ZENITH. Es de 32 bits y es compatible con ISA y tiene características adicionales introducidas por IBM en su arquitectura microcanal.
3. MICROCHANEL: Es eléctrica y físicamente incompatible con el bus ISA, trabaja con un bus de 16 bits o 32 bits. Puede ser manejada independientemente por múltiples procesos.
4. PCI: (Peripheral Component Interconnect) Bus de 32 bits. Es plug and play, esto quiere decir que la configuración de la tarjeta no necesita interacción del usuario.

Cableado y conectores de red

La tarjeta adaptadora de red desarrolla tres importantes funciones en coordinación de actividades entre el computador y el cableado:

1. Hace la conexión física con el cable.
2. Genera las señales eléctricas que viajan por el cable.
3. Sigue las reglas específicas para controlar el acceso al cable.

Es común que la tarjeta tenga dos conectores. Estos se seleccionan por medio de configuración con Jumpers o Dip switches.

Una conexión de red Thinnet usa un conector BNC, una conexión Thicknet usa un 15- pin (AUI), por cable UTP usa el conector RJ-45 que tiene 8 conductos. Algunas topologías propietarias de par trenzado usan RJ-11.

Desempeño de Red

Si una tarjeta es lenta los datos no pueden ir rápidamente, se puede agilizar el desplazamiento de los datos en la tarjeta con:

DMA: (Direct Memory Acess) El computador mueve los datos directamente del buffer de la tarjeta a la memoria del computador, sin usar el microprocesador.

Adaptadores de memoria Compartida: La tarjeta adaptadora tiene RAM que comparte con el computador. Este identifica la RAM como si realmente estuviera instalada en el computador.

Sistema de memoria Compartida: El procesador de la tarjeta adaptadora de red selecciona una sección de la memoria de computador y la usa en el procesamiento de datos.

Bus Maestro: Se encarga de llevar los datos directamente a la CPU. No interviene el procesador del computador. Lo ofrecen EISA y Microchanel.

RAM Buffering: Los datos son guardados mientras la tarjeta los puede procesar.

Onboard Microprocessor: Con un procesador la tarjeta de red no necesita que el computador ayude en el procesamiento de datos.

Redes inalámbricas

Las redes inalámbricas no están totalmente libres de cables; se conocen como híbridos las redes que mezclan componentes inalámbricos y componentes de redes cableadas.

Estas pueden:

- Proveer conexiones existentes temporalmente.
- Ayudan a proveer copias (backup) de una red existente.
- Proveen cierto grado de portabilidad
- Extiende la red más allá de los límites de las redes de cobre o de fibra óptica.

Usos

Ya que su implementación es difícil se debe usar para:

- Gente en constante movimiento como médicos.
- Áreas aisladas
- Departamentos con cambios en las características físicas frecuentemente.
- Estructuras como edificios históricos

Tipos

Hay tres categorías:

1. LAN: Una red inalámbrica típica muestra y actúa igual que una red cableada excepto por el medio.
2. Puntos de acceso. El transceiver algunas veces es llamado punto de acceso(broad casts). Emite y recibe señales de los computadores que lo rodean y pasa datos entre la red inalámbrica y la red cableada.
3. La red inalámbrica LAN usa pequeños transceiver montados en la pared, para conectarse a la red inalámbrica los tansceiver establecen contactos radiales con componentes portátiles.

Técnicas de transmisión. Las LANs inalámbricas usan cuatro técnicas para transmitir:

- Infra rojo. Operan usando los pulsos infrarrojos que envían datos entre componentes. Tiene que generar señales fuertes para que no se interrumpan con la luz. Tiene un ancho de banda alto.

  Hay cuatro tipos de red infrarroja:

  1. Red en línea de vista: Transmite únicamente cuando tiene una línea clara entre el transmisor y el receptor.

  2. Red infrarroja dispersa: La transmisión rebota en paredes y techo hasta llegar al receptor. Esta es efectiva en áreas de aproximadamente 100 pies.

  3. Red reflectiva: Los transceivers son situados cerca del computador transmisor en dirección de una localización en común que redirecciona la transmisión hacia el computador apropiado.

  4. Telepoint Optical: Proviene del servicio banda ancha. Es capaz de manejar alta calidad de requerimientos multimedia que puedan provenir de redes cableadas.

  Con infrarrojo se dificultan las transmisiones en distancias mayores de 100 pies.

- Láser. Similar a infrarrojo en que requiere una línea directa de vista y cualquier persona o cosa que interrumpa el láser dañará la transmisión.

- Narrow band. Es similar a la transmisión de estación de radio. El usuario sintoniza la transmisión y la recepción en cierta frecuencia. No requiere línea de vista y tiene un rango de transmisión de 500 cuadras. Debido a que la señal es de alta frecuencia no traspasa muros de seguridad. Transmite a 4.8 Mbps.

- Spread-Spectrum. Transmite señales sobre rangos de frecuencia. Esto supera los problemas de banda estrecha. Las frecuencias disponibles son divididas en canales o saltos. Adapta tonos en un salto determinando Longitudes.

- Transmisión punto a punto. Es la transmisión de datos de un computador a otro para comunicarse entre varios computadores y periféricos. Puede ser implementado en computadores individuales o computadores de una red con transmisión inalámbrica de datos.

  Esta tecnología involucra transferencia inalámbricas serial de datos que:

  - Usa enlace de radio punto a punto rápida y libre de error en transmisión de datos.
  - La transmisión penetra paredes, techos y pisos.
  - Soporta tasas de transmisión entre 1.2 y 38.4 Kbps máximo 200 pies o una tercera parte de milla en línea de transmisión sin obstáculos.
  - Transmite entre computadores o entre computador y periférico, como impresoras o lectores de códigos de barras.

LAN EXTENDIDA: Algunos componentes inalámbricos son capaces de transmitir a distancias más amplias permitiendo conexión entre dos o más LAN.

Conectividad multipunto inalámbrico. El puente inalámbrico enlaza redes sin utilizar cables en una distancia de hasta 3 millas. AIRLAN/Bridge Plus usa Spread- Spectrum.

El costo de utilizar este componente está justificado porque elimina el gasto de líneas arrendadas.

Puentes inalámbricos de largo alcance. Utiliza tecnología Spread-Spectrum. Es compatible con redes Ethernet y Token Ring. Transmite a máximo 25 millas. Su costo se justifica con la eliminación de los enlaces T1 y los microondas.

COMPUTACIÓN MOVIL. Requiere de un teléfono portátil y una red de servicio público que transmita y reciba la señal. Puede ser:

Comunicación Packet-Radio. El sistema rompe la transmisión en paquetes. Incluye:

- Dirección fuente
- Dirección destino
- Información de corrección de errores.

Los paquetes son enlazados a un satélite que los emite. Unicamente los componentes con la dirección correcta los recibe.

Red Celular. (CDPD. Cellular Digital Packet Data) Utiliza la red análoga existente de voz para transmitir datos entre llamadas (voz) cuando el sistema no está ocupado, Es rápida pero se ve afectado por un retardo secundario que lo hace ligeramente más lenta que la transmisión en tiempo real.

Estación de Satélite. Las microondas son un buen método de comunicación en áreas pequeñas. Es una excelente forma de comunicación en :

- Satélites por enlaces terrestres.
- Comunicación entre edificios.
- A través de largas y planas áreas abiertas como cuerpos de agua o desiertos.

Un sistema microondas consiste de:

- Dos radio Transceiver, uno para enviar y otro para recibir.
- Dos antenas direccionales que captan la señal de los transceiver. Son instaladas en torres para levantar la señal sobre obstáculos que la bloqueen.

Los estándares inalámbricos como el de las LANs inalámbricas 802.11, el de DECT, y el de Hiperlan fijan unas bases necesarias para los servicios que trabajen en este ámbito. Las ventajas que proporciona el estándar 802.11 son la flexibilidad de los equipos, la robustez y el ahorro del cableado, pero tiene el inconveniente de la baja velocidad en que puede trabajar. Este inconveniente es solucionado en Hiperlan, ya que las características propias del sistema posibilitan velocidades de 20 Mbps.

Medio de transmisión

Por medio de transmisión se entiende el soporte físico utilizado para el envío de datos por la red. La mayor parte de las redes existentes en la actualidad utilizan como medio de transmisión cable coaxial, cable bifilar o par trenzado y el cable de fibra óptica. También se utiliza el medio inalámbrico que usa ondas de radio, microondas o infrarrojos, estos medios son más lentos que el cable o la fibra óptica.

Cualquier medio físico o no, que pueda transportar información en forma de señales electromagnéticas se puede utilizar en redes locales como medio de transmisión.

Las líneas de transmisión son la espina dorsal de la red, por ellas se transmite la información entre los distintos nodos. Para efectuar la transmisión de la información se utilizan varias técnicas, pero las más comunes son: la banda base y la banda ancha.

Los diferentes tipos de red: EtherNet, TokenRing, FDDI, etc. pueden utilizar distintos tipos de cable y protocolos de comunicación.

Técnicas De Transmisión

Hay dos técnicas de transmisión de datos:

1. **Banda Base** :Usa señales digitales a través de una sola frecuencia. La señal fluye en forma de pulsos discretos de electricidad o de luz. Todo el canal se usa con la transmisión de una sola señal. El ancho de banda es la diferencia entre la frecuencia más alta y la más baja soportadas por un cable. Algunos cables transmiten y reciben datos al mismo tiempo. A lo largo del cable de la red, el nivel de la señal decrece y se distorsiona, por seguridad, el sistema de banda base utiliza repetidores para que la señal llegue con la intensidad original.

2. **Banda ancha**: Usa señales análogas y un rango de frecuencia. La señal es continua, esta fluye en forma de onda electromagnética u óptica. La transmisión es unidireccional, si se dispone de suficiente ancho de banda se podrían hacer varias transmisiones al mismo tiempo. Usan amplificadores para regenerar la señal. Se necesita una ruta para transmitir y otra para recibir datos. Hay dos formas de hacer esto:

    1. Mid-split : Divide el canal en dos rangos de frecuencia, un canal es usado para transmitir y el otro para recibir.
    2. Dual-cable: Se utilizan dos cables diferentes, uno para transmitir y el otro para recibir información. Esta forma es mucho más cara que la Mid-split.

Tipos De Cable

La red de área local necesita un cableado que enlace a sus estaciones de trabajo individuales con el servidor y otros periféricos. Si solo se dispusiera de un tipo de cableado la elección sería

sencilla, pero hay varios tipos de cableado. Se va a examinar las ventajas y desventajas de cada tipo.

- **Cable de par no trenzado**

Es el medio más sencillo para establecer comunicación. Cada conductor está aislado del otro; la señal de voltaje o corriente se aplica a uno de ellos y la referencia o tierra al otro. Es muy utilizado en telefonía, pero su aplicación en transmisión de datos está limitada a la conexión de equipos entre distancias no mayores a 50 metros, con velocidades inferiores a los 19.2 Kbps.

Esta clase de cable se utiliza sobre todo para conectar computadores a equipos cercanos como impresoras o módem. Por lo general, estas conexiones necesitan múltiples líneas, por lo tanto, se debe utilizar cable multipar o cable plano (ribbon). Cuando se utiliza cable multipar hay problemas con la integridad de la información a causa del acople de señal entre los distintos conductores. Además, por la estructura abierta de cada par, es muy frecuente la captación de interferencia electromagnética. Como en el lado de la recepción se espera la señal que hay entre cada conductor y tierra, cualquier ruido extra, en un conductor, altera por completo la información que lleva.

- **Cable de par trenzado**

Es él más barato de todos los tipos de medios de transmisión. Consiste en dos conductores aislados trenzados entre sí de modo que cada uno este expuesto a la misma cantidad de "ruido" de interferencia procedente del entorno que el otro. Al trenzar los hilos el ruido se reduce, pero no se elimina.

Los conductores tienen un número de calibre, para los usos en redes, los cables de calibres 22 y 24 son los más comunes. Entre más pequeño sea el diámetro del hilo, mayor será la resistencia para la propagación de la señal. Un hilo largo con una gran sección transversal (cross-sectional) incrementa la intensidad de la señal.

Hay 2 tipos de cables de par trenzado:

1. **No blindado (UTP):** Se usa en la especificación 10 BASET. Es el tipo de cable más usado en la red LAN. La máxima longitud de un segmento es 100mtrs (328 pies).
   Hay 5 categorías de UTP:

   - **Categoría 1** transmisión de voz pero no datos. (cable para la red telefónica)
   - **Categoría 2** Para transmisión de datos. Su velocidad de transmisión es de 4mbps y tiene 4 pares trenzados
   - **Categoría 3** Transmisión de datos hasta una velocidad de 10mbps. Tiene 4 pares con 3 trenzas por pie.
   - **Categoría 4** Transmisión de datos a una velocidad de 16mbps tiene 4 pares trenzados.
   - **Categoría 5** Transmisión de datos a una velocidad de 100mbps tiene 4 pares trenzados.

   El cable UTP es susceptible al *crosstalk.*

2. **Blindado (STP):** Es menos susceptible a la interferencia puede transmitir datos a mayor distancia. Tiene una cubierta en cinta metálica que lo aísla.

Los conectores utilizados para este cable son del tipo de los enchufes telefónicos. Las redes ocasionalmente usan los conectores RJ-11, que pueden conectarse con 2 o 4 cables. Sin embargo, estos también se emplean para las instalaciones telefónicas y resulta inconvenientes en una red, ya que conectar una tarjeta de red en un enchufe telefónico puede dañar tanto a la tarjeta como al computador. Los conectores RJ-45 son versiones más grandes del mismo diseño y tienen 8 conexiones de cable.

También se utilizan los conectores tipo DB que se pueden encontrar en las conexiones de instrumentos seriales como las impresoras. Hay tres tipos de conectores DB, DB-9 con 9 pines, DB-15 con 15 pines y DB-25 con 25 pines.

Este cable es ideal para las redes de bajo nivel, se utiliza en topologías estrella, dado su carácter flexible. La distancia de la transmisión obtenida depende del calibre, la condición de la línea, el ambiente de operación y la velocidad de la transmisión.

Las principales limitaciones del cableado con par trenzado son su falta de velocidad y su limitado alcance. Puede manejar flujos de datos de aproximadamente 1 Mbps sobre distancias de algunos metros.

Se debe tener en cuenta que:

- La longitud máxima de cable UTP entre nodos y Hubs es de 100 metros.
- Las patas 1,2,3 y 6 del conector RJ-45 son conectadas de manera directa. Las patas 1 y 2 son transmisoras y las 3 y 6 son receptoras.
- Se pueden conectar hasta 12 Hubs a un Hub central.
- Sin el uso de puentes, el cable UTP puede acomodar un máximo de 1024 estaciones de trabajo.

Consideraciones.

- Puede utilizarse cuando:
  - Tiene restricciones de presupuesto para la LAN.
  - Se quiere una instalación relativamente fácil con conexiones simples.
- No utilizar par trenzado si se quiere estar seguro de la integridad de los datos, de transmisiones a grandes velocidades y a grandes distancias.

- IBM soporta para su red Token-Ring el cable telefónico de par trenzado y sin blindar tipo 3 pero de calibre 22 o 24 y con un mínimo de 2 vueltas por cada pie. Mínimo debe tener 4 pares y 2 pares de reserva para la Token Ring.

- La red AT&T exige 2 pares de hilos trenzados de calibre 24 con blindaje, un par para la transmisión de datos y otro para la recepción.

Cable coaxial

Existe desde 1940. Es casi tan fácil de instalar como el par trenzado pero es más resistente a la interferencia y atenuación. Es relativamente económico, liviano, flexible, fácil de trabajar y es seguro. Está formado por un conductor de cobre rodeado de un aislante que generalmente es un tipo de plástico flexible llamado PVC. Los cables que pasen por los *plenum* (pequeños espacios entre techos, paredes y pisos falsos de los verdaderos) no pueden producir gases tóxicos, por esta razón deben tener materiales especiales, que son más costosos y menos flexibles que el PVC. La camisa exterior de cobre o aluminio actúa como conductor y también proporciona protección.

Este cable fácilmente soporta velocidades de hasta 10 Mbps y con conectores especiales es posible alcanzar frecuencias de señal de hasta 100 Mbps.

Hay dos clases de cable coaxial:

Coaxial delgado (Thinnet): Tiene un grosor de 0.25 pulgada. Es de la familia RG-58. Tiene 50 ohm de impedancia. Consiste en un conductor interno rodeado por un aislante dieléctrico, un blindaje de hoja de metal, un conductor tejido y una cubierta exterior protectora. Es flexible y fácil de trabajar. Va conectado directamente a la tarjeta de red. Transmite bien hasta 185 metros, luego sufre atenuaciones. A una red construida con cable delgado se le aplica la nomenclatura 10BASE2: 10Mbps, banda base, máxima longitud de 200mts.

Las reglas para la instalación y la configuración de segmentos de cable coaxial delgado son:

- La longitud máxima de segmento debe ser 185mts.
- Cada segmento de red debe tener una terminación de 50 ohm en cada extremo.
- No puede conectarse en serie más de 5 segmentos de red y solo 3 pueden estar ocupados.
- La cantidad máxima de nodos por segmento es de 30.
- La distancia mínima de cable entre adaptadores de red es de 0.5 mts.
- La cantidad máxima de nodos en una red es de 1024.
- La distancia máxima entre 2 nodos es de 1425 mts.

Coaxial grueso (Thicknet): Relativamente rígido, lo cual le impide hacer recorridos difíciles. Tiene 0.5 pulgadas de diámetro. El conductor central esta rodeado por un aislante dieléctrico al que, a su vez lo rodea un blindaje de hoja de metal que también esta cubierto por un conductor tejido. La parte externa del cable tiene una cubierta protectora. Es utilizado para conectar varias redes pequeñas en thinnet. A una red construida con cable grueso se utiliza la nomenclatura 10BASE5: 10Mbps, banda base, máxima longitud de 500 mts.

- Las reglas para la instalación y la configuración de segmentos de cable coaxial grueso son:
- La longitud máxima de segmento de red es de 500mts.
- Cada segmento de red debe tener una terminación de 50 ohms en cada extremo.
- No puede conectarse en serie más de 5 segmentos de red y solo tres de estos pueden estar ocupados. (Tener nodos conectados a ellos).
- La cantidad máxima de transceivers por segmento es de 100.
- La cantidad máxima de nodos en una red es de 1024.
- Los transceivers no pueden instalarse a menos de 2.5mts.
- Los cables de bajada no pueden ser más largos de 50 mts.
- La distancia máxima entre dos estaciones cualquiera es de 3000 mts.

El BNC (British Naval Conector) también llamado conector de bayoneta, es un conector utilizado para este tipo de cable, es soldado al final del cable. El BNCT une el cable a la tarjeta o es utilizado para lograr una conexión de 3 vías: 2 conexiones para proporcionar un flujo recto para la red y otro para la tarjeta adaptadora de red. Para realizar una extensión, se unen 2 cables por medio de un conector BNC y el terminador BNC cierra el final de un cable de bus.

El cable coaxial en banda base tiene un solo canal que transporta en cada momento un solo mensaje a una velocidad muy elevada. Su conductor portador va rodeado por una malla de cobre y el diámetro total del cable suele ser aproximadamente 9.5 mm. La información digital se transmite en serie de bit en bit ocupando el ancho de banda del cable. Dependiendo de la LAN, el cable coaxial en banda base pude manejar un régimen de datos de 10 Mbps.

A causa de la limitación de un canal único no es posible transmitir por cables de banda base señales integradas compuestas por voz, datos e incluso vídeo. Una ventaja es su facilidad de conexión y el hecho de que la conexión y desconexión de estaciones de trabajo no perturba el funcionamiento de la red. Aunque la distancia máxima recomendada para una LAN en banda base es aproximadamente 3 Km, si se hace uso intensivo de la red parece más realista una cifra aproximada a 500 mts. Las redes en banda base tienen una buena velocidad de datos.

Ethernet, con interfaces y protocolos de comunicaciones no propietaria, usa cable coaxial de banda base.

En una configuración de banda ancha de cable doble, el cable coaxial forma una especie de autovía de doble dirección, constituida por 2 bandas, cada una de las cuales contiene varios canales.

Consideraciones

- Puede transmitir voz, vídeo y datos.
- Se utilizan para transmisiones de larga distancia a menor costo.
- Su tecnología es familiar y ofrece seguridad de datos.
- En lugares húmedos se debe utilizar cables especiales, debido a que si la humedad penetra causará ruido y toda clase de problemas difíciles de solucionar.
- Si se tocan la malla y el núcleo habrá corto. El ruido de la malla afectará el flujo del cable de cobre y se destruirán los datos.

Fibra óptica

La fibra óptica proporciona un método excepcionalmente atractivo para transmitir datos y señales de todo tipo con un mínimo de perdidas y libres de ruido. Actualmente los productos de fibra óptica (cables, conectores, transceivers, etc.), ocupan un lugar común en la arena de las telecomunicaciones, las redes de transmisión de datos, la televisión por cable, los sistemas de control, los equipos militares y otras aplicaciones. Además las cifras revelan que la fibra óptica es un mercado muy rentable.

Una sola fibra de vidrio, del espesor de un cabello humano, puede transportar mas información que varios miles de pares telefónicos o de cables coaxiales, con un mínimo de perdidas. Adicionalmente, los cables de fibra óptica son livianos, seguros, estéticos y resistentes, pueden transmitir anchos de banda de varios gigahertz sobre distancias de cientos de kilómetros sin necesidad de repetidoras, no pueden ser interceptados por métodos corrientes, son inmunes a la Interferencia Electromagnética (EMI), las radiaciones nucleares y a otras formas de interferencia, no generan calor ni campos magnéticos, pueden transportar señales entre dispositivos con tierras separadas o conectados a voltajes diferentes, no pueden ser cortocircuitados, no transportan corrientes letales, ahorran espacio, pueden viajar a líneas paralelas de distribución de potencia, entre otras.

El cable esta formado por vidrio puro estirado hasta formar fibras muy gruesas para constituir el núcleo, medio físico de transporte de la información que es convertida por un transmisor en energía luminosa modulada. Con el fin de evitar las perdidas de luz por radiación, el núcleo va rodeado por un recubrimiento (cladding), es decir, una capa de vidrio con un índice refractivo menor que el que constituye el núcleo, este también puede ser de plástico. El filamento de vidrio esta rodeado por un amortiguador, este a su vez por kevlar (un material sintético mas duro que el acero) para una protección mayor. La cubierta protectora exterior esta compuesta por PVC o poliuretano negro la cual tiene como función principal proporcionar protección mecánica a la fibra o fibras del cable.

Dependiendo de su configuración óptica puede ser de construcción holgada o de construcción ajustada. En un cable de construcción holgada, las fibras no están en contacto directo con la estructura de PVC del cable, sino suspendidas en un relleno de gel que las protege de la humedad y las aísla de las fuerzas axiales y transversales externas a las que el cable podría estar eventualmente sometido. Debido a su robustez, este tipo de cables se destina para exteriores y tendidos telefónicos de larga distancia. No obstante, la presencia del relleno de gel crea algunos inconvenientes de instalación y mantenimiento. En el cable de construcción ajustada, las fibras están directa y continuamente en contacto con la estructura del cable, aunque protegidas por una cubierta plástica o de Klevar y elementos de amortiguamiento que las protegen del riesgo de avería ocasionado por fuerzas axiales y transversales ejercidas sobre el cableado. Son más flexibles y livianos que los de construcción holgada, sustituyéndolos en muchos casos. Se utilizan principalmente para usos militares tácticos y aplicaciones de cortas distancias, incluyendo redes de área local (LAN) y enlaces punto a punto entre ciudades, edificios, fabricas, etc.

Para poder usar cable de fibra óptica los PC, las compuertas y otros instrumentos que se conecten directamente a la fibra deben ser compatibles con este sistema o conectarse a través de un instrumento llamado controlador de fibra de vidrio que convierte las señales eléctricas en pulsos de luz y viceversa.

La fibra óptica tiene un ancho de banda muy grande, es muy delgada y ligera de peso; no le afecta la interferencia electromagnética procedente de la maquinaria pesada, (que esto es muy importante cuando el cable se tiende a través del hueco del ascensor), los sobrevoltajes en la líneas o bien los originados por descargas eléctricas, y gozan de una excelente seguridad.

En una red de fibra óptica se emplea un láser o diodo luminiscente (Light Emitting Decode o LED) para enviar una señal a lo largo del núcleo del cable. Frecuentemente se utilizan repetidores ópticos a lo largo del circuito para amplificar la señal, de manera que llegue a su destino con toda su intensidad. En el extremo de recepción del cable, el mensaje se convierte de nuevo en una señal digital o analógica por medio de un fotodiodo. Por el cable puede ir una sola señal (monomodo) o pueden ir varias (multimodo). Pueden ser de índice gradual en el cual el índice de refracción disminuye lentamente desde el centro de fibra hacia su porción exterior, o ser de salto de índice en

el cual el índice de refracción varia bruscamente. La fibra monomodo tiene un ancho de banda muy grande pero el resumido diámetro de su núcleo hace que sus empalmes sean extremadamente difíciles. Por otra parte el monomodo exige el uso como fuente luminosa de un láser, mucho mas caro que un LED. Las fibras multimodo tienen un ancho de banda menor pero su empalme es mucho más fácil. Las frecuencias modulares de índice gradual son el medio de transmisión mas caro, pero son los que proporcionan la máxima velocidad y distancia de transmisión.

Las fibras multimodo para cableado de redes vienen en grupos que van desde 2 a 24 fibras, siendo la norma los grupos de 2 a 4 fibras. Cada fibra es unidireccional, puesto que se transmite un haz de luz en una sola dirección, la comunicación en dos sentidos exige que en el cable haya otra fibra para que la luz pueda viajar en dirección opuesta.

En el cable multimodo la señal se desvanece mas a través de una distancia dada que en un cable de monomodo. Este desvanecimiento es un fenómeno llamado atenuación.

La variedad mas nueva de cables de fibra óptica usa una fibra plástica más barata y fácil de manejar pero atenúa mas la señal que la fibra de vidrio.

El Instituto Nacional Americano de Estandarización (ANSI) estableció una norma para que el nivel dependiente del medio físico (PMD) del interface distribuido de datos de la fibra (FDDI) trabaje en conjunción con una transmisión de datos de 100Mbps.

Un sistema en fibra óptica se compone básicamente de un transmisor o fuente de luz, un receptor o detector, el cable de fibra óptica propiamente dicho, una o más estaciones repetidoras y los elementos de interconexión correspondientes (conectores, empalmes, acopladores, etc.) Una vez modulada por el transmisor, la información viaja a través de la fibra en forma de energía luminosa y es desmodulada en el receptor.

Ventajas:

- Insensibilidad a al interferencia electromagnética, como ocurre cuando un alambre telefónico pierde parte de su señal a otro.
- Las fibras no pierden luz, por lo que la transmisión es también segura y no puede ser perturbada.
- Carencia de señales eléctricas en la fibra, por lo que no pueden dar sacudidas ni otros peligros. Son convenientes por lo tanto para trabajar en ambientes explosivos.
- Liviandad y reducido tamaño del cable capaz de llevar un gran número de señales.
- Sin puesta a tierra de señales, como ocurre con alambres de cobre que quedan en contacto con ambientes metálicos.
- Compatibilidad con la tecnología digital.

Desventajas :

- El costo
- Fragilidad de las fibras
- Disponibilidad limitada de conectores.
- Dificultad de reparar un cable de fibras roto en el campo.

Redes en fibra óptica:

- FDDI (Interface de Datos Distribuidos para fibras) paso testigo en anillo.
- S/NET Estrella activa para su conmutación.
- FASNET Red de alto rendimiento. Utiliza dos buses lineales unidireccionales.
- EXPRESSNET Es similar a FASNET pero en lugar de utilizar dos buses, esta emplea solamente un bus plegado

Consideraciones

- Se utiliza cuando necesita transmitir a grandes velocidades y a grandes distancias en un medio seguro.

No la use sí:

- tiene presupuesto bajo
- No tiene un experto para instalarla apropiadamente.

Capacidad del medio

Ancho de banda

El método de transmisión esta directamente relacionado a la capacidad del medio para transmitir información. El ancho de banda nos indica la capacidad máxima del medio.

Ancho de banda: es la diferencia entre la frecuencia más alta y más baja de una determinada onda. El término ancho de banda hace referencia a la capacidad del medio de transmisión, cuanto mayor es el ancho de banda, más rápida es la transferencia de datos.

Por encima del ancho de banda las señales crean una perturbación en el medio que interfiere con las señales sucesivas. En función de la capacidad del medio, se habla de transmisión en banda base o transmisión en banda ancha.

Banda base

Las redes en banda base generalmente trabajan con mayor velocidad de transmisión que las redes de banda ancha, aunque la capacidad de estas últimas de transmitir por varios canales simultáneamente pueden hacer que el flujo total de datos sea prácticamente el mismo en ambos sistemas.

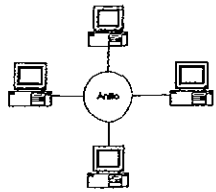
La transmisión de banda base utiliza señales digitales sobre una frecuencia. Utiliza toda la capacidad del canal de comunicaciones para transmitir una única señal de datos.

Topologías de redes:

Según la topología, o forma lógica, las redes pueden ser en:

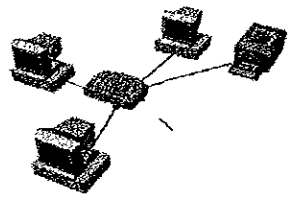
Anillo

- *Anillo:* Es una de las tres principales topologías de red. Las estaciones están unidas una con otra formando un círculo por medio de un cable común. Las señales circulan en un solo sentido alrededor del círculo, regenerándose en cada nodo.



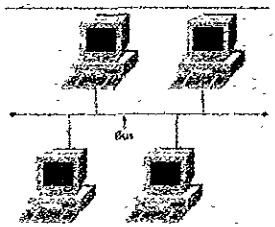
Estrella

- *Estrella:* Es otra de las tres principales topologías. La red se une en un único punto, normalmente con control centralizado, como un concentrador de cableado.



Bus

- *Bus:* Es la tercera de las topologías principales. Las estaciones están conectadas por un único segmento de cable. A diferencia del anillo, el bus es pasivo, no se produce regeneración de las señales en cada nodo.



Combinadas:

Cuando se estudia la red desde el punto de vista puramente físico aparecen las topologías combinadas.

1. *Anillo en estrella:* Esta topología se utiliza con el fin de facilitar la administración de la red. Físicamente, la red es una estrella centralizada en un concentrador, mientras que a nivel lógico, la red es un anillo.
2. *Bus en estrella:* El fin es igual a la topología anterior. En este caso, la red es un bus que se cablea físicamente como una estrella por medio de concentradores.

3. Estrella jerárquica: Esta estructura de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada para formar una red jerárquica.

