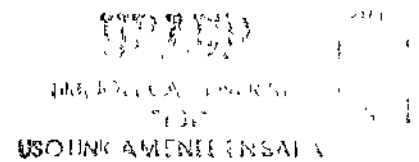
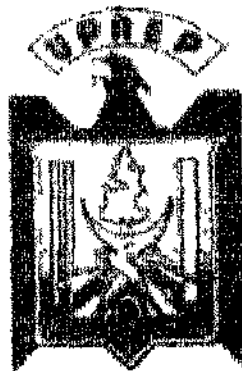


Universidad Popular Autónoma del Estado de Puebla



La Importancia de UNIX en la Implementación de los Sistemas Abiertos

Tesis que presentan :

Roxana Contreras Lobato
Adolfo Colín Toral

Asesor:

LSC. José Luis Iñigo Ortega

Para obtener el título de:
Lic. en Sistemas Computacionales

Febrero de 1995



UPAEP – Secretaría General

Dirección General de Apoyos Académicos

Dirección del Centro de Recursos para el Aprendizaje y la Investigación.

Biblioteca Central - **Karol Wojtyla**

Tesis Digitales Restricciones de uso:

DERECHOS RESERVADOS ©

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

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

El uso de textos, imágenes, gráficas, 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 de donde la obtuvo mencionando el autor o autores involucrados en el documento.

Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

**A nuestras familias por su
incondicional apoyo**

**Agradecemos al LSC. José Luis
Iñigo Ortega su valiosa
colaboración y apoyo**

	<i>Pág.</i>
Introducción	VII

Capítulo I. Introducción a las Redes de Comunicación de Datos

Introducción	1
¿Qué es una red de comunicación de datos?	2
Estación de Trabajo	3
Servidores de disco	3
Servidores de archivos	4
Servidores de archivos dedicados y no dedicados	4
Servidores de impresión	4
Topologías de red	5
Topología Mesh	5
Topología Star	6
Topología Bus	7
Topología Ring	7
Métodos de acceso	8
Ancho de banda	8
Método de acceso Contention	8
Método de acceso Polling	9
Método de acceso Token-Passing	10
Concepto de protocolo y estándares de comunicación	11
¿Qué es un sistema abierto?	13
Inicio de los sistemas abiertos	14
Medios Físicos de transmisión	16
Líneas abiertas de dos alambres	17
Cable Par-Trenzado	19
Ventajas y desventajas de cable Par-Trenzado	20
Cable Coaxial	20

Estructura del cable Coaxial	21
Ventajas y desventajas de cable Coaxial	22
Cable de Fibra Optica	23
Estructura del cable de Fibra Optica	23
Ventajas y desventajas de la Fibra Optica	25

Capítulo II. Redes de Comunicación de Datos

Tipos de redes de comunicación de datos	26
LANs	26
MANs	27
WANs	27
Redes Cliente-Servidor	27
Redes punto-a-punto	29
Aplicaciones de las redes de comunicación	29
Aplicaciones Puras de Red	30
Emulación de terminal	30
Transferencia de archivos	30
Correo electrónico	31
Aplicaciones de grupos	31
Aplicaciones de red Standalone	31
Facilidad de uso	32
Compartir archivos	32
Limitaciones de recursos	32
Economía en el crecimiento	32
Sistemas operativos de Red	33
El Microsoft LAN Manager	33
El IBM Network Program	34
Novell Netware	35
Topología	35
Netware y el concepto de un servidor de archivos	35
Administración de archivos bajo Netware	36

Apple Talk	37
Los protocolos Apple Talk y el Modelo OSI	37
Apple Share	37
AT&T StarLAN	37
Banyan Vines	38
LANTastic	38
BTOS/CTOS	39
BTOS/CTOS Open	39

Capítulo III. Modelo de Referencia OSI

Concepto de Trasposición de capas y su relación con el modelo de referencia OSI	41
La capa Física	42
La capa de Enlace de Datos	42
La capa de Red	43
La capa de Transporte	43
La capa de Sesión	43
La capa de Presentación	44
La capa de Aplicación	45
Protocolos estándar relacionados con el modelo de referencia OSI	45
Estándar CCITT X.25	45
Procedimiento de control del enlace de datos a alto nivel	47
Control Síncrono de enlace de datos	47
Estándares de red IEEE	48
IEEE 802.2	49
IEEE 802.2 / Ethernet	49
El Paquete de Datos Ethernet	50
El protocolo CSMA/CD	51
IEEE 802.3	52
IEEE 802.3 10Base2	52

IEEE 802.3 STARLAN	52
IEEE 802.3 10BaseT	52
IEEE 802.4 Token Bus	53
IEEE 802.5 / Token ring	55
IEEE 802.3 / Ethernet Vs. IEEE 802.5 / Token Ring ..	55
ARCNET	56
Local Talk	56
Protocolo de las capas superiores	
del Modelo de Referencia OSI	58
X.400	58
Protocolos Administradores de red	58
Protocolos propietarios de las capas superiores	58

Capítulo IV. Conjunto de Protocolos TCP/IP

Introducción a TCP/IP	60
Transferencia de datos en la capa de Transporte	62
Transferencia de datos en la capa de Red	62
Panorama sobre la arquitectura TCP/IP	62
Servicios del Protocolo Internet	64
El IP y las Sub-redes	65
El datagrama IP	66
Servicios mayores del IP	68
Rutina Internet header check	68
Ruteo fuente del IP	69
Operaciones de ruteo	70
Ruteo de pérdida	71
La opción timestamp	72
Fragmentación y reensamble	73
¿Existe reensamble en los gateways?	73
Tablas de dirección y ruteo del IP	74
Tabla de dirección	74
Tabla de ruteo	75

Definiciones y primitivas del Servicio IP	77
Primitivas UP/ULP	77
Primitivas IP/SNP	78
Primitivas de la capa de red/LLC	78
Multicasting	79
Protocolo de administración de grupo Internet	80
Servicios del protocolo de control de transmisión	81
Panorama de TCP	81
Características mayores del TCP	82
Puertos y Sockets	85
Aperturas Pasivas y Activas	85
Bloque de Control de Transmisión	87
Operaciones de Retransmisión	87
TCP y las interfaces del usuario	87
Consideraciones en el uso de TCP	88

Capítulo V. UNIX

Introducción...	89
Sistemas operativos de 32 bits	90
Características de los sistemas operativos de 32 bits	90
Análisis comparativo	93
Alternativas	93
UNIX y otros sistemas operativos	94
Panorama de Microsoft Windows NT	94
Breve historia de Windows NT	95
Requerimientos de Windows NT	96
Estructura de Windows NT	97
Subsistemas protegidos	99
Arquitectura abierta	100
Funcionamiento en Red	101
Portabilidad y Escalabilidad	102
Programación de aplicaciones	103
Ventajas de Windows NT	103

Desventajas de Windows NT	103
Panorama de OS/2	104
Breve historia de OS/2	104
Soporte de OS/2 para DOS	107
Soporte de OS/2 para Windows	108
Soporte de red en OS/2	109
Ventajas de OS/2	109
Desventajas de OS/2	110
Panorama sobre UNIX	111
Reseña histórica del sistema operativo UNIX	113
Versiones de UNIX	117
Sistemas UNIX de SCO	117
Open Desktop Personal System	117
Open Server Network System	117
SCO Open Desktop Network System	117
LAN Manager for UNIX	117
SunSoft Solaris	117
HP-UX	117
AIX PS/2	118
Nextstep	118
UnixWare	118
Características principales de UNIX	119
Emulación de UNIX para DOS y Windows	121
Conectividad	121
Soporte de UNIX para las redes	122
UUCP	123
Adaptabilidad de UNIX al hardware	123
UNIX & Intel	124
Consideraciones de programación	124
Aplicaciones	125
Desventajas del uso de UNIX	125
Ventajas de UNIX	126
UNIX en la implementación de los sistemas abiertos	128

El Ambiente Común del Software Abierto	128
Diferentes ambientes UNIX	130
X Window System	130
La interface Motif	131
Unix International & Open System Fundation	131
Sistemas Abiertos y Sistemas Distribuidos	132
Conclusión	133

Capítulo VI. Implementación de un sistema abierto

Especificación de los requerimientos para la implementación del sistema abierto	135
Requerimientos de hardware	136
La importancia de hardware de calidad	136
Servidores basados en procesadores Intel	137
Selección del procesador	137
Intel 80386 SX	138
intel 80386 DX	138
Intel 80486 SX	139
Intel 80486	139
Pentium	169
Requerimientos de hardware de los sistemas operativos	140
IBM OS/2	140
Microsoft Windows	140
Novell NetWare 386	141
Novell UnixWare 1.1	141
Los requerimientos de software	141
Implementación de un servidor NetWare	143
Implementación de un servidor UnixWare	152
Implementación de una estación de trabajo OS/2	155
Instalación de NetWare para estaciones de trabajo OS/2	158
Implementación de una estación de trabajo Windows	158

Implementación de una estación de trabajo	
MS-DOS/Windows	160
Instalación de NetWare para estaciones de trabajo DOS y Windows	160
Análisis de las comunicaciones establecidas dentro del sistema abierto	162
IPX/SPX	163
SPX	164
TCP/IP	164
Transporte NetBIOS	165
Transporte NetBEUI	165
El entorno STREAMS del sistema abierto	167
Habilitación de múltiples pilas de protocolos dentro del sistema abierto	168
Network Driver Interface Specification (NDIS)	169
Open Data-Link Interface (ODI)	169
Habilitación de la pila de protocolo TCP/IP	170
Conclusión	172
Glosario de Términos y Acrónimos	173
Bibliografía	176

Introducción

El objetivo principal de este trabajo es el de mostrar que el sistema operativo UNIX es el sistema operativo más viable para ser base de la implementación de los sistemas abiertos. Esto se mostrará por medio de un estudio comparativo entre UNIX y los sistemas operativos que actualmente compiten con él.

Las tendencias de la década de 80s dejaron un legado en lo que se refiere a los sistemas de información. En los 80s existían diferentes arquitecturas, y por lo tanto una gran dependencia hacia los proveedores. Esto provocó que las aplicaciones fueran monolíticas, inconsistentes y con problemas de redundancia. Este tipo de aplicaciones (propietarias) provocaron el surgimiento de islas de información.

Lo anterior muestra que dentro de la industria de cómputo no había estándares y aunado a esto existía una mayor demanda de recursos.

Las tendencias de los sistemas de información en los 90s involucran la aceleración en los cambios tecnológicos, lo que ha provocado la incorporación de nuevos tipos de usuarios finales y que los negocios abandonen los desarrollos monolíticos de aplicaciones. En la década actual la mayoría de los negocios están enfocados hacia las tendencias Down-sizing (proceso de migración y cambio desde una plataforma mayor, como mainframes, hacia una plataforma menor, como minis) y Right-sizing (elección de la plataforma más adecuada a las necesidades de una empresa), debido a la proliferación de estándares y por lo tanto de sistemas abiertos. Dentro de la nueva forma de hacer las cosas, se ha incorporado con gran auge en las empresas el modelo Cliente/Servidor, con el fin de atender de manera eficiente a un gran número de usuarios. Todo esto significa que los negocios están dirigiéndose a la implementación de sistemas distribuidos y hacia un abandono de los sistemas centralizados, sin olvidar que este proceso tomará tiempo.

Las empresas que actualmente están trabajando en la implementación de sistemas de información requieren un sistema operativo potente, que soporte los procesos down-sizing y right-sizing. Esto ha provocado que los fabricantes de sistemas operativos iniciarán una gran lucha por obtener el liderazgo en el mercado de los sistemas de escritorio.

Empresas como Microsoft, IBM y Novell, entre otras, han iniciado agresivas campañas de publicidad, anunciando que el sistema operativo que cada una de ellas ha desarrollado es la solución ideal para las empresas que manejan grandes sistemas de cómputo. Y actualmente, existen campañas publicitarias de productos que aún no están en el mercado, pero con el fin de convencer a los usuarios de que éste será su mejor alternativa.

Pero para mantener a una empresa dentro de ventajas estratégicas competitivas, la toma de decisiones tiene que estar basada en un manejo óptimo de la información. Desde el punto de vista de la funcionalidad (y no de la publicidad incrementada), este trabajo considera a todos los conceptos involucrados en la conectividad de sistemas abiertos, con el fin de proveer la información necesaria a los usuarios que requieren optimizar sus sistemas de información.

El contenido de este trabajo está dividido en seis capítulos, cuya estructura permite analizar la tecnología actual de la industria de cómputo y los términos que ésta involucra. Con el fin de no distorsionar el sentido y significado de algunos términos, éstos se conservan en inglés, sin una traducción literal al español.

Capítulo I. Introducción a las Redes de Comunicación de Datos

Este capítulo provee un panorama claro sobre qué es una red de comunicación de datos y se establecen los conceptos y términos básicos involucrados en todas las redes de comunicación.

Capítulo II. Redes de Comunicación de Datos

Este capítulo analiza los diferentes tipos y la funcionalidad de las redes de comunicación de datos, y se describen algunos de los sistemas operativos de red más populares.

Capítulo III. Modelo de Referencia OSI

En este capítulo se analiza el Modelo de Referencia OSI (Open System Interconnection), así como los protocolos estándar relacionados con dicho modelo, el cual norma la implementación del hardware y software para los sistemas abiertos.

Capítulo IV. Conjunto de Protocolos TCP/IP

En este capítulo se analizan los protocolos de comunicación relacionados con la interconexión de los sistemas abiertos.

Capítulo V. UNIX

Se presentan en este capítulo los conceptos básicos y fundamentales que hacen de UNIX el sistema operativo líder para la interconectividad de sistemas pertenecientes a distintas plataformas.

