52

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN

"COMUNICACIONES INTEGRACION DE WINDOWS NT Y UNIX"

798163

TRABAJO DE SEMINARIO

QUE PARA OBTENER EL TITULO DE:

INGENIERO MECANICO ELECTRICISTA

P R E S E N T A

DANIEL JARDINES HERNANDEZ

ASESOR: ING. VICENTE MAGAÑA GONZALEZ

CUAUTITLAN IZCALLI, EDO. DE MEXICO 2001.

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

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

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

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN

UNIDAD DE LA ADMINISTRACION ESCOLAR

DEPARTAMENTO DE EXAMENES PROFESIONALES

UNIVERSIDAD NACIONAL AVENIDA DE MEXICO

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. 51 del Reglamento de Exámenes Profesionales de la FES-Cuautitlán, nos permitimos comunicar a usted que revisamos el Trabajo de Seminario:

Comunicaciones Integración de Windows NT y Unix

que presenta el pasante: Daniel Jardines Hernández

con número de cuenta 8823449-6 para obtener el título de :

Ingeniero Mecánico Electricista

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXÁMEN PROFESIONAL correspondiente, otorgamos nuestro VISTO BUENO

A T E N T A M E N T E
"POR MI RAZA HABLARA EL ESPIRITU"
Cuautitlán Izcalli, Méx. a 23 de Agosto de 2001

MODULO	PROFESOR	FIRMA
II	Ing. Vicente Magaña González	
I	Ing. Jorge Ramírez Rodríguez	
IV	Ing. Rodolfo López González	

INTEGRACION DE WINDOWS NT Y UNIX

ALUMNO:DANIEL JARDINES HERNANDEZ
ASESOR: ING. VICENTE MAGAÑA GONZALEZ

PREFACIO

Inicialmente se lanzó al mercado el computador personal (PC), el cual se concibió como una herramienta para el trabajo individual, pero a medida que se comprobó el alcance de su capacidad para el trabajo en los negocios, su uso y aplicación comenzó a incrementarse en todo el mercado.

Los usuarios vieron la necesidad de compartir información y progresivamente, fueron reuniéndose para conectarse entre sí, formando pequeños grupos para transportar, almacenar y procesar información de forma que podían intercambiar archivos y recursos físicos como impresoras, lo cual propicio el desarrollo de los dispositivos adaptables para su mejora.

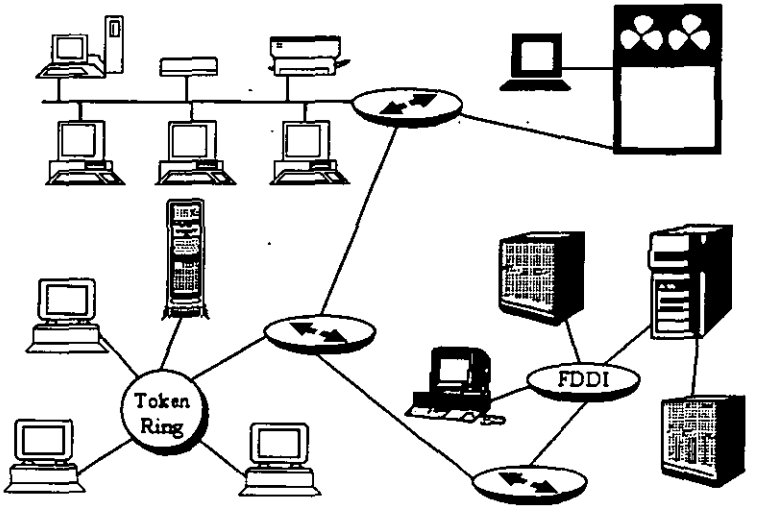
Con la introducción de las primeras redes de área local (LAN), se consiguió reducir ampliamente el costo de los recursos de cómputo requeridos por un grupo de trabajo, tales como impresoras y aplicaciones de todo tipo.

Al aumentar la demanda de procesar y obtener información se han mejorado las técnicas de procesamiento de datos, creando así los grandes avances de la tecnología informática. La unión de computadores por medio de las comunicaciones, es fundamental en la organización de los sistemas de información.

La importante estrategia de interconexión de redes se realizó rápidamente. Las organizaciones en la vanguardia tecnológica comenzaron a enlazar sus redes locales hasta entonces aisladas. La interconexión entre diferentes sistemas fomentó el uso de aplicaciones preparadas para el trabajo en redes de área amplia (WAN), como es el caso de los correos electrónicos y los programas de transferencia de archivos.

Hoy en día, en muchos negocios se tienen redes de tecnologías mixtas en las que conviven en la misma plataforma máquinas viejas y hasta las más modernas. Todas estas redes pueden trabajar en paralelo con las más innovadoras redes de área local, con disposición de datos o sistemas comerciales electrónicos como Internet y correo electrónico. Con ello el

desarrollo de aplicaciones (para el uso integrado de hosts y servidores de procesos distribuidos) ha resultado en nuevos requerimientos para la conectividad y ha generado también nuevos avances en los esquemas de tráfico de información.



Ejemplo de Tecnologías mixtas

En un conjunto de redes interconectadas la información viaja a cualquier parte de la corporación, a sistemas externos o incluso hasta los centros de información de los clientes, la interconexión entre redes, conlleva a la información. Por ello la interconexión entre sistemas representa una gran ventaja y una herramienta de uso estratégico.

La interconectividad, al menos en principio, permite a los equipos de computo intercambiar información aún desde arquitecturas distintas, eliminando las barreras asociadas con las conexiones físicas de la red y las plataformas de hardware o de software.

Para una computadora que trabaja en forma independiente accesar recursos, correr programas y copiar archivos es relativamente común. Para ello, se

identifican las peticiones de usuario por medio de comandos y sus correspondientes dispositivos de destino, además de coordinar el acceso entre ambos. En este escenario, la computadora administra los recursos requeridos de modo que resultan fáciles de utilizar y manejar.

Ya para el caso de una red en la que se tienen dos computadoras únicamente, coordinar el uso de recursos resulta mucho más complejo. La transferencia de información requiere de la capacidad de direccionamiento, detección y corrección de errores, de la sincronización entre los sistemas y también de la coordinación de la transmisión.

INDICE

CAPITULO I Conceptos Generales

CAPITULO II Redes Windows NT y UNIX

INDICE

CAPITULO III Integración de Windows NT y UNIX

CAPITULO I

Conceptos Generales

TOPOLOGIAS

El término red significa un conjunto de computadoras y periféricos que se conectan por algún medio. La conexión puede ser directa (a través de un cable) o indirecta (a través de un módem). Los dispositivos pueden estar en la misma habitación o dispersos en un edificio. La forma como se conectan unos con otros se denomina topología de red y existen tres topologías de más importancia: de bus, de anillo, y de control central o estrella.

TOPOLOGIA EN BUS

Una topología en bus, en una red de área local, define una velocidad de hasta 10Mbps, todas las estaciones se conectan directamente a un único canal físico (cable) de comunicación mediante un conector. Los extremos del cable están finalizados con un terminador de 50 ohms, el terminador elimina automáticamente la señal de los extremos. Normalmente para este tipo de topología se utiliza cable coaxial.

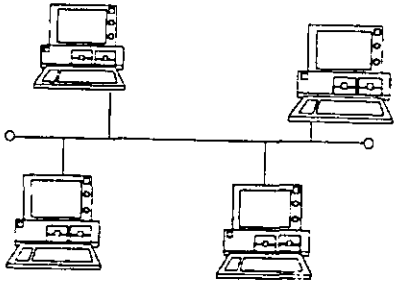


Fig. 1.1 Topología en Bus

Para cada una de estas categorías de cable, si se excede la distancia indicada al integrar más equipos a la red, es necesario la instalación de un repetidor de lo contrario el segmento completo sufrirá atenuación y dejara de transmitir paquetes.

Se recomienda que para la integración de nuevos quipos a la red, si se tiene definido un tipo de cable coaxial, no se utilice otro, ya que cada uno de estos tiene una impedancia diferente y genera una perdida de señal.

El proceso de comunicación utilizado en los buses bidireccionales es el de difusión **Broadcast**, donde todas las estaciones de trabajo reciben simultáneamente el mensaje enviado, aunque solo es procesado por aquella a la que va dirigido. Al ser el bus un canal compartido existen dos problemas que deben de ser resueltos a nivel de protocolo, uno es que varios dispositivos intenten transmitir al mismo tiempo sobre el bus, produciéndose una colisión (Se mezclan los mensajes y su resultado es incomprensible). Otro es cuando una estación esta transmitiendo continuamente y monopoliza la red. Para evitar esto, los mensajes se transmiten en paquetes de datos más pequeños, haciendo una pausa entre los mismos para dar oportunidad de transmitir a otras estaciones.

TOPOLOGIA EN ANILLO

El término de anillo se refiere al diseño de la unidad central que maneja el paso de los paquetes en la red, y se conoce como Unidad de Acceso a medios (MAU) Multi Access Unit. La unidad tiene un circuito de anillo en su interior y sirve como el bus para que los dispositivos obtengan el mensaje. Opera a velocidades de 4Mbps y 16Mbps.

La topología es un anillo en el cual las estaciones de trabajo reciben señales de su vecino inmediato, para a su vez repetir estas señales y ponerlas al alcance de su siguiente vecino más próximo, siguiendo siempre una dirección preestablecida.

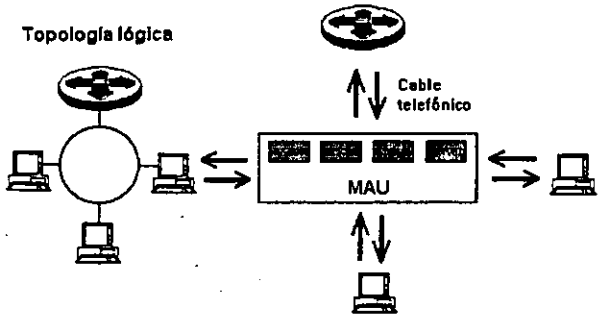


Fig. 1.2 Topología en Anillo

Las estaciones pueden conectarse a un dispositivo central con cables telefónicos. Típicamente, un MAU puede conectar hasta 8 estaciones de trabajo Token Ring. En el caso de una red que consista de más nodos o bien que se encuentren ubicados en otros pisos del edificio, se deben añadir unidades MAU adicionales interconectadas entre sí en un arreglo de cascada, para crear un anillo extendido.

Al instalar un anillo extendido, es importante asegurarse de que los dispositivos MAU están correctamente orientados a manera de formar el anillo apropiadamente, de otra forma el medio quedará truncado siendo incapaz de posibilitar la comunicación.

TOPOLOGIA EN ESTRELLA

En un arreglo en forma de estrella, se tiene un alambre individual desde cada PC hasta una estación central, donde todos los alambres se conectan a un dispositivo central que puede ser un concentrador el cual completa las conexiones electrónicas.

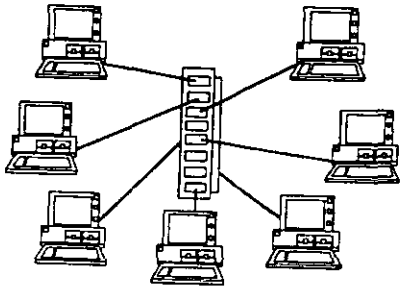


Fig. 1.3 Topología en Estrella

Los tipos de cable que se pueden utilizar para su conexión, es el cable de par trenzado y puede soportar una distancia de hasta 100 metros desde un patch pannel hasta el nodo distribuidor, y se recomienda una distancia no mayor a 5 metros a partir del nodo hasta la PC.

La forma en estrella utiliza más cable, pero tiene ventajas importantes. Como el cable de cada PC es exclusivo de esa máquina, si existe una falla en el cable, sólo la PC conectada en este es afectada.

COMPONENTES DE UNA RED

Los componentes de una red permiten la conectividad entre dos usuarios y proporcionan los servicios básicos que estos requieren de una red, estos componentes son los siguientes:

- Tarjetas de red
- Cableado
- Concentradores
- Swiches
- Ruteadores
- Servidores
- Estaciones de trabajo

TARJETAS DE RED

Son dispositivos que se instalan en una PC con el fin de ofrecer la conexión física a una red. Cada tarjeta se encuentra diseñada para trabajar en un tipo de red específico y soportar una gran variedad de cable y tipos de bus (ISA, MCA, EISA, PCI, PCMCIA)

Las nuevas tarjetas de red son configurables usando un programa de software para cargar los recursos asignados a la tarjeta. Cuando una tarjeta es instalada en una PC y es plug and play (instale y trabaje), simplifica su configuración. Con un sistema operativo como Windows 98/2000 cuentan con el auto detección de los dispositivos, es decir que al encender el equipo, este es detectado.

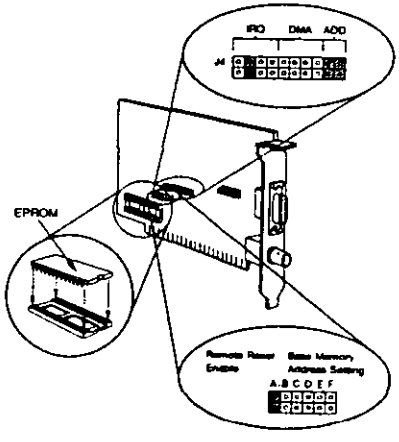


Fig. 1.4 Tarjeta de Red

Cada tarjeta tiene un conector para cada tipo de cable (coaxial, par trenzado o fibra óptica). Las tarjetas de red que funcionan para redes inalámbricas, poseen una antena para comunicarse con la estación base.

La mayoría de las tarjetas incluyen un zócalo PROM (Memoria programada de sólo lectura), esta memoria realiza una inicialización remota de la PC, es decir, que una tarjeta que cuenta con la memoria PROM instalada no necesita unidad de disquete, ni disco duro para cargar el sistema operativo, lo hace vía red, obteniendo la información de un servidor de arranque. Esta alternativa tiene la ventaja de rebajar costos y aumentar la seguridad de acceso a la red, ya que los usuarios no pueden efectuar copias de archivos a disco duro o disquetes, tampoco infectar con virus o utilizar software no autorizado.

Las fábricas productoras de tarjetas de red suministran la memoria PROM en forma separada, información que se debe tener en cuenta al hacer el pedido. En una red generalmente se usan dos clases de tarjetas:

- Una con características especiales de configuración física para un servidor, y debe ser capaz de recibir y transmitir datos a velocidades altas, con el fin de proporcionar un excelente rendimiento al servidor, ya que maneja un tráfico exigente para los usuarios conectados a la red.