Transmisión De Información En La Red

Para garantizar que los computadores conectados en la red puedan comunicarse sin problemas, deben cumplir una serie de normas que se conocen generalmente con el nombre de protocolo.

Tecnologias Clasicas

Redes Ethernet

En 1973, Robert Metcalfe escribió una tesis para obtener el grado de PhD en el Instituto Tecnológico de Massachusets - USA en la que escribió la investigación que realizó acerca de las LAN. Posteriormente se trasladó a la compañía Xerox, donde formó un equipo de trabajo para desarrollar la red ETHERNET, basada en las ideas contenidas en su tesis.

Las redes ETHERNET pertenecen a la categoría de redes LAN, por eso es muy frecuente encontrarlas en oficinas, fábricas, entidades oficiales, universidades etc.

La ETHERNET desarrollada por Xerox tuvo tanto éxito que las compañías Xerox, DEC (Digital Equipment Corporation) e Intel propusieron a la IEEE una norma para la ETHERNET de 10 mbps. Esta norma fue la base para la hoy conocida IEEE 802.3,que aunque difiere un poco de su especificación inicial, conserva muchas características originales.

Este sistema se llamó ETHERNET, en honor al éter luminífero, a través del cual se pensó alguna vez que se propagaban las ondas electromagnéticas.

Topología

Existen dos opciones para implementar una red ETHERNET. La primera consiste en conectar todos los computadores sobre el cable de la red directamente (topología bus). La segunda consiste en utilizar un hub o concentrador, en el cual se conecta cada uno de los cables de red de los computadores.

Tarjeta de red ETHERNET

Cada computador debe tener instalada una tarjeta de red, la cual incorpora los conectores necesarios para que el usuario pueda conectarse al canal. Existen tarjetas ETHERNET de uno o varios conectores. (figura revista N35 pag 47).

Esta tarjeta se debe introducir en el interior del computador. Posee un microprocesador que se encarga de controlar todos los aspectos relacionados con la comunicación y otros como el empaquetamiento y desempaquetamiento de la información que se transmite y recibe, la codificación y decodificación, detección de errores, y en general todas las tareas necesarias para que el computador solamente se preocupe por entregarle la información que se desea transmitir y viceversa.

Cables y conectores que se utilizan

En este tipo de redes se pueden utilizar el cable coaxial, cable UTP y fibra óptica.

El cable coaxial se utiliza sobre todo en la configuración tipo bus, banda base. De esta forma el canal actúa como un mecanismo de transporte, a través del cual se propagan los pulsos digitales de voltaje.

Se utilizan dos tipos de cable coaxial: cable delgado (thin wire) de 0.25 pulgadas de diámetro y cable grueso (thick wire) de 0.5 pulgadas. Por lo general los dos pueden operar a la misma velocidad, 10 Mbps, porque en el cable delgado se presenta una mayor atenuación. La máxima distancia en que se puede transmitir sin necesidad de amplificadores o repetidores es de 200 metros para cable delgado y 500 para el grueso.

Transmisión de información

La red ETHERNET utiliza un protocolo llamado CSMA/CD (Carrier Detect), que quiere decir Acceso múltiple por detección de portadora con detección de colisión.

Como todos los computadores están conectados sobre el mismo bus, se dice que el cable opera en acceso múltiple. Esto significa que cuando un computador quiere mandar información hacia otro computador, debe colocar en el cable todo el paquete de información a ser transmitido. Dicho paquete incluye los datos sobre que usuario los envía y que usuario los recibe, además de la información en sí.

Antes de iniciar, el equipo que va a transmitir debe "escuchar" el canal para saber que está libre (CS, detección de portadora). En caso de estar ocupado, debe esperar un tiempo y volver a intentarlo nuevamente. En caso de estar libre, puede empezar a transmitir los datos correspondientes.

Como se puede deducir, si dos computadores "escuchan" el canal al mismo tiempo y éste se encuentra desocupado, empezarán a transmitir sus datos sobre el canal, lo que generará lo que se conoce como colisión de información. En este caso los computadores se retiran por un tiempo y luego cada uno intenta nuevamente hacer su transmisión. Además los computadores que colisionaron colocan una señal en el cable de red que indica que se presentó un choque de datos o información.

Esta es una característica muy importante de este tipo de red, ya que cada computador se retira del canal y no intenta por el contrario, seguir con su transmisión, lo que contribuye notablemente a reducir el tiempo de fallas en la línea. Las tarjetas de red y los transceiver tienen un circuito electrónico que se encarga de realizar las funciones que permiten "escuchar" el canal y detectar las colisiones.

Formato de la información

Los paquetes de información (también conocidos como tramas) que envía cada computador por la red debe tener un formato específico y cumplir unas normas establecidas, para que sean comprendidas por todos los usuarios de la red. Esas normas cobijan aspectos como la longitud de los paquetes, polaridad o voltaje de los bits, códigos para detección de errores, etc.

Cada trama empieza con un preámbulo de 7 bytes iguales (10101010). Esto genera una onda cuadrada de 10 MHz, durante un tiempo de 5.6μs, con el objeto de que el receptor se sincronice con el reloj del transmisor. Después viene un byte llamado inicio de trama (10101011), con el fin de marcar el comienzo de la información propiamente dicha.

Los bytes correspondientes a la dirección de destino y de origen se utilizan para saber a quien va el mensaje y quien lo envía. Además, existe un carácter especial que puede indicar que el mensaje va dirigido a un grupo de usuarios o a todos los usuarios. El byte que indica la longitud del campo de datos indica al receptor cuantos bytes de información útil o verdadera debe esperar a continuación. Los datos corresponden al archivo en particular que se está enviando.

Los bytes de relleno se emplean para garantizar que la trama total tenga una longitud mínima de 64 bytes (sin contar el preámbulo ni el inicio de la trama), en caso de que el archivo de datos sea muy corto. Esto se hace con el fin de desechar las tramas muy cortas (menores de 64 bytes) que puedan aparecer en el cable de la red, como consecuencia de transmisiones abortadas por colisiones. El código de redundancia sirve para hacer detección de errores. Si algunos bits de datos llegan al receptor erróneamente (por causa del ruido), es casi seguro que el código de redundancia será incorrecto y, por lo tanto, el error será detectado.

Codificación de los bits. Aunque los bits de información que entrega la tarjeta de red al cable se podrían entregar en forma directa (por ejemplo: 1 voltio para un 1 lógico y 0 voltios para un 0 lógico), esto no le permitiría al receptor saber en que momento empieza cada uno. Además, la potencia que se pierde en el cable sería muy elevada. Por esto, la red utiliza una técnica denominada codificación Manchester, que consiste en asignar dos intervalos de tiempo iguales para cada bit.

Para representar un uno lógico se tiene que la primera mitad del bit está en nivel alto y la segunda mitad en nivel bajo. Para representar un 0 lógico, el primer intervalo está en nivel bajo y el

segundo en nivel alto. Con este esquema se garantiza que cada bit tenga una transición en la parte media, propiciando así un excelente sincronismo entre el transmisor y el receptor.

Redes Token Ring

Fue desarrollada por IBM y adoptada por IEEE como estándar IEEE 802.5 en 1986.

Hay tarjetas compatibles de General Instruments, Proteon, 3Com y Ungermann-Bass.

Por definición un "token - ring" consiste en un conjunto de estaciones conectadas en cascada formando un anillo (ring) en el que la información es transferida de una estación activa a la siguiente. Cada estación recibe y regenera los bits que recibe, de forma tal que actúa como repetidor cuando está activa. Cuando la información vuelve a la estación que originó la transmisión, el mensaje es retirado de circulación.

La velocidad de transmisión original era de 4 MBit/s, pero hay versiones de 16 Mbit/s. La codificación es Manchester diferencial. Cuando se desea armar una red Token Ring, lo intuitivo sería pensar en un bus unido por sus extremos. Sin embargo, la topología que aparenta esta red es la de una estrella (se la suele describir como "star - wired ring"). Esto se debe a que el anillo está contenido en un dispositivo denominado Multistation Access Unit (MAU).

Las máquinas se conectan a los pines 1 al 8 del MAU mediante adaptadores (el conector incluído en la tarjeta es distinto al del MAU). Si la red tiene más de 8 puestos, se forma un anillo de MAU conectando la salida de uno (Ring Output, RO) con la entrada del siguiente (Ring Input, RI).

Hay dos formas de cablear el sistema: "small movable cabling system" y "large nonmovable cabling system".En el primer caso, se tienen los siguientes límites:

- Hasta 96 estaciones.
- Hasta 12 unidades MAU.
- Distancia máxima entre el MAU y una estación: 45,7 m (150 pies) , a los que hay que sumarle 2.4m (8 pies) del adaptador.
- Distancia máxima entre dos MAU: 45.7 m (150 pies).
- No pasar el cable por exteriores ni por conductos de ventilación, no exponerlos a más de 75 grados Celsius, ni a interferencia eléctrica.

En el segundo caso, se pueden conectar hasta 260 estaciones y 33 MAU, pero se usa un montaje físico diferente.

La transmisión se efectúa mediante dos pares trenzados, pero hay de diversas clases, definidas por IBM con números de tipo. El tipo 1 posee 2 pares AWG 22 con blindaje. Se usa principalmente para conectar MAUs. El tipo 2 ofrece 2 pares AWG 22 blindados y 4 pares AWG 26 sin blindaje; los pares extras son para conectar el teléfono con el mismo cable. El tipo 3 es de 2 pares tipo telefónico sin blindar. Es una alternativa barata al tipo 1. La ventaja de usar cable tipo 3 es que en muchas empresas donde hay centrales telefónicas internas, quedan pares disponibles, por lo que no hay que hacer un nuevo tendido; la desventaja es que se limitan el alcance y la cantidad de dispositivos que se pueden soportar (72 en vez de 255). El tipo 6 consta de 2 pares de cables (no alambres) de AWG 26 sin blindaje; es flexible y se usa para los alargues entre el cable adaptador y el MAU. El cable 9 consta de dos pares de AWG 26 blindados. Tiene menor alcance que el tipo 1 (aprox. 66%) pero es más barato. Todos los cables mencionados hasta acá soportan 16 Mbit/s excepto el 3 que llega sólo a 4 Mbit/s.

Por último, el tipo 9 no es un cable sino una fibra óptica. Soporta hasta 250 Mbit/s.

Para ampliar el anillo, se puede usar el 8218 Token - Ring Copper Repeater (repetidor de cobre), llevándolo a 775 m. Otra alternativa es emplear el Token - Ring Network Optical Fiber Repeater (para fibras ópticas), que posibilita enlaces de hasta 2 km.

Hay dos modelos básicos de tarjetas: la Token Ring PC Adapter (para PC, XT, AT, y compatibles) y la Token Ring Adapter/A (TRN/A, para PS/2 Model 50 y superiores).

La diferencia entre ambas es, fundamentalmente, que la primera se conecta en un mainboard con bus tipo XT, mientras que la segunda es para un bus MCA (microchannel).

La dirección de base en el mapa de I/O es A20h (default); se puede escoger IRQ 2, 3 ó 7 (la 7 se superpone con la primera impresora). Un detalle a tener muy en cuenta es que la Token Ring PC Adapter decodifica 12 bits en I/O y no 10 (como es usual en PC).

Redes Arcnet

Fue desarrollada por Datapoint e introducida en 1977. Su nombre es la abreviación de Attached Resource Computing network. Es conocida como un arreglo de redes estrella, es decir una serie de redes estrella se comunican entre sí.

ARCNET se introdujo al mercado de redes como la solución a los problemas presentados por la red tipo estrella, como son la limitación de estaciones de trabajo, separación entre las estaciones de trabajo y el servidor, etc.

ARCNET tiene la facilidad de instalar estaciones de trabajo sin preocuparnos por la degradación de la velocidad del sistema, ya que para tal caso se cuenta con más de un servidor de red.

La no participación en el comité IEEE 802 dio lugar a que ninguna norma 802 la tenga en cuenta. Sin embargo, cuatro factores contribuyeron a hacerla tan popular que es un estándar:

1. A partir de 1982, se comenzaron a vender los chips, por lo que aparecieron "segundas fuentes" de esta tarjeta (Davong, Nestar, Standard Microsystems, Tiara y Waterloo entre otros).
2. El precio es bastante inferior a Ethernet y Token Ring.
3. Es muy confiable
4. En muchos lugares de EEUU había cableados con coaxial de 93 ohm en estrella, provenientes de hosts con terminales IBM 3270. ARCnet permite que al reemplazar las terminales por computadoras el cableado se aproveche.

En su versión original, es una red con topología tipo estrella, con protocolo de pasaje de "token", que trabaja en banda base y es capaz de transmitir a 2,5 MBit/s.

Con las tarjetas de interface es posible instalar hasta 128 estaciones de trabajo por cada servidor que se conecte a la red.

Cada una de las estaciones de trabajo puede estar conectada a una distancia máxima de 1200 metros con respecto al servidor de la red, esta distancia equivale a casi el triple de la permitida por la red tipo estrella.

El cable para esta conexión es mucho más caro porque se trata de un RG-62 coaxial que es usado no sólo para conectar esta red entre sí, también utilizado por IBM para la conexión de sus

computadoras 3270, esta es otra ventaja, ya que si se cuenta con una instalación de este tipo se puede aprovechar para instalar una red Novell ARCNET.

Una de las grandes ventajas de Novell es el uso de dos tipos de repetidores, el activo y el pasivo, ambas unidades sirven para distribuir la señal de la red entera, de tal forma que una señal determinada llega fácilmente a una estación de trabajo en particular.

Los pasivos consisten en una caja con 4 entradas vinculadas mediante resistores, de valor tal que si tres entradas cualesquiera están terminadas en su impedancia característica, la impedancia vista desde la otra entrada también sea la característica. Esta conexión permite adaptar impedancias y evitar reflexiones, pero a costa de una atenuación alta.

Justamente la atenuación limita la distancia máxima entre cada máquina y el hub a 30 m. Un hub activo, aparte de los resistores de terminación, tiene amplificadores, por lo que se pueden conectar máquinas hasta a 600 m del hub.

Los hubs activos pueden ser internos (generalmente de 4 bocas) o externos (generalmente de 8). Es posible conectar un hub a otro pero se deben respetar estas reglas:

No se pueden conectar hubs pasivos entre sí.

Cualquier entrada no usada en un hub pasivo debe llevar un terminador de 93 ohm.

Ningún cable conectado a un hub pasivo puede tener más de 30 m.

Un hub activo puede estar conectado a una máquina, a otro hub activo o a uno pasivo.

Las bocas no usadas en un hub activo no necesitan terminador, pero es conveniente usarlo.

Tanto los enlaces entre dos hubs activos como los efectuados entre hubs activos y máquinas pueden ser de hasta 600 m.

Ninguna máquina puede estar a más de 6.000 m (20.000 pies) de otra.

No crear ningún lazo.

Para efectuar pruebas entre dos máquinas, no es necesario un hub, se las puede conectar directamente pues las tarjetas poseen terminadores internos.

En la actualidad se la puede considerar obsoleta.

Red Arcnet En Topología Estrella

Existen versiones de ARCnet para topología bus y para transmisión por par trenzado, pero no se popularizaron. También se desarrolló una versión denominada "plus" de mayor velocidad de transmisión pero hasta el momento su penetración en el mercado es casi nula.

El chip de control de comunicaciones maneja un buffer de 2 KB .

Como ARCnet trabaja con paquetes de longitud fija (508 bytes) y NetWare también (pero de 560 bytes), se requiere transferir dos paquetes ARCnet para transferir un paquete de NetWare (uno de ellos sólo lleva 52 bytes útiles, el resto son 0).

La dirección de la RAM del buffer es seleccionable con jumpers. El default es D0000h - D07FFh, normalmente no interfiere con otras direcciones. La tarjeta también ocupa un espacio de 16 Bytes en el mapa de I/O, siendo el default 2E0 - 2EFh un valor que no interfiere. Emplea una línea de IRQ seleccionable, siendo la 2 por default. En las XT no hay problema, pero en las AT coincide con el IRQ generada por el segundo 8259, por lo que debe cambiarse: las opciones son: 3, 4 (ambas pueden interferir con puertas serie) , 5 y 7 (pueden interferir con puertas paralelo). Por último, hay un par de parámetros de "time - out" que deben seleccionarse mediante DIP switches con la restricción de que deben ser iguales en todas las tarjetas.

	Ethernet	StarLan	Token-Ring	ARCNET	LocalTalk
IEEE	802.3 10BaseX 10Broad36	802.3 1Base5	802.5	Sin normalizar	Sin normalizar
Método de Acceso	CSMA/CD (aleatorio)	CSMA/CD (aleatorio)	anillo testigo determinista	bus testigo determinista	CSMA/CD (aleatorio)
Origen	1975 Xerox	1982 AT&T	1985 IBM	1980 Datapoint	1984 Apple
Velocidad	10Mbps	1Mbps	4/16 Mbps	2,5 Mbps	230,4 Kbps
Topología	Bus/Estrella	Bus/Estrella	Anil./Estrella	Est./Bu./An.	Bus/Estr.
Medio	Par trenzado, coaxial, fibra óptica	Par trenzado	Par trenzado, fibra óptica	Par trenzado, coaxial, fibra óptica	Par trenzado

Hoy en día existe una necesidad, cada vez más acuciante, de incrementar el ancho de banda de las redes de área local. El mayor porcentaje de redes de área local instaladas son redes Ethernet (10Mbps) o redes Token Ring (4 o 16 Mbps). Ambas tienen limitaciones importantes:

Las primeras bajan drásticamente su rendimiento cuando crece el número de estaciones conectadas a ellas, llegando a bloquearse a consecuencia del aumento de las colisiones. Las redes Token Ring imponen limitaciones en cuanto al número de estaciones que pueden conectárseles.

Ambas proporcionan anchos de banda suficientes para aplicaciones tradicionales de computador, pero no para las nuevas aplicaciones de tiempo real (transmisión de voz y vídeo) y aplicaciones multimedia que están apareciendo, o bien, para conexiones a servidores de red que están muy solicitados y que necesitan mucho ancho de banda.

El medio de transmisión en las LANs tradicionales (incluida FDDI) es un medio compartido, es decir, hay que competir con el resto de las estaciones para acceder al medio de transmisión. Esto es también ineficaz para las aplicaciones de tiempo real.

Ante esta panorámica se empieza a estudiar la posibilidad de aumentar el ancho de banda de las redes de área local a 100Mbps. Hasta hace muy poco la única tecnología estándar que proporcionaba 100Mbps era FDDI. Sin embargo, la especificación de FDDI, a pesar de superar a todas sus predecesoras, está tardando bastante en entrar en el mercado, incluso en áreas donde en principio tenía grandes ventajas. Esta tardanza se debe, fundamentalmente a dos factores:

Los trabajos originales en la especificación del estándar FDDI comenzaron en 1984, y no finalizaron hasta ocho años después. La tecnología punta no puede esperar tanto.

Los resultados obtenidos han compensado la larga espera, pero no así los costos. A pesar que el rendimiento global de FDDI y la tolerancia a fallos son buenos, FDDI requiere un alto precio

inicial en la instalación hardware. Los precios de los interfaces, acopladores, conectores, etc. son muy altos. Además, dada la complejidad del protocolo FDDI, los costos de formación y soporte pueden doblar el precio de la red.

FDDI debería tender a reducir las diferencias de precio que presenta respecto a otros protocolos como 100 BaseT de Fast Ethernet o 100VGAnylan.

Ethernet Y Token Ring A 100mbps

Se han terminado de desarrollar nuevas tecnologías de Ethernet y Token Ring a 100Mbps. La idea de partida consistió en que los diseños de redes de área local que se plantearán en un futuro próximo estarían basados en bus de FDDI o ATM, usando una tecnología asequible de red local a 100 Mbps, que permitieran que la Ethernet o Token Ring donde trabaja el usuario final tuviera a su disposición un ancho de banda tal que las aplicaciones futuras fueran operativas y no se advirtieran retrasos en su funcionamiento. Se tuvieron que resolver varios problemas. Entre ellos está satisfacer las limitaciones FCC (Federal Communications Commission) de los Estados Unidos, que limitan la radiación emitida por los cables de categoría 3 UTP que lleven tráfico de alta velocidad. En este punto los fabricantes estaban divididos en dos grupos. Para conseguirlo, unos propusieron la propagación de la señal de datos sobre cuatro pares UTP en vez de dos y limitar las transmisiones a un único sentido. El uso de cuatro pares en vez de dos es un requerimiento fácil de cumplir ya que los cableados UTP existentes están hechos con cuatro pares, dos de los cuales no se usan. Sin embargo, la limitación de las transmisiones a un único sentido requeriría la sustitución del mecanismo de acceso al medio CSMA/CD por otro nuevo. Con CSMA/CD las estaciones son capaces de recibir y transmitir datos simultáneamente detectando cuando la red está ocupada. Los opositores sostenían que Ethernet sin CSMA/CD no es Ethernet, y que las limitaciones de las emisiones de radiación deben de superarse usando técnicas de señalización basadas en chips, en vez de reemplazar el mecanismo de acceso al medio. A pesar de los problemas y las diferencias, los grupos de estudio se pusieron de acuerdo en tres puntos cruciales en la tecnología de Ethernet a 100 Mbps:

1. Se debe basar en la misma topología en estrella usada en las redes 10BaseT, con estaciones de trabajo a distancias de hasta 100 metros del HUB.

2. Debe usar el mismo formato de trama que 10BaseT de forma que para unir las Ethernet existentes con las nuevas a 100 Mbps, sólo hagan falta HUBs equipados con buffers de memoria para manejar la diferencia de velocidades.
3. Limitar las distancias de la estación de trabajo al HUB a 100 metros, esto hace que no se pueda utilizar como tecnología de bus.

Se formalizarón varias propuestas y algunas de ellas se han establecido como estándar , las más conocidas son: 100BaseVG (IEEE 802.12), 100BaseVG-AnyLAN (IEEE 802.12) y 100BaseT(802.30).

100Base-VG o 100VG-AnyLAN

Es la tecnología de Ethernet a 100 Mbps propuesta por Hewlet Packard y At&T, a la que se unió IBM. En el estándar se propone que las señales sean transmitidas sobre cuatro pares en una única dirección ya sea de estación a HUB o al revés. Fue diseñada con dos objetivos fundamentales:

1. Aprovechar la infraestructura de cableado que muchas empresas tienen instalado
2. Favorecer aquellas aplicaciones con requerimientos críticos de respuesta en tiempo.

El primer objetivo queda cubierto ya que 100Base-VG tiene una topología en estrella basada en concentradores, y utiliza cuatro pares de hilos que pueden ser UTP de categoría 3 (categoría de voz, de ahí el término VG) o categoría 5 (categoría de datos), STP o bien fibra óptica. La información primero se codifica transformando 5 bits en 6 símbolos (5B/6B) y después éstos se transmiten con señalización NRZ distribuidos en los cuatro canales pues la comunicación es half duplex.

Para satisfacer el segundo objetivo, se propone remplazar CSMA/CD por un nuevo método de acceso llamado Demand Priority Protocol. Con este protocolo las demandas de acceso procedentes de estaciones son enviadas al HUB, encargándose este de responder. Puede funcionar en instalaciones de cableado UTP de categoría 3 (cableado de calidad de voz, o Voice Grade- VG). También se soportan los cableados de categoría 4 y 5. Los conectores que se utilizan son del tipo RJ45, así como los conectores Telco de 50 pines usados para 25 pares de cables. Usando estos conectores y un cable UTP de categoría 3 se pueden soportar las conexiones con distancias entre

estación y HUB de 100 metros. Si, en cambio, el cable es de categoría 4 o 5 se soportan distancias de 200 metros y usando conexiones de fibra óptica la distancia puede llegar a ser de 2Km.

Las principales características de 100BaseVG son:

- El formato de la trama en la capa de enlace es idéntico al usado en Ethernet.
- Posee una topología en estrella. Las estaciones están conectadas a un HUB que es un nodo de conmutación de circuitos. Se pueden asignar prioridades a los puertos de dicho HUB.
- Usa los cuatro pares del cable para cada estación (10BaseT solo usa dos). Se divide la señal de 100 Mbps sobre cuatro pares, es decir hay 25 Mbps sobre cada par. De esta forma los niveles de radiación están dentro de los permitidos por las regulaciones FCC. Utiliza un método de codificación llamado 5B6B (5bits en 6 símbolos) para remplazar al método de codificación diferencial Manchester usado en 10BaseT.

El método de acceso (Demand Priority Protocol) actúa de la siguiente manera:

1. Una estación emite una petición de transmisión (tono).
2. Recibe una autorización de transmisión por parte del HUB (tono).
3. El HUB empieza a recibir la trama y mientras determina cual es la estación de destino sigue recibiendo datos (buffer elástico).
4. El HUB avisa a la estación de destino del próximo envío de datos.
5. La estación destino responde con un preparado para recibir.
6. Durante los últimos tres pasos el HUB continua recibiendo datos.
7. Se realiza la transmisión de datos al destino (a través de los cuatro pares)
8. Ambas estaciones vuelven al estado inicial al terminar la transmisión.

100BaseVG tiene muchas similitudes con respecto a Ethernet, pero implementa varias mejoras:

- Fair Arbitration o acceso determinístico. Se sustituyen las colisiones por un procedimiento determinístico de acceso al medio para cada estación basado en un protocolo de demanda/concesión administrado por el hub. Esto proporciona un ancho de

banda ordenado sin colisiones, de forma que el 97% del ancho de banda sea usado por datos de usuario.

- Link Privacy o aislamiento de enlace. El aislamiento del enlace es inherente al protocolo 100BaseVG dado que las estaciones están generando tramas que van por un circuito virtual creado por el hub. Sigue siendo un medio compartido, pues mientras este establecido un circuito no van a poder establecer más. Los paquetes de broadcast se repiten por todos los puertos. La detección de intrusos es muy fácil de implementar con 100BaseVG.
- Demand Priority Signaling o establecimiento de prioridades por demanda. Permite a las aplicaciones multimedia u otras aplicaciones muy sensibles a los retardos aumentar su prioridad de acceso a la red.

Al unirse IBM al grupo de 100BaseVG se cambió el nombre de la especificación por 100BaseVG-AnyLAN. Es una especificación ampliada para permitir que no sólo las tramas Ethernet vaya a 100 Mbps sino también las de Token Ring. Este cambió no retrasó la aparición del estándar ya que incluir dentro de éste formato de las tramas Token Ring no supuso cambios significativos.

Las reglas para la topología y recomendaciones para las redes 100VG-AnyLAN :

- **Regla 1**: La topología de red debe ser una estrella física punto a punto, sin ramificaciones ni bucles.
- **Regla 2**: En una red 4-pares UTP, se requieren los cuatro pares.
- **Regla 3**: No se usa cable liado UTP (cable que consta de 25 o más pares trenzados en una funda) para los enlaces de redes donde los nodos terminales están configurados en modo promiscuo.
- **Regla 4**: No se usa cable liso en una topología de par trenzado.
- **Regla 5**: Debe haber un único camino activo entre un par de hubs en la red.
- **Regla 6**: La máxima distancia entre un nodo terminal y el hub raíz en una red de segundo nivel es 4 Km. (usando cableado de fibra óptica).

Máximas distancias entre Hub raíz y nodo terminal.

Numero de Hubs entre hub raíz y nodo terminal	Numero de niveles en la red	Máxima distancia entre hub raíz y nodo terminal
1	2	4 km.
2	3	3 km.
3	4	2 km.
4	5	1 km.

- **Regla 7**: El numero máximo de niveles en una red 100VG-AnyLAN es de 5.
- **Regla 8**: No hay limites en el número de nodos en un segmento no apantallado 100VG-AnyLAN.
- **Regla 9**: Todos los nodos en una porción simple (campo simple a 100 Mbit/s) de una red 100VG-AnyLAN deben usar el mismo formato de paquete soportado por Ethernet/802.3 y token Ring 802.5.
- **Regla 10**: Entre cualquier par de nodos en una red 100VG-AnyLAN, no debería de haber mas de 7 bridges.

  Recomendación: Minimizar los niveles de cascada.

100Base-T (Fast Ethernet)

En un principio llamada 100BaseX. Esta especificación fue promovida por Grand Junction, es la evolución de 10BaseT a altas velocidades. 100Base-T utiliza CSMA/CD como protocolo de acceso al medio, transmite tramas con el formato Ethernet a 100 Mbps y emplea una topología de estrella basada en un concentrador. En la capa física existen tres propuestas diferentes: 100Base-TX, 100Base-T4 y 100Base-FX, que permiten utilizar diferentes medios de transmisión. El subcomité 802.3 ha dicho que los esquemas de señalización serán interoperables en una misma red .

Muchas empresas interesadas en desarrollar estas tecnologías formaron una agrupación, The Fast Ethernet Alliance, que entre otras cosas ha logrado presionar al subcomité 802.3 para acelerar los procesos de estandarización. El trabajo original de la propuesta 100Base-TX fue desarrollado por Grand Junction Networks, y a ella se han sumado muchas otras empresas como David Systems, Chipcom, SynOptics, 3Com, Intel, National Semiconductor, DEC y Sun.

100Base-TX consolida dos estándares: el protocolo de acceso al medio CSMA/CD de 802.3 (cambiando únicamente la duración del intervalo entre tramas de 9.6 a 0.96 μs), y la subcapa física dependiente del medio TP-PMD de FDDI. Así, 100Base-TX requiere dos líneas UTP de categoría 5, a través de los cuales transmite con señalización MLT-3, para conectar cada estación al concentrador. Se define una capa de convergencia para mapear la señalización continua full duplex de FDDI con el esquema asíncrono half duplex usado en Ethernet. También puede utilizarse STP como medio físico.

Por otra parte, la tecnología 100Base-T4 es propuesta con el objetivo fundamental de transmitir información a 100 Mbps a través del cableado que se utilizaba hasta 1992 y que se sigue utilizando para redes de voz y de datos a velocidades hasta de 10 Mbps. Este cable es UTP de categoría 3. La especificación sometida a consideración del subcomité 802.3 ha sido desarrollada por SMC, 3Com e Intel.

Utiliza cuatro pares UTP (de ahí el término T4), tres pares se utilizan para transmitir o recibir la trama (la comunicación es half duplex) mientras que el último par se utiliza exclusivamente como entrada para detección de colisiones. Antes de ser transmitidos, los datos se codifican transformando 8 bits en 6 símbolos ternarios (8B/6T). La información ternaria es entonces transmitida por los canales de datos. Este modelo es técnicamente similar a la señalización MLT-3, ofreciendo un nivel adecuado de emisiones electromagnéticas.

Por último, la propuesta 100Base-FX emplea dos fibras ópticas multimodales.

Al igual que en 10BaseT, la distancia máxima entre una estación y el concentrador en 100Base-T es de 100 metros. Sin embargo, las reglas de topología permitidas son diferentes en 100Base-T: sólo se permiten dos repetidores, y la distancia máxima de una red es de 205 metros si se utiliza par trenzado y 325 si se emplea fibra óptica .