Capítulo VI. Implementación de un Sistema Abierto

En este capítulo se describen los pasos necesarios para implementar un sistema abierto, basado en UNIX, incluyendo la interconexión de hardware y la instalación del software necesario para comunicar a los diferentes sistemas operativos que residen en cada una de las computadoras que forman parte del sistema

Capítulo I. Introducción a las Redes de Comunicación de Datos

Dado el objetivo principal de este trabajo que es el de mostrar que el sistema operativo UNIX es el sistema operativo más viable para ser base de la implementación de sistemas abiertos, este capítulo provee un panorama claro sobre qué es una red de comunicación de datos y se establecen los conceptos y términos básicos que están involucrados en todas las redes de comunicación.

Introducción

Las computadoras actualmente son utilizadas en varias actividades de la vida diaria y en muchos casos éstas desempeñan su tarea en forma individual, pero existen situaciones en las cuales es necesario conectarlas e intercambiar datos con otras computadoras. En el hogar, por ejemplo, para transferir un archivo de datos desde una computadora personal hacia otra o para acceder a la información de una base de datos pública utilizando la red telefónica; en la oficina para intercambiar los mensajes del correo electrónico dentro de un mismo establecimiento o entre dos establecimientos diferentes; en instituciones financieras para realizar transferencias de fondos desde la computadora de una institución a otra, en las agencias de viajes para acceder a los sistemas de reservación de varias aereolíneas, en las universidades y en otros centros de investigación para acceder a los resultados de una supercomputadora, en los procesos industriales para coordinar el control de los equipos de instrumentalización asociados con una planta; en la industria manufacturera para controlar la transferencia de partes y datos desde una unidad automatizada hacia otra.

El requerimiento fundamental en toda aplicación que involucra dos o más computadoras es proveer el tipo de comunicación de datos más adecuada. Sin embargo, en la práctica, se utilizan varios tipos de comunicación de datos, donde cada tipo cubre las necesidades de una aplicación específica. Por ejemplo, si los requerimientos de comunicación son simplemente transferir un archivo de una computadora a otra del mismo tipo, dentro de una misma habitación, resulta más sencillo especificar el tipo de comunicación de datos que

si se tratara de una transferencia de datos entre dos computadoras diferentes, colocadas en habitaciones distintas. Cualquiera de estos tipos de comunicación se lleva a cabo por medio de una red, por lo que analizaremos este concepto más detalladamente.

¿Qué es una red de comunicación de datos?

"Una red es un sistema en el cual ocurre la transferencia de información. Las redes de computadoras incluyen hardware y software especial para conectar las computadoras con otros dispositivos electrónicos a través de un canal de comunicación, así dichos dispositivos pueden comunicarse entre sí. Cuando se tiene una red de computadoras se pueden compartir el software y los recursos, tales como las impresoras, con los usuarios de otras computadoras." [16: unidad 1, sección 1, lección 1]

Las redes permiten a las impresoras y discos, que físicamente no forman parte de la computadora de un usuario, aparentar por medio de las aplicaciones que realmente estos dispositivos forman parte de la computadora de dicho usuario. Esto es posible añadiendo nuevas letras a la unidad manejadora de disco y a los puertos de impresión. De esta forma todas las aplicaciones y las impresoras pueden ser tratadas como si formarían parte del desktop (superficie de trabajo) de cada una de las computadoras de la red.

De acuerdo a lo anterior, el tipo de comunicación de datos que debe ser usado está en función de la naturaleza de la aplicación, del número de computadoras involucradas y de su separación física. De esta situación se han derivado los diferentes tipos de redes de comunicación de datos .

"Cuando más de dos computadoras están involucradas en la aplicación, el tipo de comunicación provee la capacidad de que todas las computadoras puedan comunicarse con otras en intervalos de tiempo distintos. Si todas las computadoras están distribuidas dentro de una misma área, es posible instalar una red de trabajo propia. Tales redes de trabajo son conocidas como Redes de Area Local o LAN (*Local Area Network*). Si las computadoras están localizadas en diferentes establecimientos o lugares pueden utilizarse los servicios de una red pública. La red resultante es conocida como Red de Area Amplia o WAN (*Wide Area Network*). El tipo WAN que es utilizada depende de la naturaleza de la aplicación.

En todas las aplicaciones se asume que todas las computadoras están unidas a la misma LAN o WAN. En algunas aplicaciones, sin embargo, la comunicación de datos involucra múltiples redes. Por ejemplo, una computadora unida a la LAN en un establecimiento requiere comunicarse con otra computadora que está unida a una LAN en un establecimiento diferente, donde tales redes están comunicadas por medio de una red pública. Este tipo de comunicación es conocida como internetwork o *internet*, que requiere características adicionales para poder direccionar los mensajes" [16: unidad 1, sección 1, lección 4].

A continuación se describen los conceptos básicos involucrados en las redes de comunicación de datos

Estación de trabajo (Workstation)

"Una estación de trabajo (*workstation*) es una microcomputadora conectada a la red que mantiene su habilidad de trabajar como una computadora personal independiente, además, es capaz de acceder a la información localizada en el disco del servidor de la red. El usuario puede seleccionar entre dos opciones, usar la microcomputadora como una unidad independiente o ser parte de la red" [16: unidad 1, sección 1, lección 2].

Servidores de disco (Disk Servers)

Las primeras redes utilizaban servidores de disco, un disco duro que contenía la información que podía compartirse entre las diferentes estaciones de trabajo de la red. Para cada una de las estaciones de trabajo este servidor de disco aparentaba ser simplemente otro disco duro.

"El proceso a través del cual una estación de trabajo accesa al servidor de disco para almacenar archivos, es el mismo que si la estación de trabajo almacenara dichos archivos en su propio disco duro. La operación es más compleja si la estación de trabajo desea un archivo en particular, el cual se encuentra almacenado en el servidor de disco. El servidor de disco de la red localiza cada uno de los archivos almacenados en él, por medio de la *FAT (File Allocation Table)*. El servidor de disco envía una copia de su FAT a cada una de las estaciones de trabajo de la red, dicha copia se almacena en la RAM de cada workstation" [2:pág. 27].

Cada vez que es necesario, el sistema operativo de la estación de trabajo usa la FAT de la red para acceder a sus archivos almacenados en el servidor de disco

Servidores de archivos (File Servers)

"Un servidor de archivos contiene software especial que forma el shell (interface con el usuario) del sistema operativo normal, en cada computadora de la red. Este shell filtra los comandos, dados por el usuario, hacia el servidor de archivos antes de que el sistema operativo pueda recibirlos. El servidor de archivos mantiene su propia FAT, la cual le ayuda al servidor a localizar el sector del disco en el cual está almacenado un archivo particular. Cuando una workstation demanda un archivo específico, el servidor de archivos localiza el archivo y lo manda directamente a la workstation. Es importante hacer notar que la workstation no tiene designado el servidor de archivos como una unidad de disco, como es el caso de un servidor de disco" [2:pág. 29]

Servidores de archivos dedicados y no dedicados

"Un servidor de archivos *dedicado* es una microcomputadora (con un disco duro) usada exclusivamente como un servidor de archivos, la cual dedica todos sus recursos de procesamiento y memoria al servicio de archivos. Esta microcomputadora usualmente provee a la red eficiencia y un aumento en la velocidad de procesamiento.

Cuando un servidor de archivos es *no dedicado*, éste es usado como una estación de trabajo en adición a sus funciones de servidor de archivo. Esto significa que la RAM debe ser dividida para que parte de ésta esté disponible para correr programas. Esto, también significa que una estación de trabajo de la red tendrá que esperar el archivo que le va a ser enviado, mientras el usuario del servidor llama a un programa desde la memoria, usando el microprocesador de la máquina" [2:pág. 31] El servidor de archivos puede desempeñar esta tarea, ya que generalmente los servidores de archivos son las computadoras más caras y rápidas en la red.

Servidores de impresión

"Al igual que un servidor de archivos, el servidor de impresión permite compartir el disco duro de la red, un servidor de impresión puede habilitar a docenas de workstations para compartir varios tipos de impresoras. Con el servidor de impresión las impresoras pueden estar limitadas a ciertos usuarios de la red. El software de compartición de

impresora debe contener un *spooler* de impresión, software que crea un buffer donde los trabajos de impresión deben ser almacenados mientras esperan su turno para ser impresos" [2.pág 32]. Esto es similar a una lista de trabajos de impresión, en la cual, después de que cada archivo es impreso y el siguiente archivo en la lista toma su lugar. Sofisticados spoolers de impresión incluyen la capacidad de enviar un trabajo al inicio de la lista si éste requiere imprimirse inmediatamente.

Topologías de red

"La topología de la red es el arreglo físico del cableado estructural y de los dispositivos involucrados en la interconexión de computadoras y equipos servidores" [16: unidad 2, sección 2, lección 2]. La red debe tener un cableado que una a todas las estaciones de trabajo individuales con el servidor de archivos y otros periféricos. Cuando se diseña una red, los factores más importantes para la elección de la topología son los siguientes:

- El patrón de comunicación entre dispositivos
- El volumen de información que habrá de transmitirse
- La necesidad de tolerancia a fallas y trayectorias redundantes
- La frecuencia con que se agregan o eliminan estaciones de la red
- El tamaño de la red
- El valor de la información que se manejará en la red
- La distribución que tendrán los equipos en la oficina

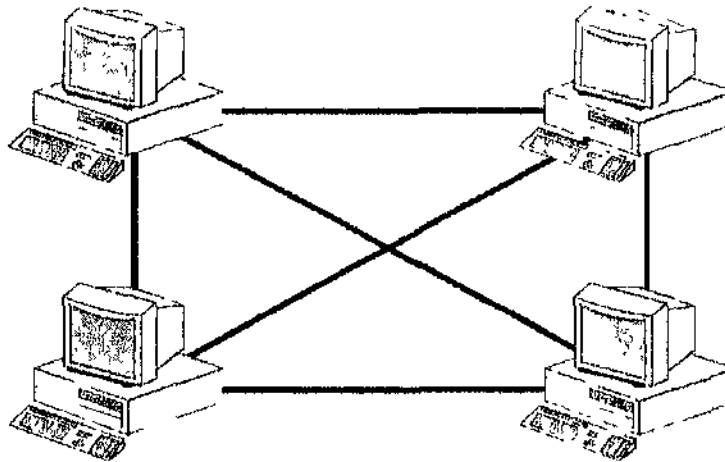
Existen varios tipos de topologías de red; algunas de las más populares son las siguientes: *Mesh*, *Star*, *Bus*, *Ring* e *Hybrid*.

Topología Mesh

"La arquitectura de *Mesh* permite proveer múltiples rutas como destino, lo cual hace que la red sea más tolerante a las fallas y que tenga un tiempo mínimo de espera, ya que el *ancho de banda* está garantizado" [16. unidad 2, sección 2, lección 1] Para la mayoría de las instalaciones de red, sin embargo, las desventajas de una red *Mesh*, pesan más que

las ventajas, por lo cual esta topología es raramente utilizada. Algunas de sus desventajas son: la gran cantidad de cable que utiliza y la interface de red compleja y costosa de cada máquina.

Figura 1-1 Topología Mesh

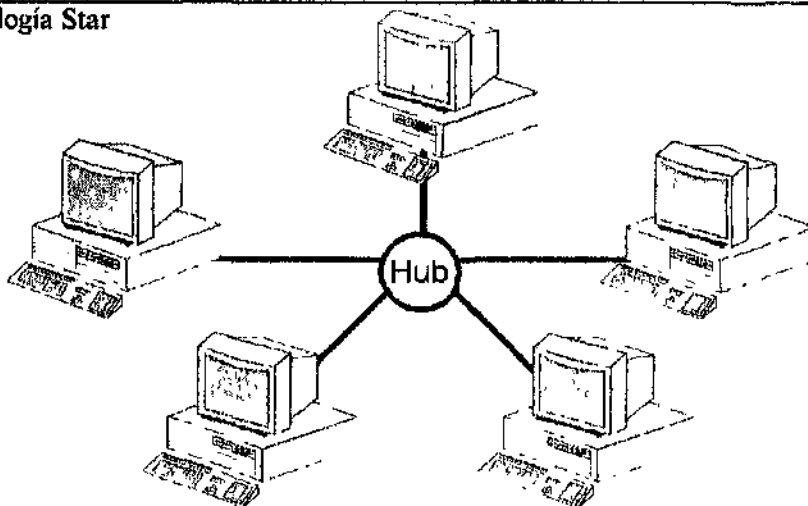


Fuente: Introduction to Networking Technologies, 1994

Topología Star

Toda la información en una red de star parte de un punto central; las estrellas pueden estar relativamente expuestas a los problemas. Pero también las workstation pueden ser añadidas a la red fácilmente. Sin embargo, dependiendo de la localización del hub, las redes de estrella pueden requerir más cableado que otras topologías. Las características del *hub* permiten desactivar grandes partes de la red. El sistema telefónico es un ejemplo de una red con una topología de Estrella.

Figura 1-2 Topología Star

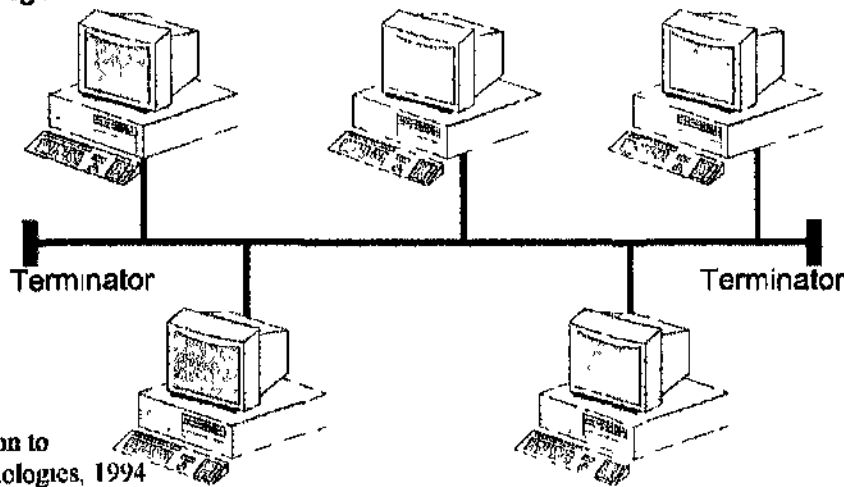


Fuente: Introduction to Networking Technologies, 1994

Topología Bus

"Una topología *Bus* amplía un medio de transmisión lineal, en el cual todos los nodos directamente involucrados son conectados por enlaces relativamente cortos. Si la señal no es absorbida, ésta se reflejará hacia fuera hasta el final del cable, causando un eco, para prevenir la reflexión de señales, el bus está terminado en ambos extremos por un dispositivo que absorbe la señal" [16: unidad 2, sección 2, lección 1].