- Las tarjetas para las estaciones de trabajo pueden no ser tan exigentes, esto depende de la carga de trabajo de la estación.

CABLEADO

El cableado se refiere a los alambres que conectan las PC´s individuales a la red. El cableado es utilizado en las redes como medio de transmisión, el cual cumple la función de trasladar los datos de un lugar a otro, existen varios tipos de cables con los cuales se puede efectuar la transmisión de datos. Dependiendo del cableado utilizado se maneja la topología de red y sus componentes. El cableado escogido debe ser capaz de transmitir cantidades masivas a grandes velocidades y a través de grandes distancias. Esta

capacidad es llamada alto ancho de banda, que es importante para la transmisión de multimedia a través de la red. El cableado puede ser:

Cable coaxial

Un cable coaxial está compuesto de cobre rígido como núcleo, rodeado de material aislante, el aislante esta rodeado a su vez con un conductor cilíndrico, que es una malla de tejido fuertemente trenzado y a su vez un conductor externo que se cubre con una envoltura de plástico. La malla de tejido protectora que rodea el conductor sirve como tierra. Los tipos de cable coaxial son los siguientes:

10Base5: Conocido como Ethernet grueso, utilizado en sistemas de transmisión de banda base (Baseband), soporta segmentos de red con longitudes de hasta 500 metros con cable coaxial grueso **RG-62**. Tiene una impedancia de 50 ohms.

10Base2: Se conoce como Ethernet delgado, utilizado en sistemas de transmisión de banda base (Baseband), permite segmentos de troncal de hasta 185 metros de longitud, también con cable coaxial delgado **RG-58**. Tiene una impedancia de 50 ohms.

10Broad-36: Cable coaxial tipo **RG-59** A/U CATV, con una longitud extrema de 3,600 metros, utiliza métodos de transmisión de banda ancha (broadband). Tiene una impedancia de 75 ohms

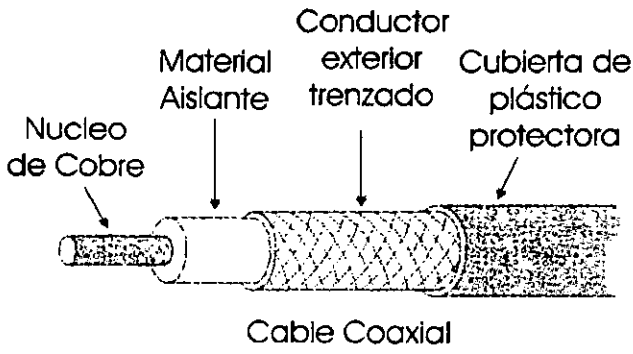


Fig. 1.5 Estructura de un Cable Coaxial

Cable de Par Trenzado

Existen tres tipos de par trenzado, el no apantallado UTP (unshield Twisted Pair), el apantallado por par de cables STP (Kshielded Twisted Pair) y el apantallado global FTP (foiled Twisted pair)

El cable de par trenzado más empleado es el UTP con una impedancia característica de 100 ohms. El conector más frecuente con el cable UTP es el RJ45, aunque también pueden usarse otro tipo de conectores como el RJ11, DB25, DB11, etc. Dependiendo del adaptador de red.

Por su costo y accesibilidad tiene una gran aceptación y ha demostrado un buen desempeño en la transferencia de datos, sin embargo a altas velocidades puede ser vulnerable a interferencias electromagnéticas del medio ambiente.

Fig. 1.6 Cable de Par Trenzado No apantallado UTP y Apantallado FTP

El cable de par trenzado apantallado por par, tiene una impedancia de 150 ohms, el nivel de protección de STP ante perturbaciones externas es mayor que el ofrecido por UTP, sin embargo es más costoso y difícil su instalación. La pantalla del STP para que sea más eficaz requiere una configuración de interconexión con tierra a través de todo el cableado y suelen utilizar conectores RJ49.

El cable STP es utilizado generalmente en las instalaciones de procesos de datos por su capacidad y sus buenas características contra las radiaciones electromagnéticas, pero el inconveniente es que es un cable robusto, caro y difícil de instalar.

El cable FTP es parecido a un cable UTP, sus pares no están apantallados, pero si dispone de una pantalla global para mejorar su nivel de protección a interferencias externas. Su impedancia característica es de 120 ohms y sus propiedades de transmisión son más parecidas a las del UTP, además puede utilizar los mismos conectores RJ45 y tiene un precio intermedio entre el cable UTP y STP. El cable de par trenzado se maneja por categorías de cable.

CATEGORIA 1: Cable de par trenzado sin apantallar, se adapta para los servicios de voz pero no de datos.

CATEGORIA 2: Cable de par trenzado sin apantallar con cuatro pares trenzados y está certificado para transmisiones de 4Mbps.

CATEGORIA 3: Cable de par trenzado con cuatro pares que soporta velocidades de transmisión de 10Mbps de Ethernet (10 Base-T)

CATEGORIA 4: Cable de par trenzado de cuatro pares, certificado para velocidades de 16Mbps.

CATEGORIA 5: Cable de par trenzado de cobre con cuatro pares de 100 ohms con una transmisión de 100Mbps para soportar las nuevas tecnologías como ATM.

Existen varias opciones para el estándar 802.3 que se diferencian por la velocidad, el tipo de cable y distancia de transmisión:

10BaseT: Cable de par trenzado con una longitud extrema de 500 metros y una velocidad de 10Mbps

100BaseT: (Ethernet Rápida) Cable de par trenzado, nuevo estándar que soporta velocidades de 100Mbps que utiliza el método de acceso CSMA/CD.

Cables de Fibra Optica

La fibra óptica es un filamento cristalino o plástico que tiene la propiedad de transmitir la luz a lo largo de ellas con pérdidas muy reducidas En este caso los datos se transmiten mediante pulsos de luz en lugar de señales eléctricas. El núcleo contiene un mayor indice de refracción y se encuentra rodeado por un revestimiento de vidrio con un menor indice de refracción y posteriormente viene una capa plástica delgada para proteger el revestimiento.

Un sistema de transmisión óptico consiste de tres componentes:

1) La fuente de luz: Es un puso de luz que indica un uno lógico y la no presencia de luz indica un cero lógico. Para emitir las señales de luz se pueden utilizar dos métodos: a) utilizando un diodo led y b) Utilizando un semiconductor láser.

2) El medio de transmisión: Es la fibra de vidrio ultra delgada, el cable de fibra óptica transmite señales luminosas (fotones) por en medio del núcleo de dióxido de silicio puro, las transmisiones fotónicas no emiten señales externas al cable y no son afectadas por la radiación externa.

3) El detector: Origina un pulso eléctrico cuando la luz incide en él. El extremo receptor de una fibra óptica es un fotodiodo que emite un pulso eléctrico cuando lo golpea la luz. El tiempo de respuesta es de 1ns, limitando su velocidad de datos a 1Gbps aproximadamente.

Algunas de las grandes ventajas de utilizar fibra óptica son que las señales transmitidas no son distorsionadas por señales eléctricas, magnéticas o interferencia de señales de radio, son inmunes a interferencias de alto voltaje, no emite radiación y su diámetro es muy pequeño, lo que facilita su instalación en ductos de difícil acceso además de ser muy ligero.

Fundamentalmente existen tres tipos de fibra en función del indice de refracción de los materiales que la componen, así con del diámetro de su núcleo. Estas son:. Fibra multimodo de indice escalonado, Fibra multimodo de indice gradual y Fibra monomodo.

CONCENTRADORES DE RED (HUBS).

Los concentradores conectan un grupo de equipos de computo que se encuentran en una misma área de trabajo, tienen su propio procesador y pueden ejecutar programas para controlar paquetes de datos y errores, a la vez almacenan información pertinente a la red en una base de datos denominada MIT (Manage-ment Information Base).

Existen Hubs de arquitectura multicanal que contienen varios canales que definen redes de diferentes tipos tales como Ethernet, Token Ring o FDDI. También hay de arquitectura monocanal los cuales soportan un solo tipo de red.

Un hub comparte todo el ancho de banda en el numero de canales que tiene, es decir, si se tiene un hub a una velocidad de 100Mbps con 8 puertos, y todos los puertos están solicitando transmisión de datos al mismo tiempo, cada uno tendrá un ancho de banda de 12.5Mbps siendo notorio el retardo en la transmisión de datos.

SWITCHES

Un switch es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. El switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto. Opera en la capa 2 del modelo OSI y reenvia los paquetes basándose en la dirección MAC.

El switch segmenta económicamente la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final.

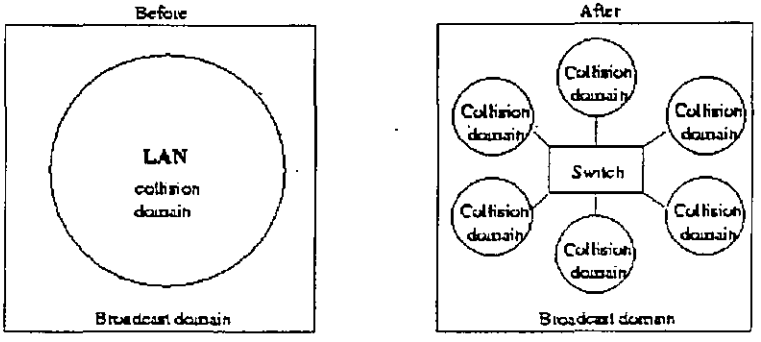


Fig. 1.7 Segmentación en pequeños dominios de colisión

Al segmentar la red en pequeños dominios de colisión, reduce o casi elimina que cada estación compita por el medio, dando a cada una de ellas un ancho de banda comparativamente mayor.

RUTEADORES

Un ruteador es un dispositivo de propósito general diseñado para segmentar la red, con la idea de limitar tráfico de brodcast y proporcionar seguridad, control y redundancia entre dominios individuales de brodcast, también puede dar servicio de firewall y un acceso económico a una WAN.

El ruteador opera en la capa 3 del modelo OSI y tiene más facilidades de software que un switch. Al funcionar en una capa mayor que la del switch, el ruteador distingue entre los diferentes protocolos de red, tales como IP, IPX, AppleTalk o DECnet. Esto le permite hacer una decisión más inteligente que el switch, al momento de reenviar los paquetes.

El ruteador realiza dos funciones básicas:

1. El ruteador es responsable de crear y mantener tablas de ruteo para cada capa de protocolo de red, estas tablas son creadas ya sea estáticamente o dinámicamente. De esta manera el ruteador extrae de la capa de red la dirección destino y realiza una decisión de envio basado sobre el contenido de la especificación del protocolo en la tabla de ruteo.

2. La inteligencia de un ruteador permite seleccionar la mejor ruta, basándose sobre diversos factores, más que por la dirección MAC destino. Estos factores pueden incluir la cuenta de saltos, velocidad de la linea, costo de transmisión, retraso y condiciones de tráfico. La desventaja es que el proceso adicional de procesado de frames por un ruteador puede incrementar el tiempo de espera o reducir el desempeño del ruteador cuando se compara con una simple arquitectura de switch.

SERVIDORES

Son equipos potentes que ofrecen servicios a un grupo de PC's clientes, estos servicios pueden ser acceso a archivos, aplicaciones, impresiones, etc En una red pueden existir varios tipos de servidores y cada uno de ellos cumplir con una función especial, como por ejemplo:

- SERVIDOR PROXY: Es un servidor que permite controlar el acceso de los usuarios hacia Internet, además de que funciona como un servidor de cache para paginas de Internet lo cual incrementa la velocidad de acceso a esta, ya que la transferencia de la pagina consultada no se hace desde el sitio en que esta instalada si no que toma gran parte del servidor. Con este servidor se puede restringir el acceso a sitios no autorizados y genera bitácoras de acceso de los usuarios.

➢ SERVIDOR WEB: Contiene todos los archivos HTML de una pagina WEB y los publica hacia una Intranet o Internet

➢ SERVIDOR DE CORREO ELECTRÓNICO: Es el lugar donde se almacenan los mensajes de correo electrónico y es capaz de efectuar la traducción entre diferentes tipos de correo.

➢ SERVIDOR DNS: Es un servidor de nombres de dominios de Internet, el cual permite relacionar un nombre con una dirección IP y así poder accesar a una pagina WEB.

➢ SERVIDOR DE BASE DE DATOS: Es utilizado cuando hay necesidad de almacenar y procesar grandes cantidades de información y brindar la información necesaria de una forma más eficaz a los usuarios.

➢ SERVIDOR DE MONITOREO: Permite al administrador saber información sobre el estado de la red en cuanto a tráfico, colisiones, enlaces fuera de servicio etc.

➢ SERVIDOR DE IMPRESIÓN: Permite la rápida impresión en una o más impresoras en la red permitiendo a cualquier usuario enviar trabajos de impresión.

ESTACIONES DE TRABAJO

Es una PC de usuario que utiliza los servicios de red y los recursos que el servidor tiene a su disposición. En redes de Internet se llama host a cualquier PC conectada a la red y que dispone de una dirección IP y un nombre definido, es decir, cualquier computador que puede enviar o recibir información a otro computador. El nombre de host es un nombre que facilita a los usuarios identificar un computador en una red TCP/IP.

En un principio Cada fabricante de computadoras personales tenía su propia arquitectura de red y en ningún caso existía la compatibilidad. Virtualmente, la industria informática, en su totalidad, ha acordado una serie de Normas Internacionales para describir las arquitecturas de redes. Estas normas se conocen como el Modelo de Referencia OSI (Interconexión de Sistemas Abiertos). La idea consiste en diseñar redes como una secuencia de capas, cada una de ellas construida sobre el anterior.

EL TRABAJO EN LA RED Y EL MODELO OSI

Para conectar distintos recursos informáticos en la red, tenemos que conocer los detalles de la arquitectura de red. Para que las computadoras puedan comunicarse entre sí, deben hablar el mismo lenguaje o protocolo. La mayoría de los protocolos tienen muchas funciones distintas y operan en capas. Además de los protocolos, las computadoras deben disponer de un hardware compatible para comunicarse.

En 1978 una organización conocida como la Organización Internacional de Estándares (ISO), desarrolló un modelo para describir las arquitecturas de red. En 1984 la ISO revisó su modelo y lo denominó modelo de referencia de interconexión de sistemas abiertos (OSI) El modelo OSI es el marco más ampliamente utilizado para la descripción de redes y la manera en que los componentes de red interactúan en distintos niveles.