Fddi: Una Red De Fibra Optica

FDDI (Fiber Distributed Data Inteface) es una evolución de Ethernet, token bus a protocolos de mayores prestaciones. Propuesto por ANSI (standard X3T9.5).

Hacia 1980, comienzan a necesitarse redes que transmitan datos a alta velocidad.

También se necesitaba transmitir datos en tiempos cortos y acotados. En respuesta a estas necesidades, se desarrolla FDDI. FDDI ofrece 100 Mbps, con hasta 500 estaciones conectadas y un máximo de 100 km entre ellas. Las estaciones se conectan en un doble anillo de fibra óptica por seguridad. Por su alta velocidad de transmisión, también puede usarse como una red de conexión entre redes más pequeñas.

Funciones de FDDI

Las funciones de FDDI se define en el SMT (Station ManagemenT). Abarcan la capa física (PMD y PHY) y parte de la capa de enlace (MAC). Por ello, FDDI se instala en los niveles más bajos de la torre OSI. No habría problemas en usar otros protocolos para las capas superiores, en principio. Por lo contrario, las implementaciones sólo han conseguido encapsular correctamente ARP e IP sobre FDDI.

Nivel Físico: PMD

En el nivel dependiente del medio (PMD), FDDI no impone restricciones al tipo de fibra que debe usarse. Puede utilizarse fibra multimodo (MMF), o fibra monomodo (SMF). Las fibras serán de dimensiones 62,5/125 o 85/125 (diámetro del núcleo/di metro de la fibra). MMF necesita mejores emisores y receptores que SMF para mantener las mismas longitudes de enlace. En cualquier caso, la potencia de transmisión mínima es de -16 dBm y la potencia recibida mínima es de -26 dBm, lo que deja un margen de 11 dBs para pérdidas. Los transmisores pueden ser LED o láseres. Los receptores pueden ser diodos PIN o de avalancha. Se trabaja en la ventana de 1300 nanómetros. En una misma red puede haber enlaces con fibras MMF y SMF, aunque deben examinarse con cuidado. Se recomienda emplear conectores SC preferentemente. También pueden emplearse conectores ST. La probabilidad de error requerida es 4*10-11.

Nivel Físico: PHY

El otro subnivel físico, PHY, define el protocolo de introducción de datos en la fibra. FDDI introduce redundancia en los datos en transmisión. Usa un código 4B/5B, transmite 5 bits por cada 4 bits que le envía el nivel superior. La elección de los códigos se hizo para equilibrar la potencia continua del código, y evitar secuencias de 0's o 1's demasiado largas. El régimen binario efectivo que soporta la fibra son 125 Mbps.

MAC define la longitud máxima de trama en 4500 bytes para evitar problemas de desincronización. No hay longitud de trama mínima. El formato de trama es:

- PA = Preámbulo: 30 caracteres IDLE, para sincronismo.
- SD = delimitador de inicio. No se repite en el campo de datos.
- FC = control de trama. Tipo de trama (síncrona, etc.).
- DA = Dirección de destino.
- SA = Dirección de destino.
- INFORMACION: Datos transmitidos.
- FCS= Redundancia de la trama con CRC-32.
- ED = Delimitador de fin de trama. No se puede repetir en el campo de datos.
- FS = Frame Status. Receptor informa a origen del resultado de la trama (trama errónea, bien recibida, etc.)

Una estación que está transmitiendo trama debe retirarla del anillo. Mientras lo hace, puede introducir nuevas tramas, o transmitir caracteres IDLE, hasta retirarla completamente. Dado que protocolos superiores (UDP, por ejemplo) definen longitudes de trama diferentes, las estaciones deben estar preparadas para fragmentar/ensamblar paquetes cuando sea necesario.

Nivel de enlace: MAC

MAC aporta las mayores novedades de FDDI. FDDI soporta dos tipos de tráfico:

- Tráfico síncrono: voz, imágenes, etc., información que debe ser transmitida antes de un determinado tiempo. Podría decirse que es tráfico de datos en tiempo real.
- Tráfico asíncrono: e-mail, ftp, etc., información para la cual el tiempo que tarde en llagar al destino no es el factor decisivo.

La filosofía que persigue FDDI es atender primero el tráfico síncrono y después el tráfico asíncrono. Para ello, cada estación tiene varios temporizadores:

- Token Rotation Time (TRT): tiempo transcurrido desde que llegó el último testigo.
- Token Hold Time (THT): tiempo máximo que una estación puede poseer el testigo.

Todas las estaciones tienen un parámetro fijo, el Target Token Rotation Time (TTRT), que fija el tiempo que tarda el testigo en dar una vuelta al anillo, y cada una tiene un parámetro propio, Syncronous Time (ST o Ci, dependiendo de autores). Este parámetro fija el tiempo máximo que una estación está transmitiendo tráfico síncrono.

1) Cuando llega el testigo, comprueba que ha llegado a tiempo. Para ello, ve si TRT > 0. Si es cierto, la estación captura el testigo. Si es falso, la estación la estación lo deja pasar a la siguiente estación. En cualquier caso, TRT se reinicializa a TTRT.
2) Una vez la estación posee el testigo, el valor de TRT se carga en THT. Se comienzan a transmitir tramas síncronas.
3) THT llega a cero. En ese caso, se termina el turno de la estación, y se pasa el testigo a la siguiente.
4) Antes de que THT llegue a 0 se acaban las tramas síncronas que tenía la estación preparada para transmitir. Se transmiten ahora todas aquellas tramas asíncronas de que se dispongan, hasta que THT llegue a cero.
5) Si se acaba también las tramas asíncronas, pasa el testigo.

Se plantea un problema cuando se acaba el THT mientras se está transmitiendo una trama. Este fenómeno se llama overrun.

El intervalo máximo entre dos testigos en una estación ronda 2*TTRT.

Las estaciones se conectan mediante un doble anillo de fibra óptica. En cada anillo, la información circula en una dirección. En caso de que caiga un enlace entre dos estaciones, las fibras se puentean internamente en las estaciones, de modo que el anillo no se para. Esta configuración clasifica las estaciones en dos clases:

1. **DAS** : Dual Attachment Station. Estación conectada al doble anillo. Capaces de reconfigurarse. Más caras.
2. **SAS** : Single Attachment Station. Estación conectada a uno de los dos anillos solamente. Más baratas.

Otras soluciones alternativas

Se han planteado otras soluciones al standard original expuesto anteriormente. Todas las soluciones se basan en el estándar FDDI, aunque varían algunos niveles, para adaptarlo a determinadas situaciones. Las soluciones más atractivas son CDDI, FDDI-II, y LCF-FDDI

CDDI

CDDI (Copper Distributed Data Interface) no es otra cosa que FDDI utilizando cables de cobre en lugar de fibra óptica como medio de transmisión. Sólo afecta al PMD. Para seguir cumpliendo los requerimientos de ruido y velocidad de transmisión se reduce la distancia máxima de enlace a 100 m. Para evitar también la radiación que produce el par trenzado sin blindaje (Unshielded Twisted Pair, UTP) cuando se utilice este medio de transmisión se utiliza un código diferente, NRZ- III. Básicamente, es NRZ con tres niveles, subiendo y bajando niveles hasta llegar a los extremos. De este modo, baja la frecuencia máxima que soporta el par trenzado, reduciéndose las radiaciones. La principal ventaja que aporta CDDI es la reducción en los costos de implantación de FDDI, sobre todo cuando se quiere hacer llegar FDDI hasta los terminales de usuario (FDDI- on-desk). Los terminales suelen estar ya cableados, por lo que sustituir el cobre por la fibra óptica aparece como un costo innecesario en muchos casos. Además, los receptores y transmisores ópticos que emplea FDDI resultan demasiado caros frente a los dispositivos electrónicos que utiliza CDDI. Por lo demás, los cambios en el código no son relevantes y la reducción en la distancia máxima no es importante, puesto que CDDI se utilizaría dentro de los edificios, en los que las distancias suelen ser inferiores a esos 100 metros críticos.

FDDI-II

FDDI-II cambia el servicio que ofrece. Amplía SMT hasta completar el nivel de enlace. Ahora el nivel de red no ve un único canal de 100 Mbps sino que este canal se divide en 16 canales isócronos de 6,144 Mbps (WBC), y un canal de transmisión de paquetes, de 768 Kbps (PDG). Las

tramas son de 0.125 ms y contienen intercalados los distintos canales. Inicialmente, se envían 2,5 bytes de preámbulo que sincronizan el reloj de 8 Khz que inicia las tramas y 12 bytes de cabecera de la trama. Se envía el byte correspondiente al PDG. Luego se envía un byte de cada canal. Cuando se llega a un byte múltiplo de 8 en los WBC se vuelve a enviar 1 byte de PDG.

Usualmente, los testigos se pasan a través del PDG. Los WBC pueden subdividirse en canales menores, en funciones de las necesidades de las estaciones.

Aparece ahora un nuevo tipo de tráfico, de prioridad mayor que el síncrono de FDDI, que es el tráfico conmutado. Hay dos testigos, testigo restringido y testigo sin restricciones. Dependiendo de las restricciones en tiempo de llegada de las tramas se utiliza una combinación de tráfico y testigos.

LCF-PMD

LCF-PMD (Low-Cost Fiber Physical Medium Dependent) surge también como necesidad económica. Se busca reducir el costo de implantación de una red FDDI. Para ello, se cambia de nuevo el PMD. Se introduce unos nuevos tipos de fibra (200/230), más baratos y de peores prestaciones. Igual que en CDDI, se amplían los márgenes de ruido, y se reducen las longitudes de los enlaces, ahora hasta los 500 metros. Se reduce la potencia mínima de transmisión en 2 dBm. Se relaja en 2 dBm la potencia mínima de recepción, quedando sólo 7 dBs para pérdidas. El resto del protocolo no se altera.

Rendimiento

El rendimiento de FDDI se mide en dos aspectos: Retardo de as tramas en llegar a la estación destino y cantidad de datos que llegan a destino por segundo. Un primer par metro de importancia es el TTRT. Si es pequeño, el testigo circula muy rápidamente, de modo que el retardo es pequeño. Si es grande, el desempeño es mayor, pero estaciones con mucha carga retrasan a las demás. Los valores típicos de TTRT rondan los 4 ms o los 165 ms,. Otro factor a tener en cuenta es el tamaño de los paquetes. Si es grande, aumenta el desempeño. Si es pequeño, disminuye el retardo.

Conclusiones

En conclusión, FDDI ofrece transmisión de datos a alta velocidad, en tiempo real o no, entre un número de estaciones alto y separadas una distancia elevada. También puede servir como red de conexión entre LANs que estén funcionando previamente. Se ha sabido adaptar a las características de entornos en los que resulta muy deseable disponer de ella, pero su elevado costo inicial parecía prohibir. Esto hace de FDDI y LCF alternativas muy interesantes para LANs. Sin embargo, la irrupción de ATM ha hecho que FDDI se considere "la hermana pequeña" de las redes de comunicación óptica. ATM ha hecho que FDDI ya no sea un campo de investigación tan activo como fue a finales de los 80, ni siquiera en FDDI-II, que aprovecha parte de las ideas que utiliza ATM. Por ejemplo, la inclusión de canales virtuales conmutados.

ATM

ATM se originó por la necesidad de un standard mundial que permitiera el intercambio de información, sin tener en cuenta el tipo de información transmitida. Con ATM la meta es obtener un standard internacional. ATM es una tecnología que va creciendo y es controlada por un consenso internacional, no por la simple vista o estrategia de un vendedor.

Desde siempre, se han usado métodos separados para la transmisión de información entre los usuarios de una red de área local (LAN) y los de una red de gran tamaño(WAN). Esta situación traía una serie de problemas a los usuarios de LAN's que querían conectarse a redes de área metropolitana, nacional y finalmente mundial. ATM es un método de comunicación que se puede implantar tanto en LAN's como en WAN's. Con el tiempo, ATM intenta que las diferencias existentes entre LAN y WAN vayan desapareciendo.

Actualmente se usan redes independientes para transportar voz, datos e imágenes de video debido a que necesitan un ancho de banda diferente. El tráfico de datos no necesita comunicar por un periodo extenso de tiempo sino transmitir grandes cantidades de información tan rápido como sea posible. Voz y video, por otra parte, tienden a necesitar un trafico mas uniforme siendo muy

importante cuando y en el orden en que llega la información. Con ATM, redes separadas no serán necesarias. ATM es el única tecnología basada en estándar que ha sido diseñada desde el comienzo para soportar transmisiones simultaneas de datos, voz y video.

ATM es un standard para comunicaciones que esta creciendo rápidamente debido a que es capaz de transmitir a una velocidad de varios Megabits hasta llegar a Gigabit.

Cuando se necesita enviar información, el emisor "negocia" un camino en la red para que su comunicación circule por él hacia el destino. Una vez asignado el camino, el emisor especifica el tipo, la velocidad y otros atributos de la comunicación.

Otro concepto clave es que ATM está basado en el uso de conmutadores. Hacer la comunicación por medio de un conmutador (en vez de un bus) tiene ciertas ventajas:

1. Reserva de ancho de banda para la conexión
2. Mayor ancho de banda
3. Procedimientos de conexión bien definidos
4. Velocidades de acceso flexibles.

Si se usa ATM, la información a enviar es dividida en paquetes de longitud fija.

Estos son mandados por la red y el destinatario se encarga de poner los datos en su estado inicial. Los paquetes en ATM tienen una longitud fija de 53 bytes, esto permite que la información sea transportada de una manera predecible. El hecho de que sea predecible permite diferentes tipos de trafico en la misma red.

Los paquetes están divididos en dos partes, la cabecera y payload. El payload (que ocupa 48 bytes) es la parte del paquete donde viaja la información, ya sean datos, imágenes o voz. La cabecera (que ocupa 5 bytes) lleva el mecanismo direcccionamiento.

ATM a pasado de la teoría a la realidad con productos y servicios disponibles hoy en día. EL ATM forun ha patrocinado demostraciones de interoperatibilidad para demostrar la tecnología y continua reuniéndose para discutir sobre la evolución de ATM.

EL ATM coexiste con la actual tecnología LAN/WAN. Las especificaciones de ATM están siendo descritas para asegurar que el ATM integre las numerosas tecnologías de red existentes, a varios niveles(ie, Frame Relay, Ethernet, TCP/IP).

Equipos, servicios y aplicaciones están disponibles hoy en día y están siendo actualmente usadas en redes.

La industria de la telecomunicación se dirige al ATM.

CAPITULO 2

La Familia de Sistemas Operativos de Red Microsoft Windows NT

Windows NT

El sistema operativo NT Server y Nt Workstation son sistemas operativos de red a 32 bits multitarea. NT Workstation ayuda a crear un poderoso y flexible ambiente de cómputo para negocios, finanzas, ingeniería, construcción, manufactura, procesos de control, investigación, sistemas de tiempo real, automatización, etc. ejecutando varias de estas tareas al mismo tiempo.

Windows NT Server

Es un poderoso sistema operativo diseñado para las organizaciones con aplicaciones de misión crítica. NT Server provee una nueva generación de aplicaciones y herramientas, así como servicios de impresión de archivos. Su plataforma cliente-servidor esta diseñada para integrar tecnologías actuales y futuras, proveyendo grandes ventajas al mejor acceso a la información.

Asi mismo, Windows NT Server es un sistema operativo para servidores, ampliable e independiente de la plataforma, ya que puede ejecutarse en sistemas basados en procesadores Intel x86, RISC y DEC Alpha, ofreciendo al usuario mayor libertad a la hora de elegir sus sistemas informáticos. Es ampliable a sistemas de multiproceso simétrico, lo que permite incorporar procesadores adicionales cuando se desee aumentar el rendimiento.

Internamente posee una arquitectura de 32 bits. Su modelo de memoria lineal de 32 bits elimina los segmentos de memoria de 64 KB y la barrera de 640 KB de MS-DOS. Posee múltiples threads (subprocesos) de ejecución, lo que permite utilizar aplicaciones más potentes. La protección de la memoria garantiza la estabilidad mediante la asignación de áreas de memoria independientes para el sistema operativo y para las aplicaciones, con el fin de impedir la alteración de los datos. La capacidad de multitarea de asignación prioritaria permite al sistema operativo asignar tiempo de

proceso a cada aplicación de forma eficaz. Windows NT Server incluye, asimismo, diversas funciones de red.

Windows NT Server es el sistema operativo ideal para la implementación de las herramientas del sistema BackOffice de Microsoft, tales como:

- SQL Server: sistema de administración de bases de datos en estructura clientes-servidor.
- Systems Management Server: administración centralizada de sistemas.
- Exchange Server: sistema de administración de correo electrónico cliente-servidor con capacidades de groupware.
- Internet Information Server: sistema de administración de servicios World Wide Web.
- Proxy Server Firewall: sistema para el control de acceso entre Internet y la red privada.

Windows NT Workstation

Este sistema operativo incluye todas las capacidades de Windows For Workgroups y Windows 95, es además un sistema operativo multitarea, multithreading, y con capacidades de red mejoradas. NT Workstation puede ser usado como sistema operativo de escritorio, en redes punto a punto, o en el ambiente de dominios de NT Server.

Asi mismo, NT Workstation puede ser usado como cliente de las herramientas de BackOffice.

Clientes

Windows para Trabajo en Grupo, Windows 95 y 98 son los sistemas operativos de eleccion ideales para clientes de red punto a punto con una interface gráfica, diseñados para compartir entre un número pequeño de personas y tareas similares.

Características de Windows NT

Características y servicios	NT Workstation	NT Server
Conexiones concurrentes	10 como servidor	Ilimitadas
	Ilimitadas como cliente	
Multiprocesamiento simétrico (*)	2 procesadores	4 procesadores
Remote Access Service (RAS)	Una sesión	256 sesiones
Replicación de Directorios	Importa	Importa y Exporta
Validación de Dominio	No	Sí
Servicios para Macintosh	No	Sí
Herramientas de tolerancia a fallas en disco	No	Sí

*existen versiones especiales hasta de 32 procesadores

Grupos de Trabajo y Dominios

De acuerdo a las necesidades de la organización donde la red sé este utilizando, Windows NT puede organizar el trabajar en grupos de trabajo o en un sistema de dominios.

Grupos de Trabajo

Es el conjunto de computadoras lógicamente agrupadas con un propósito, como compartir discos o impresoras. Los miembros de trabajo pueden ver los recursos compartidos de otras computadoras. Cada computadora tiene su propia base de datos de cuentas de usuarios y políticas de seguridad (administración descentralizada). Cada grupo de trabajo esta identificado por un nombre único.

Un grupo de trabajo es bueno para pequeñas organizaciones con pocas personas, con tareas comunes y con necesidades de accesar recursos en otras computadoras.

Dominio

Un dominio en el ambiente NT es un conjunto de computadoras compartiendo una base de datos de cuentas de usuarios y políticas de seguridad (administración centralizada). Un dominio provee una validación para asegurar que las cuentas de usuario y las políticas de seguridad se cumplan. Cada dominio tiene un nombre único.

Windows NT Server puede crear dominios y así administrar cuentas de usuario de dominio, seguridad y recursos de red centralizadamente.

NT utiliza un modelo de objetos para proveer a los usuarios con acceso a los recursos locales y remotos y ejecutar varios tipos de aplicaciones. El modelo de objetos usados en NT es modular, compuesto por un grupo de componentes relativamente independientes. Cada componente desarrolla una tarea específica dentro de todo el ambiente sistema operativo. Esto es realizado por subsistemas y servicios ejecutivos que conforman la plataforma sobre la cual las aplicaciones se ejecutan.

Subsistema de Ambiente

Uno de los mayores propósitos de NT es soportar diferentes tipos de aplicaciones sobre la misma interface gráfica. NT ejecuta aplocaciones DOS, OS&2, Win 16, Win 32 y POSIX.

NT soporta esta variedad de aplicaciones a través del uso de los subsistemas de ambiente. Los subsistemas de ambiente son procesos que emulan los ambientes de diferentes sistemas operativos. Los subsistemas interactuan con los servicios ejecutivos para producir ambientes de acuerdo a las necesidades de las aplicaciones que sean ejecutadas usando Windows NT.

Servicios Ejecutivos

La función de los Servicios Ejecutivos es proveer un conjunto de funciones fundamentales de sistema operativo sobre la cual acoplar funciones más poderosas. Los servicios incluyen administración de:

- Procesos y threads
- Entrada/Salida
- Seguridad
- Memoria
- Comunicación entre procesos

Manejo de Memoria en NT

NT utiliza un sistema de paginación de memoria virtual basándose en la demanda con un direccionamiento *flat* lineal de direcciones de 32 bits.

Este modelo de memoria lineal permite direccionar hasta 2GB de RAM directamente, en vez de segmentos de 64, permitiendo a los programadores generar grandes aplicaciones.

El Virtual Memory Manager (VMW) mapea las direcciones virtuales de las aplicaciones en páginas físicas en memoria física (RAM) o en el archivo de paginación (Pagefile.sys). Esto oculta la organización de la memoria a la aplicación y asegura que cuando las aplicaciones soliciten localidades de memoria, ellas son mapeadas a direcciones sin conflictos de memoria.

El término de paginación en base a la demanda se refiere al método para mover los datos en páginas de 4K de la memoria física a un archivo en disco temporal (archivo de paginación). Según la aplicacion va necesitando los datos, estos se transfieren a la memoria fisica (acceso rápido) y los datos en memoria no usados se pasan al archivo de paginación. El algoritmo de paginación está optimizado para efectuarse por procesos y no por *systemwide*.

El esquema de direccionamiento lineal favorece la portabilidad de NT por que es compatible con el direccionamiento de procesadores Intel y RISC.

Arquitectura de Red

Una diferencia significativa entre NT, con otros ambientes y sistemas operativos (MS-DOS, Windows 3.x, OS/2), es que las funciones de red están integradas.

Windows NT es compatible con los estándares NDIS (Especificación de la interfaz del controlador de red) y TDI (Interfaz del controlador de transporte). NDIS es una interfaz estándar para comunicación entre controladores de tarjetas adaptadoras de red y protocolos de red. NDIS le permite combinar y coordinar tarjetas y protocolos de red sin que sea necesario disponer de una versión diferente del protocolo de red para cada tipo de tarjeta.

Permite también utilizar varios protocolos en una misma tarjeta de red. Con Windows NT se suministran cuatro protocolos compatibles con el estándar NDIS: TCP/IP, Microsoft NWLink, NetBEUI y DLC (Control de vínculos de datos). La interfaz TDI se comunica entre el protocolo de red y el software de red de alto nivel (como el servidor y el redirector). TDI elimina la necesidad de que el redirector y el servidor se comuniquen directamente con los protocolos de red, o de tener información de los mismos, permitiendo de esta forma utilizar protocolos, servidores o redirectores diferentes con Windows NT. También es compatible con aplicaciones de RPC (Llamada a

procedimientos remotos), aplicaciones de sistema de entrada/salida básico de red (NetBIOS) y aplicaciones con Windows Sockets.

Las computadoras con NT pueden actuar como clientes y servidores en ambientes de aplicaciones distribuidas y en redes punto a punto.

NT tiene la capacidad de operar en diferentes ambientes de red como:

- Redes Microsoft, Windows NT Server 3.5, Windows for Workgroups, LAN Manager, y otras redes basadas en Ms-Net.
- Novell NetWare.
- Transport Control Protocol/Internet Protocol (TCP/IP) hosts (incluyendo sistemas UNIX).
- Apple Macintosh Apple Talk.
- Clientes de Acceso Remoto.

Componentes de Red Integrados en Windows NT

Para comprender el funcionamiento en red de Windows NT es necesario entender su arquitectura modular. Windows NT permite reemplazar un nuevo componente sin modificar el resto de la configuración.

Los componentes de red de NT pueden ser organizados en tres categorias: sistemas de archivos, protocolos de transporte y controladores de las tarjetas de red. Estos componentes se comunican entre sí a través de las capas de enlace. Las capas de enlace traducen los datos al formato de los componentes usados. Además las capas de enlace incluyen interfaces de programación: la Transport Driver Interface (TDI) y NDSI 3.0.

Los componentes de red incluyen:

- Protolocos de Transporte (DLC, NetBEUI, NWLink, and TCP/-IP), los cuales definen las reglas de comunicaciones entre dos computadoras.
- Componentes de comunicación entre procesos (inter-process communication, IPC), como los *named pipes* y los *mail slots*, permitiendo la comunicación entre aplicaciones a través de la red.
- Interfaces de programación: NetBIOS, Windows Sockets, RPC, NetDDE.

- Componentes de compartición de archivos e impresoras a través de la red como el redirector y el server.
- El multiple uniforms naming convention *(UNC)* Provider *(MUP)* y el *Multi-Provider Router (MPR)* hacen posible escribir aplicaciones con una sola API para comunicarse utilizando cualquier redirector.

Capas de Red

Los componentes de red de NT y sus capas de enlace pueden compararse con las siete capas del modelo OSI.

Los sistemas de archivos accesan a los recursos como una llamada de E/S a una partición NTFS o a un archivo de red. Ellos operan al nivel de Aplicación y Presentación del modelo OSI.

Los protocolos de transporte definen las reglas de comunicación entre las computadoras. Ellos operan al nivel de la capa de enlace y normalmente cumplen las reponsabilidades de la capa de sesión, transporte y red del modelo OSI. Es posible instalar y ejecutar varios protocolos en una sola computadora.

Los controladores de red coordinan la comunicación entre la tarjeta de red, el ambiente y el hardware y software de la computadora. Para cada tipo de tarjeta de red debe haber un controlador que cumpla con la norma NDIS 3.0. Los controladores de red operan a nivel de la capa de *Media Access Control*, mientras la tarjeta representa la capa física del modelo OSI.

Capas de Enlace (Boundary Layers)

Un enlace es la interface unificada entre las capas en el modelo de arquitectura de NT.

El uso de Boundaries como un punto intermedio entre las capas de red abre el sistema para el desarrollo de controladores de red y servicios gracias a que la funcionalidad implementada entre las capas de enlace está bien definida. Así solo es necesario programar entre las capas de enlace en vez de hacerlo des la capa suaperior o inferior de una forma estándar, por ejemplo, los protocolos funcionan sin importar el controlador de la tarjeta de red usada.

Las dos capas de enlace mas importantes en la arquitectura de red de NT son:

Network Driver Interface Specification (NDIS) 3.0, provee la interface entre el *NDIS* wrapper y los protocolos de transporte.

Transport Driver Interface (TDI), provee la interface para que componentes como el redirector y servidor de NT se comuniquen con cualquiera de los diferentes protolos de transporte. TDI no es un controlador como TDI, simplemente es un estándar para el paso de mensajes entre dos capas de la arquitectura de red.

Protocolos de Red de Windows NT

NT incluye cuatro protocolos: Data Link Control (DLC), Transport Control Protocol/Internet Protocol (TCP/IP), NWLink, y NetBEUI.

DLC (Data Link Control)

A diferencia de los otros protocolos de NT (NWLink, TCP/IP, y NetBEUI), DLC no está diseñado para ser un protocolo primario para la comunicación entre PCs. DLC solamente provee aplicaciones con acceso directo a la capa de enlace de datos, y no es usado por el redirector de NT.

DLC es principalmente usado para:

- Accesar a mainframes IBM y AS/400 con emuladores 3270 y/o 5250 como la hace el SNA Server.
- Imprimir en impresoras HP que esten conectadas directamente a la red.
- En impresoras de red como la HP 4/Si utilizan el protocolo DLC porque los paquetes recibidos son fáciles de distinguir, y las funciones de DLC pueden ser fácilmente codificadas en ROM.

DLC solo necesita ser instalado en computadoras que realizan las funciones anteriormente mencionadas y no en todas las computadoras de la red, por ejemplo, un servidor de impresión.

Los parámetros de DLC están localizados en el registry en:

HKEY_LOCAL_MACHINES\System\CurrentControlSet\Services\DLC.

TCP/IP

El *Transport Control Protocol/Internet Protocol* (TCP/IP) es una suite de protocolos diseñado para redes de area amplia. Fue desarrollado en 1969 como resultado de un proyecto de investigación de interconexión de redes de la *Defense Adnvanced Research Projects Agency* (DARPA). El crecimiento de esa primera red desenvoco en la actual Internet.

El TCP/IP incluido en NT permite a los usuarios conectarse a Internet y a cualquier máquina con los servicios de TCP/IP configurados.

Las ventajas de TCP/IP incluyen:

- Provee conectividad entre diferentes plataformas y sistemas operativos
- Brinda acceso a Internet
- Capacidades de ruteo
- Soporta el protocolo Simple Network Management Protocol (SNMP)
- Soporta el protocolo Dynamic Host Configuration Protocol (DHCP).
- Soporta el protocolo Windows Internet Name Service (WINS).

Los parámetros de TCP/IP están localizados en el registry en:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Service\TCPIP.

NWLink

NWLink es un protocolo compatible con IPX/SPX para Windows NT. Puede ser usado para establecer conexiones entre computadoras Windows NT, MS-DOS, OS/2, Windows a través de varios mecanismos de comunicación. Como NWLink es simplemente un protocolo no permite el acceso a archivos o impresoras de un servidor Netware, o actuar como un servidor de archivos e impresoras para clientes NetWare. Para accesar a archivos o impresoras en un servidor Netware, es necesario utilizar un redirector como el Client Service for NetWare (CSNW) o un Client NetWare para Windows NT. Para actuar como un servidor de archivos e impresoras para clientes NetWare se debe instalar los File & Print Sharing for Netware.

NWLink es útil al contar con aplicaciones cliente servidor que utilicen sockets o NetBIOS sobre el protocolo IPX/SPX como SQL Server, SNA Server y SMS. La parte del cliente puede ser accesada en un servidor NetWare o viceversa. NWNBlink contiene mejoras al NetBIOS de Novell. El NWNBlink es usado para dar formato NetBIOS a las requisiciones y pasarlas al componente NWLink para la transmisión en la red.

Los parámetros de NWLink están localizados en el registry en:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NWLink

NetBEUI

NetBIOS Extended User Interface (NetBEUI) fue introducido por IBM en 1985. NetBEUI fue desarrollado para pequeñas LANs de 20 a 200 computadoras, asumiendo que la conexión con otros segmentos y mainframes se haría con traductores (gateways).

La versión de NetBEUI incluida en NT es la 3.0, y contiene las siguientes características:

- Optimizado para pequeñas LANs siendo el protocolo más rápido.

- Soporta mas de 254 sesiones.
- Autooptimizable.
- Buena protección contra errores.
- Uso de poca memoria.

No ruteable.

- Mal rendimiento en redes de area amplia

Los parámetros de NetBeui están localizados en el registry en:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Nbf

La interface NetBIOS provee la capa de mapeo NetBIOS entre las aplicaciones NetBIOS y los protocolos TDI compatibles.

La interface NetBIOS puede ser configurada en el Panel de Control en la opción de Network.