Figura 1-3 Topología de Bus

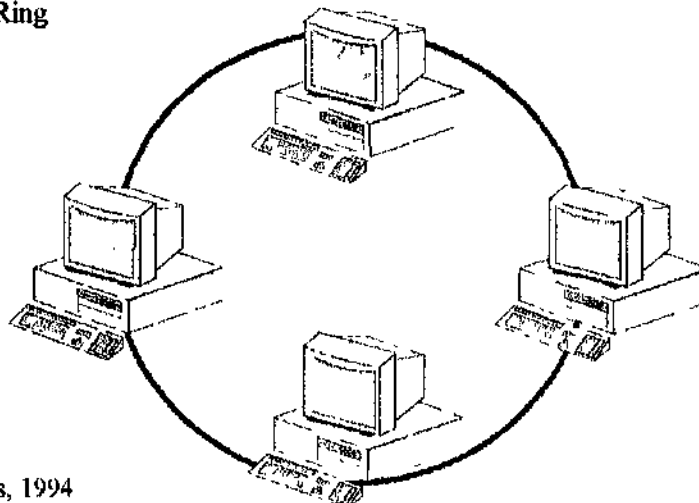


Fuente: Introduction to
Networking Technologies, 1994

Topología Ring

"Un anillo es un ciclo cerrado de enlace punto-a-punto entre dos estaciones de la red. Ya que cada estación regenera la señal, la degradación es mínima" [16: unidad 2, sección 2, lección 1]. La implementación más común de una topología de anillo es la red *Token-Ring* de IBM (esencialmente equivalente al *IEEE 802.5*, discutido más adelante)

Figura 1-4 Topología Ring



Fuente: Introduction to
Networking Technologies, 1994

Métodos de acceso

Los métodos de acceso describen la forma en que los dispositivos de la red accesan al medio físico de transmisión. Existen tres métodos básicos de acceso al canal o medio de transmisión:

- *Contention*
- *Polling*
- *Token -Passing*

Es necesario, en primer lugar, explicar uno de los conceptos más importantes y que está involucrado con los métodos de acceso. el ancho de banda.

Ancho de banda

Bajo condiciones teóricas óptimas, cada red puede ser capaz de transmitir un número dado de bits por segundo (velocidad máxima de transmisión) Por lo que el ancho de banda de una red es la velocidad máxima de señal para un canal de transmisión, usualmente expresada en bits por segundo Esta velocidad está basada en límites físicos, en lugar de prácticos.

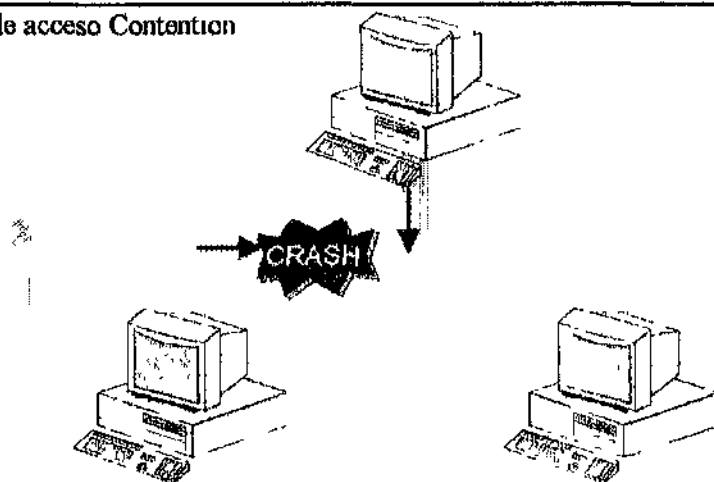
Método de acceso Contention

Con los primeros sistemas *contention*, los dispositivos de la red transmitían hasta que tenían los datos. No había un procedimiento formal para determinar cuándo una estación debía de transmitir Este sistema fue eficiente, siempre y cuando la cabecera (intercambio de información extra) no fuese usada antes de que los datos reales fueran enviados Sin la cabecera, el dispositivo teóricamente gasta todo su tiempo de comunicación sin transmitir datos. Los dispositivos simplemente usan el canal sin compartirlo. Desafortunadamente estos primeros sistemas utilizaban solamente una fracción de la máxima capacidad del canal. También, a menudo dos o más dispositivos transmitían a la vez, resultando ésto en una *colisión*. Debido a que las colisiones típicamente destruyen la información transmitida, la transferencia de información usando este sistema está limitada.

Para solucionar estos problemas, fueron desarrollados nuevos sistemas de *contention* llamados CSMA/CA (*Carrier Sense, Multiple Access/Collision Avoidance*). Las redes CSMA/CA hacen una llamada a cada estación que está esperando para transmitir en un

sentido del canal, para una señal existente. Si la señal existe, la estación espera, si no, la estación transmite mensajes cortos que esencialmente actúan como un detector de colisiones. Si una colisión está ocurriendo, es mejor que ésta ocurra durante un mensaje de control corto que durante un mensaje largo con información del usuario dentro de él. Este sistema es más eficiente, pero está todavía muy lejano de estar habilitado para una detección rápida y recobrase de una colisión. *Local Talk* utiliza CSMA/CA.

Figura 1-5 Método de acceso Contention



Fuente. *Introduction to Networking Technologies*, 1994

Hasta que los nuevos sistemas de contention, llamados *CSMA/CD* (*Carrier Sense, Multiple Access/Collision Detection*) fueron desarrollados, se ha logrado detectar las colisiones rápidamente. La temprana detección de las colisiones ahorra tiempo y hace que el canal sea más eficiente. Los sistemas *CSMA/CD* son actualmente los tipos más populares de canales de contention en el mercado, con *Ethernet* como principal ejemplo.

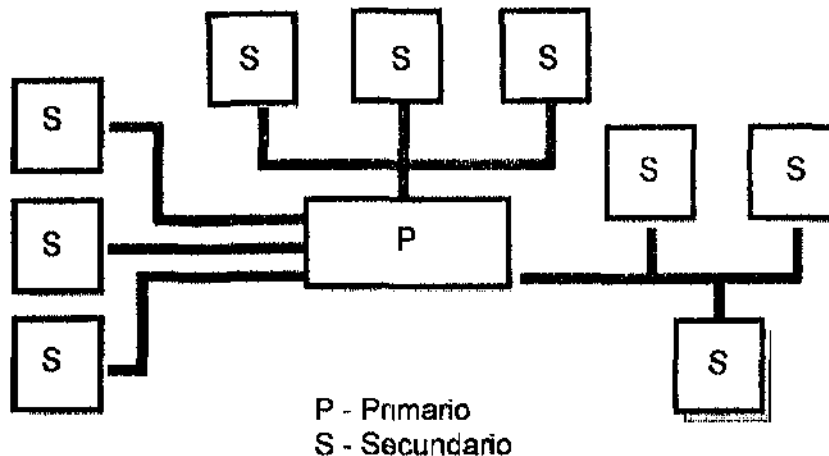
Polling

El método de acceso *polling* designa un dispositivo (llamado dispositivo primario, controlador, o master) como un administrador del canal de acceso. Este dispositivo busca o pregunta a cada uno de los otros dispositivos (referidos aquí como dispositivos secundarios) en un orden predeterminado para ver cuál de ellos tiene información para transmitir. Las reglas de los sistemas limitan el tiempo con el que cuenta cada dispositivo secundario para poder transmitir en cada poll.

El Polling puede incurrir en un acceso substancial al canal. El mecanismo del polling toma tiempo y restringe las oportunidades de acceso de cada dispositivo secundario.

Cuando los dispositivos secundarios rara vez tienen datos para transmitir, el ancho de banda de la red puede ser utilizado para enviar los mensajes del polling y recibir las respuestas de los dispositivos secundarios.

Figura 1-6 Método de acceso Polling



Fuente: Introduction to Networking Technologies, 1994

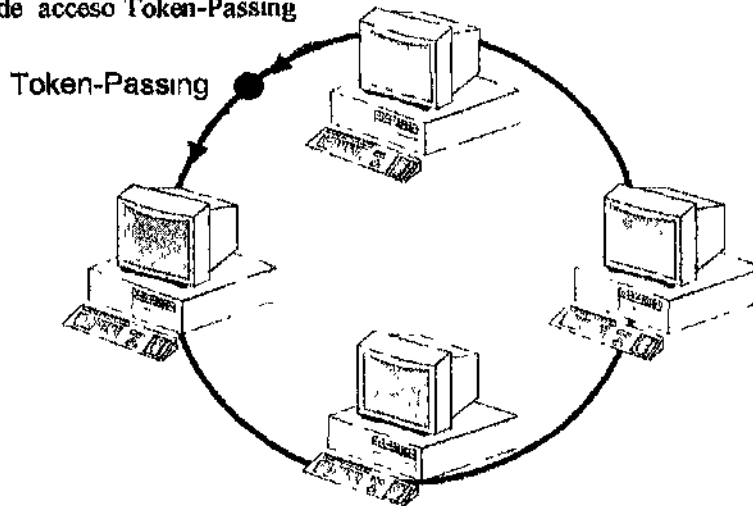
Por otro lado, el polling elimina completamente las colisiones. Cuando los dispositivos secundarios regularmente tienen información para transmitir, este método puede hacer un mejor uso del ancho de banda de la red. Los dispositivos secundarios pueden estar conectados a un dispositivo primario en varias configuraciones distintas. Una de las topologías más comunes es la topología de estrella, en la cual cada uno de los puntos de la estrella es un dispositivo secundario y el *hub* es un dispositivo primario. Los grandes mainframes de IBM y las minicomputadoras a menudo usan el polling para buscar los datos relacionados con las entradas a los dispositivos que van a transmitir información.

Token-Passing

El *token-passing* es similar al polling, pero éste no cuenta con un controlador central. El sistema token-passing designa a los diferentes dispositivos primarios un turno para transmitir por medio de pasar un token desde un dispositivo hacia otro. Un *token* es una entidad especial de autorización que temporalmente da el control del canal al dispositivo que contiene el token. El resto de los dispositivos en la red temporalmente se convierten en secundarios. Cada dispositivo sabe desde cual dispositivo éste recibió el token y hacia cuál dispositivo debe enviar dicho token. El token-passing diseña reglas límite que determinan cuánto tiempo cada dispositivo puede controlar el token.

El método de acceso token-passing es similar al polling, en cuanto a que los dos eliminan las colisiones. Ambos optimizan el uso del ancho de banda de la red cuando los dispositivos frecuentemente tienen información para enviar. Ambos pueden determinar quién puede acceder a la red.

Figura 1-7 Método de acceso Token-Passing



Fuente: Introduction to Networking Technologies, 1994

La mayor ventaja del token-passing, sobre el polling, es el beneficio del control distribuido de token-passing contra el control centralizado del polling. Cuando algunos de los dispositivos, de una red que utiliza el método token-passing, sufren una avería no es necesario desactivar la red, sin embargo el daño del dispositivo primario, en el medio ambiente polling, a menudo deshabilita esta pseudo-red de la red total. Por otro lado, las redes token-passing requieren inteligencia por parte de todos los dispositivos. Los dos estándares token-passing más comunes son IEEE 802.5 (Token Ring) y el IEEE 802.4 (Token Bus), ambos discutidos más adelante.

Concepto de protocolo y estándares de comunicación

Los *protocolos* especifican las reglas para la comunicación. Ellos forman los bloques que construyen o forman a los cables que comunican a las computadoras, dentro de un sistema de comunicación de datos funcional, lo que significa que sin los protocolos las comunicaciones de red serían ineficientes. Los protocolos que han adquirido amplio soporte a través del tiempo han llegado a ser *estándares*. Un protocolo puede llegar a ser un estándar como resultado de sus características superiores o simplemente porque es soportado por varios fabricantes influyentes.

Una *especificación de protocolo* documenta formalmente a un protocolo y describe cómo se deben construir las redes. Este detalla el orden en el cual los dispositivos deben comunicarse, en un medio de transmisión compartido. Los dispositivos checan los problemas en la comunicación, el tamaño de las piezas (*packets*) de información enviadas entre los nodos, la resistencia que ofrece el medio de transmisión, y muchas otras características.

Una *implementación de protocolo* es la implementación de un protocolo, hecha por un fabricante en particular. Los vendedores de redes producen sus propias implementaciones a partir de las especificaciones de protocolo. Por ejemplo el término "TCP/IP" se refiere a un conjunto de protocolos de comunicación (TCP e IP) ofrecidos literalmente por cientos de fabricantes. Cada implementación tiene algunas diferencias con respecto a las demás. Para entender mejor la diferencia entre la especificación de protocolo y la implementación de protocolo, consideremos el ejemplo de la construcción de una casa. Las especificaciones del protocolo son similares a los planos de la casa. Ellos especifican el número de habitaciones, en dónde se localizan en relación a otras habitaciones, el tamaño de cada habitación, etc. Las implementaciones de protocolo son las diferentes casas construidas, a partir del mismo plano, por diversos constructores. Dichas casas probablemente sean similares, pero nunca idénticas, el hecho de que sean parecidas es lo que las hace compatibles.