LA ARQUITECTURA DEL MODELO OSI

El modelo OSI persigue que las redes operen en capas, donde en cada capa se localiza un conjunto específico de responsabilidades. Cada capa particular en el modelo OSI abarca las responsabilidades de funcionamiento de red, hardware y protocolos.

Al dividir la red en siete capas, los distintos servicios y funciones pueden especificarse en las distintas capas. Cada capa de red se comunica con las capas adyacentes por arriba y por abajo por medio de un conjunto de fronteras denominadas interfaces.

El papel fundamental de cada capa es proporcionar a la capa inmediata superior un conjunto de servicios y ocultarle los detalles de cómo se han implementado esos servicios. Esto permite que cada capa actúe como si se comunicara directamente con su capa correspondiente en otra computadora, cuando en realidad los datos están bajando por las capas OSI hasta la red y subiendo a través del modelo OSI en la computadora receptora. La apariencia de estarse comunicando directamente con la capa correspondiente de otra computadora se conoce como *comunicación virtual*.

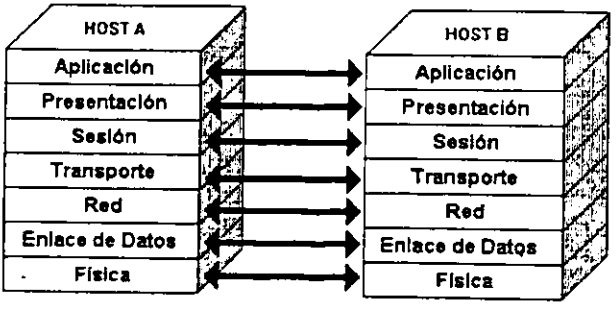


Fig. 1.8 Modelo OSI

LA CAPA FISICA

La capa inferior del modelo OSI es la capa física. La capa física es la responsable de transmitir el flujo de datos a través de un modelo físico, como Ethernet o un cable de fibra óptica. La capa física define los detalles del medio de transmisión, los detalles de la interfaz de la computadora para la transmisión de datos y el esquema de codificación de datos que se está usando al nivel de hardware. El esquema de codificación de datos define como envía el medio un 1 o un 0 lógico y se asegura que los datos enviados se reciben al otro extremo como un 1 o un 0 lógico. También define como se traducen los bits en señales ópticas o eléctricas.

LA CAPA DE ENLACE DE DATOS

La segunda capa desde abajo es la capa de enlace de datos. Esta capa es la responsable de tomar los datos de la capa de red y transmitirlos a través de la red. Toma partes de datos de la capa de red, conocidos como *tramas*, añade información de control y pasa las tramas a la capa física para su transmisión.

Además de los datos concretos, una trama de la capa de Enlace de datos puede contener información como los identificadores (ID) del origen y del destino, así como códigos de detección de errores, de modo que la capa de Enlace de datos del otro extremo pueda verificar que la trama de datos está libre de errores. Puesto que la capa de Enlace de datos es la responsable de que no haya errores en la transmisión, reenviará todas aquellas tramas que estén dañadas o contengan errores.

LA CAPA DE RED

La capa que esta encima de la capa de enlace de datos es la capa de red. Es la responsable del direccionamiento de los datos en la red, de traducir los nombres y direcciones lógicas a direcciones físicas, determina la mejor ruta desde la computadora de origen hasta la de destino. Cuando un bloque de datos es muy grande la capa de red segmenta el paquete en fragmentos más pequeños. La capa de red correspondiente en el receptor ensambla los fragmentos para reconstruir el paquete original. Este proceso es conocido como segmentación y ensamblaje.

LA CAPA DE TRANSPORTE

La capa de transporte se encuentra encima de la capa de red. Su función es la de garantizar que los paquetes se envien sin errores, de manera secuencial y sin duplicaciones o pérdidas. Esta capa toma mensajes grandes de flujo de datos y los divide en paquetes. Puesto que la capa de transporte es la responsable de asegurar el envio de paquetes, exigirá una nueva transmisión de aquellos paquetes que contengan errores o que no se hayan recibido.

LA CAPA DE SESIÓN

La capa de sesión permite que dos aplicaciones mantengan un diálogo llamado *sesión*. Igualmente gestiona el reconocimiento de nombres y la seguridad entre los dos extremos de la conversación; asi como la interacción en el diálogo entre las dos computadoras.

LA CAPA DE PRESENTACIÓN

La capa de presentación proporciona las funciones de traducción para el flujo de datos. Traduce los formatos, protocolos, conjuntos de caracteres, etc. Puede traducir los datos en un formato intermedio ampliamente implementado antes de enviarlo a la red, y es responsable de cifrado y la compresión de datos.

LA CAPA DE APLICACIÓN

La capa de aplicación ocupa el lugar más alto en el modelo OSI de siete capas. Esta capa proporciona los servicios que interactúan directamente con las aplicaciones del cliente. Sus servicios proporcionan soporte de red para aplicaciones, como el correo electrónico o la transferencia de archivos.

EL CONJUNTO DE PROTOCOLOS TCP/IP

Los protocolos son los lenguajes que las computadoras utilizan para hablar entre sí. El protocolo TCP/IP es un conjunto de protocolos de comunicación de red más utilizado actualmente y constituye la espina dorsal de Internet. Puesto que ya estaba en funcionamiento cuando se desarrollo el modelo OSI, no se ajusta ese perfectamente a ese modelo. Sin embargo. Podemos servirnos del modelo OSI para ayudar a percibir cómo interactúan los distintos protocolos que conforman TCP/IP.

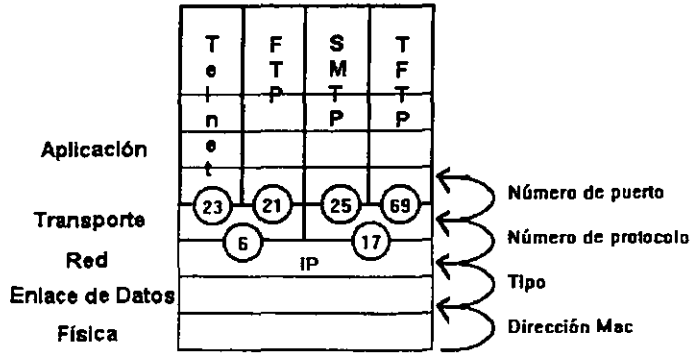


Fig. 1.9 Conjunto de Protocolos TCP/IP

En la parte superior del conjunto de protocolos TCP/IP tenemos los protocolos de interfaz con las aplicaciones de usuario, como *telnet* para conexión remota, el *protocolo de transferencia de archivos* **FTP**, *protocolo simple de administración de red* **SNMP**, el *protocolo simple de transporte de correo* **SMTP**, *sistema de archivos de red* **NFS**, *servicio de nombres* **DNS**, y **HTTP**. Estos protocolos se proyectan más o menos sobre las capas de presentación y aplicación del modelo OSI. Algunos de estos protocolos también incorporan propiedades definidas de la capa de sesión.

En el nivel medio de conjunto de protocolos TCP/IP, se encuentran dos protocolos que soportan las funciones definidas en la capa de transporte del modelo OSI. Estos protocolos son el Protocolo de control de transmisión **TCP** y el protocolo de datagramas **UDP**. TCP es un protocolo orientado a la conexión y es responsable de proporcionar un envío fiable, secuenciado y sin errores, de los paquetes por la red. Cuando se establece una sesión con el protocolo TCP, las dos computadoras crean una conexión lógica, transmiten una secuencia de datos y entonces deshacen la conexión.

UDP tiene una función similar a TCP, pero no está orientado a conexión y no garantiza un envío fiable, UDP es un protocolo *no conectivo*. Con UDP no es necesario realizar el esfuerzo de crear y disolver una conexión de red, simplemente transmite un paquete, conocido como *datagrama*, a su destinatario. UDP no comprueba si el paquete se ha recibido correctamente.

En el nivel más bajo del conjunto de protocolos TCP/IP se encuentra el *protocolo de Internet* **IP**. Proporciona un protocolo de la capa de red no conectivo que direcciona y encamina paquetes. También proporciona soporte para la segmentación y ensamblaje. Puesto que IP es un protocolo no conectivo, no garantiza un envío fiable de los paquetes de red.

TIPOS DE DIRECCIONES IP

Para propósitos de ruteo, todos los objetos en la red deben tener asignada una dirección IP, la cual es de 32 bits, acomodados en cuatro octetos y separados por un punto. Cada octeto es representado por un número decimal que puede llegar hasta 255. Esta dirección identifica el número de hosts y también identifica la red de acuerdo a la siguiente clasificación:

Clase A (redes muy grandes)

Para obtener esta red el primer bit del primer octeto de la dirección IP se establece en cero y se varían todos los demás, de esta manera el rango para las redes es de 1 a 126. La red 127 se utiliza para loopback.

1.0.0.0 al 126.0.0.0

0**0000000**	00000000.00000000.00000000
	254 x 254 x 254
1-126	1-254 1-254 1-254
Numero	Número de host
De Red	

Total de redes: **(1 al 126) = 126**

Total de hosts: **(254x254X254) = 16,387,064**

Clase B (Redes Grandes)

En este caso los primeros dos bits son 1 y 0 respectivamente, esto permite redes del 128 al 192 haciendo un total de 16,384 redes y 64 mil hosts aproximadamente.

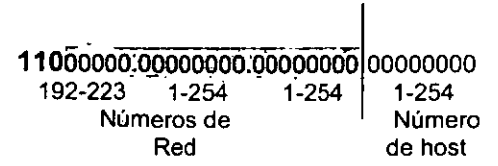
10000000.00000000	00000000.00000000
63 x 254	254 x 254
128-191 1-254	1-254 1-254
Número de Red	Número de host

Total de redes: **(128 al 191)x(254) = 16,002**

Total de hosts: **(254x254) = 64,516**

Clase C (Redes chicas)

Ahora los tres primeros bits se establecen como 1, 1 y 0 respectivamente y obtenemos aproximadamente dos millones de redes y 254 hosts por red.



Total de redes: **(192 al 223)x(254)x(254) = 1,999,996**

Total de hosts: **254**

La dirección 255 se usa para el broadcast.

MASCARAS DE SUBRED

La dirección IP esta compuesta de dos partes una es la identificación de la red y otra es la identificación del host. La mascara de subred tiene un tamaño de 32 bits en cuatro octetos separados por un punto. Las mascaras de subred determinan cual de los bits en el campo del hosts es utilizado para especificar diferentes partes o subredes de una red en particular. Mascara de red sin subredes.

	RED	HOSTS
131.108.2.160	10000011 . 01101100 . 00000010 . 10100000	
255.255.0.0	11111111 . 11111111 . 00000000 . 00000000	
	131 . 108 . 0 . 0	

El ruteador extrae la dirección destino IP del paquete y lleva esa información a la mascara de subred. El ruteador realiza una

multiplicación lógica para obtener el número de la red. Durante estas operaciones una parte de la dirección es removida de la cadena. Las de los ruteadores están basadas únicamente en los números de red. Mascara de subred con subredes.

	RED			HOSTS
131.108.2.160	10000011 .	01101100 .	00000010 .	10100000
255.255.255.0	11111111 .	11111111 .	11111111 .	00000000
	131 .	108 .	2 .	0

En este caso el número de subred extraído es **131.108.2.0**

Clases de Red y sus Mascaras de Subred Típicas

TIPO DE RED	INICIO	FIN	Mascara de subred
Clase A	1.0.0.0	126.0.0.0	255.0 0 0
Clase B	128.0.0.0	191.0.0.0	255.255 0 0
Clase C	192.0.0.0	223.0.0.0	255.255 255 0

Tabla 1.1

CAPITULO II

Redes Windows NT y UNIX

Windows NT y UNIX han crecido por distintos caminos y como resultado han jugado papeles distintos en la red moderna profesional. Estos dos sistemas operativos tienen historias y legados muy diferentes. Se encontrará que muchos administradores de sistemas son radicalmente partidarios de uno o del otro. Los administradores de NT se quejan de que UNIX es viejo, caduco y de que tiene órdenes crípticas. Los administradores de UNIX se quejan de que NT no es fiable, no es estable y no se adapta bien. Lo curioso es que los dos extremos tienen la razón.

Los usuarios prefieren PC´s sobre sus escritorios, por una buena razón, las herramientas de productividad. Ellos quieren usar los programas de PC. Pero a los administradores les gustan los sistemas DE UNIX por su confiabilidad y configuración.

HISTORIA DE UNIX

UNIX se desarrollo a finales de los sesenta. Desde entonces, ha avanzado como el sistema operativo predominante en el mundo empresarial, proporcionando un entorno fiable estable, multitarea, multiprocesador y multiusuario. Una de las razones de la actual popularidad de UNIX entre los fabricantes de estaciones de trabajo es su portabilidad.

HISTORIA DE NT

Microsoft comenzó a vender Windows NT en 1993. Anteriormente, Microsoft e IBM habian desarrollado conjuntamente OS/2. Microsoft sabia que OS/2 no tendría una larga vida si no podia adaptarse al nuevo hardware. Por tanto, Microsoft comenzó su propio proyecto, independiente de IBM, para producir una versión portable de OS/2 que pudiera adaptarse rápidamente a las distintas plataformas de hardware. El resultado fue el proyecto NT y este se convirtió posteriormente en Windows NT cuando Microsoft abandonó el

esfuerzo de OS/2. Las primeras versiones de Windows NT eran toscas. Sin embargo con Windows NT 4.0 Microsoft ha puesto una auténtica cabeza de puente en el territorio tradicional de UNIX. Microsoft incluye servicios de archivo e impresión, servicios de comunicación, aplicaciones y servicios de Intranet e Internet.

EL PAPEL DE UNIX

UNIX creció en el mundo de la Ingenieria; ha sido el sistema operativo en aquellos negocios que requerían llevar aplicaciones críticas a computadoras centrales, dadas sus posibilidades de actuación, robustez y flexibilidad. UNIX ha tenido su mercado principal en la computación de alto rendimiento. Algunos de los papeles que UNIX ha realizado tradicionalmente dentro del mercado son:

- TAREAS CON MUCHA CARGA DE ENTRADA/SALIDA. Las aplicaciones que requieren de un gran ancho de banda de E/S, como son las bases de datos, normalmente utilizan una plataforma con implementación UNIX.

- SERVIDOR MULTITAREA. UNIX es un sistema operativo diseñado para facilitar el trabajo con múltiples procesos.