NDIS 3.0

NDIS (Network Device Interface Specification, Especificación de la Interface del Dispositivo de Red) es un estándar que permite convivir a los múltipels protocolos de transporte con los diversos adaptadores de red. NDIS permite a los componentes de los protocolos ser independientes de la tarjeta de red. Existen los estándares NDIS 2 (modo real), NDIS 3 (modo protegido) y NDIS 3.1 (modo protegido con soporte a Plug & Play). WFW y OS/2 soportan NDIS 2, Win95 NDIS 3.1 y NT NDIS 3.

El controlador de la tarjeta de red está en la parte inferior de la arquitectura de Windows NT. NDIS 3.0 permite un número ilimitado de tarjetas de red en una conmputadora y un número ilimitado de protocolos que pueden ser enlazados a una sola tarjeta de red.

NDIS 3.0 de acuerdo a los estándares establecidos por NT para un controlador de dispositivo:

- Se invoca como una función de C.
- Tiene acceso a las rutinas de ayuda.
- Es a 32 bits, portable y compatible con multiprocesamiento.

NDIS Wrapper

En Windows NT, NDIS ha sido implementado en un módulo llamado NDIS.SYS conocido como el NDIS wrapper.

El NDIS wrapper es una pequeña pieza de código alrededor de los controladores NDIS: El wrapper provee una interface uniforme entre los protocolos y los controladores NDIS y contiene

rutinas de soporte apra facilitar la creación de drivers NDIS: Las implementaciones anteriores de NDIS necesitaban de un Protocolo Manager (PROTMAN) para controlar el acceso a las tarjetas de red. La función principal del PROTMAN era controlar los parámetros en la tarjeta de red y los bindings hacia los stacks de los protocolos. Windows NT no necesita al PROTMAN porque los parámetros de la tarjeta y los bindings son guardados en el registry y configurados usando el icono de red del Panel de Control.

Como el NDIS wrapper controla la comunicación de los protocolos con la tarjeta de red, el protocolo se comunica con el NDIS wrapper en vez de hacerlo directamente con la tarjeta de red. Este es un ejemplo de la modularidad del modelo de capas. La tarjeta de red es independiente a los protocolos; así cambiar un protocolo no requiere cambiar la configuración de la tarjeta de red.

Mecanismos IPC para el Proceso Distribuido

En proceso distribuido, las tareas son divididas en dos partes, una en el cliente (front end) y otra en el servidor (back end). El propósito es mover el proceso de la aplicación desde la estación del trabajo del cliente hacia un sistema servidor para ejecutar grandes y poderosas aplicaciones como el acceso y consulta de bases de datos.

La parte del cliente (IPC-Client) de la aplicación normalmente es la interface del usuario de la aplicación. Esta se ejecuta en la estación de trabajo cliente utilizando una pequeña parte del poder de proceso. La parte del servidor (IPC-Server) normalmente requiere de gran capacidad de almacenamiento, poder de cómputo y hardware especializado.

Las diferentes formas de establecer la conexión entre las aplicaciones en NT se conocen como los mecanismos de comunicación entre procesos (Interprocess Communication Process, IPC).

Named Pipes and Mailslots

Los Named Pipes y los mailslots están actualmente implementados como sistemas de archivos. Así, en el Registry hay entradas para el NPFS (Named Pipe File System) y el MSFS (Mailslot File System). Como sistemas de archivos, ellos tienen la misma funcionalidad de otros sistemas de archivos como la seguridad. Además los procesos locales pueden usar named pipes y mailslots con otros procesos en la computadora lcoal sin accesar los componentes de red. El accseo

remoto a los named pipes y mailslots, así como por los otros sistemas de archivos, es realizado a través del redirector.

Los named pipes utilizan una transmisión de mensajes orientados a la conexión permitiendo establecer una sesión entre las aplicaciones, compartiendo memoria y rectificando la transmisión/recepción de información. Windows NT provee una API especial para incrementar la seguridad al usar named pipes. Una característica añadida a los named pipes es la impersonalización, con ella el servidor puede adoptar el identificador de seguridad del cliente realizando solamente las funciones a las cuales el cliente tiene permiso.

La implementación de los mailslot en Windows NT es un subconjunto de la usada en OS/2 LAN Manager de Microsoft. Provee una transmisión de mensajes de broadcasts connectionless, por lo que no hay la garantía de haberse recibido el mensaje. Es muy usado para la idetnficación de otras computadoras y servicios en la red. El servicio de Computer Browser de NT utiliza mailslots.

NetBIOS

NetBIOS es una interface de programación estándar en el ambiente de desarrollo de aplicaciones cliente-servidor. NetBIOS ha sido usado como un mecanismo de IPC desde su introducción a principios de los 80s. A nivel de programación, capas superiores como los named pipes y RPC son superiores en flexibilidad y portabilidad.

Una aplicación cliente-servidor puede comunciarse sobre varios protocolos: NetBUI (NBF), NWLink NetBIOs (NWNBLink) y NetBios sobre TCP/IP (NetBT).

La interface NetBios provee la capa para mapear las aplicaciones NetBIOS con los protocolos TDI.

Windows Sockets

La API de los Windows Sockets proveen una interface estándar para varios protolocos con diferentes esquemas de direccionamiento, como TCP/IP e IPX. La API de los Windows Sockets fue desarrollado con dos objetivos. Uno migrar la interface sockets desarrollada por la Universidad de Berkeley, California en 1980, en los ambientes Windows NT provee a Windows Sockets en NWLink y TCP/IP.

Remote Procedure Calls (RPC)

EL RPC puede usar otros IPCs para establecer comunicaciones entre las computadoras con partes de la aplicación cliente servidor.

En un ambiente de red, las aplicaciones pueden ser divididas en procvesos separados ejecutados en diferentes computadoras. RPC permite ejecutar funciones potencialmente complejas en computadoras remotas incrementando la velocidad de respuesta de las aplicaciones . RPC es el método preferido por los desarroladores para escribir aplicaciones en NT por el mayor control sobre la comunicación que en los *Named pides.*

Las partes del RPC son:

- *Remote Procedure Stub (Proc Stub)* empaqueta las llamadas a ser enviadas al servidor por medio del RPC runtime.
- RPC Runtime *(RPC RT)* responsable de la comunicación entre la computadora local y la remota, incluyendo el paso de parámetros.
- *Application Stub (APP Stub)* recibe las requisiciones RPC del RPC RT, desempaqueta el paquete y hace la llamada al Remote Procedure apropiado.
- *Remote Procedure* el procedimiento actualmente usado a través de la red.

El RPC Usado en NT es compatible con la especificación distributed computing environment (DCE) de la Open Software Foundation (OSF). NT puede usar RPC para interoperar con cualquier otra estación de trabajo que soporte este estándar.

Network Dynamic Data Exchange (Net DDE)

Net DDE provee capacidades de comparticion de información abriendo dos pipe unilaterales entre las aplicaciones. Net DDE es una extensión del *Dynamic Data Exchange (DDE)* y puede ser usado entre dos computadoras a través de la red.

El servicio Net DDE no se inicializa automáticamente, debe ser inicializado utilizando Servicios dentro del Panel de Control, el comando NET START desde la línea de comandos, o utilizando el Server Manager.

Componentes para compartir Archivos e Impresoras

Los servicios de compartición de archivos e impresoras se realizan por medio de dos servicios: el Workstation (Redirector) y el Server. Ambos servicios se ejecutan a 32 Bits.

El Servicio de Workstation

Todas las requisiciones del modo usuario son atendidas por el servicio de Workstation y transferidas al redirector en modo protegido (Kermel mode). Este servicio consta de dos componentes:

- La interface en modo usuario.
- El redirector (RDR.SYS), sistema de archivos que interactua con los componentes inferiores de red a través de la interface TDI.

Dependencias del Servicio de Workstation

El servicio de *Workstation* es dependiente de los siguientes componentes:

- Un protocolo que soporte la interface TDI debe estar inicializado.
- *Multiple Universal Naming Convention Provider* (MUP)

El servicio de Workstation (Redirector) como un Sistema de Archivos

El redirector es un componente a través del cual una computadora accesa a otra. El redirector de NT permite la conexión con NT, WFW, LAN Manager, LAN Server y otros servidores MS-Net. El redirector se comunica con los protocolos a través de la interface TDI.

El redirector está implementado como un sistema de archivos de NT. Esto tiene los siguientes beneficios:

- Permite a las aplicaciones llamar a una sola API (llamada I/O API) para accesar archivos en computadoras locales o remotas. Desde el punto de vista del Administrador de E/S, no hay diferencia entre accesar archivos almacenados en una computadora remota y los almacenados en el disco duro local.

- Al ejecutarse en modo protegido puede llamar directamente a otros controladores y componentes como el administrador del cache. Esto incrementa el rendimiento del redirector.
- Puede ser cargado y descargado de memoria dinámicamente como cualquier otro sistema de archivos.
- Puede coexistir fácilmente con otros redirectores.
-

Accesando a un Archivo Remoto

Cuando un proceso de NT trata de abrir un archivo que reside en una computadora remota ocurren los siguientes sucesos:

- El proceso llama al Administrador de E/S solicitando abrir un archivo.
- El Administrador de I/O distingue si el archivo es local o remoto. Si es local lo transfiere al sistema de archivos local FAT, NTFS o CDFS, en caso contrario, lo para al redirector.
- El redirector para la requisición a los controladores inferiores para transmitirla al *Server* remoto para su procesamiento.

El Servicio De Server

NT también incluye un componente llamado el Server el cual reside de la TDI. Como el redirector el Server está implemendado com un sistema de archivos e interactua directamente otros sistemas de archivos para responder las requisiciones I/O como leer o escribir un archivo.

El *Server* procesa las solicitudes de conexión del cliente (redirector), proporcionándole acceso a los recursos solicitados. Como el servicio de Workstation, el servicio de Server esta compuesto de dos partes:

- *Server*, es un servicio ejecutándose en el proceso SERVICES.EXE. A diferencia del servicio de Workstation no es dependiente del servicio de MUP, porque el Server no es un proveedor de UNC. El no trata de conectarse a otras computadoras, al contrario, otras computadoras se conectan con él.
- SRV.SYS, es un sistema de archivos que maneja la interacción con los niveles inferiores de la red y otros sistemas de archivos (FAT, NTFS, CDFS) para satisfacer las requisiciones de lectura o escritura de un archivo.

Procesando Requisiciones Remotas

Cuando el servicio de *Server* recibe una solicitud de lectura de un archivo local de una computadora remota, ocurren los siguientes pasos:

- Los controladores de red inferiores reciben la requisición y la transfieren al *Server.*
- El servidor transfiere la requisición de lectura del archivo al sistema de archivos local apropiado.
- El sistema de archivos llama al controlador de dispositivo de disco para accesar al archivo.
- Los datos son regresados al sistema de archivos local y este al *Server.*
- El servidor retorna los datos a los controladores de red inferiores para devolver los datos al cliente.

Multiple Universal Naming Convention Provider (MUP)

Las aplicaciones residen arriba del Redirector y el Server en modo usuario. Como las otras capas de la arquitectura de red de NT. Existe una sola interface para accesar a los recursos de red, independientemente del redirector o redirectores instalados en el sistema. Esto es hecho a través de dos componentes: el *Multiple Universal Naming Convention Provider* (MUP) y el *Multiprovider Router* (MPR).

Cuando las aplicaciones hacen llamadas de E/S conteniendo nombres UNC, estas requisiciones son pasadas al MUP. El MUUP selecciona el redirector apropiado para manejar la requisicion de E/S.

La Universal Naming Convention (UNC) es una forma convencional para nombrar a los servidores de red y sus recursos compartidos. Los nombres UNC comienzan con dos diagonales invertidas seguidas del nombre del servidor. El resto de los campos en el nombre son separados por una sola diagonal. Un típico nombre UNC aparece como sigue:

\\servidor\recurso{\subdirectorio}{nombre del archivo.}

No todos los componentes de un nombre UNC necesitan ser usados para cada comando; solamente el recurso necesario. Por ejemplo, dir \\server\share puede ser usado para obtener una lista de directorios de la raíz del recurso compartido especificado.

Uno de los mayores propósitos de diseño para el ambiente de red de NT fue proveer una plataforma abierta la cual otros desarrolladores pueden integrar servicios de red. MUP es una parte vital que permite a múltiples redirectores coexistir en una sola computadora al mismo tiempo. MUP libera a las aplicaciones de administrar a los redirectores ellas mismas.

A diferencia de la interface TDI, MUP es actualmente un controlador. Mientras TDI define la forma de comunicarse con otro componente de una capa diferente, MUP define formas de accesar a los redirectores los cuales actúan como UNC *providers.*

Las requisiciones de E/S de aplicaciones con nombres UNC son recibidas por el Administrador de E/S el cual pasa las requisiciones al MUP. Si el MUP no ha visto el nombre UNC en los 15 minutos pasados, el MUP enviará el nombre a cada uno de los UNC providers (redirectores) registrados. (Por esto el MUP es un prerequisito del servicio de Workstation. Una de las principales tareas del servicio de Workstation durante la inicialización es registrarse con el MUP. El MUP busca al redirector con la prioridad más alta registrada intentando establecer una conexión durante 15 minutos de un nombre UNC el MUP lo olvida y la siguiente requisición volvera a negociarse.

No todos los programas usan nombres UNC en sus requisiciones de E/S. Algunas aplicaciones utilizan WNet APIs (APIs de red de Win32) El Multi-Provider router (MPR) fue creado para soportar estas aplicaciones.

El MPR recibe comandos WNet, determina el redirector apropiado, y le transfiere el comando solicitado. Debido a que los desarrolladores de red utilizan diferentes interfaces para comunicarse con otro redirector, hay una serie de *provider* DLLs entre el MPR y los redirectores. El *provider* DLLs contiene una interface estándar para que el MPR pueda comunicarse con ellos, y ellos sepan como aceptar la requisición del MPR y comunicarla con su redirector respectivo.

Capitulo 3

Instalando Componentes de Red

La instalación y configuración de los componentes de red de NT sé realizan utilizando la opción de Red en el Panel de Control. Un componente de red puede ser añadido, configurado, actualizado y removido. También aquí se instalan los controladores de las tarjetas de red.

Además este cuadro de diálogo puede ser usado para cambiar el nombre de la computadora y el grupo de trabajo o dominio al cual pertenece.

Propósito y uso de las opciones de Binding

La arquitectura de red de NT consiste de una serie de capas. Los componentes en cada capa proveen una función específica a las capas de arriba y abajo de este. La arquitectura finaliza en la tarjeta de red, la cual mueve la información entre las computadoras a través del medio físico usado.

Un *Binding* es la liga que permite la comunicación entre los componentes de red de las diferentes capas. Es posible ligar un componente de red con uno o más componentes superiores o inferiores. Los servicios de cada componente pueden ser utilizados por los componentes ligados a él.

Cuando se añaden componentes de red, NT automáticamente liga todos sus componentes relacionados.

Configurando los Bindings *de Red*

Los bindings se configuran en el botón Bindings de la opción de Red. El cuadro de diálogo de Bindings de red, muestra los bindings de los componentes instalados como una serie de rutas desde los servicios hasta los controladores de red.

Los Bindings pueden ser habilitados o deshabitados de acuerdo a los componentes usados en el sistema.

Los bindings pueden ser usados para optimizar el uso del sistema en red. Por ejemplo, si se tiene instalado TCP/IP y NetBEUI y la mayoría de los servidores solo utilizan TCP/IP, el binding de Workstation debería ser ajustado para que TCP/IP sea el primer binding listado para tratar de establecer las conexiones con él.

Componentes de Red predeterminados

- Interfaces NetBIOS
- TCP/IP
- Servicio de *Workstation*
- Servicio de Server
- Servicio de *Computer Browser-Microsoft Network Browser Service*
- Controlador de la tarjeta especificada
- *RPC Name Service Provider*

Conclusión de la Arquitectura de Red

Las aplicaciones generan dos tipos de comandos que causan actividad en la red: cualquier comando de E/S con nombres UNC y comandos WNet. Los comandos UNC son enviados al MUP (modo protegido) y los comandos WNet al MPR, para seleccionar al redirector (UNC provider) adecuado.

Una computadora obtiene acceso a otra computadora por medio del redirector. El redirector se comunica a los protocolos enlazados a la capa TDI. La capa TDI es una capa de enlace entre los sistemas de archivos y los protocolos. Las capas son usadas para proveer una plataforma uniforme para el desarrollo de otros componentes.

NT incluye cuatro protocolos: TCP/IP, NetBEUI, NWLink y DLC. NDIS 3.0 provee otra capa de enlace que hace posible la interoperación entre componentes y diferentes capas fácilmente. Además para proveer compartición de archivos e impresos, NT provee cinco mecanismos para el desarrollo de aplicaciones distribuidas. Los *Named pipes* utilizan otros mecanismos IPC para transferir funciones y datos entre computadoras cliente y servidor.

Seguridad En Redes

Introduccion

El tema de la seguridad de las redes está definitivamente sobre el tapete y requiere soluciones de corto plazo. Cualquier medida de seguridad corporativa, inclusive la incorporación de complejos dispositivos de avanzadas tecnologías, podría ser improductiva si no se enmarca dentro de una estrategia organizacional que establezca las políticas de seguridad, las que deben considerar aspectos tales como autentificación, encriptación, control de acceso físico y lógico, protecciones contra virus y la aplicación de estadísticas y cálculo de probabilidades, si así se requiere, sobre las redes corporativas y, por cierto, al elemento humano que la compone. El acceso no autorizado, daño o mal uso de la información de las empresas se puede traducir en pérdidas financieras inmediatas y, en el mediano plazo, afectar su posición competitiva en el mercado con todos los perjuicios que ello podría significar. Para enfrentar este desafío, la empresa debe establecer sus propias políticas de seguridad, basadas en medidas tecnológicas y administrativas, cimentadas en la identificación de los riesgos, vulnerabilidades e impactos organizacionales a la que se expone a través de sus redes de comunicaciones.

Las redes abiertas, tales como Internet, son hoy en día una herramienta imprescindible para las empresas, sin embargo representan una amenaza constante a su seguridad, por lo que la Conectividad a estas redes requiere una adecuada evaluación de riesgos, de manera de tomar anticipadamente las medidas de seguridad e incorporar los elementos tecnológicos y medidas administrativas necesarias para minimizar los accesos no deseados. Existen innumerables ejemplos que muestran cómo costosos y complejos sistemas y dispositivos de seguridad han sido vulnerados, lo que confirma la tesis que la seguridad debe ser abordada como un todo y en forma integral en la organización. La sola incorporación de dispositivos Corta Fuego (firewall), no garantiza la seguridad de la información, por lo que su implementación debe ser parte de un conjunto de políticas de seguridad organizacional, las cuales son particulares a cada empresa en función de sus necesidades.

La elaboración de una estrategia de seguridad corporativa debe considerar la identificación de amenazas y riesgos, sus vulnerabilidades y el grado de exposición a ellas, una evaluación de los

impactos y sus costos organizacionales. Estas tareas requieren del apoyo de expertos independientes.

Firewall

Los Firewalls son barreras creadas entres redes privadas y redes públicas como Internet. Originalmente, fueron diseñados por los directores de informática de las propias empresas, buscando una solución de seguridad. Más recientemente, los sistemas de seguridad proporcionados por terceras empresas, son la solución más escogida.

Los Firewalls son simples en concepto, pero estructuralmente complejos. Examinan todo el tráfico de entrada y salida, permitiendo el paso solamente al tráfico autorizado. Son diseñados de forma que todo lo que no es expresamente autorizado, es prohibido por defecto.

Un Firewall:

protege la red interna de una organización, de los usuarios que residen en redes externas.

- permite el paso entre las dos redes a sólo los paquetes de información autorizados.

Pueden ser usados internamente, para formar una barrera de seguridad entre diferentes partes de una organización - como por ejemplo a estudiantes y usuarios administrativos de una universidad.

Reflejan un número de decisiones de diseño dependiendo del acceso, seguridad y transparencia.

Es diseñado para entregar un acceso seguro a los servicios ofrecidos por la red Internet con un mínimo esfuerzo adicional. La calidad de este "mínimo esfuerzo" es llamada la "transparencia" que significa que un usuario puede usar un gran número de software comercial sin modificaciones adicionales.

Puede mejorar significativamente el nivel de seguridad en la red y reducir los riesgos filtrando la falta de seguridad inherente en los servicios de Internet.

Implementa una política de acceso a la red, forzando que todas las conexiones a ésta, se realicen a través de él, mientras son examinadas y evaluadas.

Usan Tres Tecnologías Diferentes, son: Filtro de paquetes, Gateways a Nivel de Circuitos y Gateways a Nivel de Aplicación. A veces se usan de forma separada, a veces conjuntamente. El Filtro

de Paquetes trabaja a nivel TCP/IP y no tienen control de qué aplicaciones están filtrando. Las Gateways a Nivel de Circuitos interceptan las sesiones y las pasan a través de los Firewall. Las Gateways a Nivel de Aplicación operan al nivel más alto, controlando las aplicaciones que han generado los paquetes.

Modelo de Seguridad de Los Recursos de NT

NT protege sus recursos (archivos, impresoras y aplicaciones); restringiendo el acceso de los usuarios a ellos. A este modelo se le conoce como: seguridad por usuario; mucho más poderosa y flexible que la seguridad por recurso de Windows For Workgroups donde una clave de acceso protege el recurso.

Windows NT incorpora diversos métodos de seguridad. Estos métodos proporcionan numerosas formas de controlar la actividad de los usuarios, sin impedirles por ello el acceso a los recursos que necesitan. El fundamento de la seguridad de Windows NT es que todos los recursos y acciones están protegidos por el control de acceso discrecional, que significa que es posible permitir a determinados usuarios acceder a un recurso o realizar una determinada acción, y al mismo tiempo impedírselo a otros usuarios. Además, la seguridad es muy granular. Por ejemplo, es posible establecer distintos permisos sobre diferentes archivos de un mismo directorio.

Con Windows NT, la seguridad está integrada en el sistema operativo desde el principio, en lugar de incorporarse al mismo como un componente adicional. Esto significa que los archivos y otros recursos pueden protegerse incluso de los usuarios que trabajan en la misma computadora donde se encuentre el recurso, así como de los usuarios que accedan al recurso a través de la red. Windows NT incorpora medidas de seguridad incluso para las funciones básicas del sistema, como el propio reloj del ordenador.

Windows NT Server ofrece asimismo un modelo lógico de administración que es un gran auxiliar cuando se necesita administrar de un modo eficaz una red de gran tamaño. Cada usuario sólo necesita disponer de una única cuenta, que se almacena de modo centralizado. Esta única cuenta puede proporcionar al usuario el acceso a cualquier recurso de la red, independientemente del lugar donde se encuentre. De este modo, Windows NT facilita a los administradores de la red la administración de las cuentas y, al mismo tiempo, simplifica el uso de la red por parte de los usuarios.

Conceptos de dominios y relaciones de confianza

La unidad básica de la administración centralizada y la seguridad en Windows NT Server es el dominio. Un dominio es un grupo de servidores que ejecutan Windows NT Server y que, en cierto modo, funcionan como un único sistema. Todos los servidores con Windows NT Server de un dominio utilizan el mismo conjunto de cuentas de usuario, por lo que sólo es necesario escribir una vez la información de una cuenta de usuario para que todos los servidores del dominio reconozcan dicha cuenta.

Las relaciones de confianza son vínculos entre dominios, que permiten realizar una autenticación transparente, en virtud de la cual un usuario sólo 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 (ordenadores) con Windows NT reconocerán todas las cuentas de usuario, por lo que el usuario tendrá que iniciar una sesión y facilitar una contraseña sólo una vez para acceder a cualquier servidor de la red.

Dominios: unidades administrativas básicas

La agrupación de computadoras (ordenadores) 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 los servidores del dominio que funcionen como controlador principal de dominio o como controlador de reserva mantendrá una copia de esta base de datos. Ello significa que los administradores sólo necesitarán administrar una cuenta para cada usuario y que cada usuario sólo tendrá que utilizar una cuenta (y recordar una sola contraseña). Al extender la unidad administrativa desde la computadora individual hasta todo un dominio, Windows NT Server ahorra tiempo y esfuerzo tanto a los administradores como a los usuarios.

La segunda ventaja de los dominios es la comodidad que brindan al usuario: cuando un usuario examine la red para buscar recursos disponibles, observará que está agrupada en dominios, en lugar de ver los servidores e impresoras de toda la red al mismo tiempo. Esta ventaja de los dominios es idéntica al concepto de grupo de trabajo que incorpora Windows para Trabajo en Grupo. Además, los

dominios de Windows NT Server son compatibles con los grupos de trabajo de Windows para Trabajo en Grupo. Si desea obtener más información sobre Windows para Trabajo en Grupo, consulte la sección "Interacción con computadoras con Windows para Trabajo en Grupo", más adelante en este mismo capítulo.

Nota:

No debe confundirse el concepto de dominio de Windows NT Server con los dominios del protocolo de red TCP/IP. Un dominio TCP/IP describe parte de la Internet TCP/IP y no tiene nada que ver con los dominios de Windows NT Server.

Relaciones de confianza: vínculos entre dominios

Estableciendo relaciones de confianza entre los dominios de la red, podrá permitir que determinadas cuentas de usuario y grupos globales puedan utilizarse en dominios distintos de aquél en el que estén situadas dichas cuentas. (Si desea obtener más información sobre los grupos globales, consulte la sección "Utilidad de los grupos", más adelante en este mismo capítulo). 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 acceder a cualquier computadora de la red y no únicamente a las computadoras de uno de los dominios.

Cuando establezca una relación de confianza entre dominios, uno de los dominios (el dominio que confía) confiará en el otro (el dominio en el cual se confía).

A partir de entonces, el dominio que confía reconocerá a todos los usuarios y cuentas de grupo 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 ese 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 ilustración siguiente, los dominios Finanzas y Envío confían mutuamente entre sí 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 Ventas podrán utilizarse en el dominio Producción pero las cuentas de Producción no podrán emplearse en Ventas.

La confianza entre dominios no es una operación transitiva. Por ejemplo, si Ventas confía en Producción y Producción confía en Finanzas, Ventas no confiará automáticamente en Finanzas.

Si desea que Ventas confíe en Finanzas (para de este modo poder utilizar las cuentas de Finanzas en el dominio Ventas), deberá establecer una relación de confianza adicional directamente entre estos dominios.

Constitución de un dominio

El requisito mínimo de un dominio es un servidor con Windows NT Server, que actúa como controlador principal de dominio y que almacena la copia principal de la base de datos de grupos y usuarios del dominio. Si se desea, un dominio puede incluir también otros servidores

adicionales que ejecuten Windows NT Server (que actúen como controladores de reserva),

computadoras con Windows NT Server que actúen como servidores estándar, servidores con LAN

Manager 2.x, clientes de Windows NT Workstation y otros clientes, por ejemplo aquellos que ejecuten Windows para Trabajo en Grupo y MS-DOS. En las secciones siguientes se describen con mayor detalle cada uno de estos componentes del dominio.

Controlador principal de dominio

El controlador principal de dominio de un dominio de Windows NT Server debe ser un servidor que ejecute Windows NT Server. Cualquier modificación a la base de datos de grupos y usuarios del dominio deberá realizarse en la base de datos que está almacenada en el controlador principal de dominio. Sin embargo, no es necesario recordar el nombre de la computadora del controlador principal de dominio para cada uno de los dominios. Cuando utilice el Administrador de usuarios para dominios con el fin de modificar la base de datos de usuarios, sólo necesitará seleccionar el nombre del dominio en el cual desee realizar los cambios. El cambio se realizará Automáticamente en el controlador principal de dominio. El Administrador de usuarios para dominios no permite modificar directamente la base de datos de usuarios de un servidor de dominio que no sea el controlador principal de dominio.

Controladores de reserva

Los controladores de reserva que ejecuten Windows NT Server almacenarán también copias de la base de datos de cuentas del dominio. La base de datos de cuentas del dominio estará duplicada en todos los controladores de reserva del dominio.

Todos los controladores de reserva, además del controlador principal de dominio, podrán procesar las peticiones de inicio de sesión por parte de las cuentas de usuario del dominio. Cuando el dominio reciba una petición de inicio de sesión, el controlador principal de dominio o cualquier controlador de reserva podrá autentificar el intento de inicio de sesión.

Es conveniente que en un dominio haya uno o varios controladores de reserva, además del controlador principal de dominio. Estos servidores adicionales proporcionan un mecanismo de

seguridad: si el controlador principal de dominio no está disponible, un controlador de reserva podrá ser promovido al puesto de controlador principal de dominio, lo cual permitirá al dominio seguir funcionando. La existencia de varios controladores de dominio permite también distribuir la carga de trabajo relacionada con las peticiones de inicio de sesión, lo cual resulta especialmente útil en dominios con un gran número de cuentas de usuario.

Si en un dominio hay varios servidores que ejecutan Windows NT Server, uno de ellos será el controlador principal de dominio. Debe configurar al menos otro servidor como controlador de reserva. Si el dominio tiene servidores situados en distintas ubicaciones físicas conectadas mediante un vínculo de red de área amplia (WAN), cada ubicación deberá tener al menos un controlador de reserva.

Servidores

Además de los controladores principales y de reserva de dominio, existe otro tipo de servidor que ejecuta Windows NT Server. Se trata de servidores designados como "servidores", no como controladores de dominio, durante la instalación de Windows NT. Estos servidores pueden participar en un dominio, si bien no es necesario.

Un servidor que participa en un dominio no consigue realmente una copia de la base de datos de usuarios del dominio, pero tiene acceso a todas las ventajas de la base de datos de usuarios y grupos del dominio. Cuando asigne derechos de usuario y permisos de objetos, o cuando cree grupos

locales, dispondrá de cuentas de usuario del dominio en el que participa el servidor, así como de todos los dominios en los que confíe el dominio en el que participe el servidor. Estas cuentas de usuario pueden acceder al servidor y utilizar sus recursos, si usted lo permite.

Un servidor que no participa en ningún dominio sólo tiene su propia base de datos de usuarios y procesa por su cuenta las peticiones de inicio de sesión. No comparte la información sobre cuentas con ninguna otra computadora y no puede utilizar cuentas de ningún otro dominio. En un servidor que funciona de esta forma, sólo las cuentas de usuario creadas en el propio servidor podrán iniciar una sesión en dicho servidor; además, sólo se les concederán derechos y permisos en ese servidor. Estos servidores tienen los mismos tipos de cuentas de usuarios y grupos que las computadoras con Windows NT Workstation, no los tipos de cuentas existentes en los dominios de Windows NT Server.