Recientemente varios organismos internacionales han establecido estándares para ser utilizados en la industria de la computación, los cuales conciernen principalmente a la operación interna de una computadora o a la conexión de dispositivos periféricos locales. El resultado fue que en los primeros subsistemas de comunicación el hardware y el software, ofrecidos por un fabricante, sólo estaban disponibles para las computadoras de dicho fabricante, y fueron llamados sistemas sin compatibilidad (*plug-compatible systems*). Para la compartición de información tales sistemas son conocidos como **sistemas cerrados**. Los fabricantes de otras computadoras no podían compartir información a menos que se unieran a los estándares propietarios de un fabricante en particular.

Es importante hacer notar que los estándares no son hardware, pero tampoco son software; ellos son simplemente un *conjunto de convenciones generalmente aceptadas*.

En contraste varios organismos internacionales convinieron junto con las redes públicas, formular estándares internacionales, para poder conectar dispositivos a estas redes. Las recomendaciones *V-series*, por ejemplo, conciernen a la conexión de equipo, como lo es la conexión de un *DTE (Data Terminal Equipment)* con un modem, y a su vez éste conectado a una red pública; las recomendaciones *X-series* para conectar un DTE a una red de datos pública; y las recomendaciones *I-series* para conectar un DTE con un ISDN. Tales recomendaciones han dado como resultado la compatibilidad entre equipos de diferentes fabricantes, capacitando a los compradores para seleccionar equipo de un amplio rango de fabricantes

Inicialmente, los servicios de una red pública estuvieron relacionados principalmente con la transmisión de datos, por lo tanto los estándares asociados solo se relacionaban con el método para comunicar a un dispositivo con estas redes.

Recientemente, sin embargo, las redes públicas han empezado a proveer servicios de información distribuidos y más amplios, tales como el intercambio de mensajes electrónicos (Telex), y el acceso a bases de datos públicas (Videotext). Para acceder a estos servicios, los organismos asociados con la industria de las telecomunicaciones han formulado estándares no solo para comunicarse con estas redes, sino también estándares llamados de alto nivel que se relacionan con el formato y el control del intercambio de información entre sistemas. Consecuentemente, el equipo de un fabricante, el cual está unido a estos estándares, puede ser usado junto con el equipo de otro fabricante que también cumple con los estándares. El sistema resultante es entonces conocido como un *sistema abierto*, o más completamente, como un *medio ambiente de interconexión de sistemas abiertos (Open System Interconnection Environment - OSIE)*

Dentro de la industria de cómputo actual existen varias definiciones sobre lo que es un sistema abierto, algunos fabricantes han diseñado su propia definición acerca de este concepto. Con el fin de poder adquirir una idea clara de lo que representa un sistema abierto, se han tomado algunas de las definiciones más acertadas, planteadas por algunos fabricantes (como X/OPEN Co , Bell Labs y NCR), las cuales se ilustran en la siguiente figura.

Figura 1-8 Definiciones de Sistema Abierto

X / OPEN Co.

Ambiente de computadoras y comunicaciones basado en interfaces estándares.

Bell Labs.

Sistemas operativos portables y que corren en una variedad de plataformas.

NCR

Conjunto de relaciones estándares que habilitan a diferentes computadoras, subsistemas y a software de aplicación y de sistemas a operar conjuntamente.

Fuente: UNIX Marketing Course

A mediados de los 70s, los diferentes tipos de sistemas distribuidos empezaron a proliferar (basados en redes públicas y privadas), las ventajas potenciales de los sistemas abiertos fueron conocidas por la industria de las computadoras. Como resultado de esto, un amplio rango de estándares empezaron a ser introducidos. El primero se relacionó con la estructura total del subsistema de comunicación en cada computadora. Este fue producido por la **International Standards Organization (ISO)** y es conocido como el **Modelo de Referencia ISO para la Interconexión de Sistemas Abiertos (Open System Interconnection - OSI)**.

El *objetivo* del Modelo de Referencia OSI es *proveer un marco de trabajo para la coordinación del desarrollo de estándares y permitir a los estándares existentes y en desarrollo, trabajar en un marco de trabajo común*. Este objetivo permite a un proceso de aplicación, en una computadora que soporta un conjunto particular de estándares, comunicarse libremente con un proceso de aplicación en otra computadora que soporta el mismo estándar, independientemente de su origen (fabricante). Ahora, que la industria de las redes ha madurado, algunas organizaciones han aceptado legislar los estándares. Estos esfuerzos han contribuido con varios logros. Los estándares legislados o comúnmente aceptados son de vital importancia para los usuarios de la red. Entre más estándares de protocolos existan más aplicaciones estarán disponibles para ser seleccionadas por los

usuarios. Varios de los protocolos, sean estándares o no, ofrecen ciertas ventajas. Debido a que las ventajas ofrecidas por uno o varios protocolos no pueden satisfacer las necesidades de todos los usuarios, se han creado varios protocolos para las todas las capas del modelo de referencia OSI (discutido en uno de los siguientes capítulos). Debido a que las implementaciones de los protocolos estándares han intentado ofrecer una amplia funcionalidad, las implementaciones de protocolo de un fabricante deben ser compatibles con las implementaciones del mismo protocolo de otro fabricante.

Figura 1-9 Los estándares y los sistemas abiertos

Sistemas Abiertos / Estándares



Fuente: UNIX Marketing Course

Algunos ejemplos sobre los procesos de aplicación que pueden comunicarse de forma abierta son:

- Un proceso ejecutándose en una computadora y accediendo a un sistema de archivos remoto.
- Un proceso actuando como servidor central de archivos a una comunidad distribuida de procesos (clientes).
- Un proceso en una estación de trabajo de una oficina accediendo al servicio de correo electrónico.
- Un proceso en una computadora supervisora, controlando a una comunidad distribuida de computadoras base que instrumentan y controlan los procesos asociados con una planta de manufactura automatizada.
- Un proceso en la computadora de un banco que inicializa las operaciones de débito y crédito en un sistema remoto.

De acuerdo a lo anterior, la interconexión de sistemas abiertos está asociada con el intercambio de información entre tales procesos. El objetivo es capacitar al proceso de la aplicación para cooperar con el envío de información particular, la cual está procesándose en las computadoras respectivas.

Medios físicos de transmisión

En todas las redes de computadoras es necesario transmitir datos binarios sobre una línea de transmisión (canal.). Además los dígitos binarios que constituyen cada elemento que va a ser transmitido, deben transformarse en señales eléctricas o electromagnéticas. La transmisión de señales eléctricas requiere el uso de medios de transmisión, los cuales normalmente toman la forma de una línea o cable de transmisión. En algunos casos ésta consiste en un par de conductores o alambres. Una alternativa común es el uso de un rayo de luz guiado por una fibra de vidrio y ondas electromagnéticas propagándose a través del libre espacio.

El tipo de medio de transmisión es importante ya que éste determina el número máximo de bits (dígitos binarios) que pueden ser transmitidos por segundo o bps. En la práctica, sin embargo, al transmitir señales eléctricas éstas son disminuidas y distorsionadas por los medios de transmisión, por lo que el receptor en algunas ocasiones no puede distinguir entre un 1 y un 0 binarios. La disminución y la distorsión de las señales eléctricas pueden ser medidas en base a los diferentes tipos de medios de transmisión y por la separación física entre los dos elementos del equipo de comunicación de datos. La disminución y la distorsión de señales eléctricas está grandemente influida por: El tipo de medio de transmisión, la baja velocidad de los datos que se están transmitiendo y la distancia entre los dos dispositivos de comunicación.

Los dos organismos que definen los estándares para interconectar los equipos de comunicación de datos son la *International Telegraph and Telephone Consultative Committee (ITCC)* en Europa y la *Electrical Industries Association (EIA)* en los Estados Unidos. Los estándares definidos por ambos organismos utilizan escasas diferencias de terminología pero sus señales básicas y parte de su terminología son las mismas. Estos estándares no solo definen los niveles de las señales eléctricas, sino también el uso y significado de algunas señales de control adicionales y reglas convencionales que son usadas en la interface física.

Una red es a menudo creada después de que varias computadoras han sido adquiridas por la empresa. Sin embargo, las decisiones sobre el cableado están basadas en la compatibilidad con el equipo existente. Otra limitación en la selección del cableado, incluye una nueva tendencia llamada *Outsourcing*, que considera el hecho de que más de una opción de cableado soporte a la red, ya que los proveedores actuales, de diferentes compañías, cuentan con su propio sistema de cableado.

Los medios de transmisión son comúnmente clasificados como medios limitados (bounded) e ilimitados (unbounded). Los medios limitados transmiten la señal dentro de un conductor físico, mientras que los ilimitados no. Los tipos más comunes de medios limitados son el alambre *Par -trenzado (Twisted Pair Wire)*, el cable *Coaxial (Coaxial Cable)*, y el cable de *Fibra Optica (Fiber-Optic Cable)*. Un medio de transmisión ilimitado es el aire, a través del cual las micro-ondas y las señales transmitidas viajan.

En un área pequeña, como lo es una habitación o un edificio, un medio de transmisión limitado usualmente conecta a las computadoras. Los medio limitados de propósito especial o una combinación de los medios limitados e ilimitados comúnmente son utilizados para comunicar sitios distantes. Los medios ilimitados son especiales para las redes de área amplia (Wide Area Networks - WAN) con estaciones móviles.

Toda red debe tener un cableado que una las diferentes estaciones de trabajo con el servidor de archivos y con otros periféricos. Existen diferentes tipos de cableado y cada tipo tiene asociado un costo y una capacidad de transmisión.

En esta sección se analizan las características, las ventajas y desventajas de los diferentes tipos de medios físicos de transmisión.

Líneas abiertas de dos alambres (Two-wire open lines)

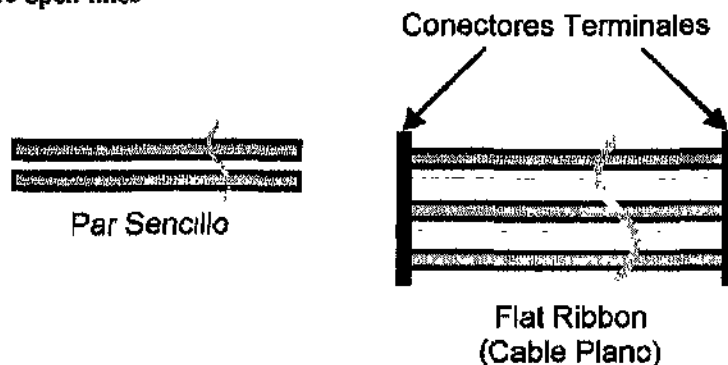
"El *Two-wire open lines* es el medio de transmisión más simple. Cada cable está separado del otro y ambos están abiertos al libre espacio" [1 pág. 26]. Este tipo de línea es adecuado para conectar equipo que está alejado no más de 50 mts. y que tiene una velocidad moderada de transmisión (menos de 19.2 kbps). La señal, la cual es típicamente un voltaje o un nivel actual relativo a alguna referencia de tierra, es aplicada a un alambre.

Con este tipo de línea, es necesario tener cuidado para evitar el cruce de señales eléctricas entre los alambres adyacentes dentro del mismo cable. Este cruce de señales (*crosstalk*) es causado por la capacidad de empalme entre los dos alambres. En adición, la estructura abierta de los alambres hace que este medio sea susceptible a las señales de ruido que provienen de otras fuentes de señales eléctricas, y que además son causadas por la radiación electromagnética.

El principal problema con la interferencia de señales es que éstas pueden ser captadas sólo por uno de los alambres, creando una diferencia de señal adicional entre los dos alambres. A partir de que el receptor opera normalmente utilizando la diferencia de señal entre los dos cables, éste puede tener una interpretación errónea de las señales combinadas (señal más ruido) recibidas. Todos estos factores contribuyen a limitar las distancias de la línea y las velocidades de transmisión y recepción de datos que pueden ser utilizadas.

Por medio de una línea abierta de dos alambres pueden ser conectadas dos computadoras (DTEs) directamente, este medio de transmisión es usado principalmente para conectar un DTE a un equipo terminal de circuito local (DCE), por ejemplo un modem. Como se verá más adelante, tales conexiones usualmente utilizan líneas múltiples, el arreglo más común es un cable separado y aislado para cada señal y un cable de señal para la referencia común de tierra. El conjunto completo de cables es entonces encerrado en un protector simple de cable multinúcleo (*multicore cable*) o moldeado dentro de un cable de hule plano tal como se muestra en la figura 1-9.

Figura 1-9 Two wire open lines



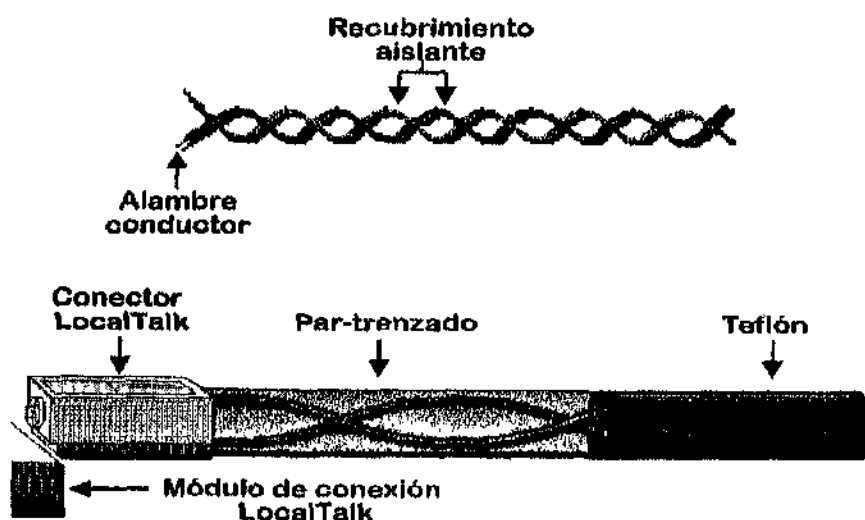
Fuente: Data Communications, Computer Networks and Open Systems

Cable Par-Trenzado (Twisted-Pair Cable)

El cable par-trenzado es el medio de transmisión de red más barato. Este cable consiste en dos alambres aislados y trenzados, así cada alambre recibe la misma cantidad de interferencia del medio ambiente. "El hecho de trenzar los cables incrementa la conductividad y disminuye la cantidad de interferencia electromagnética (*Electro Magnetic Interference - EMI*) en la información transmitida" [1: pág 26]. Este ruido en el medio ambiente viene a ser parte de la señal que está siendo transmitida. El trenzar los alambres reduce (pero no elimina) este ruido. La mayoría de los cables par-trenzado, incluyendo al cable telefónico estándar, están descubiertos, pero algunos pares están envueltos y empaquetados dentro de un foil protegido por una cubierta aislada. Esta cubierta reduce el efecto de la EMI, este tipo de cable es encontrado en un IBM Token-Ring y en un cable Local-Talk, de los cuales se hablará más adelante.