- SERVIDORES WEB. Durante mucho tiempo UNIX ha sido de hecho el sistema operativo para las aplicaciones de Internet con servidores de WEB incluidos. UNIX es todavia hoy la plataforma más popular para los servidores WEB de Internet.

- SERVIDOR SMTP. El correo electrónico vía SMTP reside usualmente en sistemas UNIX por su robustez y fiabilidad.

- SERVIDOR DE ARCHIVOS. Añadiendo una gran cantidad de espacio en disco duro a los servidores UNIX, Estos pueden actuar como servidores de

archivos muy efectivos tanto para las aplicaciones como para los directorios de usuario.

➢ SERVIDORES DE BASES DE DATOS. Las bases de datos comerciales a gran escala y de alto rendimiento son muy comunes en el universo de UNIX. Productos como Oracle, Sybase o Informix operan en distintas versiones de UNIX.

EL PAPEL DE NT

Windows NT a diferencia de UNIX, se ha desarrollado a partir de la plataforma de computadora personal de IBM, lo que supone un mayor énfasis en las interfaces gráficas de usuario y en las aplicaciones de escritorio. Como versión más potente de Microsoft Windows, la meta de NT es convertirse en el sistema operativo de Microsoft para estaciones de trabajo de calidad. En las redes actuales se puede encontrar Windows NT trabajando como servidor de BackOffice, proporcionando soporte para bases de datos SQL Server o servicios de correo electrónico mediante Exchange.

Otros usos comunes de los servidores NT son los de servidores de archivos, aplicaciones o impresión, para estaciones de trabajo que ejecutan alguna variante de Windows.

Microsoft, con su Internet Information Server, está haciendo algunas incursiones en el mercado de los servidores de Internet, pero esta área está todavía dominada por UNIX.

Cada día más compañías están adoptando Windows NT, pero existen reticencias; están preocupados por la escalabilidad y robustez de NT. Otros titubean frente a la idea de entregarse totalmente a la forma de vida de Microsoft.

VENTAJAS Y DESVENTAJAS

Hoy en día, las diferencias entre los dos sistemas operativos están empezando a difundirse a medida que Windows NT empieza a madurar como producto. Los entornos mixtos son cada día más corrientes. Por medio de la integración de las empresas pueden aprovechar los puntos fuertes de cada sistema para satisfacer mejor sus necesidades.

UNIX

VENTAJAS	DESVENTAJAS
➢ Estable.	➢ Existen muchas variedades distintas con diferencias muy sutiles.
➢ Fiabilidad comprobada.	
➢ Se adapta bien.	➢ Los servidores y estaciones de trabajo tienden a ser caros.
➢ Esta apoyado por múltiples fabricantes.	➢ La administración de UNIX es una técnica especializada.
➢ Proporciona una excelente capacidad de automatización y desarrollo de guiones.	➢ Las ordenes tienden a ser cripticas (poco comprensibles).
➢ Proporciona soporte para la mayor parte de los servicios de Internet, como FTP, HTTP, SMTP Y SMNTP.	➢ Carece de las mismas aplicaciones de escritorio para usuario que están disponibles en las plataformas PC.
➢ Es un sistema abierto.	

Tabla 2.1 ventajas y desventajas de los servidores UNIX

WINDOWS NT

VENTAJAS	DESVENTAJAS
➢ Los servidores y estaciones de trabajo tienden a ser más baratos que los de UNIX, a excepción de las versiones gratuitas de UNIX como LINUX. ➢ Normalmente es más fácil de usar y administrar. ➢ Hay una gran variedad de aplicaciones de usuario. ➢ Compatibilidad retroactiva con muchas aplicaciones de Windows 16-bits.	➢ Lo proporciona un único fabricante. ➢ Su estabilidad y confiabilidad están todavía por demostrarse. ➢ Es propiedad de Microsoft y está sujeto a sus planes de diseño (es un sistema Cerrado). ➢ Carece de herramientas de automatización de procesos y guiones nativos, aunque están disponibles a partir de terceros desarrolladores.

Tabla 2.2 ventajas y desventajas de los servidores UNIX

Tanto UNIX como NT son realidades en las redes de hoy en dia. Ambos sistemas operativos se solapan en los servicios que prestan ahora. La meta de un administrador es implementar estrategias efectivas para maximizar sus recursos informáticos. Si se está una red mixta con los sistemas UNIX y NT, lo más probable es que quiera desarrollar algún tipo de interoperabilidad ya que se encuentra familiarizado con los dos sistemas.

Al integrar los sistemas UNIX y NT, se vuelve esencial el conocimiento de las redes y los protocolos de red. Los sistemas UNIX proporcionan tipicamente

el trabajo en red por medio del protocolo TCP/IP, mientras que NT puede implementar distintos protocolos. Si el administrador encargado de crear una función de integración de red proviene del entorno UNIX, lo más posible es que no esté familiarizado con el uso que NT hace con NetBEUI, los nombres NetBIOS, o DHCP. Por otro lado, si el administrador proviene del entorno NT, podría no haber trabajado nunca con TCP/IP, al ejecutar su entorno NT por medio de NetBEUI o IPX.

INTRODUCCIÓN A SMB

Para hacer que los sistemas UNIX funcionen como servidores de los sistemas NT, se necesita primero hacer que los dos se comuniquen. Para comunicarlos se necesita saber un poco sobre SMB.

SMB es una abreviatura del protocolo (bloque de mensajes del servidor) y es el protocolo estándar que utiliza Windows NT para compartir servicios de archivos, impresoras y puertos entre computadoras. También admite compartir elementos de comunicación como canales de correo y conductos etiquetados. En un principio lo desarrollaron Microsoft e Intel como el protocolo para compartir archivos Open-NTE, lanzado en 1987.

SMB opera de la forma petición-respuesta, donde los clientes envían peticiones, contenidas en bloques de mensajes de servidor (SMB), al servidor; éste recibe las peticiones SMB, los interpreta y envía de regreso la respuesta al cliente. Siempre que una computadora comparte un recurso a través de la red por medio de SMB, se convierte en un servidor en este escenario. Cuando una computadora accede a un recurso compartido, se convierte en cliente. En Windows NT, es posible actuar de forma simultánea como servidor y cliente.

Una vez que el cliente se conecta al servidor y se autentifica, el cliente puede proceder a enviar órdenes al servidor para abrir, leer, escribir, cerrar o

eliminar archivos, buscar directorios y ejecutar otras órdenes de archivo o directorio. Estas órdenes se encapsulan en formatos especiales de SMB. Existen diferentes formatos de SMB para manejar las diferentes órdenes disponibles.

El protocolo SMB proporciona dos niveles de seguridad, el primer modelo que admite SMB es nivel de seguridad del recurso compartido, donde a los recursos compartidos se les asigna una contraseña; esto garantiza el acceso del usuario al recurso compartido. El segundo tipo de seguridad de SMB, se le conoce como nivel de seguridad de usuario, donde las protecciones de los accesos se aplican a archivos individuales y los derechos de acceso se determinan basándose en el usuario propietario. Cuando un usuario se autentifica, el servidor con el recurso compartido le asigna un ID de usuario (número de usuario), este es comparado después con las protecciones de acceso asignadas a cada archivo.

NOMBRES DE EQUIPOS

Los nombres de equipos (o nombres de hosts) sirven de alias para las direcciones de red. En un entorno UNIX, el término nombre de hosts designa al nombre de un dispositivo de red concreto que corresponde a una dirección IP. En el mundo Microsoft, el nombre de equipo puede designar a un nombre NetBIOS que corresponde con una dirección IP.

Se asigna un nombre a un equipo o hosts, por que es más fácil de recordar que una dirección IP. Además al usar nombres de equipos, se pueden ocultar los detalles de la dirección al usuario final. De este modo, si queremos cambiar la dirección de red de una computadora, podemos hacerlo sin cambiar su nombre.

NOMBRES NetBIOS

Windows NT puede ser compatible con múltiples protocolos de red, Microsoft utiliza los nombres NetBIOS para los nombres de dominio NT. Los nombres NetBIOS pueden tener un máximo de 15 caracteres y no son sensibles a mayúsculas y minúsculas, aunque normalmente se escriben con mayúsculas. NetBIOS en un API (Interfaz de Programación de Aplicaciones) que proporciona acceso a los servicios de red.

La comunicación SMB tiene lugar mediante la interfaz NetBIOS, la cual puede operar con una amplia gama de protocolos. Aunque normalmente se cree que NetBIOS está vinculado al protocolo NetBEUI, también puede vincularse a TCP/IP e IPX/SPX. NetBIOS es adaptable a distintos sistemas de red.

Aunque se puede ejecutar NetBIOS en una gran gama de protocolos, lo normal, si se tienen sistemas UNIX, es usar TCP/IP. Como se ha dicho, las solicitudes se mandan sobre NetBEUI, éste tiene menos carga que TCP/IP y por lo tanto es un poco más rápido; es también muy simple de instalar y configurar, sin embargo, NetBEUI es un protocolo no ruteable; se diseño para su uso en un entorno de red de área local y no funciona con equipos que estén separados con ruteadores.

Afortunadamente NetBIOS también vincula TCP/IP. A esta combinación se le suele llamar NetBT o NBT. Recuérdese que NetBIOS utiliza nombres distintos a los DNS de UNIX. Así para que NetBIOS funcione con TCP/IP debe haber alguna forma de proyectar a los nombres NetBIOS en direcciones IP. Todas las solicitudes a NetBIOS usan nombres NetBIOS. NetBIOS no entiende direcciones IP numéricas directamente.

En un entorno mixto de NT y UNIX, a la utilización más frecuente de NetBIOS se le denomina NetBIOS a través de TCP/IP, también conocida como NetBT.

EL SERVICIO DE WINS

En el momento en que un NetBT se une a la red envía una solicitud de registro a un servidor NetBIOS o se difunde por la red por medio de un datagrama UDP. El propósito es comunicar a otras computadoras que una nueva computadora se ha unido a la red.

Si hay un servidor de WINS en la red y recibe la solicitud de registro, comprueba si alguna otra computadora ya esta usando el nombre NetBIOS. Los servidores de WINS actúan como puntos de registro para clientes NetBT, de modo que puedan registrar su información de proyección de nombres NetBIOS sobre direcciones IP. Usando un servidor de WINS, los clientes NetBIOS no tienen que difundir sus solicitudes de nombre por la red. Esto beneficia al ancho de banda de red. Un servidor de VisionFS puede ser un cliente y un servidor de WINS, Las PC´s de Windows también pueden ser clientes de WINS si utilizan TCP/IP como protocolo de red.

Para proporcionar al sistema de archivos original de NT soporte para compartir e imprimir desde un servidor de archivos UNIX a una estación de trabajo NT, se tiene que encontrar la forma de convencer a UNIX para que proporcione soporte al protocolo SMB. Una de las formas más sencillas de proporcionar soporte para compartir e imprimir es el paquete **VisionFS**. Utilizando VisionFS, los sistemas UNIX pueden crear recursos compartidos que pueden utilizar las computadoras basadas en Windows. Además proporciona herramientas que permiten al usuario de UNIX acceder a recursos compartidos en computadoras Windows y transferir archivos. VisionFS se ejecuta en diversas variantes de UNIX como son SUN, HP, IBM, SCO y muchos otros.

VisionFS permite a los usuarios de PC, que accesen a los archivos de UNIX como si fuera otra PC mediante la red. También se puede imprimir en las impresoras de UNIX, estas son simplemente como otra impresora de red de Windows. Puede proveer otros servicios como el servicio de WINS, para el acceso transparente a computadoras sobre otras redes etc.

VisionFS disfraza un UNIX como una PC, para otras PC´s y usuarios, un servidor de VisionFS se ve simplemente como cualquier otra PC. No existe ninguna necesidad instalar software complejo sobre computadoras personales por lo que no usa memoria extra o espacio en disco duro en una PC.

De esta forma los sistemas de UNIX son ideales para las instalaciones de red, puede ser un disco lleno de productos para PC, a los cuales pueden accesar múltiples usuarios. Los sistemas de UNIX son robustos, confiables y escalables, perfectos para los constantes cambios y el creciente mundo de las PC´s.

CAPITULO III

Integración de Windows NT Y UNIX

INSTALACION DE VisionFS

Antes de instalar el software de VisionFS, es necesario agregar los usuarios en la base de datos del servidor UNIX a los cuales se les permitirá el acceso a este servidor. En este caso se utilizarán servidores UNIX con Santa Cruz Operation Versión 5.0.5. Para esta versión, el software de VisionFS es proporcionado gratuitamente; este tiene que ser instalado con el comando *custom*. Una vez instalado el software, estando dentro del directorio */usr/vision/bin* se debe ejecutar el siguiente script con el fin de proporcionar algunas configuraciones básicas del sistema.

```
# sh visionfs start
-------------------------------------------------------------------
VisionFS Password wizard
-------------------------------------------------------------------
This wizard helps you import your existing UNIX password database into
the VisionFS password database. This will allow Windows users
(including Windows 98 users) to access the VisionFS server more
securely.
To continue with the wizard, press [Return]. Or enter 'q' to quit now.

Continue or quit? [ ]
```

La primer pantalla ayuda a generar la base de datos para el control de acceso a los usuarios.

```
-------------------------------------------------------------------
Initial passwords
-------------------------------------------------------------------
UNIX and Windows use incompatible mechanisms for encrypting passwords.
This means the wizard can't import UNIX passwords directly into the
VisionFS database. You need to set the initial password for users.

Choose the password to set for each user (they can change it later):

  B - Use a blank password
  F - Let me type a fixed password, to use for all users
  R - Generate a random password, different for every user
  U - Make the password the same as the UNIX username

You'll be able to edit the usernames and passwords to make specific
changes before they're added to the VisionFS password database.
```

Initial password type [R]

Generating passwords, please wait...

Debido a que Windows y UNIX utilizan formas de encripción incompatibles para contraseñas, VisionFS genera una base de datos para el control de usuarios y contraseñas. Estas contraseñas se pueden generar de cuatro maneras diferentes:

1) Usando contraseñas en blanco
2) Usando una misma contraseña para todos los usuarios
3) Generando una contraseña aleatoria por el sistema
4) Hacer la contraseña igual que el nombre de usuario.

Edit the usernames and passwords

If you want, you can edit the usernames and passwords now to make specific changes. For example, you can remove users you don't want in the VisionFS password database, or change a password for a particular user.

Would you like to edit the file now, using /usr/bin/vi?

(When you've finished, save the file and exit the editor as usual. This temporary file will be removed after use.)