Habrá veces, como en las siguientes situaciones, en las que se necesitara configurar una computadora como un servidor, en lugar de hacerlo como un controlador de reserva:

- Si el servidor realiza tareas extremadamente críticas en cuanto a tiempo y no se desea que pierda tiempo en autorizar intentos de inicio de sesión en el dominio o que reciba una copia duplicada de una base de datos de usuarios del dominio.
- Si se desea que el servidor tenga distintas cuentas de administrador o de usuarios que los restantes servidores de un dominio. Por ejemplo, podría tener una persona dedicada a administrar una base de datos SQL Server. Si convierte el servidor SQL en un servidor estándar, podrá hacer que dicha persona sea un administrador del servidor SQL. De esta forma, esa persona podrá administrar ese servidor pero no tener control sobre la base de datos de usuarios del dominio o sobre sus demás servidores.
- Si es posible que el servidor se mueva a otro dominio en el futuro. Es más sencillo mover un servidor de un dominio a otro que mover un controlador de reserva de un dominio a otro.

Servidores con LAN Manager 2.x

Los servidores con LAN Manager 2.x pueden funcionar dentro de un dominio cuyo controlador principal ejecute Windows NT Server. Sin embargo, un servidor con LAN Manager 2.x no puede ser un controlador principal dentro de un dominio que ejecuta Windows NT Server, ya que

LAN Manager 2.x no incorpora todos los tipos de información que contienen las cuentas de Windows NT Server.

Los servidores con LAN Manager 2.x almacenarán una copia de la base de datos de seguridad del dominio. Podrán validar los intentos de inicio de sesión que realicen computadoras con Windows para Trabajo en Grupo o software de estación de trabajo LAN Manager 2.x, pero no podrán validar los intentos de inicio de sesión que realicen los usuarios de Windows NT. No es aconsejable recurrir únicamente a servidores con LAN Manager 2.x como servidores de reserva dentro de un dominio que ejecuta Windows NT Server, ya que no pueden autentificar las peticiones de inicio de sesión desde computadoras con Windows NT Workstation y no podrán ser promovidos a controladores principales dentro de un dominio de Windows NT Server.

Computadoras con Windows NT Workstation

Para cada una de las computadoras con Windows NT Workstation de la red, sé podra optar entre integrar la estación de trabajo en un dominio o en un grupo de trabajo. En la mayoría de los casos, lo más conveniente será integrar cada una de las estaciones de trabajo en un dominio.

Este es el único modo de que un usuario con cuenta en un dominio de Windows NT Server pueda iniciar una sesión con esa cuenta en una computadora con Windows NT Workstation.

Una computadora con Windows NT Workstation que forme parte de un dominio no obtendrá en realidad una copia de la base de datos de usuarios del dominio. Sin embargo, podrá aprovechar las ventajas que ofrece la base de datos de grupos y usuarios del dominio.

Una computadora con Windows NT Workstation perteneciente a un grupo de trabajo dispondrá de su propia base de datos de usuarios y procesará personalmente las peticiones de inicio de sesión. Ninguna de las computadoras de un grupo de trabajo comparte información sobre cuentas. En este tipo de estaciones de trabajo, sólo será posible iniciar sesiones o recibir derechos o permisos para la estación de trabajo cuando se utilicen cuentas de usuario que hayan sido creadas en la propia estación de trabajo.

Estaciones de trabajo con MS-DOS

Las computadoras con MS-DOS no pueden almacenar cuentas de usuario, por lo que no es necesario que pertenezcan a dominios como sucede con las computadoras con Windows NT.

Normalmente, cada computadora con MS-DOS dispondrá de un conjunto de dominios predeterminado para examinar la red. Si un usuario de una computadora con MS-DOS posee una cuenta en el dominio, podrá configurar cualquier dominio como dominio examinador de la computadora del usuario; no es necesario que sea el dominio que contiene la cuenta del usuario.

Operación de los sistemas de seguridad en Windows NT

A continuación se analiza la forma de operar de los esquemas de seguridad utilizados en Windows NT. Estos operan en situaciones tan diversas desde el acceso que el usuario quiere hacer de los recursos hasta la proteccion de los mas minimos detalles en el sistema.

Objetos de NT

Todos los recursos en NT son representados como objetos que pueden ser accesados solo por usuarios y servicios autorizados de NT. Un objeto en NT está definido como un conjunto de datos usados por el sistema, y un conjunto de acciones para manipular esos datos. Por ejemplo, un objeto archivo consiste en datos almacenados en un archivo y un conjunto de funciones que permiten leer, escribir o borrar el archivo. Esta definición puede ser aplicada para cualquier recurso usado por el sistema, incluyendo memoria, impresoras y procesos.

Prácticamente todo en NT está representado para el sistema operativo como un objeto. Los siguientes son los objetos más usados:

- Directorios
- Impresoras
- Puertos
- Symbolic links
- Ventanas
- Archivos
- Recursos compartidos en red
- Procesos
- Dispositivos
- Threads

Access Control Lists (ACL)

Todas las funciones usadas para accesar un objeto, (por ejemplo un archivo abierto), son directamente asociadas con un objeto específico. Además los usuarios y grupos con la capacidad de usar la función también son asociados dentro del objeto. Solo los usuarios con los derechos apropiados podrán usar las funciones del objeto. Como resultado, funciones de un proceso no pueden accesar objetos de otros procesos. Esta característica de los objetos provee seguridad integrada. El acceso a cada objeto es controlado a través del *Access Control Lists (ACL)*

El ACL contiene las cuentas de usuarios y grupos con permiso de accesar el objeto. Cuando un usuario quiere accesar el objeto, el sistema checa su identificador de seguridad y de los grupos a los que pertenece con el ACL para determinar o no acceso a la función requerida.

Access Control Entries

Una cuenta de usuario, grupo, o servicio y el permiso sobre un objeto forman un Access Control Entries (ACEs). Un ACL es un conjunto de ACEs.

Dentro del ACL primero se encuentran los ACEs que niegan el acceso al recurso, con la finalidad de calcular más rapidó los permisos de acceso sobre un objeto.

Acceso seguro a los Recursos

Cuando el usuario desea accesar a un recurso, ocurren los siguientes eventos:

1. El usuario se valida *(Mandatory Logon)*.
2. Creación del Access Token.
3. Solicitud de acceso al recurso.
4. Evaluación de los permisos.
5. Acceso (o no acceso) al recurso.

Mandatory Logon

Los usuarios de NT requieren un nombre y una clave de acceso para validarse dentro de una computadora. Este proceso de *Mandatory Logon* no puede deshabilitarse.

Access Tokens

Cuando el usuario se valida en NT, el susbsistema de seguridad crea un objeto y un proceso para el usuario llamado: access token. El *access token* incluye información como el nombre del

usuario y los grupos a los que se pertenece. Mientras el usuario este validado en el sistema, el es identificado por su *access token.*

Security IDS

Aunque los usuarios y grupos están representados por nombres, la computadora los almacena con un identificador de seguridad (SID). Un SID es un identificador único para representar usuarios, grupos o cualquier tipo de autorización de seguridad. Los SIDs son usados dentro del *access token* y el ACL en vez del nombre del usuario y el grupo. El SID está representado con un número único como:

S-1-5-21-76965814-1898335404-322544488-1001

Como resultado de identificar a los usuarios con SIDS, una misma cuenta de usuario creada varias veces será representada con un SID único, cuando se borra una cuenta aunque se vuelva a crear con las mismas características el SID es diferente, por lo tanto, esta nueva cuenta no tendrá acceso a los mismos de la cuenta anterior.

Evaluación de los Permisos

Cuando el proceso del usuario trata de accesar a un objeto, el subsistema de seguridad compara el SID del usuario almacenado en el access token contra el ACL, para validar o negar el permiso sobre el recurso. Esta evaluación se realiza de la siguiente forma:

1. Se revisan los ACE desde el principio, para ver si se niega el acceso al usuario o alguno de los grupos a los cuales pertenece, el tipo de acceso requerido. De encontrarse alguna coincidencia el proceso finaliza.
2. Checa para ver si el acceso requerido ha sido otorgado al usuario o alguno de los grupos a los cuales pertenece.
3. el Paso 1 y 2 se repiten para cada una de las entradas del access token hasta encontrar un acceso denegado, se acumulan los permisos necesarios para el acceso requerido o se revisan todas las entradas del *access token.*

Como se observa un permiso denegado (No Access) se antepone a cualquier permiso otorgado (Incluso Full Access).

Optimización de la Evaluación de Permisos

Cuando NT otorga el acceso a un objeto, al proceso del usuario (access token) se le asigna un apuntador (Handle). Este apuntador un identificador usado internamente por el sistema para identificar y accesar el recurso. El sistema también crea una lista de permisos la lista de derechoas de acceso.

Así el ACL solo es revisado cuando se abre el objeto. Las subsecuentes acciones se checarán de acuerdo a la lista de derechos del proceso del usuario.

Sistemas de Archivos

Al elegir un sistema de archivos, es importante mencionar que se pueden tener particiones múltiples con formatos diferentes de texto de archivo sobre NT dependiendo de las necesidades actuales de compatibilidad y seguridad de la computadora.

Sistema de Archivos	Sistemas Operativos Soportados
FAT	DOS, Windows NT, y OS/2
HPFS	OS/2 y Windows NT
NTFS	Windows NT

```
File Allocation Table (FAT)
High-Performance File System (HPFS)
New Technology File System (NTFS)
```

File Allocation Table (FAT)

El sistema FAT de archivos se usa ampliamente y es soportado por una variedad de sistemas operativos tales como DOS, NT y OS/2. Si usted planifica usar dual boot en la computadora con NT y DOS la partición de istema debe formatearse con el sistema de archivos FAT.

Convenciones de Nombres en Fat

El sistema FAT de archivos en DOs utuliza una convención para nombrar a los archivos y directorios de tres partes: nombre del archivo de hasta ocho caracteres, un periodo (.) separador, y una extensión de tres caracteres.

La siguiente tabla describe algunas características básicas de FAT en NT.

Longitud del Nombre del Archivo y del Directorio	255
Tamaño del archivo	4 GB (232 bytes)
Tamaño de la partición	4 GB(232 bytes)
Atributos	Solo lectura, Archivo, Sistema y Oculto
Sistema de Directorios	Lista ligada
Accesible a través de	MS-DOS, OS/2 y Windows NT

Consideraciones del Sistema de Archivos FAT

- No se puede deshacer el borrado de ningún archivo de cualquier sistema operativo porque las utilerías de recuperación accesan directamente al hardware y eso es invalido dentro de NT. Sin embargo, si los archivos son borrados sobre particiones FAT, los archivos pueden ser recuperados desde DOS.
- FAT tiene un consumo mínimo (menos de 1 MB)
- FAT es el sistema de archivos más eficiente en particiones de menos de 200 Megabytes. El rendimiento disminuye con un gran número de archivos, porque FAT utiliza una estructutra de directorios con listas ligadas. Si la cantidad de datos aumenta, el archivo comienza a fragmentarse en el disco duro, y el proceso de lectura se hace más lento.
- FAT es el sistema de archivos necesario en computadoras ARC (computadoras con procesadores RISC)
- El acceso a los archivos y directorios no puede ser protegido con la seguridad de NT.

High-Performance File System (HPFS)

HPFS es el mismo sistema de archivos usado en OS/2, NT no le provee mejoras. Típicamente es usado durante la migración de OS/2 hacia NT.

Convenciones de Nombres en HPFS

- Soporta nombres largos de hasta 254 caracteres con multiples extensiones.
- Los nombres preservan las mayúsculas y minúsculas, pero no hace diferenciación.
- Los nombres pueden contener cualquier caracter (incluyendo espacios) excepto: ? " / \ < > * |

Consideraciones del Sistema de Archivos HPFS

- Los nombres largos no son visibles en las aplicaciones Windows 16 ni DOS ejecutándose en NT, porque no se tiene soporte a nombres cortos.
- Las particiones HPFS son normalmente usados para migrar de OS/2 hacia NT.
- HPFS no soporta adecuadamente discos muy grandes. Hay una degradación del rendimiento a partir de los 400 MG.
- HPFS consume aproximadamente 2MG para el sistema de archivos.
- Una partición HPFS no puede ser protegida con la seguridad NT.

La siguiente tabla describe algunas características básicas de HPFS:

Longitud del Nombre del Archivo y del Directorio	254
Tamaño del archivo	4GB (232 bytes)
Tamaño de la partición	4TB (teóricamente (241 bytes),
	7.8 GB actual (debido a la geometría de los discos)
Atributos	Sólo lectura, Archivo, Sistema, Oculto y *extendidos
Sistema de directorios	Arbol Binario
Accesible a través de	OS/2 y Windows NT

*permite atributos adicionales representados como textos y pueden ser usados de manera arbitraria por las aplicaciones, por ejemplo iconos para el archivo o el nombre de la aplicación asociada.

New Technology File System (NTFS)

NTFS es el sistema de archivos más usados en NT por varias razones, principalmente la seguridad. Sin embargo, puede haber casos en donde es necesario usar otros sistemas de archivos como por compatibilidad con otros sistemas en una NT Workstation con arranque dual.

Otra ventaja de NTFS es el soporte a particiones de hasta 16 hexabytes, muy superior a otros sistemas de archivos. Sin embargo el tamaño mínimpo de una partición es de 5MB.

Propósitos de Diseño de NTFS

- Proveer una mejor confiabilidad (suficiente para servidores de archivos y sistemas de misión crítica).
- NTFS es un sistema de archivos recuperables porque mantiene un registro de las transacciones efectuadas en el sistema de archivos. Esta información puede ser usada para reintentar o deshacer una operación fallida debido a algún error, pérdidas de corriente, etc.
- Además NTFS soporta Hot Fixing. Hot fixing es una técnica para la resolución de problemas. Por ejemplo, si un error ocurre por algún sector dañado, el sitema de archivos mueve la información a un sector diferente y marca el sector como defectuoso, sin que la aplicación se de cuenta.
- Soporta el modelo de seguridad de NT, permite configurar permisos y registro de auditoría sobre archivos y directorios.
- Soporta los requerimientos de POSIX: distingue nombres con mayúsculas y minúsculas, registra la última hora de acceso al sistema y soporta *hard links* (dos nombres de archivos en diferentes directorios, apuntan a la misma información).

Convenciones de Nombres en NTFS

- Los nombres de archivos pueden ser de hasta 255 carácteres de longitud, incluyedo varias extensiones.
- Se preservan las mayúsculas y minúsculas aunque NTFS no hace distinción.
- Los nombres pueden contener cualquier caracter (incluyendo espacios)excepto: ? " / \ < > * | :

Consideraciones del Sistema de Archivos NTFS

- La recuperación está diseñada en NTFS para que los usuarios no necesiten ejecutar utilerías para la recuperación de partición NTFS.
- NTFS provee seguridad en archivos y directorios, pero no encripción de archivos.
- No hay forma de recuperar un archivo borrado.
- NTFS consume más recursos que FAT o HTPS.
- El tamaño mínimo recomendado de las particiones es de 50MG.
- No es posible formatear discos flexibles con NTFS por el consumo de recursos.
- La fragmentacion es enormemente reducida en particiones NTFS.NTFS siempre trata de localizar un bloque contiguo de espacio en disco lo suficientemente grande para almacenar el archivo completo. Una vez almacenado en disco. Para defragmentar el archivo, se recomienda copiarlo a otro disco y de ahí al disco original. Al copiarse al archivo original, NTFS iantentará localizar un bloque contiguo de espacio en disco.

La siguiente tabla describe algunas características básicas de NTFS.

Longitud del Nombre del Archivo y del Directorio	255
Tamaño del archivo	16 EB (264 bytes)
Tamaño de la partición	16 EB teoricamente (264 bytes)
Atributos	Solo lectura, Archivo, Sistema, Oculto y *extendidos
Sistema de Directorios	Arbol Binario
Accesible a través de	Windows NT

* como almacenar la fecha y hora de la creación y modificación de archivos y directorios.

Convirtiendo a NTFS

Cuando se tienen particiones FAT o HPFS, y se desean obtener los beneficios de NTFS conservando la información, es posible por medio del comando CONVERT.EXE.

Ventajas y Desventajas de los Sistemas de Archivos

Sistemas de Archivos	Ventajas	Desventajas
FAT	Poco consumo de sistema. El mejor para discos y/o particiones de menos de 200MB.	El rendimiento decrece con particiones de más 200MB. No se pueden aplicar permisos sobre archivos y directorios.
HPFS	El mejor para discos y/o particiones entre 200 y 400 MB. Elimina la fragmentación almacenando en un solo bloque el archivo completo.	No es eficiente para menos de 200MB. No soporta hot fixing. No se pueden aplicar permisos sobre archivos y directorios.
NTFS	El mejor para volúmenes de 400MB o más. Recuperable (registro de transacciones), diseñado para no ejecutarle utilerías de reparación. Es posible establecer permisos y registro de auditoría sobre archivos y directorios.	No recomendable para volúmenes de menos de 400MB. Consume de 1 a 5 MB de acuerdo al tamaño de la partición.

Nombres de Archivos

NT soporta múltiples sistemas de archivos. Por esto es necesario considerar las diferencias en la estructura de los nombres cuando se transfieren de un sistema de archivos a otro.

Para todo nombre largo (LNF) creado se autogenera un nombre corto (alias) convencional de 8 caracteres para el nombre y 3 para la extensión. EN particiones FAT, un LFN tomará una entrada del directorio por cada 13 caracteres, más otra para su alias.

Cada LFN tiene los siguientes atributos:

1. Volúmen (V): un conjunto especial para designar la entrada como una partición del disco duro.
2. Solo-Lectura (R): se puede escribir sobre el archivo
3. Sistema (S): no es un archivo de acceso normal para el usuario (no escritura y oculto)
4. Oculto (H): el archivo no aparece en el directorio.

Los nombres de DOS no contienen estos cuatro atributos. Un archivo puede tener RSH pero no el de vólumen. Al contrario, un archivo con vólumen no tendrá RSH. Esta especial combinación protege la información de la mayoría de utilerías de disco.

Nombres 8.3 sobre NTFS y FAT

Bajo NT los nombres largos son convertidos a nombres 8.3 para crear un alias para los clientes DOS. Esta conversión tomas los 6 primeros carácteres del nombre y añade un subfijo ~número para asegurar la unicidad del nombre.

A continuación un ejemplo:

Nombre Largo	Nombre Corto
Mi Documento 1.doc	MIDOCU~1.DOC
Mi documento 2.doc	MIDOCU~2.DOC
Mi documento 3.doc	MIDOCU~3.DOC
Mi documento 4.doc	MIDOCU~4.DOC

Despues de los primeros cuatro archivos, iguales, la convención cambia. El quinto archivo usará los dos primeros carácteres del nombre, y los siguientes cuatro serán generados por un algoritmo de hashing. Cuando el hashing de los cuatro carácteres no pueda generar un nombre único se produce el siguiente ~número

Nombre Largo	Nombre Corto
Mi Documento 5.doc	MIX49F~5.DOC
Mi documento 6.doc	MIT3GA~5.DOC
Mi documento N.doc	MI3X9I~6.DOC

Consideraciones para la creación de nombres de archivos largos y cortos

HPFS no genera automáticamente nombres cortos. Como resultado, las aplicaciones DOS y Windows 16 no podrán accesar a los archivos con nombres largos, y el comando dir /x desplegará una columna en blanco donde se listarían los nombres 8.3. Al contrario, las aplicaciones DOS y Windows 16 si podrán accesar a los archivos con nombre largo sobre particiones NTFS y FAT debido a la autogeneración del alia (nombre corto).

Uso de Nombres con mayúsculas y minúsculas

NTFS almacena los nombres con mayúsculas y minúsculas para soportar POSIX. Sim embargo las interfaces de programación DOS, OS/2 y Win32 no hacen diferenciación. Debido a esto algunas aplicaciones podrían llegar a causar confusión, por ejemplo. al guardar un archivo con nombre NAT.XLS reescribirá al archivo nat.xls.

Uso del Disk Administrator

El Disk Administrator es una herramienta gráfica para la administración de discos. Esta herramienta es utilizada para establecer, configurar y organizar los discos duros locales del sistema. El Disk Administrator despliega los recursos del disco por medio de una barra de estado y una leyenda.

Creando y Formatenado Particiones

El Disk Administrator provee una forma sencilla para administrar los discos: crear, formatear y borrar particiones desde una aplicación gráfica.

Un disco debe ser particionado antes de ser formateado con cualquiera de los sistemas. Las particiones de disco son una parte del disco fisico que funcionan como si fueran diferentes únidades físicas.

Servicios de Impresión

Terminología de NT

Dispositivo de Impresión vs Impresora

Un dispositivo de impresión es el dispositivo de hardware encargado de producir la impresión. Una impresora es la interface de software entre la aplicación y el dispositivo de impresión. Múliples impresar pueden ser ruteadas a un solo dispositivo de impresión.

Cada impresora tiene su propio controlador, modo de impresión, horarios de impresión y prioridad.

Impresora vs Cola de Impresión

En NT, los trabajos son enviados a una impresora, donde esperan a ser enviados al dispositivo de impresión. en otros ambientes de red, como Netware, a esta función se le conoce como cola de impresión.

Puerto Físico de Impresión vs Puerto Lógico de Impresión

Un puerto físico es la conexión de hardware entre la computadora y el dispositivo, como LPT1: o COM2:. Un puerto lógico es una conexión de red a un dispositivo o servidor de impresión remoto, conocido como \\server\printer. NT permite crear una impresora para usar un puerto físico o lógico como destino para la impresión.

Dispositivos de Impresión Locales o Remotos

Los dispositivos de impresión locales son los conectados directamente a la computadora NT. Los dispositivos remotos son accesados a través de la red. Los dispositivos de impresión con interface de red, son los dispositivos de impresión con tarjetas de red integradas y se conectan directamente a la red.

Pools de Impresoras

En un pool de impresión, varios dispositivos de impresión son asociados a una sola impresora. Los dos dispositivos de impresión deben ser iguales o emular al mismo dispositivo de impresión, o sea, utilizar el mismo controlador de impresión. NT no pone límite al número de dispositivos de impresión en un pool de impresión.

Proceso de Impresión

1. El usuario elige imprimir desde su computadora cliente. Si el cliente imprime desde una aplicación Windows, la aplicación llama al GDI (graphics device interface). El GDI junto con el controlador de impresión traducen la información a comandos del dispositivo de impresión, colocando la información en el spooler cliente (Winspool.drv). Si la aplicación no es Windows un componente similar al GDI realiza la operación.
2. La computadora cliente envía el trabajo al servidor de impresión. Si el cliente es NT, el spooler cliente (Winspool.drv) hace un RPC al spooler Server (SPoolss.exe), el cual hace llamadas a la API router (Spoolss.dll). El router hace un "poll" al remote print provider (Win32spl.dll), y hace un RPc al Spoolss.exe en el servidor de impresión, el cual recibe el trabajo de impresión a través de la red. Si el cliente NT creó una impresora local y redirigió la salida, el trabajo lo envia el redirector. si el cliente es UNIX o utiliza algún software LPR, el trabajo se envía a través de TCP/IP al servidor con el servicio LPD. Si

el cliente es Macintosh, el trabajo se manda via Apple Talk hacia los Servicio para Macintosh (SFMMon).

3. El router o el print Server reciben el trabajo.
4. El router o el print Server pasan el trabajo de impresión al print provider local en el servidor (un componente del spoller), el cual encola el trabajo de impresión.
5. El print provider local hace un "poll" al print procesor. Cuando el print processor reconoce el tipo de datos del trabajo, lo altera (o no) de acuerdo a la configuración de la impresora.
6. El control del trabajo pasa al sapator page processor, el cual le añade el separador de página antes del trabajo si así se especificó.
7. El trabajo es entregado al print monitor. Si el dispositivo de impresión es bidireccional, el trabajo primero se dirige al language monitor, el cual maneja la comunicación bidireccional entre la impresora y el port monitor. Si el dispositivo no es bidireccional, el trabajo se dirige directamente al port monitor, el cual lo transmite al dispositivo de impresión o a otro servidor especificado.
8. El dispositivo de impresión recibe el trabajo, traduce la página a un mapa de bits y lo imprime en papel o algún otro medio.

Administración de Impresoras

Usando el Folder Impresoras

El folder de Impresoras de NT 4.0 equivale al Administrador de Impresión de NT 3.X. Ambos son usados para:

- Crear impresoras (instalar dispositivos de impresión).
- Controlar las características de la impresora, como fuentes y tamaño de papel.
- Establecer permisos de acceso.
- Auditar el uso de la impresora.
- Administrar impresoras remotas.
- Redireccionar la salida impresa.
- Conectarse a impresoras remotas.
- Revisar el estado de impresoras locales o remotas.

Creando una Impresora

El cuadro de diálogo create Printer es usado para instalar y configurar controladores de impresión para dispositivos locales o remotos. Si el servidor de impresión remoto es de tipo NT, es mas recomendable conectarse a éste.

Conectándose a una Impresora

Para conectarse a una impresora compartida de otra computadora NT se debe usar el comando Connect to Printer. Esto provee dos beneficios:

1. El administrador solo necesita actualizar el controlador en el servidor de impresión. Los clientes automáticamente actualizan el controlador al conectarse a la impresora.
2. La computadora cliente no necesita tener instalada su propio controlador para utilizar el dispositivo de impresión.

Esta función no se puede realizar con servidores WFW, Novell o Win95. En estos casos se crea una impresora local con su controlador de red local, y la salida redirigirla al puerto remoto.

Instalando el Controlador de Impresión en Plataformas RISC e INTEL

Los controladores de dispositivos de NT son específicos a la plataforma. Las computadoras RISC no pueden utilizar controladores Intel y viceversa. Además, los controladores son diferentes para cada plataforma RISC soportada. Así para realizar una conexión entre varias plataformas se requiere instalar controladores de acuerdo a la plataforma de los clientes.

Para evitar instalar un controlador de impresión en cada computadora Intel cuando se imprime en RISC, la versión Intel del dispositivo debe ser intalado en el servidor de impresión RISC. Lo mismo ocurre de RISC a Intel. Así al conectarse el cliente, obtendrá el controlador correcto.

Administrando Impresoras Remotas

El folder de impresoras o el administrador de impresoras permiten administrar impresoras remotas. Es posible cambiar las propiedades, configurar charolas de impresión, asignar permisos, etc. Para esto es necesario tener un permiso de Full Control sobre la impresora.

Implementando Pools de Impresoras

Un pool de impresoras es un grupo de varios dispositivos conectados a una sola impresora. Un pool de impresoras permite a los usuarios imprimir a una sola impresora y que el print spooler determina cual de los dispositivos de impresión esta disponible. Cuandouna impresora es creada, se debe seleccioanr el puerto mas eficiente para el dispositivo conectado porque éste será el primer dispositivo considerado por el spooler.

Para asignar más de un dispositivo de impresión a un pool, se deben asignar dentro de las propiedades (NT 4.0) o los detalles (NT 3.X) de la impresora. Los puertos pueden ser combinando seriales y paralelos. El ruteo está basado en el orden de como se elijan. Todos los dispositivos de impresión del pool utilizarán el mismo controlador.

Servicios de Acceso Remoto (RAS)

RAS conecta al usuario con una red remota a través de una línea telefónica. Una vez hecha la conexión, la línea telefónica se hace transparente y el acceso a los recursos de red se efectua como si la computadora estuviera conectada directamente a la red. Con RAS el modem actua como una tarjeta de red añadiéndo la computadora a la red.

Características Generales

Servidores Dial-in Soportados

Los clientes NT con RAS pueden conectarse a LAN Manager, WFW, Win95 y NT. Además los clientes RAS también pueden conectarse a otros servidores dial-in, como UNIX a través de los estándares SLIP y PPP.

Clientes Dial-in soportados

Los clientes LAN Manager, WFW, Win95 y NT pueden conectarse a los servidores NT con RAS: Además otros clientes pueden conectarse a través de los estándares SLIP y PPP.

Interfaces de Red Soportadas

Cualquier aplicación que utilice cualquier de las siguientes interfaces operará bajo RAS.

- Windows Sockets
- NetBios
- Mailslots
- Named Pipes
- RPCs
- APIs de red de NT (Win32) y Lan Manager

Limitaciones de las conecciones RAS de NT

El RAS de NT Server soporta hasta 256 conecciones simultáneas y una en RAS de NT Workstation. Un dispositivo serial multipeurtos puede proveer varios puertos seriales al servidor RAS.

Compresión de datos en RAS

Esta compresión a nivel de software se basa en los algoritmos de DRVSPACE con un promedio de 2 a 1. Esta compresión puede mejorar la velocidad de las conecciones hasta ocho veces.

Escalabilidad

El servidor RAS es multithreaded y puede soportar multiprocesamiento. Esto permite a los threas del RAS ejecutarse en los varios procesadores de una computadora, mejorando el rendimiento del RAS.

Soporte a Redes de Area Amplia

RAS soporta los siguientes métodos para establecer una conexión entre clientes y servidores:

- Líneas públicas estándares.
- X 25
- Integrated Services Digital network (ISDN)

Seguridad

El servicio de RAS de NT implementa varias medidas de seguridad para asegurar el acceso de los usuarios remotos a la red. En ciertos aspectos, la conección con RAS es mas segura que trabajar en la red local.

Seguridad del Dominio Integrada

El servidor RAS utiliza la misma base de datos de usuarios de NT. Esto facilita la administración porque los usuarios se validan con la misma cuenta adquiriendo los mismos derechos y permisos.

Un usuario debe tener una cuenta de NT, permiso de dialin y ser autentificado para conectarse a través de RAS.

Validación y autentificación Encriptada

La información de la autentificación y validación es encriptada cuando se transmite a través de la línea telefónica. El resto de la sesión no es encriptada a menos que se configura manualmente.

Auditoría

Con la audirotía habilitada, RAS registrará todas las conecciones remotas incluyendo actividades como la autentificación, validación, etc.

Hosts intermedios de Seguridad

Es posible añadir otro nivel de seguridad a la configuración de RAS conectando un host intermedio de seguridad, el usuario escribirá una clave de acceso a un código antes de establecer la conección con el servidor RAS.

Call Back Security

El servidor RAS puede ser configurado para proveer call backs (regresar llamadas) como un medio para incrementar la seguridad. El call back puede ser al teléfono de donde se marcó o a un número especificado. El método de call back se define por usuario.

Capitulo 4
Intranet

Una Intranet es una infraestructura de comunicación que es posible construir basicamente apartir de un conjunto de redes de area local, con accesos directos a y desde Internet. La Intranet esta basada en los estándares de comunicación de Internet y en los del World Wide Web. Por lo tanto, las herramientas usadas para crear una Intranet son identicas a las mismas de Internet y las aplicaciones Web. La diferencia principal de la Intranet es que al acceso a la información publicada esta restringido a clientes dentro del grupo de la Intranet.

La principal razon para que las compania adopten una Intranet es la facilidad de implementacion de una. Las Intranets han llegado a ser el equivalente en el cyber espacio de los enfriadores de agua de oficina, donde se obtienen las ultimas noticias, la vision y las pistas acerca de las actividades de la compania.

Tecnicamente, las intranets estan a salvo de intrusiones por uso de lineas de comunicación privadas, en lugar de utilizar las mismas lineas de comunicación publicas de internet.