"El cable par-trenzado está envuelto en grupos de pares de alambres, los cuales pueden estar separados por diferentes tipos de materiales, pero la mayoría de los cables de par-trenzado están aislados por *Poly Vinil Chloride (PVC)*" [16. unidad 2, sección 1, lección 1]. Sin embargo este material emite gases tóxicos a altas temperaturas, por lo que los cables de par-trenzado instalados cerca de conductores de aire, deben ser aislados con otra sustancia como el Teflón.

Figura 1-10 Cable Twisted-Pair



Fuente Introduction to Networking Technologies, 1994

El número de pares trenzados en cada grupo puede estar en un rango de 2 hasta 3000 pares; muchas de las redes utilizan 25 pares. Algunas redes utilizan el cable par-trenzado más barato y desprotegido, el cual es utilizado para los teléfonos. Todos los cables tienen un tamaño o medida (*American Wire Gauge Number - AWG*) que está basada en su diámetro, un alambre de medida 26, por ejemplo, tiene un diámetro de 0.01594 pulgadas. Para los propósitos de una red, los tamaños de 22 y 24 son los dos tipos más comunes de cableado de par-trenzado.

Ventajas y desventajas del cable Par-trenzado

El cable par-trenzado tiene diferentes propiedades eléctricas causadas por las diferencias en los tamaños de los alambres, el aislante y el número de pares trenzados. Comparado de forma general con otros medios limitados, el par-trenzado es el más común, tiene un ancho de banda menor y es el más barato. Además, es susceptible a la EMI y más delgado. Recientes adelantos tecnológicos han permitido que el par-trenzado soporte altas velocidades de transmisión, ya que se están revitalizando al par-trenzado como medio de transmisión.

Las mayores limitaciones del cableado de par-trenzado son su utilización sólo en distancias limitadas y su sensibilidad a la interferencia eléctrica. Cuando por primera vez se establecieron los estándares para las redes de par-trenzado, el medio fue habilitado para manejar velocidades de aproximadamente un millón de bits por segundo (1 Mbs) sobre varios miles de pies. Hoy la nueva industria de los estándares conocida como *10baseT*, la cual será descrita a detalle más adelante, refleja los avances tecnológicos que hacen posible transmitir información a 10 Mbs en un alambre de par-trenzado.

Cable Coaxial

El cable coaxial es casi tan fácil de instalar como el par-trenzado; éste es el medio de transmisión que utiliza la mayoría de las redes locales. El coaxial está compuesto de un cobre conductor rodeado por un aislante y una cubierta exterior de cobre o de aluminio que también actúa como un conductor y provee protección. Este tipo de cable es comúnmente encontrado en el hogar como parte integral del cable de televisión.

El principal factor limitante de una línea de par-trenzado es causado por un fenómeno conocido como el *efecto skin*, debido a este fenómeno el flujo actual en el alambre del cable

coaxial tiende a fluir en el recubrimiento exterior, lo que incrementa la resistencia eléctrica en los alambres para aumentar la frecuencia de las señales y disminuir la distorsión de las mismas. A pesar de las altas frecuencias, mucho del poder de la señal es perdido como resultado del *efecto de radiación*. El cable coaxial minimiza ambos efectos ya que el centro del conductor está separado o aislado efectivamente de señales de interferencia externas, por lo que ocurren mínimas pérdidas de la señal como resultado de la radiación electromagnética y del efecto skin.

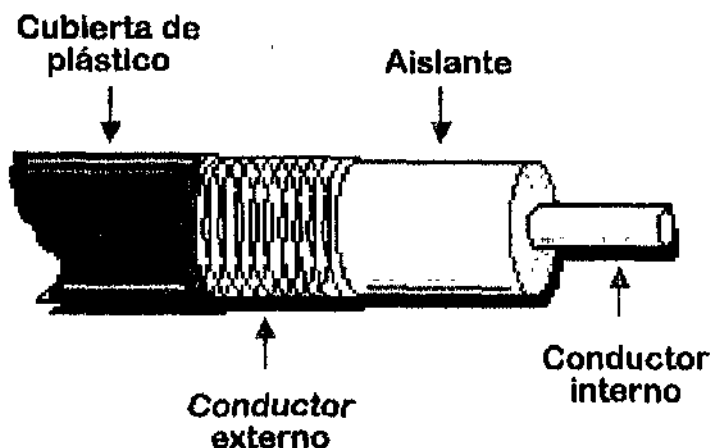
La figura 1-11 muestra como la señal y la referencia a tierra de los alambres toman la forma de un conductor de centro sólido corriendo concéntricamente (coaxialmente) dentro de un conductor exterior también sólido. Idealmente el espacio entre los dos conductores debería ser llenado con aire, pero en la práctica este espacio es llenado normalmente con un material aislante eléctrico de una estructura sólida o con perforaciones.

El cable coaxial puede ser usado con diferentes tipos de señales, pero típicamente es viable para comunicaciones entre varios cientos de metros, el cable coaxial es aplicable a topologías punto a punto y multipunto.

Estructura del cable Coaxial

El cable coaxial, comúnmente llamado coax, está formado por dos conductores. El nombre "coax" se deriva del hecho de que estos dos conductores comparten el mismo eje al centro del cable, que es un alambre relativamente rígido, dentro de una cubierta de plástico aislante.

Figura 1-11 Cable Coaxial



Fuente: Introduction to Networking Technologies, 1994

La cubierta está rodeada por un segundo conductor, un tubo de malla de alambre (algunos incluyen una lámina delgada de metal como recubrimiento) el cual también sirve como un protector. Un tubo de plástico grueso aislante forma la cubierta externa del cable.

Ventajas y desventajas de cable coaxial

El cable coaxial viene en una gran variedad de tipos y gruesos. El cable coaxial grueso transmite señales a distancias mayores que el cable coaxial delgado, pero el cable coaxial grueso es mas caro y menos flexible. Comparado con el cable Par-trenzado, el cable Coaxial:

- Transmite los datos a velocidades mayores
- Es menos susceptible a la EMI y a la interferencia
- Es más caro y el proceso de instalación es más complejo
- Ethernet (tratado posteriormente) usa cable coaxial

Cable de Fibra Optica (Fiber-Optic Cable)

En años recientes, uno de los avances más excitantes dentro de los medios de transmisión ha sido el uso de la fibra óptica en las redes de comunicación, ya que ésta tiene varias ventajas sobre otros medios de transmisión. El cableado de fibra óptica trabaja con velocidades de transmisión de datos superiores a las del par-trenzado y del cable coaxial y es inmune a las interferencias electromagnéticas o de radio-frecuencia. El cable de fibra óptica es capaz de enviar varios miles de señales sin perderlas y es virtualmente inmune a recepciones de datos no autorizadas.

El cable de fibra óptica transmite la información en forma de un rayo de luz a través de una fibra de vidrio, más rápidamente de lo que una señal eléctrica se transmite en un cable. Las ondas de luz tienen un ancho de banda más amplio que las ondas eléctricas, lo que habilita al cable de fibra óptica a aumentar la velocidad de transmisión a cientos de *megabits* por segundo. Además las ondas de luz son inmunes a la interferencia y el cruce de señales. Consecuentemente, el cable de fibra óptica puede transmitir señales a alta velocidad en ambientes con mucho ruido.

Una red de fibra óptica utiliza un Láser o LED (*Light-Emitting Diode*) para enviar una señal a través de una porción del núcleo del cable. Repetidores ópticos son a menudo

utilizados a lo largo de la ruta para amplificar la señal, así ésta llega a su destino con su intensidad completa. En la parte final del cable, el mensaje es recibido y traducido nuevamente a una señal digital o analógica por un *photodiode*. El cableado puede consistir en una sola fibra (monomodo), varias fibras (multimodo), o una variación del multimodo (*Graded-index*) en el cual el índice de la refracción cae lentamente desde el centro de la fibra hacia la superficie exterior.

La fibra monomodo tiene un amplio ancho de banda, pero un núcleo pequeño el cual hace extremadamente difícil empalmarlo sin equipos especiales y pericia técnica. También, el monomodo requiere un láser como fuente de señales, el cual es más caro. La fibra multimodo tiene un pequeño ancho de banda pero es mucho más fácil de empalmar. La fibra multimodo con índice graduado (*Graded-index*) es el medio más caro, pero éste provee la velocidad más alta de transmisión a través grandes distancias.

La fibra óptica multimodo para cableado de red viene en grupos de 2 hasta 24 fibras. Cada fibra es unidireccional, así cada rayo de luz es transmitido en una sola dirección. Las comunicaciones en dos direcciones requieren de otra fibra en el cable, así la luz puede viajar en direcciones opuestas.

El *American National Standards Institute* ha establecido un estándar para la capacidad dependiente del medio (*FMD*) de la Interface Distribuida de Datos de la Fibra (*Fiber Data Distributed Interface - FDDI*) para trabajar en conjunción con la transmisión de datos a 100 Mbs. Esto hace posible alcanzar velocidades arriba de 1 Gps. En el presente, el cableado de fibra óptica es caro y su sofisticada tecnología hace difícil el añadir una nueva estación de trabajo después de la instalación inicial. Si una compañía tiene serios problemas de interferencia o necesita absoluta seguridad en la red sobre el envío de varios miles de señales, la fibra óptica es la mejor y única solución.

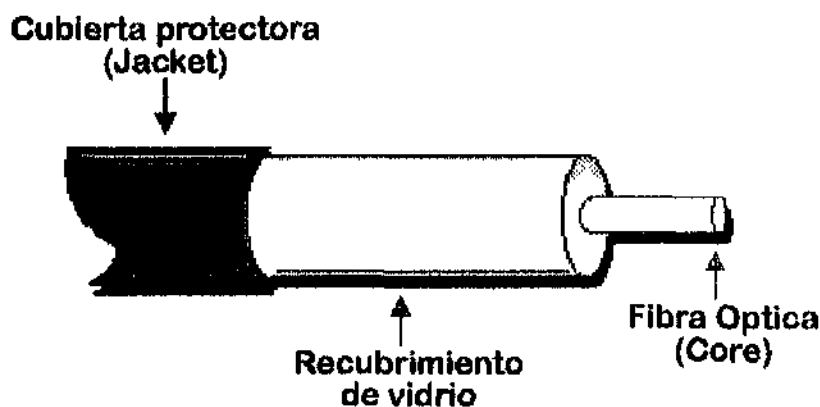
Estructura del Cable de Fibra Optica

"El cable de fibra óptica está hecho de vidrio puro, cuyo núcleo está formado por numerosas fibras delgadas. Estas fibras están rodeadas por una vestidura (*cladding*), que es una capa de vidrio con un índice de refracción más bajo que el del núcleo. La fibra en sí misma está formada por dos partes: el núcleo y la cubierta de vidrio con un índice bajo de refracción.

Las fibras de vidrio conductor de luz o fibras plásticas son individuales para cada señal a ser transmitida, contenida en un recubrimiento protector duro, el cual aísla a la fibra de fuertes señales de luz externas. Una o varias fibras pueden estar envueltas en el centro del cable, el cual puede ser enteramente no metálico. La señal de luz es generada por un transmisor óptico, el cual realiza la conversión de una señal eléctrica normal como es usada en un DTE. De forma similar, un receptor óptico es usado para realizar la función inversa al final del cable. Típicamente, el transmisor utiliza un Diodo Emisor de Luz (Light-Emitting Diode - LED) o un Diodo de Inyección Láser (*Injection Láser Diode - ILD*) para desempeñar la operación de emisión de pulsos de luz y conversión de los mismos, mientras el receptor usa un protodiodo o prototransistor (fotodetectores) sensible a la luz, al final de la fibra.

En una fibra multimodo con un índice uniforme, el material de la cubierta y del núcleo tienen un índice distinto pero uniforme de refracción. Toda la luz emitida por el diodo es

Figura 1-12 Cable de Fibra Optica



Fuente: Introduction to Networking Technologies, 1994

deflectada, en un ángulo menor al ángulo crítico de deflexión, hacia la cubierta de interface y propagada a lo largo del núcleo por rayos de múltiples reflexiones internas. Dependiendo del ángulo al cual la luz es emitida por el diodo, la luz tomará una cantidad variable de tiempo para propagarse a lo largo del cable. La señal recibida tiene un pulso más amplio que el de la señal emitida, así como un decremento en la velocidad.

Ventajas mayores pueden ser obtenidas por medio de reducir el diámetro de las

ondas individuales (3-10 μ) así toda la luz emitida es propagada a lo largo de la ruta única. Consecuentemente las señales recibidas son de una amplitud comparable a la señal emitida. Esta fibra *singlemode*, la cual es normalmente usada con IDLs, pueden operar a cientos de megabits por segundo" [1: pág. 27].

Ventajas y desventajas de la Fibra Optica

El cable de fibra óptica es mucho más pequeño y ligero que el par-trenzado y el coaxial. Las extensas y múltiples conexiones de fibra óptica pueden transmitir más información que los alambres de cable de medidas similares, ya que la fibra óptica soporta velocidades más altas que los cables par-trenzado y coaxial.