Edit usernames and passwords? [y]

lromero:isela
danielj:djh
root:root

Para permitir el acceso se editan los nombres de usuario y contraseñas. Estos usuarios se generan antes de la configuración de VisionFS. El nombre de usuario esta separado de la contraseña por dos puntos. En la parte izquierda se presenta el nombre de usuario y en la parte derecha se presenta la contraseña correspondiente. Como parte de seguridad, el usuario root no se encuentra relacionado en esta base de datos, por lo que es necesario integrarlo y asignarle una contraseña.

Overwrite existing entries

Some users may already have entries in the VisionFS password database.

R - Replace any existing passwords with new ones
K - Keep the existing passwords

Overwrite or keep? [k]

Si por alguna razón la base de datos de usuarios y contraseñas ya contiene datos, es necesario confirmar si se Reemplaza cualquier contraseña existente con una nueva o Guarda las contraseñas existentes.

Send email? [y] n

You can find the usernames and passwords in /usr/vision/vfsprofile/password.default

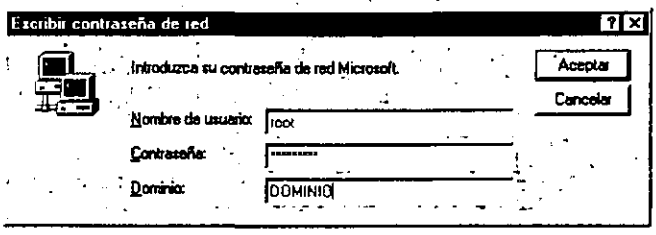
Use this information to tell your users how to access this VisionFS server.

IMPORTANT: For security reasons you should delete the file once you're finished with it.

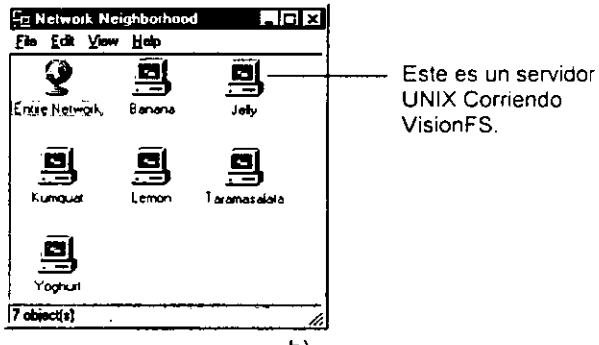
Por último se pregunta si se quiere enviar un correo electrónico a cada uno de los usuarios para hacerle saber la contraseña de acceso al servidor de VisionFS. Se indica la existencia un archivo ubicado en */usr/vision/vfsprofile/password.default* el cual contiene una lista de los nombres de usuario y contraseñas en caso de emergencia.

ADMINISTRACION DE VisionFS

Una vez instalado el servidor de VisionFS, éste se puede visualizar en el entorno de red. Para configurar el servidor de VisionFS desde su PC, se debe entrar a Windows como un Administrador de VisionFS, (en este caso root) y Buscar el servidor de VisionFS en el entorno de red,



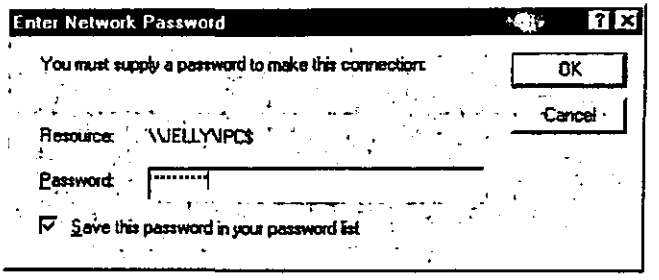
a)



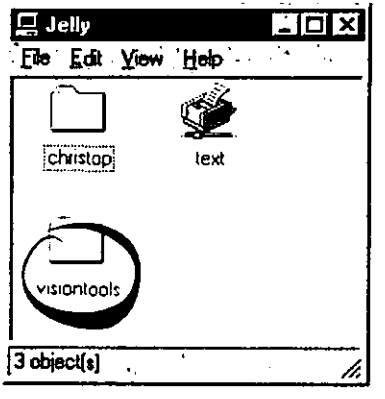
b)

Fig. 3.1 a) Usuario valido en el servidor de VisionFS
b) Servidor Unix corriendo VisionFS en el entorno de red

Al accesar al servidor, se pueden visualizar las impresoras y directorios de UNIX disponibles para su uso sobre la red. Estos recursos de red son llamados compartidos (share).



a)



b)

Fig. 3.2 a) Autentificación de un servidor UNIX en el entorno de red
b) Carpeta para configuración del servidor

Para configurar el servidor por medio del Profile editor se debe entrar a las carpetas visiontools, visionfs y ejecutar el programa profedit.exe. En la ventana del Profile Editor (Editor de Perfiles) aparece lo siguiente:

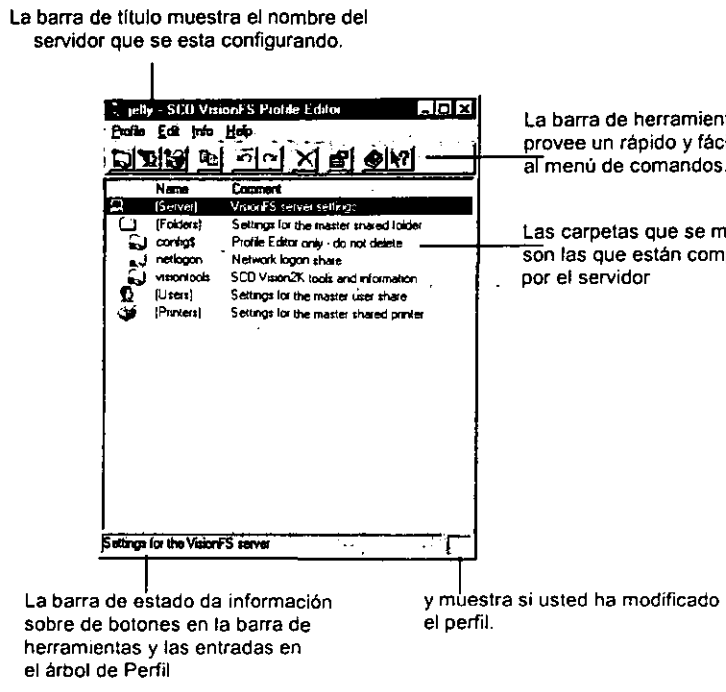
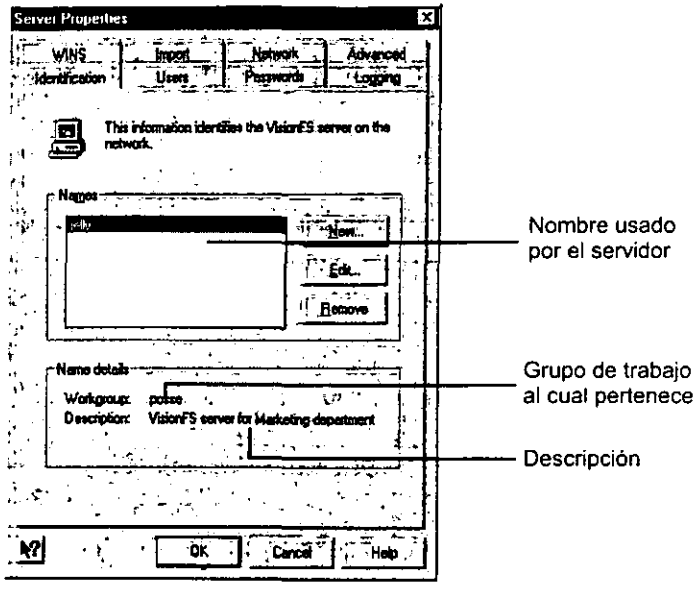


Fig. 3.3 Profile Editor (Editor de Perfiles)

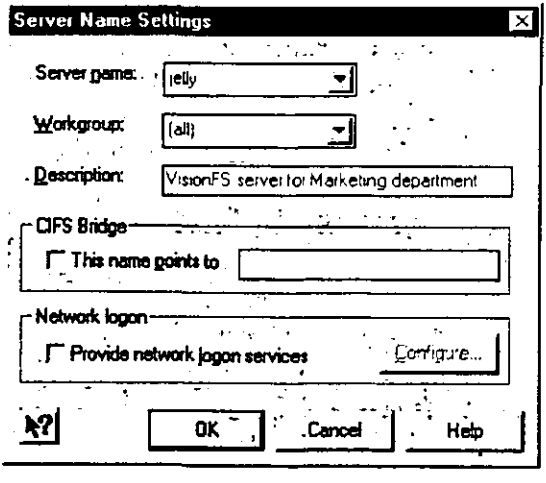
Para ver una descripción de algún botón en la barra de herramientas sólo se necesita posicionarse en el botón y en la parte de abajo aparecerá una descripción de ese botón.

CONFIGURACION DE VisionFS

Una vez que se ha ejecutado el Profile Editor lo primero que se debe de hacer es configurar los parámetros del servidor, a continuación se describen los más importantes (para entrar a la configuración del servidor seleccionar en la parte superior Server).



a)



b)

Fig. 3.4 a) Asignación de un nombre NetBios al servidor UNIX.
b) Determinación de un grupo de trabajo y un comentario.

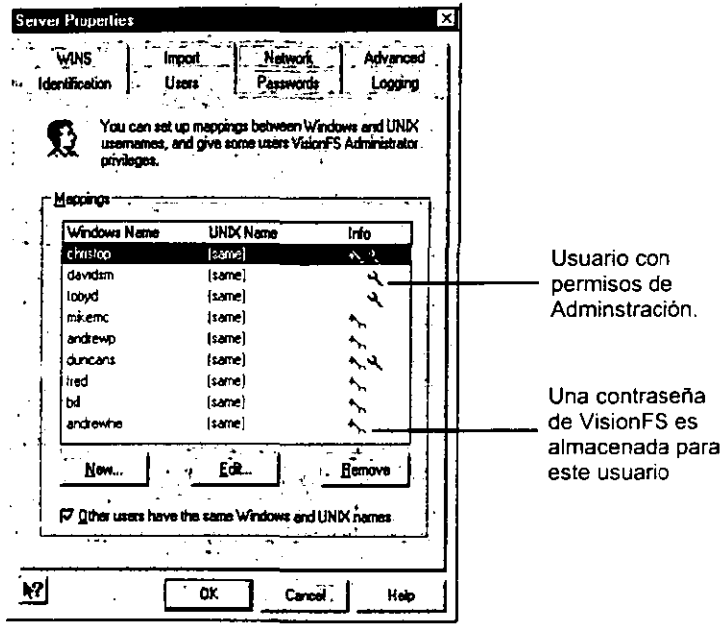
La identificación que aparece, es el nombre del servidor, el cual toma del nombre de hosts del servidor UNIX y puede ser modificado para su mejor identificación. Posteriormente aparece el grupo de trabajo al cual pertenece el servidor, que pueden ser todos, ninguno, o un grupo de trabajo específico (contabilidad, financiera, informática, etc.). Posteriormente aparece una descripción del servidor, la cual puede ser modificada.

Se puede poner varios nombres al mismo servidor, si es que se quiere que el servidor aparezca en un grupo de trabajo con un nombre y en otro grupo de trabajo con otro nombre. Solo es necesario agregar un nuevo nombre y el grupo de trabajo al cual se quiere que pertenezca.

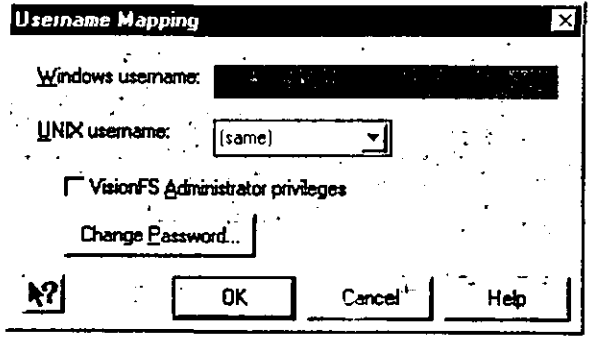
Si se quiere importar un equipo que pertenece a otra red al cual no se puede accesar directamente, ya sea una PC, un servidor de Windows NT o un servidor de VisionFS, se debe agregar un nuevo nombre el cual debe de ser idéntico al nombre del equipo remoto, integrarlo a un grupo de trabajo y seleccionar la opción de CIFS bridge agregando la dirección IP del sistema remoto en el recuadro posterior.

MAPEO DE USUARIOS DE WINDOWS NT UNIX

Los usuarios de Windows y UNIX pueden ser diferentes. Por ejemplo un usuario de Windows puede ser un nombre largo que incluye espacios mientras el nombre de usuario de UNIX puede ser solo sus iniciales. Alternativamente todos los nombres de usuarios de Windows y UNIX pueden ser los mismos.



a)



b)

Fig. 3.5 a)Usuarios existentes en la base de datos de VisionFS
b) Mapeo de usuarios de Windows con los de UNIX

Al agregar un nuevo usuario en el primer recuadro se pide el nombre de usuario de Windows y en el recuadro posterior se debe seleccionar el nombre de usuario de UNIX con el cual será mapeado; en el caso de que el usuario de Windows y UNIX sea el mismo en el segundo recuadro seleccionar same (mismo).

Al agregar un nuevo usuario se puede decidir si éste es un administrador de VisionFS. Se recomienda utilizar un usuario diferente de root para ser administrador de VisionFS ya que este no puede modificar ni eliminar archivos importantes para el sistema, solo puede realizar configuraciones del servidor de VisionFS.

TIPOS DE AUTENTIFICACION

Existen tres métodos para controlar el acceso de los usuarios a las carpetas compartidas, lo cual permite que la transmisión de las contraseñas sea encriptadas o no. También es posible que otro servidor ya sea de VisionFS o un servidor de Windows NT se encargue de autentificar a los usuarios.

El tipo de autentificación puede ser mediante una base de datos que genera VisionFS, la cual permite una encripción de la información. Otro tipo de autentificarse es mediante la base de datos de usuarios de UNIX la cuál no se encuentra encriptada por lo que no se recomienda. Por último utilizando otro servidor, de esta forma la base de datos de usuarios y contraseñas en este servidor son ignoradas. El otro servidor puede ser un UNIX que utiliza la base de datos de VisionFS o de él mismo.

También puede ser un servidor Windows NT mediante el cual los usuarios accesan al servidor de VisionFS usando las contraseñas del servidor Windows NT.