Características y Beneficios

La Intranet tiene las siguientes características:

- Rápido Diseño.
- Escalabilidad.
- Fácil navegacion.
- Accesible para la mayoría de las plataformas de cómputo.
- Integra la estrategía de cómputo distribuido.
- Adaptable a los sistemas de información propietarios.
- Uso de multimedia.

Los beneficios para la empresa son:

- Requiere poca inversión para su inicio
- Ahorra tiempo y costos en comparación de la distribución de información tradicional (papel).
- Su estrategia de cómputo distribuido utiliza los recursos de cómputo mas efectivamente.
- Tiene una interfase sencilla y flexible (vínculos).
- Independiente de la plataforma.

Nuevo Paradigma de la Información

La Intranet propone el concepto de usar el paginador de Web como la interface de información universal. Las ventajas de este nuevo paradigma son:

- Reduce el tiempo de aprendizaje de los usuarios.
- Simplifica la instalación de aplicaciones.
- Presenta diferentes tipos de información: texto, gráficas, sonido y video.
- Actua como "front-end" para las aplicaciones cliente-servidor.
- Permite el acceso a bases de datos.

Publicación en Base a la Demanda

Una de las principales motivaciones para la adopción de la Intranet es que permite a las organizaciones evolucionar de una estrategia de publicación calendarizada a publicación en base a la demanda.

Tradicionamente, las compañías publican una vez al año el manual del empleado. cualquier cambio de último momento o ajuste importante, sería actualizado hasta el siguiente año. La Intranet ofrece dos soluciones a este problema:

1. El empleado decide cuando consultar la información.
2. La información puede actualizarse instantáneamente.

Reducción de Costos

El modelo de publicación tradicional incluye varios pasos:

1. Creación del contenido
2. Migración del contenido a una publicación electrónica.
3. Producción del original
4. Revisión
5. Producción del original corregido
6. Duplicación
7. Distribución

El modelo de publicación con la Intranet incluye un proceso mucho más bajo en costo:

1. Creación del contenido
2. Migración de los actuales al ambiente de Intranet

En este último modelo la revisión se convierte en parte del proceso de actualización y la información es usada cuando se necesita.

Desarrollo de Aplicaciones Cliente/Servidor

Las aplicaciones cliente/servidor tradicionalmente manejan dos o tres capas:

1. Front End
2. (Middleware)
3. Back End

Actualmente el desarrollo del Front End se realiza por medio de herramientas como Visual Basic, Delphi, C++ y se instala en cada una de las computadoras. Actualizar o añadir nuevos módulos a las aplicaciones es costoso y lento. Además las aplicaciones se deben compilar para cada plataforma.

Con el nuevo paradigma del paginador como cliente universal este problema es eliminado por varios factores:

- Las aplicaciones residen en las páginas Web.
- Los objetos y componentes se instalan automáticamente o de manera muy sencilla.
- Existen paginadores para todos los sistemas operativos.

Aplicaciones de la Intranet en las Empresas

Las siguientes secciones ejemplifican el uso de la Intranet en los principales departamentos de las empresas.

Difusión y Comunicación

Difusión y comunicación puede ser uno de los primeros departamentos en implementar la Intranet, sirviendo como modelo para otros grupos. Por esto, es importante desarrollar el con gran calidad incluyendo textos, gráficos, sonidos, etc. adecuados.

A continuación se presentan usos comunes de la Intranet para Difusión y Comunicación

Revista de la Compañía

La Intranet es una excelente forma para publicar las revistas semanales o mensuales de la compañía, ahorrando costos de producción y distribución. También las revistas pueden ser fácilmente archivadas para posibles referencias. Para comenzar el uso de esta revista, el editor debe avisar por medio de e-mail o en la revista impresa la dirección y las instrucciones de como accesar a la revista.

Las contribuciones para la revista, su edición y revisión pueden realizarse combinando el e-mail, con el browser, y las herramientas de publicación.

Comunicados de Prensa

El ciclo de revisión de los comunicados de prensa se simplifica con la intranet, facilitando la autorización por parte de los departamentos de dirección, jurídico y mercadotecnia.

La intranet puede servir para archivar los comunicados de prensa junto con documentos capturados de revistas, periódicos, libros, etc.; y para publicar los resultados de la empresa, acontecimientos sociales, etc.

Preguntas Frecuentes

Algunos ejemplos de preguntas frecuentes para el departamento de difusión y comunicación son:

- ¿Quiénes son los encargados de la revista la compañía?
- ¿Cuál es el procedimiento para publicar un comunicado de prensa?
- ¿En cuánto tiempo se produce un nuevo folleto?

- ¿Cómo puedo ordenar una hoja de especificaciones?
- ¿Cuándo estará el nuevo folleto de la compañía disponible?
- ¿Quién es el responsable de los avisos de la compañía?
- ¿Dónde puedo encontrar los últimos comunicados de prensa?

Listas

Un uso muy práctico para la intranet es la publicación de listas. Algunos ejemplos típicos de listas son: comunicados de la empresa, libros, boletines, hojas de especificacioens, presentaciones.

Una lista muy importante es la del personal del departamento de Difusión y Comunicación. Esta lista debe contener el nombre, función, teléfonos, dirección, y dirección de correo.

Formas

El uso de formas en la Intranet facilita a los empleados la solicitud de folletos, libros, presentaciones, tarjetas de presentación, etc. El empleado exclusivamente necesita llenar con los datos adecuados y esta información es transferida a bases de datos, o a los encargados por medio de e-mail.

Reportes Anuales, Folletos y Hojas de Especificaciones

Los reportes anuales, folletos y hojas de especificaciones pueden ser almacenados en la Intranet, con ligas entre sí, y a otros documentos. Esto permite a los empleados obtener rápida y facilmente información actualizada, reduciendo los costos de impresión y envio de información.

La Intranet también permite producir materiales mas creativos sin costo adicional, añadiendo capacidades de audio y video a las presentaciones.

La intranet puede ayudar a reducir los costos de materiales con un periodo de vida corto o con revisiones frecuentes.

Ventas y Mercadotecnia

Intranets permiten la frecuente adición y actualización de materiales de Ventas y Mercadotecnia, como respuesta a un ambiente de negocios competitivo y dinámico. La principal

ventaja es la eficiente forma de distribuir información crítica a vendedores, distribuidores, sucursales, franquicias y al corporativo.

Una intranet bien organizada para Ventas y Mercadotecnia puede ayudar a eliminar el exceso de información duplicada. Ella permite resolver las necesidades de los representantes de ventas, quienes necesitan acceso instantaneo a información especifica, sin leer grandes cantidades de material impreso.

Otra gran ventaja es la mejora en el flujo de la información y los mensajes. Los representantes de ventas de todo el mundo, cuentan con acceso a las mismas presentaciones, descripciones de producto, resumenes, etc. Así, la productividad se incrementa al evitar las búsquedas de hojas de especificaciones y promociones.

Los principales usos de la Intranet en Ventas y Mercadotecnia son:

Boletines de Mercado

Una vez implementada la intranet, se vuelve casi inecesario la distribución de largos boletines de ventas semanales, quincenales o mensuales. La distribución es mucho mas sencillas, además estos boletines pueden ser fácilmente archivados para usos futuros.

Kits de Ventas

La Intranet provee un medio eficiente y poco costoso para distribuir los kits de ventas en vez del tradicional correo. La Intranet elimina el problema de la pérdida o daños en los paquetes. Esta característica es especialmente importante para los kits de nuevos productos en compañías mundiales.

A diferencia de los kits de ventas en papel, los cambios de último minuto pueden ser hechos sin ningún costo adicional, generalmente es tan simple como añadir nuevos documentos con código HTML.

El de los kits de ventas puede incluir gráficas, audio y video fácilmente.

Cambios en Productos

Además de los anuncios de nuevos productos, la Intranet es un perfecto medio para aununciar los cambios de productos o actualizaciones. Estos pueden ir desde anuncios de mejoras hasta notificaciones de modelos obsoletos.

Presentaciones

La Intranet al actuar como un almacén de presentaciones, permite su estandarización y elimina costos de producción y distribución mejorando la calidad de las mismas.

La intranet puede contener gráficas, íconos, logotipos, fotografías, etc. de la compañía para facilitar la creación, personalización y actualización de las presentaciones. La capacidad de personalizar las presentaciones a las necesidades y espectativas del cliente, facilita la publicidad y venta del producto.

Guías de Ventas

Las Guías de Ventas en la Intranet son mas funcionales y menos costosas. Las revisiones y cambios se actualizan inmediatamente. Los vendedores pueden buscar rápidamente información de los productos sin perder tiempo entre papeles.

Las gráficas mejoran la calidad de las guías e ilustran mejor las características de los productos.

Información de Clientes

Almacenando los datos, opiniones y testimonios de los clientes en la Intranet, y ligándolos a ciertas áreas de los productos, se puede crear una poderosa herramienta de consulta de clientes y productos.

Asumiendo que la lista de clientes se expande regularmente, se debe planear un calendario de actualizaciones.

Listas de Precios

Las listas de precios son mas sencillas de actualizar que las listas impresas. Las listas de precios están disponibles en base a la demanda, eliminando los costos de impresión y distribución, mientras que los vendedores no necesitan cargar las "pesadas" listas impresas.

La principal ventaja es que los vendedores no cometen errores al hacer referencias a listas desactualizadas. Debido al acceso en base a la demanda, la necesidad de verificar los precios con la oficina central se elimina, algo muy benéfico para las grandes compañías con diferencias de horarios entre sus sucursales.

Preguntas Frecuentes

Las preguntas frecuentes simplifican el proceso de ventas y ayudán a los nuevos vendedores. Algunas preguntas frecuentes son:

¿Cómo puedo facturar una orden?

¿Cuál es el proceso de autorización de una compra?

¿Cuáles son los descuentos en base al volumen de compra?

¿Cuál es el procedimiento para solicitar descuentos especiales?

¿Dónde están las referencias de los clientes?

¿Dónde puedo encontrar las descripciones de los productos?

¿Dónde están las presentaciones actualizadas de los productos?

¿Cuál es el calendario para los nuevos boletines de ventas?

¿Cómo puedo obtener una copia de los kits de ventas?

Formas

Las formas mas usadas pueden ser llenadas directamente en la Intranet. Ejemplos comunes son: autorizaciones de compra, solicitudes de producto, peticiones de equipos, viajes y viáticos, reservaciones para conferencias, etc.

Especificaciones de Productos

Las especificaciones y las presentaciones de los productos pueden ser almacenadas y actualizadas en la Intranet, simplificando su consulta, reduciendo costos y eliminando la necesidad de tener personal dedicado.

En algunos casos es necesario manejar presentaciones especiales, para en el caso de hacer varios clientes con el mismo requerimiento, evaluar como satisfacer esos requerimientos.

Información de la Competencia

La información de la competencia puede ser fácilmente actualizada en la Intranet. Esto hace mas eficiente la distribución de reportes competitivos en vez de hacerlos sobre material impreso. En condiciones especiales, la información puede ser accesada incluso desde las oficinas del cliente.

Propuestas

La intranet es idonea para almacenar simples propuestas, incluyendo material temporal. Este material puede contener: objetivos y alcances de proyectos, resúmenes corporativos, descripciones de productos.

Televentas

La forma mas eficiente de proveer a los empleados de televentas con información de precios y productos es por medio de la Intranet. Las principales ventajas son el acceso a bases de datos, información adicional no incluída en la guía de ventas, formas de comentarios especiales de clientes e información del cliente.

Listas de Contactos

Las intranets permiten almacenar las listas del personal de mercadotecnia y ventas, incluyendo dirección, números telefónicos y direcciones de e-mail. Un directorio de mercadotecnia por función y producto sirve como una fácil referencia para determinar quien es el encargado de un producto en particular. La lista del personal de ventas cuando incluye a sus respectivos clientes y cuentas, facilita la transferencia de llamadas al departamento de ventas. Las fotos pueden mejorar la calidad del directorio.

Las compañías que trabajan con distribuidores externos, pueden listarlos de acuerdo a su ubicación geográfica, número de teléfono e información de contactos. Esta es una gran ventaja cuando para una venta se necesitan de diferentes distribuidores.

Encuestas y Reportes

Cuando los gerentes de ventas y finanzas necesitan reportes o encuesstas mensuales o quincenales para la planeación estratégica, la Intranet ofrece un excelente medio para lograrlo. Combinando otras herramientas de administración de proyectos y bases de datos, es posible mejorar las encuestas para una mejor planeación.

Información de Distribuidores

La Intranet es un medio efectivo para la comunicación con distribuidores externos, proveedores y subsidiarias, ahorra tiempo y costos, por lo que es importante considerar una Intranet accesible solamente para este tipo de canales. Para lograr una implementación exitosa, el , gráficas y otros requerimientos, deben estar de acuerdo a las necesaridades del canal.

Información Miscelanea

Como un boletín, la Intranet puede ser usada para anunciar información miscelanea como: promociones y descuentos especiales, comisiones e incentivos a ventas, mayores ventas, calendarios de eventos y el empleado del mes. Con gráficas, fotos y videos, la Intranet será mas atractiva.

Recursos Humanos

La información de Recursos Humanos debido a la gran cantidad de papeles y gráficas se puede usar en una Intranet. La Intranet hace sencilla la comunicación de prestaciones, gráficas de la empresa, políticas y manuales de procedimientos. La intranet permite también administrar el reclutamiento, promoción, salarios y asistencias de los empleados.

La intranet ofrece un medio mas eficiente y económico de responder a preguntas típicas de Recursos Humanos que el teléfono o los mensajes. La intranet ahorra gran tiempo y dinero de Recursos Humanos, además da a los empleados rápido acceso a información de su interés como: planes de compra, vacaciones, gastos médicos, etc.

A continucación se presentan algunos usos comunes en Recursos Humanos:

Manuales de Políticas y Procedimientos

Uno de los primeros proyectos para la Intranet de Recursos Humanos debe ser publicar los manuales de políticas y procedimientos. Como mucha de esta información ya esta en computadora, simplemente hay que convertirla a formato HTML.

Guardando los manuales de políticas y procedimientos en la Intranet, se eliminan lo difícil y caro de regularmente actualizar y distribuir el material que refleje los cambios de políticas o las nuevas decretos gubernamentales. La Intranet asegura que los empleados utilizan la última versión y les ayuda a buscar información específica, y simplifica el proceso de aprendizaje de los nuevos empleados. Este uso es ideal para empresas nacionales e internacionales con diferentes regulaciones estatales.

Programas de Beneficios

La Intranet simplifica la comunicación de los planes de retiro, médicos y dentales de la empresa, los programas de seguridad, etc. Los empleados pueden revisar esta información desde su computadora del trabajo o de la casa. Esta capacidad ahorra considerablemente tiempo y esfuerzo, y es muy util para nuevos empleados.

Dentro de las Preguntas Frecuentes se puede incluir la información de los programas de beneficios mas utilizados.

Planes de Compra

La Intranet permite publicar los detalles del programa de planes de compra de la empresa. Información sobre los artículos, descuentos, modos de pago, precios, etc.

Programas de Fondos y Compensación

En la Intranet los gerentes de la compañía pueden encontrar la información acerca de bonos especiales, compensaciones y planes de incentivos. Si solo ciertos niveles de gerencia son autorizados para revisar esta información, la Intranet provee controles de seguridad para limitar el acceso.

Empleos Internos

En vez de usar boletines o enviar mensajes a los miembros de la compañía sobre empleos internos, estos pueden ser publicados en la Intranet eliminando la necesidad de imprimir o fotocopiar los anuncios. Estableciendo vínculos a las "descripciones de empleos" o a las "formas de solicitud de empleo", los empleados rápidamente pueden accesar a información detallada o registrarse inmediatamente.

Descripción de Puestos

En vez de usar una copia impresa del manual de descripciones, es mas eficiente publicar las descripciones en la Intranet. Las descripciones completas pueden ser de todos los puestos (aun sino estan ocupados), clasificación de los puestos (con explicaciones), y otros datos útiles. Para una mejor referencia se recomienda ligar esta información a otras páginas como la de empleos internos.

Promoción y Reclutamiento

Para las activiades de reclutamiento y promoción, la intranet permite almacenar los procesos y procedimientos para las revisiones de trabajo anuales,solicitudes de empleo, promociones, e información relacionada a la promoción y reclutamiento.

Curriculums

Muchas compañías capturan los curriculums en sus sistemas computacionales por medio de OCR. Convirtiendo estos documentos a páginas HTML, esta información puede estar en la Intranet y ser utilizada por el personal autorizado.

Gráficas de la Empresa

La naturaleza dinámica de la Intranet es ideal para las gráficas de la empresa y su organigrama. Ellas pueden ser fácilmente actualizadas y cambiadas para reflejar las nuevas estructuras de la empresa o cambios en puestos. Esta información también es útil para los empleados quienes necesitan conocer información de otros departamentos. El organigrama de la empresa es especialmente útil en corporativos nacionales e internacionales, para mejorar los procesos de comunicación.

Listas de Contactos

Publicando los nombres, funciones y teléfonos del personal de Recursos Humanos en la Intranet ahorra mucho tiempo y esfuerzo en la empresa. Esta información ayuda a los empleados a comunicarse con los encargados de Recursos Humanos para resolver dudas o problemas

Preguntas Frecuentes

Algunas preguntas típicas para colocar en la Intranet son:

- ¿Dónde puedo encontrar las solicitudes de vacaciones?
- ¿Cuántos días de vacaciones recibiré por cada año de antigüedad?
- ¿Cuáles son las políticas en caso de enfermedad?
- ¿Dónde puedo encontrar información acerca de créditos?
- ¿Cómo funcionan los depósitos directos?
- ¿Cuál es el procedimiento para solicitar un trabajo interno?
- ¿Cómo es el programa de retiro?

Formas

La cantidad de tiempo perdido analizando solicitudes en formas, justifica el uso de la Intranet para almacenar las formas de recursos humanos, especialmente para empresas con diferentes oficinas. Para el empleado es fácil encontrar la forma apropiada actualizada.

Las siguientes son ejemplos de formas utilizadas en la Intranet:

- Depósitos directos
- Créditos
- Compras de productos
- Reemboolsos
- Solicitudes de vacaciones
- Maternidad y enfermedades
- Solicitudes de trabajo
- Cambios de area
- Evaluaciones
- Encuestas
- Prestaciones

Calendario de Vacaciones y Días de Descanso

Los empleados pueden planear sus vacaciones y actividades de acuerdo al calendario de vacaciones y días de descanso publicado en la Intranet.

Registro de los Empleados

Estableciendo reglas de seguridad, el personal autorizado de Recursos Humanos puede accesar al registro de los empleados en la Intranet. Este es una manera segura de compartir información confidencial, para que los gerentes de recursos humanos puedan analizar el historial de salarios, el comportamiento de algún empleado, o ver su antigüedad en la empresa, para propositos de planeación, ascensos, etc.

Educación y Capacitación

La Intranet ofrece creativas posibilidades para los departamentos de capacitación, universidades, escuelas privadas y públicas, y otras organizaciones para educar. La intranet es ideal para almacenar los planes de estudios, temarios, manuales de capacitación, presentaciones, videos, bibliografías, listas de esstudiantes, horarios de clases,e tc.

La Intranet mejora las comunicaciones, promueve la colaboración, elimina la duplicación de funciones y provee de información precisa y actualizada. La intranet permite que las revisiones y cambios de último minuto sean sencillas. El uso de ligas facilita la referencia a otros materiales.

Los colegios y universidades que están implementando educación a distancia por Internet, pueden combinar este neuvo medio educacional con la Intranet. Por ejemplo, los estudiantes e instructores pueden intercambiar e-mail en Internet. Sin embargo, los materiales del curso, lecturas y tareas solo podrán ser publicadas en la intranet para uso de los estudiantes registrados.

Finalmente, la Intranet representa una solución muy económica. Como los materiales están disponsibles electrónicamente, la Intranet reduce los costos de impresión.

Los principales usos de la Intranet en Educación y Capacitación son:

Planes de Estudio

La intranet reduce el tiempo para desarrollar y revisar los planes de estudio, entre una o varias personas sin importar su ubicación. Por ejemplo, la intranet permite a los miembros de un proyecto compartir sugerencias y comentarios, sin tener una reunión o una teleconferencia.

La distribución electrónica elimina los tiempos de impresión. Una vez implantada la intranet, distribuir los planes de estudio a instructores en campus externos es simple.

Otra ventaja es la oportunidad de compartir los planes de estudio con otros instructores para revisar, complementar o adaptar sus materias.

Temarios

Al formar parte de la Intranet los temarios, aseguran la consistencia de los s. También facilita los procesos de modificación y actualización.

Los temarios pueden irse enriqueciendo añadiendo esquemas, gráficas, videos, autoevaluaciones, proyectos, etc.

Manuales de Capacitación

La Intranet facilita el largo y caro proceso de actualización de los manuales de capacitación para reflejar los cambios del producto y la organización, especialmente para los manuales de capacitación de ventas que necesitan revisarse y adecuarse a ajustes en la organización, introducción de nuevos productos, mejoras, y cambios en la estrategia del corporativo.

Otra ventaja es la capacidad de poder revisar los manuales después del curso, buscando dudas específicas sobre algún tópico.

Añadiendo audio o videos, los programas de capacitación aumentan su efectividad, simplificando el aprendizaje de conceptos difíciles.

Catálogos de Cursos

La Intranet es ideal para universidades y corporaciones que producen y distribuyen catálogos de sus cursos. Esto permite incorporar revisiones de último minutos, cursos extraordinarios, cambios de instructores, cancelaciones de cursos. Reduciendo o eliminando el número de catálogos impresos. Es importante añadir ligas entre el catálogo de cursos, sus planes de estudio y temarios.

Presentaciones

Las presentaciones pueden ser fácilmente creadas, actualizadas y compartidas por medio de la Intranet. Esto es ideal para instructores en ambientes de capacitación corporativa e insticuiones académicas, ayudándoles a mezclar y adecuar los materiales de diversas presentaciones existentes a un tópico en particular.

Una ventaja adicional es la consistencia en las presentaciones. Los instructores pueden transmitir las mismas ideas en diferentes ciudades, sin "reinventar la rueda" y concentrándose en el de su exposición.

Videos

Añadiendo videos a las presentaciones y materiales del curso, la calidad del del aprendizaje aumenta. Debido a la velocidad de la Red de Area Local, el video puede ejecutarse rápidamente en la Intranet con un hardware y software mínimo.

Bibliografías

Con la Intranet, la bibliografía es fácil de revisar para preparar y complementar el de las materias, o bien, para resolver tareas y exámenes. La lista puede modificarse dinámicamente manteniendo actualizados a los estudiantes de nuevos libros o materiales.

Listas de Estudiantes y Profesores

Tener las listas de estudiantes y profesores en la Intranet es mas simple que reproducir y distribuir las listas manualmente, facilitando las revisiones de último minuto.

Las listas deberían contener las fotos de los estudiantes y profesores, incluso sus biografías. Así los estudiantes pueden escoger mejor a sus profesores, además puede funcionar como un anuario escolar.

Calendarios y Horarios de Clases

Publicando los calendarios de clases en la Intranet, la información se comunica rápidamente a estudiantes y empleados, especialmente a los de oficinas o campus externos. Esta solución incluye situaciones de cancelaciones e inscripciones de último minuto, y recalendarizaciones de cursos. Este método es mejor que la comunicación por boletines, porque los estudiantes pueden revisar sus programas de actividades, evitando viajes cuando los cursos son en otras ciudades.

Preguntas Frecuentes

Ligando las preguntas frecuentes en la Intranet con los catálogos y formas se incrementa la productividad. A continuación se presentan algunos ejemplos:

- ¿Cómo me inscribo a un clase?
- ¿Cuál es el último día para inscribirse a una clase?
- ¿Cuál es el procedimiento para darse de baja en una clase?
- ¿Cuál es la penalización por darse de baja en una clase?
- ¿Cuál es el último día para añadir o cambiar un curso?
- ¿Dónde son las inscripciones?
- ¿Cuál es la forma de pago?

Encuestas y Formas

Colocar las formas y cuestionarios en la intranet incrementa la productividad, es mas eficiente y menos caro que la distriución en papel.

Algunas formas típicas son:

- Registro a un curso
- Interés en un curso
- Solicitud de libros
- Encuestas

Por medio de encuestas, los instructores y estudiantes pueden opinar sobre el del curso, su duración, etc.

Boletines

Con un boletín electrónico en la Intranet los estudiantes e instructores pueden manifestar ideas, compartir noticias, nombrar el estudiante y el instructor "del mes", comentar proyectos especiales, eventos deportivos, etc.

Noticias

Extraer Noticias y Páginas de Internet relacionadas a los cursos, materias o carreras; simplifica las búsquedas en Internet de material educativo y mantiene al tanto de las tendencias a los estudiantes y maestros. Una forma para implementar este programa es hacer encuestas sobre los tópicos de mayor interés relacionados con las materias.

Requerimientos

Los requerimientos mínimos para una Intranet son:

- Red TCP/IP
- Servidor de Web
- Paginador
- Equipo de Desarrollo del Web
- Herramientas de creación HTML
- La intranet es complementada con:
- Herramientas de Indexación
- Servidores de Correo Electrónico
- Servidores de Noticias
- Herramientas de Desarrollo

Windows NT 4.0 incluye la mayoría de estas herramientas integradas:

- TCP/IP
- Internet Information Server: servidor de Web.
- Internet Explorer: paginador.
- Front Page. Herramienta de creación HTML.
- Index Server. Herramienta de Indexación.
- Extensiones del Internet Information Server para Acceso a Bases de DAtos.
- Sistema de Archivos NTFS.

El NTFS se requiere para las extensiones del Servidor Frontpage, para que proporcione seguridad en los Webs que estén expuestos a FrontPage y a Visual InterDev.
Se requiere software para crear y administrar las páginas de World Wide Web.

Cuentas

Las cuentas deben ser creadas con los derechos y permisos mínimos requeridos para permitir el acceso a los servicios proporcionados desde este servidor. La cuenta que IIS usa por defecto para que los usarios accesen los servicios es IUSR_nombre del servidor. IUSR_nombre del servidor es creada por el programa de instalación y colocada en el Grupo local de invitados.

Entradas DNS

Si en la Intranet existe un servidor DNS, una entrada DNS será requerida para cada Servidor Virtual que sea definido dentro del servidor y cada servicio tendrá su propia entrada. Otros tipos de resoluciones de nombre incluyen archivos HOST, servidores WINS con clientes configurados para usar aquellos servidores para resolver nombres HOST, etc.

Instalación del IIS

Durante el proceso de instalación de Windows NT Server 4.0, se ofrece la oportunidad de instalar IIS. Si no se instala IIS durante la instalación de Windows NT Server 4.0, un shortcut para la instalación de IIS es puesto en el escritorio.

Para instalar IIS desde el shortcut de el escritorio:

1. Dar doble click en el shortcut.
2. En el cuadro de dialogo de la instalación de IIS , teclear la ruta a los archivos de Windows NT Server.
3. Seleccionar O.K.
4. En el cuadro de dialogo de instalación seleccionar O.K.
5. En el cuadro de dialogo de Instalación, verificar los servicios y opciones a instalar.
6. Seleccionar O.K. para aceptar las opciones de instalación.
7. Seleccionar Yes en el prompt del cuadro de dialogo para crear el directorio: C:\\WINNT\SYSTEM32\INETSRV
8. Confirmar los Directorios de publicación para los servicios de publicación de World Wide Web, FTP y Gopher y selecciona O.K.
9. Selecciona Yes en el prompt de dialogo para crear los Directorios de Publicaión.

Opciones de Instalación

El segundo cuadro de dialogo presentado durante la instalación permite al administrador seleccionar los servicios y opciones que serán instalados en la base de datos actual del servidor basado en Windows NT.

La sección de Opciones proporciona siete selecciones:

- Internet Service Manager. Puede ser instalado por sí mismo para permitir el manejo de una istalación de IIS existente.
- World Wide Web. Instala y configura para inicializar automáticamente el Servidor WWW.
- Gopher Server. Instala y configura para inicializar automáticamente el Servidor Gopher.
- FTP Server. Iinstala y configura para inicializar automáticamente el Servidor FTP.
- ODBC Drivers and Administration. Ofrece drivers ODBC para la instalación, e instala el ODBC Configuration Manager.

- Help and Sample Files. Instala los archivos de ayuda formateados en HTML y los archivos de ejemplo de aplicación (Tales como acceso ODBC, Formas, etc.)
- Internet Service Manager (HTML). Instala páginas de HTML las cuales permiten administrar el IIS remotamente a través de HTTP.

Opción para el Directorio de Instalación

Al seleccionar el botón de Change Directory se le permitirá al administrador cambiar el directorio de instalación para el IIS.

Espacio Requerido/Disponible

El espacio requerido en el directorio de instalación será presentado al administrador. Este es únicamente el espacio requerido para el software del IIS y no incluye ningún directorio que vaya a ser compartido.

Directorios de Publicación

El siguiente paso en el proceso de la instalación es seleccionar los directorios que serán usados como los directorios raíces por defecto para cada servicio que sea seleccionado para la instalación.

El administrador puede seleccionar directorios que existan actualmente y estos directorios pueden ser aumentados con archivos. El programa de instalación no copia ningún archivo del Directorio de Publicación FTP o del Directorio de Publicación de Gopher, pero copiará un archivo default.htm para el Directorio de Publicación WWW llamado SAMPLES.

Si el Directorio de Publicación WWW está instalado, un directorio adicional será creado en el mismo drive llamado SCRIPTS que contendrá los mismos scripts.

Instalación del Driver ODBC

Si el driver de instalación es seleccionado en la pantalla de opciones, se le pedirá al administrador que seleccione uno o más drivers ODBC para instalar con el servidor.

Para seleccionar, simplemente se ilumina el driver deseado y seleccionar el botón de OK para instalar el driver seleccionado.

La opción avanzada en el cuadro de diálogo de instalación del ODBC presentará el Administrador con opciones para verificación de versión. Regularmente la verificación de versión no debe ser cambiada de su estado original.

Los defaults asegurarán que las últimas versiones de los drivers y traductores sean instaladas en el servidor.

Además actualmente gratuitamente están disponibles servidores de correo electrónico y noticias:

- MCIS Mail Server

- MCIS News Server

El uso de estas herramientas es opcional, sin embargo para el presente trabajo, cumplen los requisitos para desarrollar una Intranet flexible, escalable y cumple con las necesidades actuales.

Internet Information Server

Servicios de Publicación

FTP

Este servicio de publicación proporciona los servicios estándar del Protocolo de Transferencia de Archivos (FTP) para servidores basados en Windos NT . La Transferencia de Archivos permite que sean transferidos archivos de texto o archivos binarios por medio de conexiones de TCP/IP. FTP usa el protocolo TCP, un protocolo orientado a conexión que requiere la instalación de un circuito virtual entre el cliente y el servidor FTP.