Las señales de luz no pierden su intensidad a través de la distancia, como lo hacen las señales eléctricas. La transmisión de fibra óptica sin embargo, requiere pocos dispositivos intermediarios de regeneración de señal. La fibra óptica no es susceptible a la EMI y es muy difícil interceptar o desviar las señales, este principio contribuye a compensar su relativo costo alto, lo que ha logrado que la fibra óptica sea más popular.

La fibra óptica a recibido recientemente una gran aceptación y su uso se ha incrementado dramáticamente, su costo ha disminuido y su velocidad se ha convertido en una necesidad crítica.

Capítulo II. Redes de Comunicación de Datos

Dado el objetivo principal de este trabajo que es el de mostrar que el sistema operativo UNIX es el sistema operativo más viable para ser base de la implementación de sistemas abiertos, este capítulo analiza los diferentes tipos y la funcionalidad de las redes de comunicación de datos, y se describen algunos de los sistemas operativos de red más populares.

Tipos de redes de comunicación de datos

Las redes se dividen en tres tipos basados en el área geográfica que abarcan: *LAN (Local Area Network - Red de Area Local)*, *MAN (Metropolitan Area Network - Red de Area Metropolitana)* y *WAN (Wide Area Network- Red de Area Amplia)*

LANs

Como se explico anteriormente una red de área local es un sistema el cual permite a las microcomputadoras compartir información y recursos en un área limitada (local), generalmente a una distancia menor a una milla entre el servidor y una workstation. Una LAN requiere que las estaciones de trabajo individuales estén conectadas entre sí por medio de un cable (usualmente coaxial o par-trenzado), y que parte del software de la red esté residente en el disco duro de las estaciones de trabajo, lo que permite compartir periféricos, datos y programas de aplicación.

Anteriormente, el compartir equipo periférico (tales como las impresoras, los discos duros y los plotters) fue la tarea principal de las LAN, pero debido a que el hardware representa actualmente inversiones significativas dentro de la mayoría de las oficinas, este costo no puede justificarse solo con el poder compartir el equipo periférico, por lo que los fabricantes de equipo y software de red están desarrollando redes que permitan disminuir los costos de adquisición de equipo, introduciendo al mercado estaciones de trabajo sin disco duro y sin unidades de disco flexible, sino con un chip ROM especial de "autoboot",

colocado en cada una de las estaciones de trabajo de la red, que permite a la computadora formar parte de la red cuando ésta es encendida.

Sin embargo, a pesar de las ventajas que este chip representa es difícil generalizar acerca de las microcomputadoras de una red, ya que dentro de esta industria aún existe la incompatibilidad a pesar de los esfuerzos del IEEE para estandarizar la forma en que debe ser transmitida la información en una red.

MANs

Si una red cubre una ciudad entera, se le llama normalmente Red de Área Metropolitana (*MAN*). Las *MAN* son el tipo más nuevo de red, sin embargo, tienen mucho en común con las LAN aunque en muchas ocasiones son más sofisticadas. Por ejemplo, además de manejar comunicaciones de voz y datos, las *MAN* pueden transmitir video y otra información de audio. Las *MAN* están diseñadas para manejar distancias más grandes que las LAN.

Las *MAN* pueden ser usadas para unir varias LAN en un sistema integrado de red de alta velocidad. Las *MAN* combinan los mejores aspectos de las LAN, tales como bajos porcentajes de error y grandes cantidades de datos, con una cobertura geográfica mayor.

WANs

Cuando una red está esparcida sobre áreas amplias, tal que atravesase estados o países, es llamada Red de Área Amplia (*WAN*). Las comunicaciones a través de una WAN pueden tomar lugar vía línea telefónica, satélite, o sistemas terrestres de micro-ondas.

Las WAN son creadas a veces para conectar MANs y LANs. De hecho, el conectar LANs y MANs para formar WANs es una tendencia actual de las redes. Desde que las WANs envuelven la interconexión de muchas LANs y MANs, ellas a menudo representan una conglomeración de diferentes tecnologías.

Comparada con las LANs y las MANs, la mayoría de las WANs existentes son lentas y con muchos errores, por lo que nuevos desarrollos tecnológicos están dirigiéndose a corregir esos problemas.

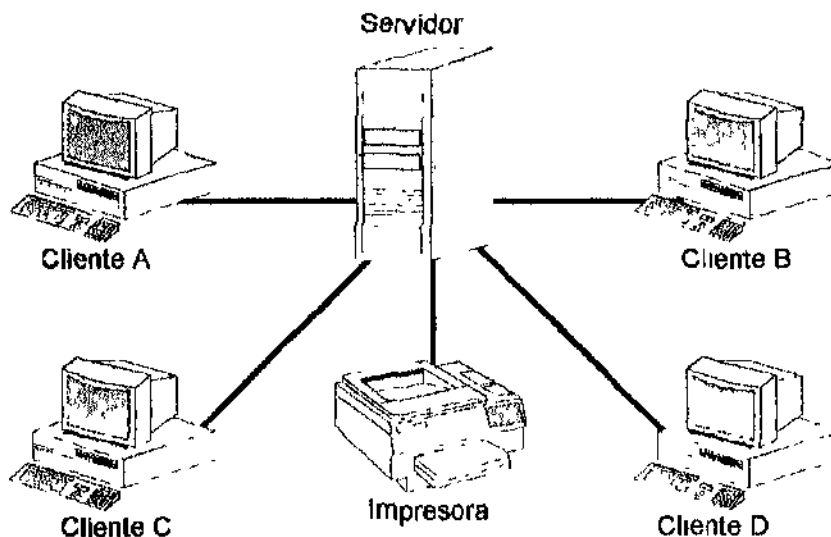
Redes Cliente-Servidor

Existen dos formas distintas de crear una red, una de estas formas es una red cliente-servidor, en la cual el servidor es la parte central de la red dedicada a administrar y compartir los recursos de la red. Otras computadoras, conocidas como clientes acceden al servidor central por aplicaciones, datos y espacio de disco duro. El servidor maneja la compartición de aplicaciones y archivos de datos entre los clientes que usan estos recursos.

Los servidores también manejan las impresiones por medio de almacenar los trabajos de impresión hasta que las impresoras están disponibles y después redireccionan estos trabajos de impresión hacia sus respectivos destinos de impresión. Por ejemplo, cuando una computadora (cliente) requiere al servidor la aplicación de un procesador de palabras y el archivo de un documento, el servidor envía la aplicación y el archivo a través de la red. La aplicación y el documento son almacenados en la memoria propia del cliente y el servidor simplemente provee los archivos o imprime los documentos como sea necesario.

Muchas aplicaciones por defecto imprimen en LPT1, pero por conveniencia el software de la red permite redireccionar la salida que empieza a ser enviada hacia LPT1, ya que esta salida es enviada a la impresora de la red y no al puerto de la computadora o cliente.

Figura 2-1 Red Cliente-Servidor



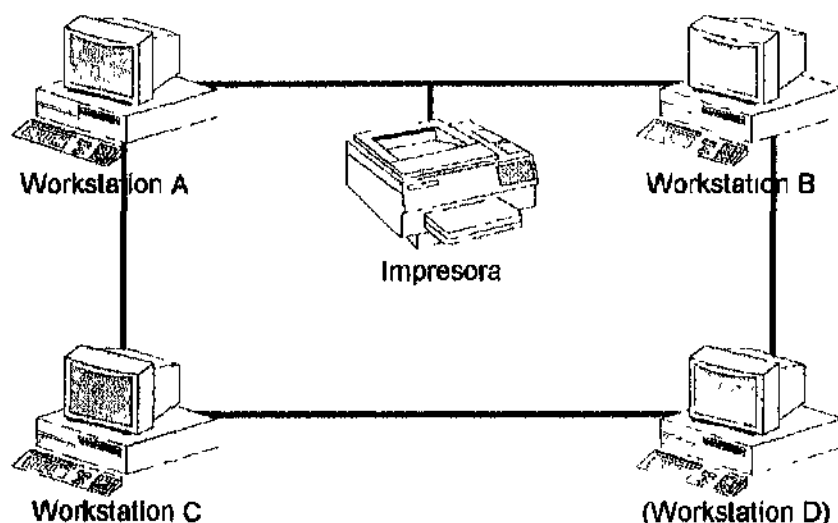
Fuente: Novell DOS 7 User Guide, 1993

Red punto-a-punto

En una red punto-a-punto, algunas computadoras con discos duros actúan como servidores potenciales. Son servidores las computadoras que en la red ofrecen aplicaciones, archivos e impresoras, y espacio libre en el disco duro para otras computadoras. La computadora que hace un requerimiento de los recursos de la red es llamada *cliente*. En una red punto-a-punto los recursos no están localizados en una sola computadora central, pero los recursos son compartidos por la computadora en donde dichos recursos están residentes.

La ventaja del método punto-a-punto es que se pueden compartir impresoras, aplicaciones, CD-ROMs, archivos de datos y otros recursos sin la necesidad de que éstos estén centralizados en un solo lugar. Además, no se debe de asignar una de las computadoras para que actúe únicamente como servidor, ya que cualquiera de las computadoras puede ser un servidor cuando sea necesario.

Figura 2-2 Red Punto-a-Punto



Fuente: Novell DOS 7 User Guide, 1993

Aplicaciones de las redes de comunicación.

Existen dos tipos de aplicaciones de red:

- *Aplicaciones Puras y*
- *Aplicaciones Standalone.*

Aplicaciones Puras de Red

Las aplicaciones puras de red fueron creadas para utilizarse en redes. Cada una tiene una distinta y separada interface del usuario y requiere la ejecución de una serie de comandos de red que son únicos para cada aplicación. Entre las aplicaciones puras de red están las siguientes:

- *Emulación de Terminal*
- *Transferencia de Archivos*
- *Correo Electrónico*
- *Aplicaciones de Grupos*

Emulación de Terminal

La emulación de terminal fue una de las primeras aplicaciones de las redes. Anterior a las redes la gente usaba terminales para acceder a programas de aplicación en mainframes y minicomputadoras. Cuando las terminales fueron reemplazadas por microcomputadoras, se necesitó un método para acceder a las viejas aplicaciones de los mainframes y las minicomputadoras.

La emulación de terminal realiza la función que hace que la microcomputadora aparezca como si fuera una terminal conectada directamente al mainframe. Las funciones de la Unidad Central de Procesamiento (CPU) de la microcomputadora son transparentes al usuario así que el usuario parece estar operando desde el CPU de la computadora host (anfitrión) a la cual la microcomputadora está conectada.

La emulación de terminal brinda lo mejor de ambos mundos al usuario de microcomputadoras. Las aplicaciones de los mainframes y minicomputadoras pueden seguir siendo ejecutadas, pero además el usuario puede correr aplicaciones standalone (tales como procesadores de palabra y hojas de cálculo) en la microcomputadora.

Transferencia de Archivos

La transferencia de archivos es una aplicación esencial en las redes actuales. Las aplicaciones de transferencia de archivos mueven archivos de una computadora a otra, por ejemplo desde una PC hacia un mainframe. En algunos casos, los archivos que son transferidos entre diferentes tipos de computadoras requieren una traducción del formato de los datos de una computadora al formato de la otra.

Correo Electrónico

Las aplicaciones de correo electrónico permiten a un usuario teclear un mensaje en una PC o una estación local y enviar el mensaje a alguien más en la red. El correo electrónico es tal vez la aplicación de red más común. Esto representa una forma en que las redes pueden mejorar la comunicación inter-departamental.

Aplicaciones de Grupos

Las aplicaciones de grupos usan las redes para automatizar electrónicamente las funciones administrativas de la oficina moderna. La mayoría de las oficinas se caracterizan por tener administradores tratando frenéticamente de coordinar las actividades y tareas. Las aplicaciones de grupo permiten a los usuarios coordinar calendarios, juntas, llamadas telefónicas, y otras actividades electrónicamente. Las aplicaciones de grupos utilizan otras aplicaciones de red puras o standalone para proveer servicios administrativos de oficina. Por ejemplo una aplicación de grupos puede incorporar una aplicación de correo electrónico como un medio para enviar mensajes de ida y vuelta entre los empleados de la oficina. Puede también usar un programa de calendario para coordinar las agendas de los empleados. Lo que intentan las aplicaciones de grupos es integrar esas funciones aparentemente.

Aplicaciones de Red Standalone

Todas las aplicaciones mencionadas son consideradas aplicaciones puras de red, desarrolladas específicamente para correr en un ambiente de red. "Recientemente, muchas de las aplicaciones de computadoras standalone originales (y algunas más nuevas) han sido adaptadas para correr en ambientes de red cliente-servidor. Entre éstas se incluyen software de procesamiento de palabras, de hoja de cálculo, de base de datos, de presentaciones gráficas, y de manejo de proyectos" [16: unidad 1, sección 1, lección 3].

Cuando una aplicación de red standalone es adaptada para correr en una red, es dividida en dos partes. La primera parte incluye la interface del usuario y los procesos relacionados que típicamente corren en el *cliente* y la segunda parte de la aplicación corre en el *servidor* (incluyendo operaciones intensivas de CPU tales como consultas a bases de datos, transferencia de correo electrónico, u otras aplicaciones dependientes del procesamiento).

Las aplicaciones de red standalone aseguran que la interface del usuario de la aplicación permanezca razonablemente consistente, sin importar si la aplicación está en dos piezas o en una.

Muchas aplicaciones de computadora standalone están siendo adaptadas para correr en red, algunas de las razones son las siguientes:

- *Facilidad de uso*
- *Compartir archivos*
- *Limitaciones de recursos*
- *Economía en el crecimiento*

Facilidad de uso

Los mismos comandos usados para operar la versión standalone de la aplicación son usados para operar la versión de red. A diferencia de las aplicaciones puras de red, los usuarios no necesitan aprender nuevos comandos para realizar su trabajo usual.