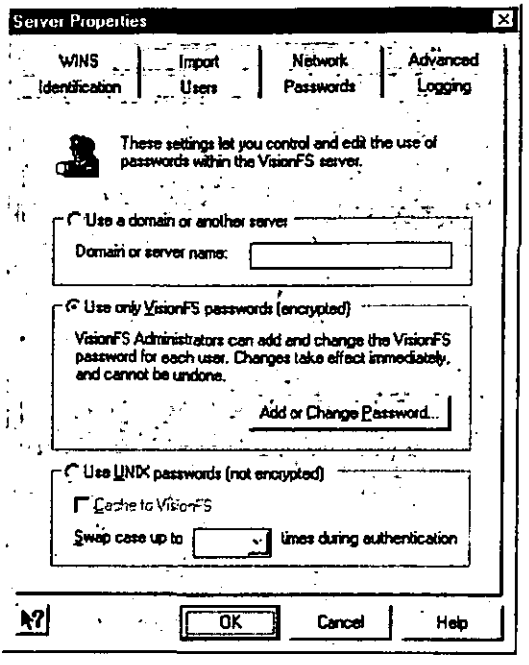


Fig. 3.6 Definiendo el tipo de autentificación

Un servidor de VisionFS puede ser un cliente y un servidor de WINS. Las PC's de Windows también pueden ser clientes de WINS si utilizan TCP/IP como protocolo de red. Si se quiere que el servidor de VisionFS funcione como servidor de WINS, en la parte inferior seleccionar el cuadro pequeño Una vez habilitado el servidor de WINS, se puede consultar la base de datos, la cual contiene los nombres NetBIOS con sus respectivas direcciones IP y el tiempo de expiración de estas, con el fin de no mantener información obsoleta.

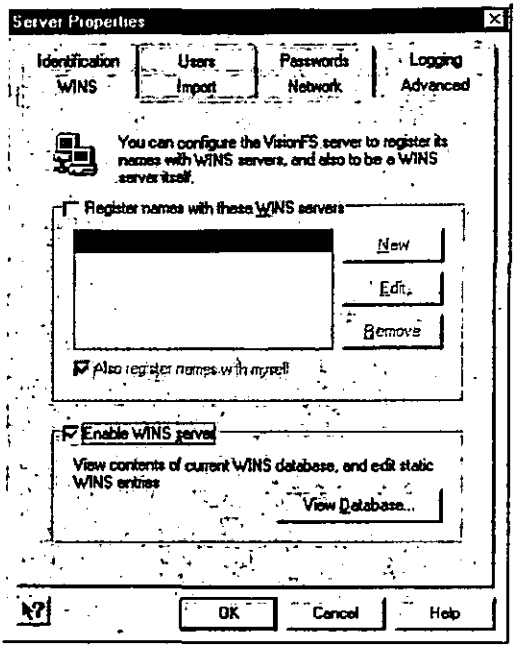


Fig. 3.7 Habilitando el servicio de Wins

También es posible asignar nombres y direcciones IP estáticas las cuales no tienen tiempo de expiración.

En el caso de que existan redes remotas y en estas se encuentren servidores de WINS, es posible importar los grupos de trabajo y las PC's que en este se encuentren en esa red, e integrarlos a nuestra red como si fuera un grupo de trabajo de la red local. Para esto es necesario seleccionar las opciones que presentan para importar grupos de trabajo, e información de la base de datos WINS del servidor remoto, además de integrar la dirección IP del servidor remoto en el recuadro posterior.

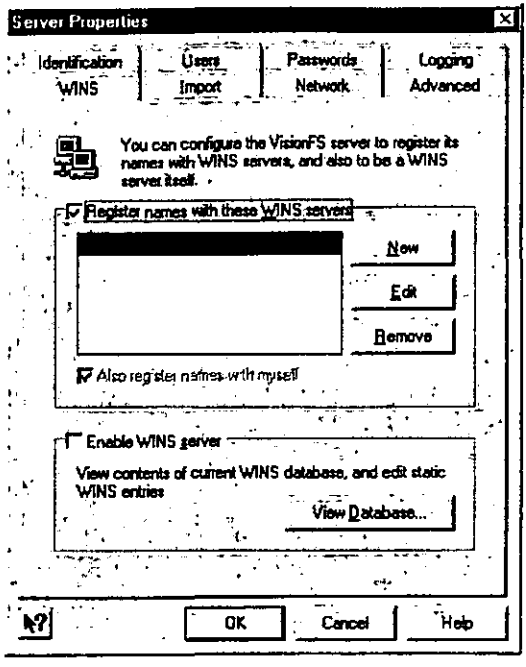


Fig. 3.8 Registrando el nombre en otro servidor de Wins

Una vez que se han hecho los cambios necesarios se requiere guardar estos cambios en la configuración del servidor de VisionFS, para esto se debe seleccionar en la barra de menú la opción Profile y posteriormente **Update Server**.

CREACIÓN DE CARPETAS COMPARTIDAS

La creación de carpetas compartidas, permite el acceso a directorios de UNIX para la obtención de información; esta puede ser algún programa en modo cliente servidor, donde el usuario obtiene gran parte de la aplicación del servidor, o la obtención de algún programa en DOS/Windows para su instalación, además de poder obtener información de una bese de datos. La creación de carpetas compartidas es seleccionando Edit y New Shared Folder.

A continuación aparece un nuevo menú el cual nos pide el nombre, con el cual, la carpeta se publicará. En el recuadro posterior pide agregar un comentario el cual nos dará una referencia o información acerca de la capeta compartida. Por último nos pide la ubicación del directorio que se ha generado para este fin. El nombre de la carpeta compartida, no necesariamente tiene que ser igual al nombre del directorio creado en el disco duro.

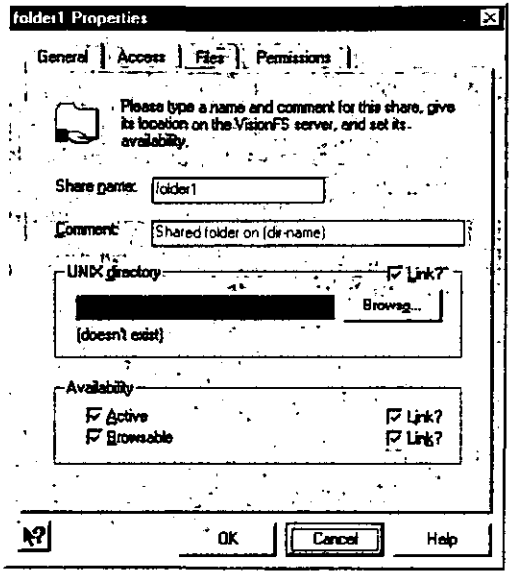


Fig. 3.9 Se indica el nombre que tendrá la carpeta compartida y su ubicación

CONTROL DE ACCESO

Se puede permitir el acceso a un Invitado y negar el acceso a los demás. Cada acción tiene una lista asociada de derechos de acceso. Un derecho particular de acceso describe:

- Un nombre de usuario y un grupo de UNIX (después de tomar un nombre de usuario lo relaciona con una cuenta), para quien este derecho de acceso aplica.

- Si este derecho aplica y el usuario es autentificado; sustituye una contraseña válida para accesar al servidor de VisionFS, según el método de autenticación.

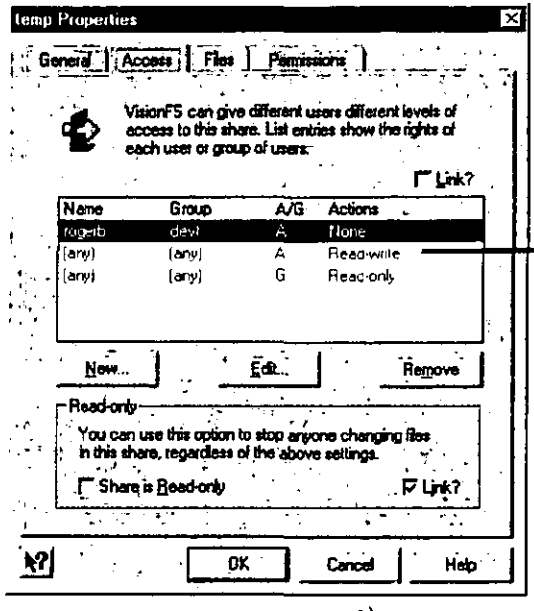
- Si este derecho aplica y el usuario es un invitado (Guest) no se tiene una contraseña para accesar al servidor, para el método actual de autenticación.

- El nombre de usuario y el grupo de UNIX se usan para un mejor desempeño en las acciones del usuario.

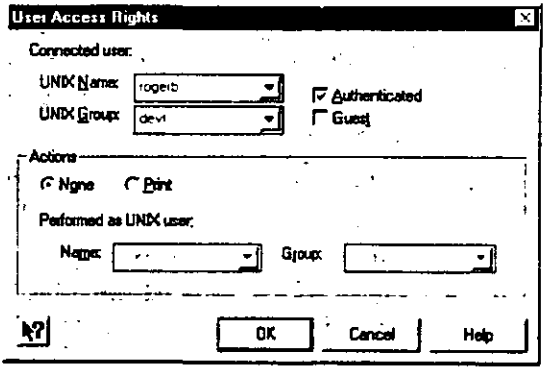
Si una acción en particular se permite, no significa necesariamente la acción triunfará; los permisos de UNIX, finalmente determinan éxito o el fracaso de la acción. Por ejemplo, si los derechos de acceso para un directorio compartida otorgan al usuario kevin el acceso libre, realizando acciones como el usuario rod, pero los permisos de UNIX para el directorio solo permiten lectura, no será posible escribir en este directorio.

Usted puede personalizar el acceso a carpetas individuales, o utilizar las configuraciones por defecto para una carpeta compartida. En el caso de que una nueva carpeta compartida sea generada.

Posteriormente es posible generar los nombres de los usuarios a los cuales se les permitirá el acceso. Estos nombres de usuarios pueden ser de Windows relacionado o mapeado con un usuario de UNIX, o ser usuarios existentes en la base de datos de UNIX. Si el usuario es seleccionado como invitado (Guest) no necesita autentificarse. Además se le permitirá o restringirá el acceso a impresoras.



a)



b)

Fig. 3.10 a) Personalizando el acceso a una carpeta compartida
b) definiendo el nombre de usuario y el grupo

Este tipo de acceso es generalmente para el acceso de usuarios especificos.

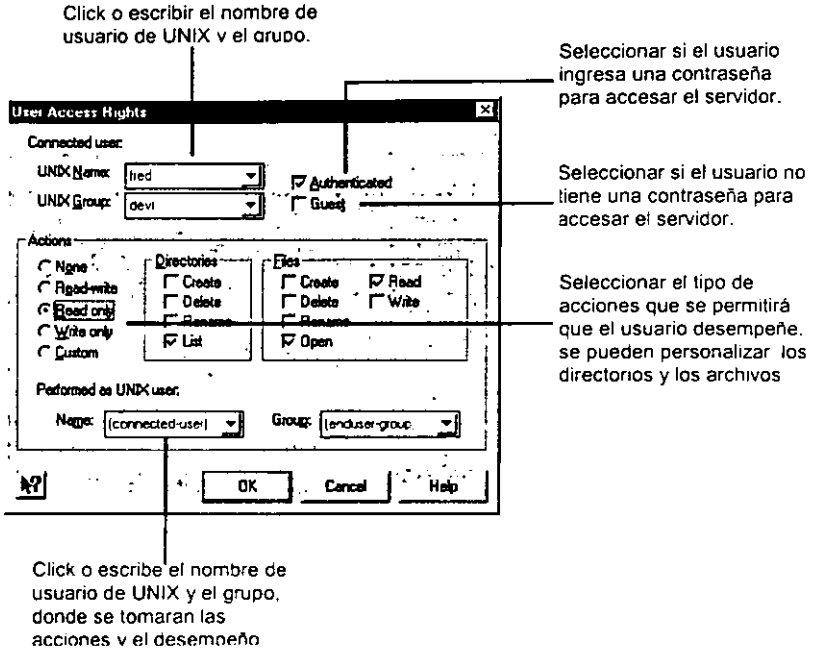


Fig. 3.11 Configurando permisos a la carpeta compartida

Por último se generan permisos de acceso, para todos los demás usuarios que pueden accesar a los recursos compartidos de un servidor.

AUTENTIFICACION DE USUARIOS POR MEDIO DE WINDOWS NT

En los capítulos anteriores se configura un servidor de VisionFS, para que la autentificación de usuarios sea por medio de un servidor de Windows NT. Esta forma de autentificar a los usuarios, permite utilizar los beneficios que proporciona un servidor de Windows NT integrando una plataforma en UNIX.

La base de la seguridad de Windows NT es que todos los recursos y las acciones están protegidos por un control de acceso. Es posible permitir a

algunos usuarios hacer conexión con un recurso y a la vez impedir que otros lo hagan. Por ejemplo pueden establecerse permisos distintos sobre archivos diferentes de un mismo directorio.

Es posible mantener la seguridad de los archivos y otros recursos tanto frente a usuarios que trabajen en el equipo donde se encuentre el recurso como frente a usuarios que se conecten con el recurso a través de red.

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

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

En NT se pueden fijar una serie de directivas comunes para todo el dominio. Entre estas se puede fijar el plan de cuentas para el dominio, que fija propiedades de las cuentas tales como la política de contraseñas, el plan de derechos de usuarios, que permite asignar determinados permisos genéricos a usuarios o grupos del dominio, o el plan de auditoria, que permite activar los elementos del sistema de auditoria en el dominio.

ADMINISTRACIÓN DEL PLAN DE CUENTAS.

Desde el menú Directivas/Cuentas podemos acceder al cuadro de diálogo "Plan de cuentas".

En este cuadro podemos fijar las limitaciones de las contraseñas y el sistema de bloque de cuentas. Cuando se ha seleccionado caducidad para la contraseña de un usuario, la contraseña utilizará las opciones elegidas en este cuadro de diálogo. Se puede elegir:

➢ **Duración máxima de la contraseña:** Intervalo de tiempo en días, que puede utilizarse para una contraseña antes del que el sistema obligue a cambiarla.

➢ **Duración mínima de la contraseña:** intervalo de tiempo que debe de usar una contraseña antes de que el usuario pueda cambiarla

➢ **Longitud mínima de la contraseña:** Numero mínimo de caracteres que debe tener una contraseña. Las contraseñas con más de 6 caracteres son difíciles de saltar por métodos de asalto masivo (crackers), también llamados de "fuerza bruta". Esto es útil en redes conectadas a Internet.