El Servicio de Publicación FTP es una versión mejorada del servicio que actualmente se incluye en el Servidor de Windows NT.

Las mejoras incluyen:

- Hacer alias de los directorios.
- Verdaderos Directorios "Raíz".
- Autentificación de Usuarios mejorada
- FTP "Pasivo"

Gopher

Este servicio es una implementación estándar del servicio de Gopher. Gopher permite búsquedas en directorios y vínculos a otros directorios y/o servicios, ambos en el mismo servidor o para un servidor localizado en cualquier parte desde donde el usuario pueda conenctarse.

Gopher proporciona algunas de las cacterísticas que tienen los servidores de Web, incluyendo los vínculos a otros servidores, la habilidad de reconocer un tipo de archivo y asociar ese tipo con una aplicación y automáticamente bajar el archivo, activando la aplicación con el archivo cargado.

World Wide Web

Este servicio, conocido también como WWW, permite que los documentos sean servidos desde el servidor basado en Windows NT a cualquier usuario con un buscador WWW, proporcionando acceso "point-and-click" a la información en ese servidor y vínculos a otros archivos y directorios world-wide con el uso de URL's (Uniform Resource Locators).

Características del IIS

- **Servidores Virtuales**

Los servidores virtuales, también conocidos como servidores Multi-Homed, proporcionan a una instancia simple del Servicio de Publicación del World Wide Web la habilidad de atender peticiones de clientes y hacer que la respuesta venga de diferentes servidores. Esto permite que un cliente haga la petición de un archivo desde un servidor WWW como:

http://abc.com/default.htm

y pedir un diferente archivo desde un URL diferente tal como:

http://xyz.com/index.htm

En el cual esos archivos son actualmente proporcionados desde el mismo servidor de publicación WWW. Esto permite, que para Intranet con un sólo servidor poderoso que se instale, pueda ser representada cierta cantidad de "sitios" diferentes.

Instalar Servidores Virtuales requiere entradas únicas en el servidor DNS que sea autoritario para los dominios afectados.

- **Creación de Alias para Directorios**

Creación de Alias para Directorios es la habilidad de crear vínculos a los directorios que se presenten al cliente como sub-directorios del directorio original del server. Estos son, de hecho, directorios que se localizan dentro de un directorio árbol diferente, un volumen diferente, o un servidor completamente diferente.

- **Administración Remota**

Tal como en la mayoría de las herramientas administrativas para servidores basados en Windows NT, el Internet Service Manager permite la administración remota de cualquiera de los servicios del Internet Information Server para ser controlados y configurados desde una estación de trabajo, un servidor remotos basados en Windows NT, o desde un paginador.

- **Registro**

El Internet Information Server, permite el registro del acceso a los servicios así como a una base de datos SQL/ODBC, o un archivo. Con la opción de registro a un archivo seleccionada, el administrador puede escoger el directorio en el cual desea colocar los archivos de registro y el criterio para crear un nuevo archivo de registro: ya sea crear un

nuevo archivo en un periodo de tiempo dado (día, semana, mes), o crear un archivo nuevo cuando el archivo existente alcance un tamaño predeterminado.

- **Configuración Usando Páginas de Propiedad**

La configuración de estas opciones se lleva a cabo por medio del Internet Service Manager, eleccionando File/Properties las hojas de propiedades para el Servicio de Publicación seleccionado.

Internet Service Manager

El Internet Service Manager (ISM) proporciona la interfase para manejar los servicios del IIS. El ISM permite la administración remota de los servidores, incluyendo la habilidad para empezar, terminar, o pausar el servicio.

El ISM permite que el administrador seleccione el servidor a manejar, o buscar otras las instalaciones del IIS. Pueden seleccionarse diferentes vistas de los servicios de los servidores dependiendo de las preferencias del administrador. Los servicios pueden ser agrupados por servidor o por estado del servicio (es decir, corriendo, detenidos o pausados). Cualquiera de los tres, o todos los servicios a la vez pueden ser desplegados.

- **Selecciones de Ordenamiento**

La información desplegada puede ser ordenada por medio de la selección de opciones desde el menú de View, o bien dando click en la aplicación en los encabezados de las columnas.

Las opciones de ordenamiento son por:

- Computadora
- Servicio
- Estado (de servicio)
- Comentarios
- Barra de Herramientas del ISM

- **Conexiones de Servidor**

Connect to Server. Permite al administrador seleccionar un IIS específico al cual conectarse.

Find Information Server. Al seleccionar este ícono se hará una búsqueda en la red de cualquier IIS.

Properties. Esta opción traerá la Página de Propiedades para el servicio seleccionado.

Estado de Servicio

Start Service. Esta selección empezará un servicio detenido o continuará un servicio que estaba en pausa.

Stop Service. Esta opción detendrá un servicio que está corriendo o en pausa.

Pause Service. Esta opción pondrá en pausa un servicio que esté corriendo o constinuará un servicio que estaba en pausa.

Vistas del Servidor

Cualquiera de estos tres botones son intercambiables. Si están seleccionados, los servicios de esa categoría se muestran, de lo contario no son desplegados.

- View FTP Serveres - Despliega los servidores FTP disponibles.
- View Gopher Servers - Despliega los servidores Gopher disponibles.
- View WWW Servers - Despliega los servidores WWW disponibles.

Internet Explorer

Internet Explorer es un navegador de Web con soporte a HTML (Hypertext Markup Languaje), ActiveX, Java y Netscape Plug-in. Internet Explorer provee una plataforma de desarrollo para usuarios, organizaciones y desarrolladores. Además Internet Explorer cuenta con capacidades de conferencia en Internet, colaboración, personalización y realidad virtual; lo cual incrementa su funcionalidad sin perder la facilidad de uso.

- **Facilidades de Uso**

Internet Explorer incluye características como:

➢ **Rápida Exploración**

Grandes barras de botones que cambian de color cuando se apunta sobre ellas y direcciones URL simplificados son algunas de las formas en que navegar el Web es más sencillo con el IE. Para buscar información más rápido, el botón de búsqueda provee acceso instantaneo a las poderosas herramientas de búsqueda en el Web: Yahoo, Lycos, Infoseek, Webcrawler, Altavista, etc.; con la posibilidad de configurar la herramienta predeterminada. También permite la creación de shorcuts a Intenet con tan solo arrastrar y soltar hiperligas al escritorio.

- **Autobúsqueda**

Con el IE, buscar dentro de Internet es mas fácil que nunca. Simplemente con escribir una prase de dos o mas palabras en la barra de direcciónes URL, y el IE despliega una lista de resultados de la búsqueda en Yahoo. Para buscar una sola palabra, basta con escribir "find" antes de la palabra, y "go" después de ella, o simplemente escribir un signo de interrogación después de la palabra.

- **Impresión mejorada**

IE provee una mejor impresión con la capacidad de imprimir tablas de hiperligas al imprimir una página Web. De esta forma conocer la URL de la hiperliga es posible, sin volver a visitar el "site". También el IE provee la presentación preliminar de la página, la impresión de partes de la página Web y soporta arrastrar y soltar páginas del IE hacia la impresora. Además permite continuar buscando otras páginas mientras imprime.

- **Botones Sensitivos**

Los grandes y amigables botones que cambian de color cuando el ratón esta sobre ellos, incrementan la facilidad con la cual las personas pueden navegar. Además, textos descriptivos bajo los botones pueden adaptarse a la apariencia de las ventanas.

- **Cuadro de Diálogo de Información para transferencias de archivos**

Este cuadro provee información acerca del tamaño del archivo y una estimación del tiempo previsto para completar la transferencia.

- **URLs simplificadas**

IE determina el protocolo para un site en particular. En una intranet o en cualquier servidor de web, no es necesario escribir "http".

- **Menúes Contextuales**

IE utiliza el estilo de Windows 95 y provee menúes contextuales para gráficas e información de las páginas Web. Estos son accesados presionando el botón derecho sobre ellos, proveyendo rápido acceso a comandos sobre el objeto seleccionado.

- **Accesos Rápidos a Internet**

IE extiende el uso de accesos rápidos (shortcuts) a sites de Internet e Intranet. En vez de apuntar a un archivo en la PC o dentro de la LAN, una Internet shorcut puede apuntar a un URL (Uniform Resource locator) en Internet. Una Internet shorcut puede ser incrustada en un documento, correo electrónico o en algún folder de la computadora. IE soporta "arrastrar y soltar" para crear los shortcuts.

➢ **Soporte a HTML 3.2**

HTML Web

Todo el del Web puede ser visto en el IE por el soporte a los últimos estándares de HTML, incluyendo HTML 3.2. Por esto, IE soporta W3C (World Wide Web Concilium) plantillas, tablas, bordes y recuadros. Esta implementación permite presentar una gran variedad de información de manera mas interesante y dinámica.

➢ **Plantillas**

IE soporta el estándar del W3C de plantillas en cascada (Cascading Stylessheets, CSS). Las plantillas permiten tener la misma flexibilidad en el diseño y formato que en los programas de publicidad, permitiendo añadir estilos (letras, colores, espacios) al texto tradicional de HTML.

Al aplicar diferentes banderas al texto, asegura la compatibilidad con otros navegador, mientras hacen mas flexible y sofisticado el diseño de páginas para los nuevos navegadores que soporten plantillas. Las plantillas mejoran las páginas Web con control sobre márgenes,espaciamiento, ubicación de los diversos elementos de la página, y especifican colores, fuentes y diferentes tamaños. Si es necesario cambiar la apariencia de cierta página, solo hay que actualizar la plantilla, en vez de cambiar todas las banderas de la página.

➢ **Paneles (frames)**

Al soportar el estandar HTML 3.2, IE permite dividir la página Web en diferentes secciones llamados paneles (frames). Cada panel despliega una diferente página HTML, desplegando varios niveles de información sin que el usuario navegue a diferentes páginas o cambie de site. IE aceptar paneles sin bordes, estáticos o dinámicos independientes entre sí.

➢ **Tablas**

La versión HTML 3.2 aumenta el número de banderas de tablas, para tener un mayor control sobre el texto, gráficas y colores e imágenes de fondo; permitiendo crear tablas atractivas y eficientes. IE permite: asignar diferentes colores y fondos a cada una de las celdas, alinear el texto de acuerdo a una línea de base, especificar bordes internos o extos, celdas que ocupen mas de una columna o fila, y agrupar celdas.

➢ **Fuentes**

IE permite especificar el tamaño, forma y color de una fuente (tipos de letras), de manera exacta. Además soporta diferentes tipos de fuentes, incluyendo las True Type Font (TTF).

➢ **Objetos**

IE utiliza las banderas OBJECT para la inserción de objetos como: controles ActiveX, Java applets, y Netscape Plug-ins, en una página Web. Esta bandera es una de las principales especificationes del W3C reemplazando a las banderas APPLET y EMBED. Esto permite a los desarrolladores generar páginas mucho mas amigables y poderosas.

➢ **Multimedia**

El uso de marquesinas, video en línea y sonidos de fondo en el IE, hace la experiencia de navegación mas útil e impactante.

Marquesinas. Permiten desplegar texto de manera dinámica, mostrando ofertas especiales e información crítica, de una forma atractiva al usuario.

Reproducción de Video en Línea. Despliega animaciones en formato AVI en una página Web al abrirla, después de presionar el ratón, o al mover el ratón sobre la animación.

Sonidos de fondo. Reproduce sonidos en los formatos mas comunes: WAV, MIDI, AU e AIFF, para crear "dramáticas" introducciones a las páginas, reproducir continuamente sonidos o translaparlos.

➢ **Apariencia**

IE brinda el poder de gráficas encontrado en herramientas de diseño, al ubicar las gráficas en la posición exacta, controlar la superposición de objetos y su transparencia. Los objetos pueden ser posicionados con respecto al alto, ancho y profundidad de una región.

Internet Mail and News

Pequeño, rápido y simplificado, el IMN, permite enviar y recibir correo rapidamente en Internet o Intranet, y subscribirse a newsgroups con su flexible lector. Su completa integración con IE permite revisar newsgroups o enviar correcto mientras se navega. Al usar la misma interface de IE, los usuarios pueden comenzar a usar IMN rápidamente, sin tener que aprender una nueva aplicación.

Una de sus principales características, es el uso de hiperligas dentro de los mensajes de e-mail y news. Cualquier texto que comienze con http:, ftp:, mailto:, telnet:,

file:, o una direección de e-mail, automáticamente se interpreta como una hiperliga. Al presionar en una dirección listada en un mensaje de e-mail, IMN abre el nuevo mensaje e coloca la dirección seleccionado al mensaje. Viceversa, seleccionando un URL en un mensaje e-mail, IE se activa en la dirección seleccionada.

IML también incluye soporte a HTML, el cual permite ver y enviar mensajes en texto simple, o en formato compuesto HTML. Además en base al soporte internacional del IE, IMN acepta cualquier caracter para enviar y recibir mensajes en diferentes lenguajes.

Microsoft Internet Mail (MIM)

Este simple y poderoso cliente utiliza los protocolos estándares de Internet: SMTP y POP3, para enviar y recibir correo e-mail a través de servidores de correo. La interface del usuario es similar a la del IE, incluyendo sus fáciles barras de herramientas, las cuales acceden a las funciones de e-mail mas comunes.

MIM incorpora una variedad de características que hacen enviar e-mail sencillo. Por ejemplo, el Inbox Asistant, administra los mensajes de acuerdo a opciones determinados por el usuario. El correo puede ser ordenado en base a las diferentes columnas seleccionadas. La fácil organización de los mensajes en folders. También existe una libreta de direcciones con funciones de búsqueda y ordenamiento.

Microsoft Exchange y MIM son compatibles. Los mensajes pueden ser importados o exportados de ambas aplicaciones, y las libretas de direcciones, ser exportadas desde Microsoft Exchange al MIM.

Otras funciones del MIM son.

- Corrección de ortografía si Microsoft Office 95 o superior, esta instalado.
- Uso en línea y fuera de línea.
- Panel de presentación preliminar, para la rápida lectura de mensajes.
- Personalización del correo con firmas automáticas.
- Automáticamente borra los objetos borrados cuando el MIM es cerrado.

Microsoft Internet News (MIN)

Este lector de news, tiene compatibilidad con los Internet newsgroups, con la capacidad de subscribirse, añadir y leer mensajes de foros de discusión de Internet o Intranet.

MIN comparte la misma interface del MIM, incluyendo la presentación preliminar de folders, con opciones adicionales a la lectura de news: personalización, newsgroups predeterminado. Además el soporte a SSL (Secure Sockets Layes) permite leer

información de manera segura. Las firmas automáticas perzonalizan los mensajes y el autor se copia automaticamente al replicar un mensaje.

Además el MIN ofrece las siguientes ventajas:

- Uso del protocolo estandar NNTP.
- Visualización de las conversaciones para fácilmente seguir un mensaje.
- Selección del newsgroup con presionar el ratón.
- Decodificación automática de archivos binarios incrustados.
- Administración de los mensajes enviados, grabados y añadidos.

Administración de Documentos

La Intranet consiste de uno o varios servidores de Web, cada uno formado por varias páginas Web. Al preparar la creación del sitio Web, el diseñador debe decidir que será publicado. La información debe estar dividida en páginas Web.

Un importante paso en el desarrollo de páginas Web es un organigrama. El organigrama permite a los diseñadores Web delinear en papel el de cada página dentro de la Intranet. Esta actividad es critica cuando mas de un diseñador esta involucrado en la preparación de la Intranet. Los pasos a seguir son:

- Organización de Documentos
- Organigrama
- Diseño de Documentos
- Equipo de Desarrollo del Web

Organización de Documentos

Antes de comenzar el desarrollado de páginas de la Intranet es necesario:

- Recolectar la información.
- Organizar la información por temas o departamentos.
- Identificar los temas para crear un organigrama, escogiendo los cambios de información como separadores de página
- Crear un logotipo para cada una de las páginas.

Para facilitar la administración de las páginas, se debe crear un documento separado para cada tópico identificado. Al punto de inicio del Web se le conoce como página de bienvenida (home page) o de índice. Desde la página de bienvenida se deben establecer los vínculos hacia otras páginas o recursos de la Intranet. No hay límite para el número de páginas dentro del sitio Web.

Existen varias consideraciones principales en el diseño de un sitio Web para Intranet:

- Informar y guiar a los usuarios de la Intranet a través de un conjunto de información vinculada.
- Crear un diseño visual del organigrama en HTML.
- Definir un formato estándar para las páginas para que los usuarios comprendan mejor el y la distribución física de la Intranet.

Organigrama

Para organizar el sitio Web, es importante esquematizar las ideas antes de crear las páginas HTML. Un organigrama sirve para arreglar la secuencia de s, vínculos, imágenes y transferencias de archivos.

Los pasos para crear el organigrama son:

1. Definir el propósito de la presentación y la audiencia de los usuarios.
2. Desglosar el en los principales temas y agrupar información similar.
3. Utilizar una plantilla o un software de diagramas de flujo para crear unn breviario de cada página Web, iniciando con la página de bienvenida.
4. Definir la siguiente información para cada página:
    - Un título descriptivo
    - El encabezado principal
    - Los subtítulos
    - El propósito de la página
    - Una descripción del
    - Los tipos de imágenes
    - Una descripción de cada vínculo

Los organigramas son especialmente útiles cuando un equipo de diseñador está construyendo el sitio. Los miembros del equipo deben reunirse para discutir la división del del sitio en las diferentes páginas. Si la organización del sitio Web no se realiza antes de crear los documentos en HTML, el sitio puede ser dificilmente desarrollado.

Título:	Página de Bienvenida a la Intranet
Encabezado:	Bienvenido a la Intranet
Nombre del Archivo:	default.htm
Propósito de la Página:	Proveer una introducción de las funciones y vínculos de la Intranet
Subtítulos:	s, Directorio, Ayuda
Gráficas Propuestas:	Intranet.Gif, Directorio.Gif, Ayuda Gif
Ligas Propuestas:	Mapa de Documentos - mapa.htm, directorio del Personal - directorio htm , Preguntas Frecuentes - pf.htm

Diseño Lineal

Un diseño lineal del sitio Web es apropiado cuando los usuarios visitan las páginas secuencialmente sin moverse entre ellas. Los materiales de capacitación y de procedimientos son ejemplos de un sitio con un diseño lineal.

Diseño Jerárquico

El diseño jerárquico comienza con una página maestra, normalmente llamada la página de bienvenida o de índice. Desde esta página, el usuario puede seguir las ligas a otras páginas subordinadas dentro del sitio Web cada una de estas páginas normalmente tiene una liga de a la página de bienvenida.

El usuario puede seguir vínculos lineales dentro del segundo nivel de la jerarquía o pueede regresar al primer nivel al mismo tiempo. Esto permite a los usuarios accesar a información dentro del sitio sin buscar en cada página.

Diseño Lineal y Jerárquico

Un sitio Web completo contiene una combinación de diseños lineales y jerárquicos. Algunas Intranets contienen múltiples páginas con jerarquías de varios niveles. La complejidad del sitio depende de varios factores incluyendo:

- La cantidad de información.
- La complejidad de la información
- Los intereses de los usuarios
- La incorporación de multimedia

Diseño de Documentos

Después de crear el organigrama del sitio, dividiendo los s lógicamente y determinando la jerarquía apropiada del sitio, se debe considerar el diseño del sitio Web. Un diseño adecuado hace a la Intranet mas atractiva para los usuarios aumentando su productividad.

Al personalizar el Web se debe balancear el aspecto creativo-artístico con la necesidad de transmitir información efectiva y eficientemente, de preferencia una interface que facilite el intercambio de información.

Un sitio bien diseñado es una organización simple. Algunos consejos son:

- Mantener una interface estandarizada para todas las páginas dentro del sitio Web.
- Limitar el número de salidas del sitio.
- Mantener los vínculos en un solo lugar, por ejemplo al final de la página.
- Permitir a los usuarios regresar a la página de bienvenida.
- No poner listas de vínculos en formas de párrafos.
- No saturar el sitio con demasiadas imágenes.
- Evitar largos párrafos.

Equipo de Desarrollo del Web

El desarrollo del Web de la Intranet es mejor con un equipo de desarrollo. Para permitir a este equipo construir el sitio Web rápida y facilmente, cada miembro debe tener definido una función y una responsabilidad.

Los tres miembros básicos de un equipo de desarrollo son:

1. Desarrollador del Web
2. Programador
3. Autor de HTML

- **Desarrollador del Web**

El Desarrollador del Web es el responsable de crear el sitio Web y escribir los scripts del cliente y del servidor necesarios para mejorar la funcionalidad de las páginas Web.

- **Responsabilidades**
  - Construir la arquitectura del sitio Web. Esto incluye definir las páginas y los vínculos.
  - Añadir scripts del servidor para llamar a los componentes y controles creados por el programador.
  - Escribir scripts del cliente y servidor necesarios para proveer funciones específicas del Web.

- **Herramientas**
  - Visual Interdev. Define y construye la arquitectura del sitio Web, y edita las páginas del Web.
  - Script Wizar. Ayuda a la creación de scripts en el cliente.

- **Programador**

El programador es resonsable de crear y administrar las aplicaciones usadas por el sitio Web.

- **Responsabilidades**
  - Crear applets de Java para mejorar la funcionalidad de las páginas Web.
  - Crear componentes del servidor ActiveX
  - Crear componentes ActiveX para mejorar la funcionalidad de las páginas Web.
- **Herramientas**
  - Herramientas de Programación como Visual Java++ para crear applets de Java
  - Herramientas de Programación como Visual Basic yVisual C++ para crear los componentes y controles ActiveX.
  - Transaction Server para proveer transacciones y administración de recursos para los componentes del servidor ActiveX.

- **Autor de HTML**

El Autor de HTML es responsable de crear la presentación del del sitio Web.

- **Responsabilidades**
  - Crear y mantener las páginas HTML
  - Crear vínculos para facilitar la navegación de todo el sitio Web.
- **Herramientas**
  - FrontPage para crear y editar páginas HTML así como administrar los vínculos de las páginas.
  - Office 97 para crear y editar diferentes tipos de páginas HTML.

Seguridad

La seguridad es una preocupación constante en la Intranet. Los principales métodos de asegurar la información los provee Windows NT, pero el IIS cuenta además con características de: encriptación y autentificación.

Características de Windows NT

Algunos consejos de seguridad utilizando las características de Windows NT son:

El administrador debe controlar las cuentas de los usuarios. Las cuentas de usuarios asignadas al grupo de Administradores deben esta limitadas para evitar su mal uso. El administrador debe mantener estrictas políticas de cuentas. Por ejemplo, utilizar contraseñas alfanuméricas y cambiarlas frecuentemente para los usuarios mas importantes.

El sistema de archivos NTFS debería ser utilizado en todas las unidades accesadas desde la Intranet.

Después de instalar el servidor se deben remover todos los permisos al grupo Everyone y asignar los permisos según sea necesario. Además se deben remover todos los permisos inecesarios de los recursos compartidos.

Reducir el número de protocolos usados por las tarjetas de red, removiéndolos o desligándolos.

Detener el servicio de Server para prevenir a los usuarios de ver los recursos compartidos en el IIS.

Características del IIS

Opciones de Autentificación de la Contraseña

Los métodos soportados por el IIS para la autentificación de los usuarios son:

Allow Anonymous. El IIS acepta conecciones anónimas utilizando el nombre de usuario y contraseña especificada.

Basic (Clear Text). El IIS solicita el nombre del usuario y la contraseña, y los transmite sin encriptación por lo que no es muy recomendable aunque todos los paginadores lo utilizan.

Windows NT Challenge/Response (NTLM). El IIS solicita el nombre del usuario y la contraseña, y los transmite utilizando el protocolo de autentificación de Windows NT Challenge/Response. Este protocolo utiliza un algoritmo de hash para prevenir que la contraseña sea transmitida a través de la red. Aunque es el método mas recomendado, desgraciadamente no todos los paginadores soportan este tipo de autentificación.

Este proceso de autentificación se inicia automáticamente como resultado de un error de acceso denegado a una solicitud de acceso anónimo.

Controlando el acceso por nombre de usuario

El servicio de WWW puede ser configurado para forzar a los usuarios a identificarse con un nombre de usuario válido y una contraseña antes de utilizar el servicio.

Si se aceptan usuarios anónimos utilizando la cuenta de *Internet Guest*, se deben restringir los derechos de la Internet Guest, el grupo Guest y Everyone a "*Log on Locally*" y asignar los permisos NTFS necesarios sobre los directorios usados por el IIS.

Si se utiliza autenficación básica o Windows NT Challenge/Response, los usuarios deberán introducir su nombre de usuario y contraseña para poder utilizar los s del servidor.

Conecciones Anónimas

Una coneccion anónima occurre cuando la solicitud del cliente no contiene un nombre de usuario y contraseña. Esto ocurre en los siguientes casos:

- Un cliente FTP se valida con el nombre de usuario anonymous.
- Cualquier solicitud al servicio de Gopher
- El encabezado de la solicitud HTTP no contiene un nombre de usuario y contraseña (esta es la opción predeterminada de algunos paginadores).

Cada servicio de Internet mantiene un nombre de usuario de Windows NT y una contraseña para ser usada para procesar las peticiones anónimas. Las solicitudes son exitosas si la cuenta de usuario tiene permisos para utilizar el recurso solicitado. Para HTTP, si el usuario no tiene permisos, la contestación al cliente contiene una lista de los esquemas de autentificación soportados para poder usar el recurso basado en la configuración del servidor.

La instalación del IIS crea una cuenta de usuario en el servidor para losa ccesos anònimos. El nombre del usuario tiene la forma IUSR_*nombre_del_servidor* y una contraseña generada aleatoriamente.

Por seguridad se recomienda cambiar la contraseña desde el IIS y en el User Manager.

Controlando el Acceso a Directorios

A menos que sea parte de la estrategia para compartir información, la opción de *Directory Browsing Allowed* del servicio de Web debe estar desabilitada.

Controlando el Acceso por Direcciones IP

El IIS puede ser configurado para otorgar o denegar el acceso a ciertas direcciones IP específicas a través de las opciones avanzadas del servicio de WWW.

Encripción y Autentificación

Existen varios métodos para asegurar los paquetes transmitidos a través de la Intranet. Dos de los principales métodos son la autetntificación y la encripción. La autentificación incluye al cliente y al servidor, mientras la encriptación se refiere a la condificación de los paquetes.

La capa de filtros del *Internet Server Application Programming Interface* (ISAPI) utiliza encripción y autentificación. Esto facilita el proceso de los mensajes antes de llamar al IIS.

El IIS soporta los siguientes esquemas de seguridad:

Secure Sockets Layer. SSL es un protocolo entre las capas TCP y HTTP. SSL provee autentificación y encripción del servidor e integridad de los datos.

Personal Communication Technology. PCT es un protocolo de aplicación, abierto para el desarrollo de aplicaciones. Aunque basado en SSL, PCT esta optimizado y es mas rápido.

Secure Electronic Technology. SET es un esquema de encripción y autentificación usado para transacciones financieras. ESta diseñado para pagos de tarjetas de crédito en Internet.

Point to Point Tunneling Protocol. PPTO es un protocolo de acceso.

Rendimiento

La implementación de encripción y autentificación afecta la velocidad de transmisión de los paquetes, por lo que se debe utilizar solamente para información muy importante.

Secure Sockets Layer

El protocolo SSL provee comunicación de datos segura a través de encripción y desencripción. Un servidor con SSL habilitado, pueede enviar y recibir información a través de la Intranet a paginadores con soporte a SSL. Sin embargo, el uso de SSL requiere de un certificado digital SSL (SSL digital certificate).

SSL es un protocolo entre las capa de transporte TCP y la de aplicación HTTP. SSL provee autentificación del servidor, encripción e integridad de datos con los siguientes beneficios:

La autentificación asegura al cliente que los datos están siendo enviados desde el servidor adecuado y que el servidor esta seguro.

La encripción asegura que los datos no pueden ser leidos por nadie mas que el servidor receptor.

La integridad de los datos asegura que los datos siendo transferidos no han sido alterados.

Certificado Digital SSL

Antes de utilizar SSL se debe obtener un Certificado Digital SSL para el servidor de una autoridad de certificación (como Verising Inc.).

El Key Manager genera un par de llaves para el sistema en un archivo. Este archivo es enviado a la autoridad de certificación. La autoridad de certificación responde enviando la verificación del certificado digital. Este certificado digital se instala con el Key Manager.

Una vez aplicado el certificado, la característica de SSL es habilita del Internet Service Manager. SSL puede ser usado para cualquier directorio virtual configurado en el IIS.

Index Server

Index Server es un módulo de indexación y búsqueda del texto y propiedades de los documentos almacenados en el IIS. Con el Index Server los clientes formulan búsquedas utilizando desde cualquier paginador llenando los datos de una forma de búsqueda. El Index Server también puede indexar los s de texto de documentos con formato publicados en la Intranet, como Word y Excel.

El conjunto de todos los documentos almacenados en el IIS para ser indexados es llamado el corpus. El corpus es almacenado en uno o mas catálogos. El administrador determina el alcance del corpus indicando sobre que directorios virtuales realizar la búsqueda.

Index Server buscar los documentos del conjunto de directorios virtuales y los filtra. La salida filtrada es enviada a un word breaker, el cual divide las cadenas de caracteres en palabras. Las palabras son enviadas al normalizador, el cual remueve las palabras "ruidosas" (palabras con poco significado independientemente del contexto: artículos, preposiciones, conjunciones,etc.).

El conjunto de palabras resultante es entonces indexado en tres partes:

1. Listas de Palabras: almacenadas en RAM temporalmente.
2. Indice Shadow
3. Indice Maestro.

Instalación

Para instalar el Index Server se necesita:

- Windows NT Server 4.0
- Internet Information Server
- 16Mb RAM
- 3 a 12 MB en Disco Duro basándose en los idiomas instalados.
- Espacio en Disco suficiente para los índices, aproximadamente un 40% del tamaño del corpus.

Número de Documentos	Memoria Mínima	Memoria Recomendada
menos de 10,000	32	32
10,000 a 250,000	32	64-128
250,000 a 500,000	64	128-256
500,000 o mas	128	256

Parámetros de Instalación

Los componentes a instalar el Index Server son:

- Páginas de búsqueda de ejemplo
- Scripts de búsquedas de ejemplo
- Datos (Indices)

En particiones NTFS, la instalación establece los permisos de seguridad automaticamente.

Iniciando y Deteniendo el Index Server

Después de instalar el Index Server, las páginas de ejemplo ya permiten realizar búsquedas.

El Index Server no se inicia automaticamente con el IIS. La primera búsqueda inicia el proceso de indexación de los datos. El Index Server se detiene cuando el IIS se detiene.

Características de Indexación

Los índice son controlados por directorio. Un índice es construído sobre un conjunto de directorios y subdirectorios. Es posible incrementalmente actualizar un índice, indexando solamente los cambios.