Compartir archivos

Archivos importantes tales como grandes bases de datos pueden ser accedidos por muchos usuarios y se almacenan en un lugar común. Debido que existe sólo una copia de los archivos, no hay peligro de duplicarlos en diferentes niveles de revisión.

Limitaciones de recursos

Algunas microcomputadoras con recursos limitados (CPU lento y poca memoria) no pueden correr las grandes aplicaciones de hoy en día en su totalidad. Si la aplicación es dividida en dos partes, de alguna manera, la microcomputadora puede manejar alguna de las partes lo cual es conocido como una *relación cliente-servidor*. La microcomputadora (el cliente) generalmente corre la porción de la aplicación que corresponde a la interface del usuario y una computadora más poderosa (el servidor) ejecuta las porciones de la aplicación que corresponden al procesamiento intensivo y las entradas/salidas (I/O).

Economía en el crecimiento

El software de aplicación nuevo del servidor no es necesario para cada nuevo usuario. Si la aplicación ya existe en el servidor, sólo se genera una nueva copia de la

interface del programa para el cliente que la requiera. Esto es usualmente menos caro que adquirir el programa entero para cada usuario.

Sistemas Operativos de Red

En el mercado actual mundial existen una gran cantidad de sistemas operativos de red de diferentes fabricantes, de entre los cuales destacan los siguientes:

- *Microsoft LAN Manager*
- *IBM PC Network Program*
- *Novell NetWare*
- *AppleTalk*
- *AT&T StarLAN*
- *Banyan Vines*
- *Artisoft Lantastic*
- *CTOS/BTOS*

De los sistemas operativos de red anteriormente mencionados, quien domina el mercado de los mismos es el Novell NetWare, el cual posee alrededor del 66% del total de redes instaladas.

El Microsoft LAN Manager

Los dos componentes claves del LAN Manager son el *Redirector* y el *Servidor*. Cada estación de la red corre el software Redirector, así pueden interceptar y redireccionar a la red las llamadas de entrada y salida del sistema operativo. Este software Redirector también es responsable de la configuración de las estaciones de trabajo individuales para usar los recursos de la red.

La porción del Server del LAN Manager reside en un servidor de archivos, donde éste es responsable de la administración de los archivos, de la agenda, de la seguridad, y de los servicios de impresión. Este software también sirve como monitor de red, alertando al supervisor de la red de cualquier alarma de la red.

LAN Manager viene con una versión de OS/2 la cual está optimizada para usarse en un ambiente de red. Corriendo el sistema operativo de red LAN Manager sobre el sistema operativo OS/2 (en lugar del DOS) provee un número de ventajas

- OS/2 es un verdadero sistema operativo *multitareas*. La operación en modo protegido significa que si un programa falla, otras aplicaciones no son afectadas.
- La programación sofisticada de eventos de OS/2, asegura que todos los programas de la red reciban un acceso proporcional de acuerdo con su prioridad, hacia el procesador central del servidor de archivos.
- Debido a que el OS/2 fue desarrollado para tomar ventaja de las computadoras de 16 y 32 bits, es posible direccionar 16 Mb de memoria RAM y hasta 1 Gb de memoria virtual. Esto significa que los programas que requieren grandes cantidades de memoria pueden utilizar almacenamiento secundario (tal como espacio en disco) como si fuera una parte de la RAM.

El IBM Network Program

Para compañías con pequeñas redes basadas en DOS, IBM ofrece su *IBM PC Local Area Network Program*, corriendo en redes con hardware Token Ring. Este poderoso (aún fácil de usar) paquete de software garantiza una visión cercana a sus varias características

El programa permite compartir drives de disco e impresoras, tan bien como el envío y recepción de mensajes y archivos. Para usuarios de la red principiantes, existe una serie de menús dentro de los menús, los usuarios más experimentados pueden simplemente usar los comandos de red para enviar y recibir información.

El PC Network Program tiene cuatro configuraciones diferentes:

- Redirector (RDR)
- Messenger (MSG)
- Receiver (RCV)
- Server (SRV)

La configuración *Redirector* realmente restringe al usuario de ciertas actividades; no es recomendado como una configuración de usuario. Acepta solicitudes para aplicaciones dirigidas a los servidores, y pasa esas solicitudes a todos los servidores. Acepta y pasa los

datos, y envía los mensajes. El Redirector puede ser usado para estaciones de trabajo con recursos limitados de memoria.

La configuración *Receiver* (Receptor) incluye todas las actividades del Redirector y también recibe y muestra los mensajes. El Receiver representa una configuración mínima del usuario; un usuario necesita poder recibir y editar mensajes tanto como transmitirlos.

Un usuario experimentado usualmente optaría por la configuración *Messenger* (Mensajero), la cual provee capacidades de edición y búsqueda de mensajes en pantalla completa, además de las funciones de Redirector y Receiver.

La configuración *Server* (Servidor) incluye todas las funciones de las configuraciones Redirector, Receiver y Messenger además de la posibilidad de controlar unidades de disco, directorios e impresoras

Novell NetWare

El empeño de Novell para servir a los usuarios de LANs es único en cuanto a que ha escogido concentrar sus esfuerzos en producir software que corra en hardware de otros proveedores. NetWare corre virtualmente en cualquier PC compatible y soporta la mayoría de las tarjetas de red existentes en el mercado. La filosofía de Novell es hacer de sí mismo un estándar de facto de la industria mediante el dominio del mercado.

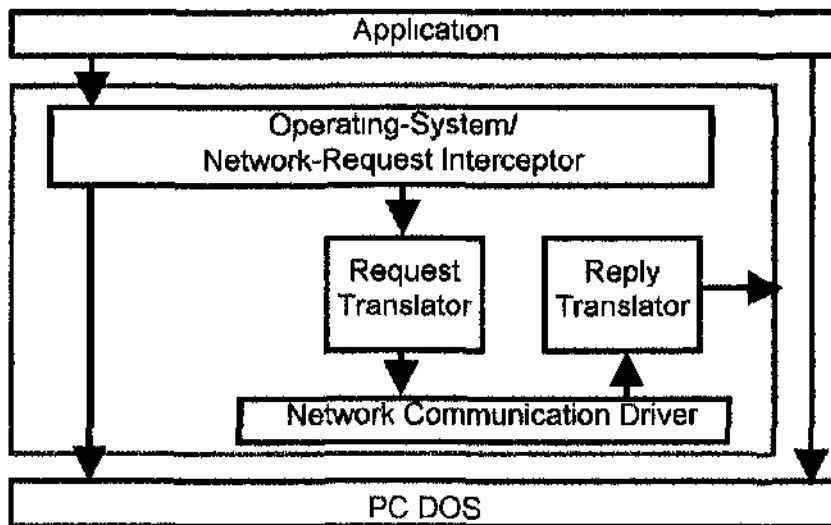
Topología

El sistema operativo de red de Novell, el NetWare, corre en diferentes topologías de red. Dependiendo del hardware que se seleccione puede correr en una red configurada como una estrella, estrella de estrellas, token ring y aún en una de bus

NetWare y el concepto de un Servidor de Archivos

NetWare está diseñado para soportar verdaderos servidores de red. Para entender esto, es útil estudiar como funciona un servidor de archivos bajo el software de Novell. Bajo el modelo OSI, el software del servidor de archivos de Novell reside en la capa de Aplicación, mientras el DOS reside en la capa de Presentación. En efecto, el software de servidor de archivos forma un shell alrededor de DOS, capaz de interceptar comandos desde los programas de aplicación antes de que lleguen al procesador de comandos.

Figura 2-3 Network Interface Shell



Fuente: Understanding Local Area Network

Cuando un programa de aplicación solicita un archivo específico, el shell debe determinar primero si el request (requisición) es por un archivo local (residente en los drives propios de la estación de trabajo) o un request de red para información localizada en el servidor de archivos. Si la información está localizada en los drives de la estación de trabajo, el request es pasado al procesador de comandos del DOS, donde es manejado como una operación normal de E/S.

"Si el archivo solicitado está localizado en el servidor de archivos, el traductor de requisiciones (request translator) manda una requisición de lectura hacia el servidor de archivos, el cual localiza el archivo y lo transmite hacia la estación de trabajo en la forma de una réplica de paquete (reply packet). El paquete es recibido por un traductor de réplicas (reply translator), el cual convierte esta información en una forma que DOS en la estación de trabajo local puede manejar. DOS entonces provee al programa de aplicación con esta información" [2: pág. 149]

Administración de Archivos bajo NetWare

"NetWare permite al supervisor definir el acceso al directorio. Ciertos usuarios pueden desear correr aplicaciones MS-DOS monousuario en un ambiente de proceso distribuido. El administrador del sistema puede designar un programa o un archivo como compartible (shareable) o no-compartible (non-shareable). NetWare además contiene

una función de bloqueo de archivo por defecto, lo cual significa que esos programas monousuario pueden ser accedidos por diferentes usuarios, uno a la vez" [2:pág. 150].

Si un archivo es non-shareable, diferentes usuarios pueden ver el archivo en modo de sólo lectura, pero ellos no pueden escribir hacia él mientras está siendo usado en modo de lectura/escritura por un usuario específico. Los programas o archivos designados como shareable, con capacidades de bloqueo de registros pueden operar en forma distribuída; varios usuarios pueden leer y escribir hacia ellos simultáneamente, siempre y cuando cada usuario esté escribiendo hacia un registro específico a la vez.

AppleTalk

Local Talk es la interface de red interconstruída de Apple, encontrada en las computadoras Macintosh e impresoras LaserWrite. Apple Talk es la familia de software de protocolos de red de Apple; controla todo, desde el ruteo hasta el acceso a archivos.

Los Protocolos AppleTalk y el Modelo OSI

"Apple ha desarrollado un conjunto de protocolos que son consistentes con el modelo OSI, Apple ha asegurado que sus redes basadas en Macintosh se comunicarán con cualquier LAN basada en PCs" [2.pág. 190]. La arquitectura de red de Apple sigue la estructura de capas, desarrollada por OSI para facilitar las comunicaciones entre redes heterogéneas.

AppleShare

Appleshare es el software de servidor de archivos de Apple para una red Apple Talk. Los discos duros conectados al servidor de archivos son conocidos como volúmenes. Dentro de cada volumen, los archivos son almacenados en folders (los cuales corresponden a los directorios bajo MS-DOS). AppleShare provee seguridad y acceso a nivel de folder, y no al nivel de archivo.

AT&T StarLAN

AT&T diseñó la red StarLAN para ser tan simple como sea posible. Con StarLAN hasta 10 PCs pueden ser enlazadas instalando una unidad de acceso a la red (*Network Access Unit - NAU*) en cada bus de expansión de las PCs, y luego usando cable par trenzado no aislado de tipo telefónico, se unen en topología *daisy-chain* (margarita). Cada NAU tiene

tres conectores (*jacks*) de teléfono. La entrada (*IN*) de un conector es enlazada a la salida (*OUT*) de otra unidad. El tercer conector es usado para conectar un teléfono analógico a una workstation. Una workstation con un disco duro está designada como el servidor de archivos, cada workstation instala una copia del software StarLAN. AT&T se refiere a una workstation que utiliza un servidor de archivos como clientes. La distancia máxima permitida para una red StarLAN en daisy-chain es 400 pies

Banyan Vines

El sistema de Banyan VINES (Virtual NETworking System) es un sistema operativo de red basado en el UNIX System V. Vines ofrece una conexión interna de red, seguridad, y operaciones transparentes. La compañía ofrece numerosos productos add-on, incluyendo correo electrónico y software de administración de red. Vines soporta una amplia variedad de plataformas de hardware. Requiere un servidor de archivos dedicado.

Todos los servicios de Vines, incluyendo nombramiento, archivos, impresoras, y correo, se ejecutan como procesos UNIX. Estos servicios pueden ser detenidos e iniciados desde el servidor sin interrumpir otros servicios. Mientras los expertos de la industria de cómputo han estado aclamando las capacidades de multitarea y el multiusuario de UNIX, ellos han apuntado que eso es de amplia aceptación por el público en general aunque pierde interés debido a la carencia de una interface amigable al usuario. La interface del usuario de Vines está basada en menús.

LANTastic

LANTastic, de Artisoft, es una serie de productos de red punto-a-punto. Originalmente LANTastic fue diseñado solo para DOS, pero ahora proporciona un soporte para Windows. El mecanismo de seguridad de LANTastic es más sofisticado que el de Windows for Workgroups.

"LANTastic siempre ha sido un sistema operativo de redes punto-a-punto. Desde esta perspectiva se puede ver que Artisoft no está posicionando este sistema como un escalón hacia un sistema operativo de red mayor. En lugar de eso ha desplazado los límites de los sistemas operativos de redes punto-a-punto, soportando hasta 300 usuarios o proviendo de funcionalidades adicionales (como lo es el compartir modems a través de la red y el acceso a la comunicación remota)" [3.pág. 764].

Artisoft usa un protocolo propietario, no ruteable, para sus redes LANtastic; si se requiere conectividad hacia redes TCP/IP o NetWare IPX, se pueden proveer servidores LANtastic especiales que hagan la función de *gateways* entre las dos redes.

BTOS/CTOS

Puede que el sistema operativo BTOS/CTOS de Unisys sea, actualmente, el secreto mejor guardado en el mundo de la computación. Su sistema operativo basado en mensajes y que corre en procesadores Intel 80286 hasta Pentium, es la clave de la ventaja funcional de BTOS/CTOS.

BTOS/CTOS Open

"BTOS/CTOS Open es una especificación para un sistema operativo multiusuario, multitareas, basado en mensajes, que puede funcionar eficientemente con menos de 1 Mb de memoria por usuario. Está diseñado para operar en un ambiente computacional donde cada usuario tiene una estación de trabajo que puede acceder a un servidor común, que también es una estación de trabajo completamente funcional.

La gran efectividad del sistema operativo BTOS/CTOS para múltiples usuarios se debe a que está basado en mensajes. En pocas palabras, esto significa que cada consulta del programa trae adjunto un mensaje que indica de dónde viene y hacia dónde se pretende que vaya. Este concepto proporciona tolerancia a fallas y búsquedas nodo a nodo de bases de datos distribuidas según el área geográfica.