➢ **Historia de la contraseña:** Número de contraseñas diferentes que debe utilizar una cuenta de usuario antes de poder reutilizar una contraseña antigua, esto obliga al usuario a no repetir las últimas contraseñas.

➢ **Bloqueo de Cuentas:** El sistema de bloqueo de cuentas permite a los controladores de dominio reaccionar frente a los intentos fallidos de iniciar sesión en el dominio. Si se activa el bloqueo de cuentas entonces al alcanzarse el número de intentos especificado, la cuenta es bloqueada. Si el número de intentos fallidos alcanza al especificado, el usuario puede esperar el tiempo fijado en "restablecer cuenta" para poder volver a intentarlo. Fijando por ejemplo estos parámetros a 4 intentos y 10 minutos suele bastar para disuadir de accesos no autorizados. Una vez bloqueada la cuenta se puede elegir entre desbloqueo automático o manual, con intervención del administrador del dominio. También en este cuadro de diálogo se puede seleccionar si los usuarios remotos serán desconectados de los servidores al acabar su tiempo de conexión y si un usuario debe iniciar sesión en una estación de trabajo para poder cambiar su contraseña.

Con la integración de estas opciones, se garantiza la seguridad en el acceso a los recursos de un servidor. También es posible garantizar que los archivos de un usuario en específico, son modificados ó eliminados por su propietario.

ADMINISTRACIÓN DEL PLAN DE DERECHOS DE USUARIOS.

Los derechos de usuarios son una serie de permisos que no se aplican sobre un objeto concreto, como un fichero, impresora o directorio, sino que se aplican al sistema completo. Estos permisos tienen prioridad sobre los permisos asignados sobre los objetos del sistema. Se pueden asignar a cada tipo de derecho de usuario los usuarios o grupos de usuarios a los que se necesite otorgar ese derecho. Los derechos de usuarios pueden ser modificados desde el cuadro de diálogo "Plan de derechos de usuarios" accesible desde el menú Directivas/Derechos de usuarios.

Si se activa la casilla *"Mostrar derechos de usuario avanzados"* se pueden ver algunos derechos de usuarios más específicos. Normalmente los derechos de usuario asignados por NT asignan derechos suficientes a los grupos de usuarios creados por NT. Cuando se instalan algunos servicios, como servidores de correo, de Web y similares suele ser necesario cambiar algunos de estos derechos. Los más frecuentes suelen ser:

- **Iniciar sesión como servicio:** Permite asignar un usuario a un servicio. Suele ser usuario en servidores de ficheros tipo FTP, Gopher y Web, ya que permite asignar permisos a los ficheros para ese usuario, limitando el acceso a otros ficheros del sistema. También lo usa el servicio de duplicación de directorios.

- **Iniciar sesión como proceso por lotes:** Este derecho está pensado para los servicios que atienden las peticiones de usuarios en forma de transacciones, como por ejemplo servidores POP3 y otros. Actualmente no

está implementado en el sistema operativo, pero algunos servicios verifican que el usuario posea este derecho antes de atender su petición.

CONFIGURACION DEL PLAN DE AUDITORIA

Mediante la auditoria es posible hacer un seguimiento de determinadas actividades de los usuarios. En un controlador de dominio, el plan de auditoria determina la cantidad y tipo de información de seguridad que registra Windows NT Server para todos los controladores del dominio. En las estaciones de trabajo y servidores miembros, el plan de auditoria determina la cantidad y el tipo de información de seguridad que se registra en cada PC individual.

Windows NT puede registrar diversos tipos de sucesos, desde los que afectan a todo el sistema, desde el inicio de sesión de un usuario, hasta los intentos por parte de un usuario de leer un archivo determinado. Es posible registrar tanto acciones que tienen éxito como las que fracasan.

Utilice el visor de sucesos, dentro de las herramientas administrativas del menú de inicio, para examinar el registro de seguridad.

TIPOS DE SUCESOS

- **Inicio y cierre de sesión**: Registra cuando un usuario ha iniciado o terminado una sesión, o ha establecido una conexión de red.

- **Acceso a archivos y objetos**: Es cuando un usuario ha abierto un directorio o un archivo elegido para auditoria en el Administrador de archivos, o ha enviado un trabajo de impresión a una impresora elegida para auditoria en el Administrador de impresión.

➢ **Uso de los derechos de usuario:** es cuando un usuario ha utilizado un derecho de usuario.

➢ **Administración de usuarios y grupos:** Se ha creado, modificado o eliminado una cuenta de usuario o de grupo. Se ha cambiado el nombre a una cuenta de usuario, se ha activado o desactivado, o se ha establecido o cambiado su contraseña.

➢ **Cambios en el plan de seguridad.** Se ha efectuado un cambio en el plan de derechos de usuario, en el de auditoria o en el de relaciones de confianza.

➢ **Re-inicio, apagado y sistema**: Un usuario ha reiniciado o apagado la PC, o se ha producido un suceso que afecta la seguridad del sistema o al registro de seguridad.

➢ **Seguimiento de procesos:** Estos sucesos proporcionan información de seguimiento detallado sobre sucesos tales como la activación de programas, algunas formas de duplicación de identificadores, accesos indirectos a objetos y salida de procesos.

Puesto que el tamaño del registro de seguridad es limitado, seleccione cuidadosamente los sucesos que se van a auditar, y considere el espacio en disco duro que desea dedicar al registro de seguridad El tamaño máximo del registro de seguridad se define en el visor de sucesos.

SECUENCIA DE CONEXIÓN

Para que un usuario de PC, pueda tener acceso a los servicios de un servidor de VisionFS, es necesario que este realice un inicio de sesión en Windows, con un nombre de usuario valido para UNIX en la base de datos de VisionFS. Si la autentificación es realizada por un servidor de Windows

NT, las contraseñas serán modificadas en este servidor, y por lo tanto, las contraseñas del servidor de VisionFS serán ignoradas.

Para un plan de seguridad en el cual se pide al usuario que cambie su contraseña cada tiempo determinado, por ejemplo cada 20 días; no es necesario el cambio de las contraseñas del servidor de VisionFS, por lo que disminuye la administración y se incrementa la seguridad en las aplicaciones de usuario.

Si se cuenta con una red LAN que utiliza los servicios de distintos servidores es recomendable la integración de los servicios de WINS del servidor UNIX, ya que esto incrementa el ancho de banda de la red, al evitar los requerimientos de red por medio de Broadcast. Cabe señalar que las bases de datos de WINS para Windows NT y UNIX no son compatibles, por lo que es necesario decidir si se utilizará Windows o UNIX.

Sin embargo es posible hacer una combinación, para asignar servidores de WINS en una PC de red, asignando como servidor primario un Windows NT y como secundario un equipo UNIX o biseversa. Al realizar un requerimiento de red; la PC iniciará su búsqueda en el servidor de WINS que tiene asignado como primario, si no encuentra respuesta iniciará la búsqueda en su servidor secundario. Si una PC es un cliente de servidor de Windows NT se recomienda que también sea cliente de WINS de ese servidor de Windows NT.

En este caso todas las PC´s están integradas como clientes de un dominio de Windows NT, el cual les puede aplicar un plan de cuentas, derechos de usuario o un plan de auditoria. Este servidor es el que se encarga de cambiar las contraseñas y de permitir o negar el acceso a un servidor de aplicaciones. Funciona como servidor de WINS, con el fin de que la autentificación y el acceso a los servidores de aplicaciones sean más rápidos.

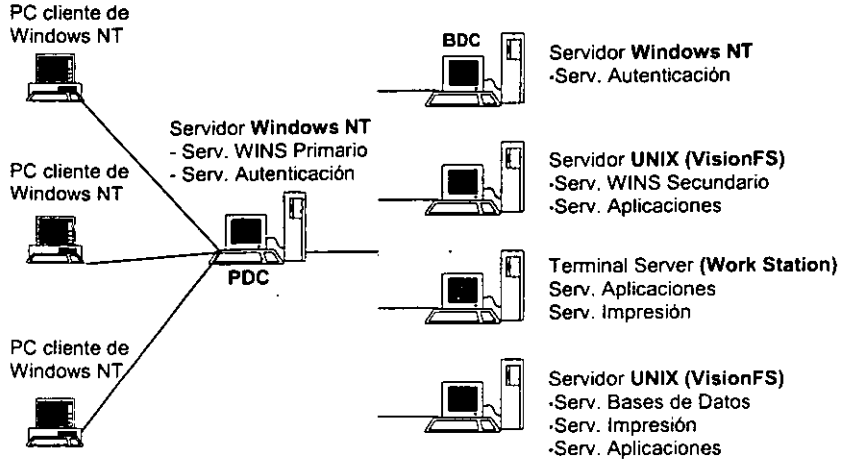


Fig. 3.12 Secuencia de conexión para un cliente de Windows NT con acceso a servidores UNIX

Para que se garantice el acceso a los servicios que proporcionan otros servidores, es necesario la existencia de un servidor Windows NT secundario (BDC). No es necesario que este servidor sea un servidor de WINS secundario.

Un servidor de Windows NT, cuenta con servicios que son útiles para un administrador de red, cuando se empiezan a incrementar la cantidad de aplicaciones que se corren en este, suele ser inestable.

Detrás de este servidor que se encarga de autentificar los usuarios, puede existir un servidor de UNIX con VisionFS instalado. Dado su alto rendimiento y capacidad comprobada, es un servidor capaz de correr múltiples aplicaciones (multitarea). Este es capaz de funcionar como servidor de WINS secundario, servidor de múltiples aplicaciones para PC´s o funcionar como base de datos, además de funcionar como servidor de impresión.

Al momento de que una PC trata de ingresar a la red y el servidor principal de Windows NT esta fuera, el servidor secundario se encarga de autentificar al usuario. Dado que este servidor no funciona como WINS, la PC busca a su servidor secundario de WINS, el cual proporciona la información para completar la conexión de este equipo.

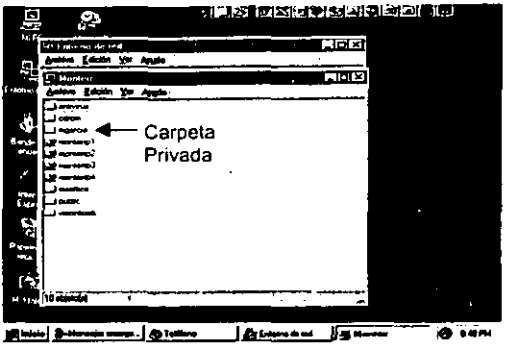


Fig. 3.13 Carpeta privada de un usuario Windows que ingresa a un servidor UNIX

Cuando un usuario de PC accesa a un servidor UNIX, este puede disponer de una carpeta privada, donde puede crear archivos y directorios.

Esta carpeta privada solo la puede ver el usuario propietario; si es un usuario de Windows mapeado con un usuario de UNIX, la carpeta que aparecerá es la del usuario de UNIX al cual fue mapeado. Además de disponer de la carpeta privada puede disponer de las carpetas publicadas en el servidor y las impresoras.

Si se tiene una red segmentada, la cual esta interconectada por medio de un ruteador y en el supuesto caso, de que existiera un servidor UNIX en esa red; es posible integrar las PC´s remotas, como si fueran de la red local.

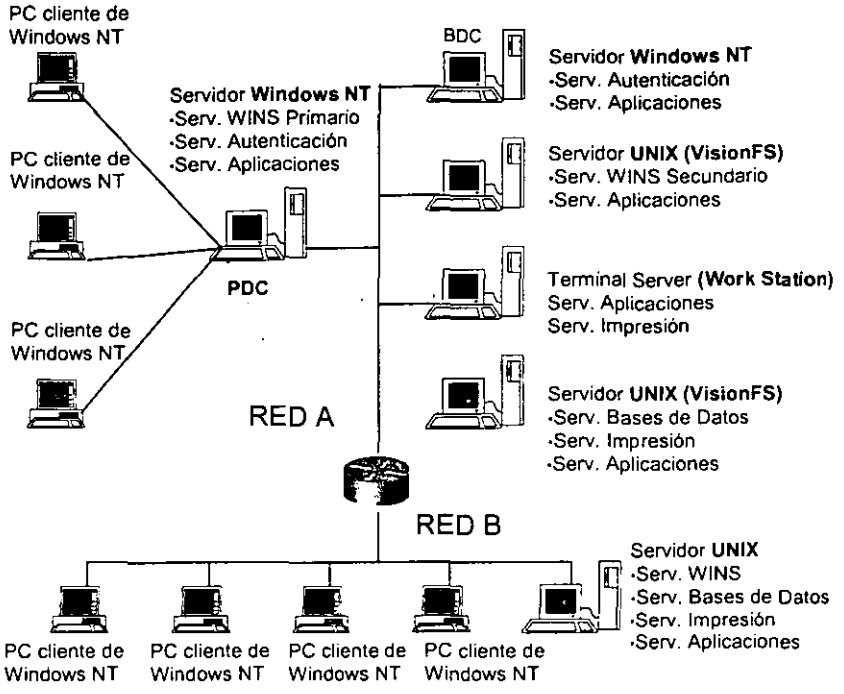


Fig. 3.14 Integración de redes Segmentadas

La integración puede ser indicando como WINS primario, al servidor de Windows NT y como secundario al servidor UNIX de la red en que se encuentra el equipo remoto. De esta forma se le indica al servidor UNIX local que importe el grupo de trabajo remoto.

Al importar el grupo de trabajo remoto, es posible integrarlo al plan de contraseñas, derechos de usuario y plan de auditoria; además de proporcionar otros servicios que se encuentren instalados en la red local.

CONCLUSIONES

Debido a la necesidad de proporcionar información y recursos, a múltiples usuarios, se desarrolla la tecnología para la conexión mediante red. La integración de múltiples plataformas es posible dada las tecnologías avanzadas que actualmente se manejan.

Es importante el conocer los distintos tipos de redes. En el caso de las redes LAN existen diferentes topologías, definidas por su forma de conexión y la forma en que realizan el acceso a la red, lo cual caracteriza cada una de ellas.

Es necesario entender la forma en que los quipos en la red se comunican. El modelo OSI nos proporciona esta información y explica dada una de sus capas de forma que sea comprensible, como se lleva a cabo la conexión entre computadores.

Para que dos equipos puedan comunicarse entre sí, necesitan de varios componentes de red, tales como: tarjetas de red, cableado, swiches, ruteadores y servidores. Cada uno de estos elementos es necesario dadas las características de cada red, es interesante saber que es cada uno de estos componentes y como trabaja, para la buena planeación de una red y con esto proporcionar un óptimo servicio a los usuarios.