Index Server incluye diferentes monitores de rendimiento para ayudar al administrador a opmitizar su servicio de búsquedas. Estos monitores miden criterios como el número de documento a ser indexados y que tan rápido son procesadas las búsquedas.

Index Server provee las siguientes características básicas:

- Indexación de páginas Web.
- Indexación de texto en documentos formateados como Word o Excel.
- Actualización incremental de los índices.
- Control de los índices por directorio.
- Indexación de propiedades
- Indexación independientemente del lenguaje.
- Actualización automática de índice.
- Monitoreo de Rendimiento
- Diseño de "cero mantenimiento".
- Poca sobrecarga del sistema.

Soporte a Varios Lenguajes

Indexación y búsquedas en diferentes lenguajes son características estándares del Index Server. Estas utilerías incluyen word breakers, stemmers, y normalizadores para varios idiomas. Index Server puede indexar documentos en varios idiomas diferenciando entre los idiomas según sea neceario.

Proceso de Indexación

Cuando un documento en el servidor IIS es modificado, el sistema de archivos notifica al Index Server del cambio. Index Server pudiera no indexar el documento instantaneamente. La indexación ocurre en background cuando hay suficientes recursos disponibles en la computadora sin afectar el rendimiento del sistema. Cuando el Index Server dice que puede indexar los cambios, abre el documento e inicia el proceso de indexación.

El proceso de indexación consiste de tres pasos principales:

1. Filtrado de los indices. Los filtros, de acuerdo al formato del archivo, extraen las cadenas de texto, se reconocen los cambios de idioma y manejan los objetos incrustados.
2. Word Breaking. Según el idioma dividen las cadenas de caracteres en palabras válidas de acuerdo a la estructura y sintáxis del idioma.
3. Normalización. La normalización depura las palabras emitidas por el word breaker, involucra detalles como el uso de mayúsculas y minúsculas, la puntuación y elimina las palabras "ruidosas" (preposiciones, conjunciones, artículos, etc.).

Una vez normalizada una palabra, finalmente, se coloca en el índice del sistema.

Tipos de Indices

Hay tres tipos de índices:

1. Listas de palabras: es volátil, los datos son almacenados en RAM.
2. Índices shadow: permanente, los datos son almacenados en disco.
3. Un índice maestro: permanente, los datos son almacenados en disco.

Las palabras y propiedades extraídas del documento primero aparecen en una lista de palabras, después se mueven al indice shadows, y finalmente al índice maestro. Esta organización esta optimizada para las búsquedas y el rendimiento de los recursos. Aunque existen varios índices internamente (máximo 255), esto es completamente oculto para el usuario.

Tipos de Merges

El proceso de combinar los datos de múltiples índice en uno solo es llamado merging. El resultado del merging en eliminar parte de los datos redundantes y también liberar recursos. Además las búsquedas son resueltas mas rapidamente con pocos índices. Los tres tipos de merges son:

Merge	Combina	Genera
Shadow	Listas de palabras Indices Shadow	Indice Shadow
Master	Indices shadow Indice maestro	Indice Maestro
Annealing(*)	Indices shadow	Indices shadow

(*) es una clase especial de shadow merge, efectuado cuando el sistema esta ocupado y se supera el número de indice persistentes ideal.

Catálogos

Un catálogo es la unidad superior de organización del Index Server. Cada catálogo es una estructura independiente, contiene un índice y las propiedades de uno o mas rutas virtuales. El Index Server no soporta búsquedas en varios catálogos.

La ubicación del catálogo predeterminado es definido durante la instalación y almacenado en la entrada del registry: IsapiDefaultCatalogDirectory.

Las dos principales razones para crear varios catálogos son:

1. Distribuir las búsquedas
2. Soportar servidores virtuales

Debido a que es imposible crear una búsqueda a mas de un catálogo es importante considerar las consecuencias de crear múltiples catálogos. Por otro lado, al dividir físicamente el conjunto de rutas virtuales en varios catálogos mejora el rendimiento de las búsquedas.

Búsquedas

Los componentes principales de una búsqueda son:

El ámbito de la consulta: especifica donde se realizará la búsqueda y describe el conjunto de documento dentro del corpus que será analizado.

Criterios de búsqueda en el de los documentos.

Criterios de búsqueda en las propiedades de los documentos almacenados (tamaño de archivo, fecha de monificación, autor, etc.).

Los resultados de la consulta.

Las características de búsquedas básicas son:

- Limitar la búsqueda a cierto ámbito.
- Buscar palabras y frases dentro del del documento.
- Buscar palabras o frases relacionados a palabras o frases.
- Buscar palabras y frases dentro de las propiedades de los documentos.
- Utilizar operadores de comparación como <, <=, =, =>, >.
- Utilizar operadores booleanos como AND, OR, y AND NOT.
- Usar comodines como "*" y "?".
- Compatible con el modelo de seguridad de NT.
- "Quality ranking for hits"
- Contestar con propieades específicas de los datos

Formas de Búsqueda

Las formas de búsqeda permiten a los usuarios especificar sus búsquedas llenando campos de una forma. El usuario puede buscar por características específicas, como todos los documentos que contengan una frase en particular con resultados ordenados de la mejor a la peor búsqueda presentados de diez en diez. El usuario puede también pedir al sistema el nombre del documento, un pequeño resumen, un vínculo al documento, su tamaño y la fecha de su última modificación.

Utilizando Index Server, el administrador de la Intranet puede crear una forma personalizada para ayudar a los usuarios a buscar sus documentos. El administrador puede modificar la forma para buscar por propiedades del documento como autor o tema. Las búsquedas son en formato estándar HTML.

Proceso de Búsqueda

El proceso de búsqueda es mas complicado que el de indexación porque debe interactuar con el IIS. El proceso de indexación no interactua con el IIS y es completamente independiente al proceso del servidor Web.

El database connector es una característica del IIS que permite buscar directamente con una base de datos de sistema tipo ODBC. Index Server utiliza este modelo para resolver sus búsquedas. Un programa convierte las datos de las formas a búsquedas compatibles con los índices. El sistema ejecuta la consulta y los resultados son convertidos a una página Web y enviados al usuario.

El database connector utiliza un archivo de ayuda con extensión IDC para realizar la conversión desde la forma. También utiliza un archivo con extensión HTX para dar formatoa los resultados de la búsqueda. Index Server en vez de usar archivos IDC utiliza archivos IDQ.

Parámetros del Archivo IDQ

El archivo IDQ permite declarar parámetros de búsqueda como el ámbito, criterios y forma de desplegar los resultados. Algunos parámetros comunes son:

Código	Significado
[Query]	
CiColumns=filename,size,rank,characterization, vpath, DocTitle, write	Son las propiedades devueltas en los resultados.
CiFlags=DEEP	Realiza la consulta sobre todos los subdirectorios del ámbito.
CiRestriction=%CiRestriction%	Los criterios de la búsqueda a ser evaluados
CiMaxrecordsInResultSet=nnn	El número máximo de resultados
Ci MaxRecordsPerPage=nnn	El número de resultados por página.
CiScope=\	Inicia la consulta desde la raíz
CiTemplate=/scripts/[archivo htx]	Especifica el archivo HTX para dar formato. (*)
CiSort=rank[d]	Ordena los resultados descendentemente.
CiCatalog=[root]	Utiliza el índice almacenado en la ruta especificada.

(*) la ruta debe ser del tipo de los directorios virtuales (/scripts/mibusqueda idq), no como una ruta relativa (../ejemplo.idq), física (c.\inetsrv\scripts\mibusqueda), o con notación UNC (\\servidos\scripts\ejemplo.idq).

Resultados de la Búsqueda utilizando archivos HTX

El archivo HTX es un archivo HTML que contiene variables relacionadas con los resultados de la búsqueda. A continuación se presenta un ejemplo:

Código	Significado
<%if CiMatchedRecordCount eq 0%> <H4>Ningún documento cumplió el criterio" <%CiRestrictionHTML%>".</H4> <%else%> <H4><%CiMatchedRecordCount%> documento(s) encontrados </H4>	Ningún documento cumplió el criterio "precios" ó 50 documento(s) encontrados.

Administración Básica

Index Server está diseñado para minimizar la administración, como el indexar los archivos. Por omisión, todos los directorios virtuales raíces son idexados.

Las formas de administración son muy similares a las búsquedas, excepto que los parámetros son almacenados un archivo IDA en vez de un IDQ. El Index Server incluye una página de administración.

Algunas funciones administrativas pueden cambiar el estado de los índices. Las funciones administrativas están restringidas de acuerdo a los permisos de Windows NT.

Monitoreo de Rendimiento

Las dos formas para monitorear el rendimiento del Index Server son:

1. Performance Monitor
2. Script IDA.

La información es muy similar, sin embargo el método de traer los datos son muy distinos. Ambas soluciones pueden ser usados localmente o desde el cliente. El Performance Monitor tiene la ventaja de actualizarse automáticamente, además de las capacidades gráficas y de registro. El método de los scripts es mas flexible porque pueden ser vistos desde cualquier paginador.

MCIS Mail Server

Mail Server es un servidor de correo electrónico basado en los estándares de Internet y hecho para Windows NT Server. Mail Server provee administración de buzones de usuarios, es escalable, tiene capacidades de ruteo y funciones de autentificación. Mail Server aprovecha las características de NT y el IIS, como puertos y threads, para soportar múltiples conecciones simultaneas. Mail Server es compatible con productos basados en SMTP y POP3.

Características

Las principales características del Mail Server son:

- Cumple con SMTP, POP3 y MIME.
- Arquitectura de almacenamiento escalable. El almacenamiento de los buzones utiliza NTFS y permite incrementar la capacidad para distribuirlos entre varios servidores. Mail Server divide los procesos de almacenamiento y atención al cliente para escalar el número de buzones independientemente del número de conecciones simultaneas.
- Administrable a través del Internet Service Manager. Los administradores pueden aprovechar características de administración como el registro de transacciones.
- Administrable a través de cualquier paginador.
- Utiliza características de administración de Windows NT como el Performance Monitor, monitoreo SNMP y registro de eventos. Estas herramientas permiten

a los administradores realizar monitoreo proactivo del rendimiento del servidor e identificar problemas potenciales.

- Fácil de Instalar.
- Utiliza NTLM, el mecanismo de seguridad de Challenge/Response de Windows NT.
- Junto con el Microsoft Membership System, Mail Server usa Microsoft Distributed Password Authentication (DPA), el cual provee un avanzado y distribuido método de autentificación de usuarios, con una sola validación de usuario.
- Definición de listas de distribución para todas las cuentas de correo o para ciertos grupos de cuentas de correo.
- Permite colocar todo el correo recibido en un *drop directory*, permitiendo que el Mail Server sea usado para recibir correo de cualquier otra aplicación.
- Permite colocar todo el correo enviado en un *pickup directory*.

Arquitectura

Mail Server utiliza un servicio de correo distribuido utilizando SMTP y POP3. SMTP representa el agente de transferencia de correo del sistema y es responsable mover el correo a otros servidores de correo. El servicio de POP3 representa el buzón del servidor para los usuarios y es responsable de administrar el buzón del servidor y rutear los mensajes a los usuarios. Mail Server soporta el método de autentificación de POP3, enviando las contraseñas sin encriptar, pero también soporta autentificación.

Mail Server utiliza el formato MIME para añadir documentos dentro del correo y es compatible con cualquier cliente SMTP/POP3.

Integración del Mail Server con el IIS

IIS provee las funciones de administración y puertos de administración y entrega para el Mail Server.

Los servicios de SMTP y POP3 se ejecutan como servicios del IIS. Para consumir pocos recursos, los servicios se ejecutan como threads del proceso IIS.

Componente	Descripción
Routing Table Database	Es una base de datos de SQL con información de las direcciones email y la configuración de los buzones.
Mailbox file Store	Archivo de almacenamiento para los buzones de los usuarios
SMTP Server	El servidor ejecutando el IIS con el servicio de SMTP
POP3 Server	El servidor ejecutando el IIS con el servicio de SMTP
Clientes Externos	Cualquier cliente SMTP/POP3 como Eudora, Netscape, Pine, etc.
Internet Mail and News Client	El cliente integrado con el Internet Explorer, soporta seguridad DPA.
SMTP/POP3 Provider	Un proveedor de MAPI SMTP/POP3
MAPI Client	Cualquier cliente MAPI como el Inbox de Windows 95

Cada uno de los componentes del Mail Server puede ejecutarse en diferentes computadoras o en una sola dependiendo del tamaño y rendimiento del sistema

Routing Table Database (RTD)

La RTD es usada por los servicios de SMTP y POP3.

El servicio de SMTP utiliza la RTD para conocer si una dirección es valida, local o remota.

SMTP y POP3 utilizan la RTD para determinar la ubicación (ruta virtual del IIS) de los buzones locales.

La RTD del Mail Server ha sido diseñada para usar una base de datos de SQL Server para proveer un eficiente proceso de consulta y una gran capacidad.

Mailbox File Store (MFS)

El MFS es utilizado para guardar el correo nuevo de los buzones. La cantidad de espacio en disco disponible afecta la capacidad del sistema de correo.

El MFS del Mail Server es almacenado en directorios virtuales del IIS. Estos directorios del IIS pueden estar mapeados adirectorios locales o a servidores remotos con rutas UNC. Por omisión, todo el correo es almacenado en el directorio vitual MailRoot.

Los buzones utilizan NTFS para hacer uso de los *streams* de NTFS. Los buzones tan solo son directorios, y los mensajes archivos dentro de los directorios.

Instalación

Requerimientos del Cliente

Usuarios

- Windows 95, NT Workstation o NT Server version 3.51 o superior, o cualquier sistema operativo que soporte a un cliente SMTP/POP3.
- Cualquier cliente mail SMTP/POP3.

Administrador

- Windows NT Server o Windows NT Workstation version 4.0.

- Internet Information Server (IIS) version 2.0 (seleccionado Internet Service Manager Extensions en la instalación del Mail Server).

Requerimientos del Servidor

Las computadoras servidor deben cumplir los siguientes requerimientos mínimos:

- Routing Table Database
- Intel 486+ o procesador DEC Alpha
- NT Server version 4.0
- Microsoft SQL Server version 6.5
- 16 MB de RAM
- 50 MB de espacio para SQL Server y la instalación de la base de datos básica, mas ½ GB por cada millón de usuarios.

Servidor de Mailbox File Server

- Intel 486+ o procesador DEC Alpha
- NT Server version 4.0
- 16 MB de RAM
- Espacio en disco duro equivalente al número de buzones por el tamaño máximo mas 30% de sobrecarga de sistema.

Servidor SMTP y POP3

- Intel 486+ o procesador DEC Alpha
- NT Server version 4.0
- IIS version 2.0 con al mennos un servicio (WWW, Gopher, or FTP) instalado
- NT 4.0 Service Pack 1
- NTFS en la partición oara el directorio raíz del correo (solamente en SMTP)
- 16 MB de RAM
- 1-GB en disco duro
- 10 MB de espacio libre para los archivos de programa de SMTP and POP3. SMTP requiere espacio adicional para el directorio *mailroot*. El tamaño depende de la cantidad de correo enviada o entregada por el SMTP.

En instalaciones pequeñas del Mail Server, los cuatro servicios pueden operar en una computadora con 32Mb de RAM y un 1GB en disco duro.

Opciones de Instalación

Durante la instalación se pueden instalar tres componentes:

- Internet Service Manager Extensions. Permite administrar los servicios de SMTP y POP3 desde el ISM.
- SMTP/POP3 Service.
- Routing Table. Permite crera la tabla de ruteo en una base de datos SQL Server. La tabla de ruteo debe existir antes de instalar otros servicios.

Opciones de Intalación de la Tabla de Ruteo

Para cada sitio lógico se debe crear una tabla de ruteo. Durante la instalación es necesario proveer la siguiente información:

- Nombre del servidor SQL.
- Nombre de la cuenta de validación en SQL para crear la base de datos.
- Nombre de la base de datos
- Número de los servidores que utilizarán la tabla de ruteo (para optimizar la base de datos).
- Número de usuarios y listas de distribución (para optimizar la base de datos).
- Información de *devices* para datos, registro y *tempdb.*
- Cuenta de usuario para accesar la lista de direcciones.

La instalación crea siete tablas en la base de datos del Mail Server con información sobre: direcciones email, localizaciones de los buzones, dominios, tamaño máximo del buzón, etc. Además instala ciertos *stored procedures.*

Operación

Iniciando, pausando y deteniendo los Servicios del Mail Server

El Mail Server inicia automáticamente con el servidor por omisión.

Las formas para iniciar, pausar o detener son:

- Internet Service Manager (ISM)
- Servicios del Panel de Control
- Server Manager
- Comando en línea NET

Además desde el Panel de Control y el Server Manager es posible cambiar el modo de inicio del Mail Server a manual o deshabilitarlo.

Administrando la Seguridad y el Acceso

Los clientes POP3 del Mail Server tienen dos piezas de información: la cuenta de NT usada para autentificar las conecciones POP3 y la entrada de la tabla de ruteo que define el dominio del usuario, la ubicación del mailbox e información de configuración de su buzón.

El servicio de POP3 también soporta comunicación secura por medio de Secure Sockets Layer. Instalando un certificado SSL asegura todas las comunicaciones del servidor POP3 independientemente del directorio virtual del buzón. El puerto POP3 SSL es el 995.

Las conecciones del servicio de SMTP y POP3 a la tabla de ruteo de SQL son protegidas por la seguridad por usuario de NT.

Configurando las opciones del Mail Server

El Mail Server es configurado desde la interface gráfica del ISM y con el comando en línea INETCFG, local o remotamente.

Configuración del Servicio SMTP con el ISM

El ISM permite configurar las siguientes opciones del servicio SMTP:

- **Service.** Configura los parámetros de las conecciones y el método de autentificación. Además lista los usuarios conectados.
- **Domains.** Define los dominios a rutear y el dominio predeterminado para correo sin información específica del dominio.
- **Directories.** Da al administrador la opción de especificar donde almacenar la información de los buzones y cuales tablas de ruteo utilizar.

Configuración del Servicio POP3 con el ISM

El ISM permite configurar las siguientes opciones del servicio POP3:

- **Service.** Configura los parámetros de las conecciones, el método de autentificación y el intervalo de expiración del buzón. Todos los usuarios deben autentificarse para que el Mail Server sepa cual buzón utilizar. Además lista los usuarios conectados.
- **Aliases.** Crea los buzones de usuario y las listas de distribución con la siguiente información:
    - Cantidad máxima de correo almacenada por usuario.

- Directorio donde el correo del usuario es almacenado. (Si el usuario no es local, sse puede especificar una dirección remota donde enviar el correo).
- A quien retransmitir el correo enviado para la cuenta configurada.

La tabla de ruteo añade entradas al crear una lista de distribución. El correo enviado a la lista de distribución es automáticamente retransmitido a las direcciones especificadas por la lista.

- **Directories.** Da al administrador la opción de especificar donde almacenar la información de los buzones y cuales tablas de ruteo utilizar.

Registro de Eventos y Transacciones

Mail Server incluye varios tipos de registros para monitorear la operación del servicio.

Registro de Eventos de Windows NT

El Registro de Eventos de Windows NT es usado por el Mail Server para dos tipos de eventos: de sistema y de aplicación.

1. La información, advertencias y errores de los servicios SMTP y POP3 son almacenados en la bitacora de sistema.
2. Los eventos relacionados a la tabla de ruteo son almacenados en la bitacora de aplicación.

Registro de Transacciones del IIS

El Mail Server puede también ser configurado para escribir un registro de transacciones. El registro de transacciones es utilizado para monitorear la actividad del servicio. Por ejemplo, para SMTP, se puede determinar cuando un mensaje ha sido recibido y cuando el mensaje fue entregado a un buzón local. Con el registro de POP3 se puede determinar cuando el mensaje fue extraído del buzón del usuario.

Respaldando y Restaurando el Mail Server

Respaldar y restaurar los archivos de datos del Mail Server involucra a la tabla de ruteo de SQL Server y los directorios virtuales del buzón.

Como los directorios virtuales trabajan sobre particiones NTFS. aunque Mail Server no incluye ninguna utilería de respaldo, se puede utilizar cualquier herramienta para Windows NT. En base a la herramienta usada el respaldo y restauración de archivo puede efectuarse con los servicios de SMTP y POP3 en ejecución.

SQL Server cuenta con sus propias utilerías para respaldar la base de datos con la tabla de ruteo.

Acceso a Bases de Datos

El Internet Information Server actúa como una interfaz entre las páginas de Web de la Intranet y la base de datos en el servidor.

El de los datos se hace a través de un componente del Internet Information Server llamado el Internet Database Connector. Este componente es un DLL llamado HTTPODBC.DLL y es un API de Internet (ISAPI) que usa a ODBC para consultar datos.

Cómo trabaja el Internet Database Connector

La extensión del Internet Database Connector usa dos archivos para controlar la manera en que las bases de datos se consultan y para controlar el resultado de esas consultas:

1. **Internet Database Connector (.IDC):** Este archivo contiene la información necesaria para conectar la página de WEB a un ODBC Data Source y para la sentencia SQL que se piensa ejecutar. Este archivo también contiene el nombre y el lugar donde se encuentra el archivo html.
2. **HTML Extension (.HTX):**Una vez que la conección al Data Source se estableció y la sentencia se ha ejecutado, los registros que se regresaron se mezclan en el archivo html y después se le pasa al Web Browser. La extensión .HTX es una plantilla de un HTML que se regresa al browser.

En su forma más simple, el acceso a los datos con el Internet Database Connector necesita que se le envie la consulta que se ejcutará en la base de datos y que se le regresen los registros en forma de una página de WEB.

Este requiere de cuatro pasos: crear un ODBC Data Source, crear el archivo .IDC, crear el archivo .HTX e iniciar el acceso a los datos llamando al IDC.

Creando un System ODBC Data Source

El primer paso para implementar el acceso es el crear el ODBC Data Source. El DSN o Data Source Name se necesitará más tarde como parámetro para el archivo .IDC.

Un Data Source Name es un nombre lógico que se usa por ODBC para hacer referencia al driver del manejador y cualquier otra información requerida para accesar los datos, cómo el nombre del servidor o la ruta del archivo de la base de datos. El Data

Source Name se usa en los archivos .IDC para decirle al Internet Information Server donde están localizados los datos que se van a accesar.

Nota. El Internet Database Connector trabaja solamente con data sources de ODBC.

Para crear un System Data Source:

1. Abra el Panel de Control
2. Dé doble click sobre el ícono de ODBC. Así se desplegará la caja de diálogo correspondiente.
3. Seleccione el botón System DSN
4. Presione el botón Add
5. Seleccione el nombre del manejador de donde se quiere sacar la información y presione Ok.
6. Escriba en la caja de texto correspondiente el nombre que desea ponerle a su Data Source Name.
7. Termine de llenar la caja de diálogo con la información correspondiente.
8. Presione el botón Ok para cerrar la caja de diálogo.
9. Cierre todas las cajas de diálogo.

Archivo IDC

El archivo IDC contiene la información necesaria para conectarse a un Data Source y para que se ejecute una sentencia SQL. También contiene el nombre y el lugar del archivo para regresar los datos al cliente.

Bajo los términos de Internet un cliente será una computadora que está corriendo un Browser.

Una vez creado, el archivo se almacena en el directorio \Scripts del servidor. Este directorio se establece cuando se instala con permisos de Execute, que crea una asociación entre el archivo .IDC y el HTTPODBC.DLL.

Un .IDC es un archivo de texto simple. Contiene varios parámetros con el siguiente formato:

```
Campo: Valor
```

Cómo mínimo se requieren de 3 parámetros: DataSource, Template y SQLStatement.

DataSource

Este es el nombre del Data Source que se creo para accesara la base de datos y tendría el siguiente formato:

```
DataSource: DSN Name
```

Template

Es el nombre del archivo HTML. Por ejemplo:

```
Template: sample.htx
```

SQLStatement

Esta es la sentencia que se quiere ejecutar. Un ejemplo:

```
SQLStatement: Select ProductName, UnitPrice from Products where UnitPrice<10
```

La sentencia SQL debe de estar en una sola línea. Puede usar el signo de más (+) para dividor una sola sentencia en varias líneas. Solamente se puede ejecutar una sentencia por archivo IDC.

La sintaxis de la sentencia va a variar dependiendo del manejador de base de datos de donde estén pidiendo la información. Por ejemplo, una sentencia que manda a invocar un procedimiento almacenado sería la siguiente:

```
SQLStatement: EXEC MyStoredProc
```

Otros ejemplos de campos son:

UserName: Qué es el nombre válido para validarse en el servidor.

Password: Clave secreta para poder validarse en el servidor

Ejemplo:

```
Datasource: Ejemplo
Template: Ventas htx
SQLStatement:
+SELECT Sum([Order Details].UnitPrice * Quantity)/100*100 as Total
+ FROM [Order Details]
```

Archivo HTX

El archivo HTX es un archivo html que contiene las etiquetas necesarias para los datos que se pidieron. El archivo HTX se debe encontrar en el mismo directorio que el IDC.

El campo SQLStatement del archivo IDC define los campos de datos que quiere se regresen de la base de datos. El archivo HTX toma los datos y define cómo se presentarán los mismos en el Browser. Los campos en los archivos .HTX hacen referencia al nombre que se uso en la sentencia SQL del archivo IDC. El siguiente ejemplo regresa el nombre del producto y el precio unitario al archivo HTX.

```
Resultados de la Consulta:
<B>Lista de Precios</B><BR>

    <%begindetail%>
    <%Producto%>$<%PrecioUnitario%><BR>
    <%enddetail%>

<P>
```

Las etiquetas <%begindetail%> y <%enddetail%> de HTML determinan donde aparecerán los renglones en el documento. Los campos van delimitados por <%%> como <%Producto%> y <%PrecioUnitario%>.

Colocando los registros en una tabla

Los registros que fueron pedidos al servidor se ponen típicamente en una tabla. Para ello se utiliza la etiqueta <TD>. Por ejemplo:

```
Resultados de la Consulta:
<B>Lista de Precios</B><BR>
<TABLE>

    <TR><TH>Producto</TH><TH>Precio Unitario</TH></TR>
    <%begindetail%>
    <TR><TD><%Producto%></TD><TD>$<%PrecioUnitario%></TD></TR
    >
    <%enddetail%>

</TABLE>
<P>
```

Llamando a la Extensión IDC

Una vez que el Data Source, el IDC y el HTX están listos, se puede iniciar el acceso a los datos simplemente pasando un URL al servidor que identifique al IDC. Para llamar al URL, asigne una HyperLink de texto, imagen o control, por ejemplo:

```
http://server/httpodbc dll/scripts/sample.idc
```

El Internet Database Connector se instala en donde se encuentre el Internet Information Server y se crea una asociación entre el archivo .IDC y el HTTPODBC.DLL. Por esa razón hay que usar ligas relativas. Por ejemplo:

```
/scripts/sample.idc
```

Conclusiones

Las redes de computadoras, en el relativamente corto tiempo de su existencia, han probado ser un gran activo para las organizaciones que las utilizan. Esto es debido a que permiten a los miembros de la organización el compartir el recurso más importante que es la información. La información no solo pueden ser datos pertinentes a la actividad de la organización, si no que va mas alla, por que permite el que tambien se pueda compartir la vision, opinión y conocimiento de todos los miembros de la organización involucrados en algun proceso de toma de desición, lo que hace más eficientes y fuertes a las organizaciones.

El Internet ha hecho posible lo que la humanidad soño por tanto tiempo: el tener al alcance de la mano todo el conocimiento que el genero humano ha sido capaz de lograr. El Internet es un logro que la tecnologia de las redes ha permitido en gran escala.

El futuro de las redes es difícil de predecir, pero es facil el imaginar que el siguiente paso seran las redes inalámbricas, lo cual es una tendencia muy fuerte en los ultimos meses. Con la aparición de los sistemas de telefonia celular que incluyen servicios de mensajeria de internet, estamos viendo los primeros brotes de una gran rama de información enviada por medio de redes inalámbricas. En este tipo de tecnologías, la historia lo ha mostrado, es imposible predecir como sera el futuro de las redes de comunicación y el de las computadoras en los sistemas de información.

Las tendencias de estas ramas nos dejan entrever el corto plazo, en el cual, podemos vaticinar que las computadoras de grandes dimensiones van a regresar como administradores de grandes bases de datos, y apareceran pequeñas computadoras que solo nos permitiran visualizar esta información, desapareciendo lo que conocemos como computadora personal. La aparicion de sistemas de acceso a internet en la forma de aparatos domesticos, tales como televisores, acercara aún mas la super autopista de la información a toda la gente. Los sistemas financieros tendran un impacto aun no visualizado completamente con el flujo del recién creado dinero electrónico lo cual trasladara cuantiosas cantidades de dinero a través de las fronteras.

Internet es el principio de lo que sera el centro de convivencia humana en el futuro, debido ha que este ha probado ser un iman muy poderoso de las actividades humanas en el corto tiempo de su existencia. Este medio ha atraido desde formas de comunicación

humana, hasta ser un gran centro de transacciones financieras de miles de millones de dolares por hora.

BIBLIOGRAFÍA:

- COMUNICACIONES WORLD, abril de 1993
- CURRID, Cheryl, Introduction to Networking, Ed. IDG Books, 1997.
- DESBOROUGH John, Building a Windows NT 4 Internet Server, IDG Books, 1999.
- EVANS Tim, Building an Intranet With Winodows NT 4, Microsoft Press, 1999.
- FERRERO Lopez Miguel, Redes de área extendida, Mundo electrónico, marzo de 1994.
- FRANCIS, Charles. Networking essentials. Microsft Press. Ed. Microsoft Corporation. 1996.
- GIBBS, Mark. Redes para todos. Ed SAMS Publishing. 1994.
- GONZALEZ, Felipe. Revista electrónica y computadores. Año 1 No. 1,3,35. De. Publicaciones CEKIT S.A. 1994
- IRFAN Ali M, Frame relay in Public netword, IEEE Comunications Magazine, marzo de 1992.
- MAC CLAIN, Gary R. Handbook of networking & connectivity. Ed AP Professional. 1994
- RAO Editor, Interworking in Broadband Networks, IOS Press Amsterdan. Oxford. Washington.
- STALLING William, Data And Computer communication, Prentice Hall, 1997
- STAN, Schatt. A fondo redes de area local. De Amaya multimedia. 1987.
- STINSON Craig, Running Microsoft Windows NT, Microsoft Press 1997.
- STOLTZ, Kevin. Todo acerca de redes de computadores. Ed. Prentice hall hispanoamericana S.A..1994.
- TANENBAUM, Andrew, Computer Networks, Prentice Hall, 1997
- TANENBAUM, Andrew. Redes de ordenadores.
- UYLESS, Black. Data networks concepts, theory and practice. De Prentice hall. 1989
- WILLIAMSON John, senior Editor,Global Telephony, julio de 1994.
- WINDOWS NT MAGAZINE, Varios Numeros y Articulos.