Un protocolo es un lenguaje que permite que dos computadoras se entiendan, actualmente el protocolo de mayor aceptación es TCP/IP dadas sus caracteristicas para encaminar datos y su utilización para el acceso a Internet. Las direcciones IP determinan el tipo de red que se está utilizando y esta puede ser de clase A, clase B o clase C. Para evitar una saturación en el ancho de banda de una red se debe poner la mascara de subred apropiada para cada tipo de red.

CONCLUSIONES

Dos de los sistemas operativos que han tenido más aceptación son Windows NT y UNIX, cada uno de ellos tiene sus cualidades y sus defectos, la integración de estos dos sistemas operativos para proporcionar servicios de red. incrementa la confiabilidad en la red, utilizando las cualidades de los dos sistemas operativos y disminuyendo los defectos.

El realizar esta integración por medio de VisionFS hace que los recursos de un servidor UNIX estén disponibles como si fuera un servidor de Windows NT. Una de las características de UNIX es proporcionar al usuario una carpeta privada donde pueda resguardar sus programas y archivos. Además es capaz de trabajar en un esquema cliente servidor y funcionar como servidor de aplicaciones para usuarios Windows.

VisionFS puede funcionar como servidor WINS lo que nos ayuda a disminuir el tráfico en la red y proporciona un protocolo de red llamado CIFS el cual es capaz de importar equipos de otras redes e integrarlos como si fueran de la red local. La forma de configuración de este programa es muy sencillo dada su característica por medio de ventanas y no en línea de comandos como suele ser en un sistema operativo en UNIX.

Un servidor de Windows NT tiene la capacidad de controlar el acceso a los usuarios y aplicar políticas de seguridad, como el plan de cuentas, que obliga al usuario a cambiar su contraseña cada determinado tiempo, el plan de derechos de usuario el cual permite al usuario solo correr los protocolos que se le indiquen, o el plan de auditoria, que nos permite observar los sucesos que el usuario realiza.

El integrar una plataforma en UNIX con sus recursos compartidos validados por un servidor de Windows NT hace más robusto el plan de seguridad y disminuye la administración de los servidores.

CONCLUSIONES

La forma en que se define la conexión de los usuarios a los servidores y la utilización de los servicios de red como WINS incrementan el ancho de banda de una red proporcionando un mejor servicio al usuario.

DEFINICIONES

LAN (LOCAL AREA NETWORK): Red de área local, o Red local de computadoras. Se refiere a una red de computadoras conectadas bajo un mismo protocolo y tipo de conexión física, sin modulación de la señal y de distancias cortas (generalmente menores a 10 Km. por ejemplo el diámetro de un campus universitario)

WAN (WIDE AREA NETWORK): Red de área extensa. Es una red que interconecta a varias redes LAN y abarca un área geográfica amplia, desde el equivalente a un país, un continente, e incluso varios continentes.

10BASE-T: Se trata del estándar IEEE 802.3 para Ethernet con una velocidad de transmisión de 10 Mbps. Que utiliza un cable UTP (par trenzado sin apantallar). Utiliza una topología en estrella, que es más robusta y ofrece más seguridad, pero que requiere un dispositivo central común.

100BASE-T: Se trata del estándar IEEE 802.3 para Ethernet con una velocidad de transmisión de 100 Mbps a tráves de un cable UTP

METODO DE ACCESO: Es un protocolo que determina qué dispositivo en una red de área local tiene acceso al medio de transmisión en cualquier momento. CSMA/CD es un ejemplo de método de acceso.

ANCHO DE BANDA (BANDWIDTH): Es un rango de frecuencias comprendidas entre dos límites, que pueden pasar a través de un canal de comunicación. En un circuito digital, el ancho de banda representa la habilidad máxima del circuito para mover bits por unidad de tiempo y se expresa en unidad por segundo (bps).

ESTA TESIS NO SALE
DE LA BIBLIOTECA

ANSI (AMERICAN NATIONAL STANDARD INSTITUTE): Es una organización no gubernamental donde sus miembros apoyan, diseñan, adoptan y generan comunicación.

ARCNET: Sistema de red de área local (LAN) desarrollada por Datapoint. Utiliza las técnicas de pasa fichas (token) pero no es un anillo (ring) sino que sigue la topología física de estrella y permite un máximo de 256 nodos en la red. Datapoint licenció la tecnología ARCNET para la Tandy Corporation Davon (Fuera del mercado actualmente), Novell y Standard Microsystws. Es una de las redes locales más baratas actualmente. Su velocidad máxima actuales de 2.5 Mbps.

ARPA (ADVANCED RESEARCH PROJECTS AGENCY): Agencia del departamento de defensa de los estados unidos.

ARPANET: Red desarrollada por ARPA que utiliza técnicas de "packet-switching" fue la primera red que trabajó con estas técnicas.

ASCII (AMERICAN STANDARD CODE FOR INFORMATION INTERCHANGE): Código de caracteres de siete bits estandarizado por ANSI y está designado como X3.4-1977 en donde 1977 es el año de la ultima revisión. ASCII también fue estandarizado por ISO y CCITT y es conocido internacionalmente como Alfabeto #5 Internacional de Telégrafos. Es casi el código universal de representar caracteres en las computadoras, a excepción de algunas máquinas de IBM que aún emplean EBCDIC y BCD

ATM (ASYNCHRONOUS TRANSFER MODE): Es una tecnología de red que transfiere paquetes de datos para el posterior reenvio de diferentes tipos de información (video, datos, voz)

ARP (ADDRESS RESOLUTION PROTOCOL): Protocolo a nivel de red de resolución de correspondencias dirección MAC-dirección IP.

BAUDIO: Número de señales transmitidas sobre una conexión lógica cada segundo.

BCD: Siglas en inglés de "Binary Coded Decimal" (Decimal Codificado en Binario). Tecnica para representar los digitos de número en decimal (0-9) cada uno mediante unà secuencia de cuatro bits.

BPS (BITS POR SEGUNDO): se refiere a la cantidad de bits que se transfieren en un segundo y determina la velocidad a la que la información es enviada sobre una conexión lógica.

BROADCAST: se refiere al mensaje que se envía a todas las estaciones en una conexión lógica multipunto.

BACKBONE: Aquella parte de la red que soporta el tráfico más denso, interconecta redes de área local (LAN), formándose grupos que pueden abarcar un área limitada a un edificio, a una ciudad o a una región.

BANDA BASE: Es una tecnologia de comunicación, que utiliza una frecuencia eléctrica para representar los datos; en unos y ceros lógicos.

BANDA ANCHA: Una tecnología de comunicación, que utiliza las frecuencias de radio en un cable.

BRIDGE (PUENTE): Un bridge conecta entre si dos segmentos de la misma red e intercambia datos.

CCITT: International Telegraph and Telephone Consultative Committee (Comité consultivo Internacional de Teléfonos y Telégrafos) Agencia de la Unión Internacional de Telecomunicaciones.

CSMA/CD: siglas de "Carrier Sense Multiple Acces with Collosion Detectión". Acceso múltiple de sensor de portadora con detección de colisión. Es un procedimiento de protocolo de capa lógica de tipo contención muy popular en los LAN´s como Ethernet. Antes de enviar un mensaje, detecta la señal de la portadora para ver si esta vacia la conexión, si no es así, se contiene de efectuar el envio. Pudiera sin embargo haber dos o más mensajes simultáneos que colisionan, tales colisiones las detecta un "tranceiver". Después de efectuarse una colisión, los nodos se contienen un tiempo al azar antes de volver a intentar la comunicación.

CATV (COMMUNITY ANTENNA TELEVISION): Red de televisión por cable.

DHCP (DINAMIC HOST CONFIGURATION PROTOCOL): Protocolo de configuración dinámica de direcciones IP.

DIRECCION MAC: Una dirección única, que se adjudica a toda estación final activa dentro de la infraestructura (entre ellos se encuentran los adaptadores LAN en la placa base, a puertos de conmutadores y puertos de encaminadores (routers)).

EIA (ELECTRONICS INDUSTRIES ASSOCIATION). Asociación de Industrias Electronicas, es una organización de manufactureros de equipo electrónico de los E.U. que crea estándares.

FAST ETHERNET: Una tecnología de redes con amplio ancho de banda y que se basa en el estándar 802.3 Ethernet (100BASE-T), de 100Mbps. Diez veces más rápido que el Ethernet (10BASE-T) a 10 Mbps.

HUB (REPETIDORES MULTIPUERTO): Dispositivo que ejerce de nodo central en redes en estrella.

ISO (INTERNATIONAL STANDARDS ORGANIZATION): Organización de estándares Internacionales. Es un Organismo de las Naciones Unidas, con sede en Paris, cuya misión es el generar y difundir estándares entre las naciones, logrando así la compatibilidad y complementación en servicios y productos internacionalmente. Desarrolló el modelo de comunicación abierta OSI.

IEEE (INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERES): Instituto de Ingenieros eléctricos y electrónicos. Es una entidad que ha generado muchos estándares en telecomunicaciones.

IEEE 802: Estándares para la conexión física y eléctrica de LAN's desarrollado por IEEE.

IEEE 802.1D: Estándar de la IEEE para el nivel de acceso de control para puentes o "bridges" InterLAN, entrelazando redes IEEE 802.3, 802.4 y 802.5

IEEE 802.3 1Base5: Especificación que iguala el antiguo producto de AT&T StarLAN. Este designa una velocidad de 1 Mbps, Técnica de banda base y un máximo de distancia de cable de 500 metros.

IEEE 802.3 10Base2: Esta especificación iguala el cableado estrecho de Ethernet. Este designa una velocidad de señal de 10 Mbps, técnica de banda base y un máximo de distancia de cable de 185 metros.

IEEE 802.3 1Broad36: En esta especificación se describe un tipo de cableado de la Ethernet pero de larga distancia con una velocidad de 10 Mbps y una distancia de cable de 3,600 metros.

IEEE 802.4: Aquí se describe un LAN que usa una velocidad de 10 Mbps, control de acceso para "token-passing" y una topologia de bus física. Este es tipicamente usado como parte de redes que siguen a MAP (Manufacturing

Automation Protocol) desarrollado por General Motors. Este es a veces confundido con ARCnet pero no es el mismo.

IEEE 802.5: Esta especificación describe un LAN que usa 4 o 16 Mbps MAC "token-passing" y una topología física de anillo. Es utilizado por los sistemas IBM de Token-Ring.

IEEE 802.6: Este estándar de la IEEE para MAN´s describe lo que se llama un "Distributed Queue Dual Bus" (DQDB). La topología DQDB incluye cableadoparalelo típicamente de fibra óptica entrelazando cada nodo (típicamente un router para un segmento de LAN) utilizando una velocidad de 100 Mbps.

IMPEDANCIA: propiedad eléctrica de un cable, combinando capacidad, instalación y resistencia y se mide en "ohms"

INTERFACE: Una interface provee los medios para la interconexión de equipo o procesos.

MAC (MEDIA ACCESS CONTROL): Control de acceso al medio

MULTIPLEXOR: El multiplexor MPX, es un dispositivo que acepta varias lineas de datos a la entrada y las convierte en una sola linea corriente de datos compuesta de alta velocidad. Esto hace la función de transmitir "simultáneamente" sobre un mismo medio varias señales.

NIC: Network Interface Card.

OSI (Open Systems Interconexión): Interconexión de sistemas abiertos. Arquitectura de redes definida por ISO. Es una recomendación de ISO que describe una estructura de siete capas para la partición de comunicación de datos y funciones de telecomunicaciones en capas.

PBX: Siglas en inglés para Private Branch Exchange. Este es un conmutador telefónico privado que sirve a una localización específica. La mayoría de los PBX pueden transportar datos de computadoras sin el uso de modems.

PROTOCOLO: Este es el procedimiento (conjunto de pasos, mensajes y secuencias) que se utiliza para mover la información de una localización a otra sin errores.

PAQUETE: un conjunto de bits de datos e información conectada, entre la que se encuentra la dirección del remitente y la dirección del receptor, que se formatea para su transferencia de un ordenador a otro.

REPETIDOR: Un sistema que regenera y amplia las señales digitales; y se utilizan en redes extensas.

SONET (SYNCHRONOUS OPTICAL NETWORK): Red Óptica Síncrona.

SEGMENTO: La longitud máxima que un cable debe tener para poder descubrir colisiones. En un cable Fast Ethernet, que utiliza 100 Base-Tx, la longitud del segmento es de 205 metros.

SERVIDOR: Un dispositivo de red que ofrece servicios a una PC cliente; por ejemplo, acceso a ficheros, cola de impresión o acceso remoto.

SNMP (STANDARD NETWORK MANAGEMENT PROTOCOL): Un estándar que controla los dispositivos de conexión en red, entre los cuales se encuentran los adaptadores, conmutadores, rutas, servidores y estaciones de trabajo; recogen información de diferentes agentes.

THICK ETHERNET: El original estándar para cables de Ethernet, que requiere un conector AUI; de gran resistencia contra interferencias, pero difícil de instalar y mantener.

THIN NET (THIN ETHERNET): una red CSMA/CD, que se basa en un cable coaxial fino (también denominado Thin Ethernet), que requiere un conector BNC, que se basa en el estándar 10Base-2 de IEEE.

TOKEN PASSING: Un método de transmisión en secuencia cerrada, por cuyos sistemas activos circulan los así llamados "testigos"; más fáciles que CSMA/CD en redes con mucho tráfico, pero de difícil implementación.

TOKEN RING: La implementación de IBM del token passing, basado en el estándar 802.3 de IEEE; la segunda topología de red más popular después de Ethernet.

VLAN (LAN´s virtuales) Tecnología de conexión, que hace posible una segmentación de la red, que es independiente de la agrupación física o de dominios de colisión.

BIBLIOGRAFIA

MICROSOFT WINDOWS PARA TRABAJO ENGRUPO
Cherly Currid & Company
Editorial Limusa
Primera edición.

Guía de Integración de Windows NT y UNIX
David Gunter, Steven Burmett, Lola Gunter
McGraw-Hill

Introducing SCO VisionFS
The Santa Cruz Operation
Fourt Edition 1998.

Redes y Comunicaciones para Computadores
Comercializadora Editorial y Sistemas LTDA
Tomos I, II y III

Redes de Ordenadores
Andrew S. Tanenbaum
Prentice Hall
Segunda Edición

MICROSOFT WINDOWS 95 KIT DE RECURSOS
Traducción Fernando Saenz Pérez y Rafael Moreno Vozmediano
Mc Grawll Gil