Cuando un usuario desea acceder a un archivo en cualquier parte de una red de información basada en BTOS/CTOS, éste lo encontrará en forma transparente donde quiera que se encuentre, incluso si se ha desplazado a otro sistema.

Por último, BTOS/CTOS proporciona toda la capacidad de un sistema operativo de red. Como tal puede funcionar en forma efectiva como una LAN, incluso para aplicaciones MS-DOS que se ejecutan bajo BTOS/CTOS. BTOS/CTOS puede ofrecer toda la capacidad actual de conexión requerida para SNA de IBM, así como también soporte de TCP/IP para sistemas UNIX, y los protocolos que pertenecen a OSI, incluyendo X.25, FTAM y X.400, para la interoperación de sistemas abiertos.

En pocas palabras, BTOS/CTOS es tan abierto como lo es UNIX en la actualidad. Mientras varios grupos ofrecen estándares UNIX alternativos, Unisys ha consolidado BTOS/CTOS y sus derivados en un único estándar abierto: BTOS/CTOS OPEN" [20].

Desafortunadamente, debido a que BTOS/CTOS es un sistema propietario y a que no existen tantas aplicaciones comerciales que puedan desplazar a las aplicaciones que actualmente dominan el mercado de cómputo, este sistema operativo no tiene el mismo nivel de crecimiento que otras plataformas de la industria han logrado.

Capítulo III. Modelo de Referencia OSI

Dado el objetivo principal de este trabajo que es el de mostrar que el sistema operativo UNIX es el sistema operativo más viable para ser base de la implementación de sistemas abiertos, en este capítulo se analiza el Modelo de Referencia OSI (Open System Interconnection), así como los protocolos estándar relacionados con dicho modelo, el cual norma la implementación del hardware y software para los sistemas abiertos

Concepto de transposición de capas y su relación con el modelo de referencia OSI

"La estructura lógica del modelo de referencia OSI está formada por siete capas de protocolos, las cuales describen la forma en la cual los datos deben ser manejados durante los diferentes estados de la transmisión. Cada capa desempeña una función bien definida y provee un servicio a la capa inmediata superior e inferior" [16: unidad 1, sección 2, lección 1]. Esto opera de acuerdo a un protocolo de comunicación definido para intercambiar mensajes, los datos del usuario y la información adicional de control, con la capa correspondiente. Las funciones desempeñadas en cada capa han sido seleccionadas en base a la experiencia ganada durante la etapa temprana de la estandarización.

Las tres capas inferiores son dependientes de la red y están involucradas con los protocolos asociados con la transferencia de datos entre dos computadoras. En contraste, las tres capas superiores están orientadas a la aplicación e involucradas con los protocolos que permiten a dos procesos, de las aplicaciones de dos usuarios finales, interactuar uno con otro, normalmente dentro del rango de servicios del sistema operativo local.

El modelo está diseñado para facilitar la comunicación entre las diferentes capas. Cada capa tiene una interface bien definida entre sí misma y la capa inmediata superior e inferior, consecuentemente la implementación de un protocolo de una capa particular es independiente de todas las otras capas. Las capas que componen al modelo de referencia OSI se describen a continuación.

Tabla 3-1 Capas del Modelo de Referencia OSI

Aplicación
Presentación
Sesión
Transporte
Red
Enlace de Datos
Física

Fuente Understanding Local Area Networks

La Capa Física (Physical Layer)

La primera capa de los estándares -la *capa Física*- es un conjunto de reglas referentes al hardware utilizado para transmitir datos. Entre los elementos involucrados en este nivel se encuentran: Los voltajes utilizados, la coordinación de la transmisión de datos, y las reglas para el establecimiento de la conexión inicial de la comunicación.

La capa Física determina si los bits están siendo enviados hacia un *half duplex* (el cual es bastante similar a la forma en la cual los datos se transmiten a través de un CB) o por un *full duplex* (el cual requiere un envío y recepción simultánea de datos)

Otras descripciones de hardware, incluidas en los estándares de la capa Física, son los *conectores* y los *medios de interface*. En esta capa, el modelo OSI toma en cuenta las consideraciones eléctricas y los bits (1s y 0s). Los bits realmente no tiene un significado en este nivel, ya que el asignarles un significado corresponde a la siguiente capa.

Capa de Enlace de Datos (Data Link Layer)

Anteriormente se mencionó que cada capa provee elementos claves a su la capa superior, en este caso la capa Física provee los bits a la *capa de Enlace de Datos*. Por lo que ahora, es tiempo de asignar un significado a dicho grupo de bits, para lo cuál se utilizan los *data frames*, paquetes que contienen tanto los datos como la información de control.

La Capa de Enlace de Datos adhiere banderas para indicar el comienzo y el término de los mensajes. Los estándares de esta capa desempeñan dos funciones importantes: ellos aseguran que los datos no sean erróneos para las banderas y checan los errores en los data frames. Este chequeo de errores puede tomar la forma de información enviada a la computadora receptora, y de un mensaje recibido, si es que todos los datos han sido recibidos correctamente.

Capa de Red (Network Layer)

La *capa de Red* es la tercera capa del modelo OSI, la cual concierne al intercambio de paquetes (*packet switching*). Esta capa establece los *circuitos virtuales* (rutas entre dos computadoras o terminales) para la comunicación de datos. Al término del envío, la capa de Red re-empaqueta los mensajes, que las dos capas anteriores han transmitido, y envía dichos paquetes de datos hacia la capa de Transporte. Para entender el uso de estos paquetes de datos, es necesario analizar los estándares de la industria, localizados en las tres capas inferiores del modelo OSI.

La Capa de Transporte (Transport Layer)

La *capa de Transporte* del modelo OSI tiene varias funciones, incluyendo varias órdenes de reconocimiento y recuperación de errores. En un nivel superior, la capa de Transporte puede detectar (y a veces corregir) errores, identificando los paquetes que han sido enviados correctamente, y reordenándolos en la secuencia correcta. Esta capa funciona también como multiplexor de varios mensajes, ya que ésta debe colocar los mensajes dentro de un circuito, dando la indicación de qué mensaje debe ir a qué circuito. La capa de Transporte también regula el flujo de información, para controlar el movimiento de los mensajes.

La Capa de Sesión (Session Layer)

Como se ha visto el modelo OSI está relacionado con los bits y con los mensajes de datos, no con el reconocimiento de un usuario particular de la red. Podemos conceptualizar a la capa de Sesión como el administrador de la red. Esta capa tiene la habilidad de dar por terminada una sesión y controlar el orden en el cual cada una de las sesiones debe terminar. El usuario se comunica directamente con esta capa. La capa de Sesión puede verificar el *password* escrito por el usuario, y capacitar a dicho usuario a pasar de la transmisión half-duplex a la full duplex. Esto controla la transferencia de datos y a veces

la recuperación de los mismos en caso de que el sistema falle. Finalmente, la capa de Sesión puede monitorear el uso del sistema y contabilizar el tiempo de trabajo de los usuarios.

La Capa de Presentación (Presentation Layer)

La capa de Presentación del modelo OSI está asociada con la seguridad de la red, la transferencia de archivos y las funciones de formato. A nivel de bits, la capa de presentación es capaz de codificar los datos en una gran variedad de formatos distintos, incluyendo *ASCII* y *EBCDIC*.

El *American Standard Code for Information Interchange (ASCII)* es un código de caracteres (de siete bits, más el bit de paridad) para la transmisión de datos. Esta es la convención más utilizada universalmente. Muchas de las grandes computadoras IBM usan el *Extended Binary Coded Decimal Interchange Code (EBCDIC)*. La capa de Presentación es capaz de manejar ambos estándares para la transmisión de datos. Para una verdadera comunicación, ambas capas de Sesión, de las computadoras comunicadas, deben de tener el mismo protocolo o reglas para manejar los datos. Esta capa maneja la conversión de protocolos de las computadoras que utilizan diferentes formatos.

La mayoría de las funciones de procesamiento de palabras están asociadas con el formato del texto (incluyendo la paginación, el número de líneas por pantalla y los movimientos del cursor a través de la pantalla) y son manejadas por la capa de presentación.

La proliferación de terminales con códigos incompatibles son tratadas en este nivel. Un *protocolo de terminal* resuelve estas diferencias al capacitar a cada terminal de datos para planear o diseñar la misma terminal virtual. En efecto, este procedimiento significa que existen un conjunto de tablas de traducción entre una terminal local y una terminal remota. La terminal local envía una estructura de datos que define su pantalla actual en términos de cuántos caracteres por línea serán desplegados (este número puede variar considerablemente); la mayoría de las terminales despliegan 132 caracteres por línea, pero otros formatos son variables. La estructura de los datos es enviada hacia el objeto de control correspondiente, de la terminal remota, el cual traduce este número en un código

que esta terminal pueda entender e implementar. Otros códigos indican el grosor, el subrayado, las gráficas, etc.

Capa de Aplicación (Application Layer)

La *capa de Aplicación* maneja los mensajes, los *logons* remotos y la responsabilidad de manejar las estadísticas de la administración de la red. En este nivel, se encuentran los programas administradores de bases de datos, los comandos del sistema operativo y el lenguaje responsable.

La mayor parte de las funciones desempeñadas en esta capa son especificadas por el usuario. A partir de que los diferentes usuarios del programa establecen diferentes necesidades, es difícil generalizar acerca de los protocolos encontrados aquí. Ciertas industrias, como los bancos, han desarrollado conjuntos de datos para este nivel.

Los programas de red encontrados en la capa de Aplicación incluyen software de correo electrónico, manejadores de bases de datos, software de servidores de archivos y software de servidores de impresión.

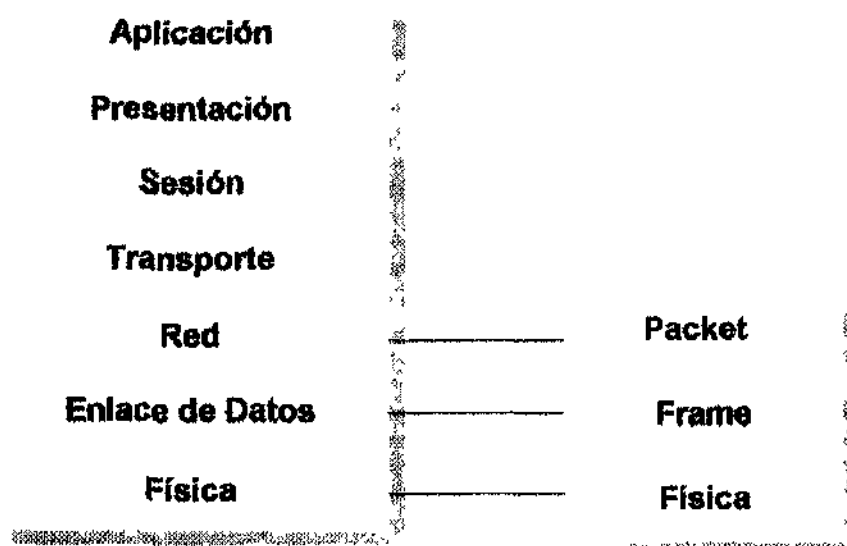
Protocolos estándar relacionados con el modelo de referencia OSI

Estándar CCITT X.25

"El *Consultative Committee for International Telephony and Telegraphy* (CCITT) ha desarrollado un conjunto de estándares internacionales de telecomunicación. Como se muestra en la siguiente tabla, las primeras tres capas de el estándar X.25 (physical, frame, and packet) corresponde a las tres primeras capas del modelo OSI (física, enlace de datos y red).

- La *capa Física* del X.25 corresponde a la capa Física del modelo OSI. Esta capa utiliza la recomendación X.25 del CCITT para definir el estándar RS-232, para la transmisión de datos asíncrona entre una DTE y la red pública de datos.
- La *capa Frame (Frame layer)* del X.25 corresponde a la capa de enlace de datos del modelo OSI. Aquí los datos son intercambiados entre el DTE y la red.

Tabla 3-2 Relación entre el estándar X.25 y Modelo de Referencia OSI



Fuente: Understanding Local Area Networks

- En la *capa de Paquetes (Packet layer)* del X.25, que corresponde a la capa de red del modelo OSI, los datos están en forma de paquete, los cuales son requeridos para intercambiar información en las redes públicas

Los estándares X.25 aseguran que la información que sea enviada desde un DTE pueda ser entendida, cuando sea recibida por la red pública de paquetes (*Public Packet Network*)" [2:pág. 50].

Los paquetes de datos contienen varios tipos discretos de información, lo cual hace que pueda distinguirse un paquete de otro. El paquete contiene un campo de dirección (*ADDRESS field*) el cual indica su destino. El campo de control (*CONTROL field*) contiene varios tipos de información, incluyendo las indicaciones de dónde un mensaje comienza o termina, si el mensaje ha sido recibido exitosamente, o si ha ocurrido un error y se ha detectado.

Los estándares X.25 están diseñados para el intercambio de paquetes (*packet switching*); utilizando esta convención particular, la capa de red del modelo OSI funciona como una gigantesca oficina de correos. Los mensajes son recibidos desde el *host* y son puestos en paquetes, direccionados y enviados hacia las dos capas inferiores para su transmisión.

Debido a que existen diferentes formas de rutear un mensaje hacia una estación de trabajo particular, tablas especiales de ruteo (*routing tables*) mantienen parte del tráfico en orden, con el fin de mantener un balance en el trabajo de recuperación de archivos (*workload*). La mayoría de las aplicaciones de los estándares X.25 están en conjunción con las comunicaciones de mainframes y redes públicas.

La capa de red contiene otras convenciones además de las X.25 existen procedimientos para reconocer la prioridad de los mensajes y el envío de mensajes en el orden adecuado. Finalmente, esta capa controla la congestión de la red, por medio de prevenir que la información sea enviada a una velocidad mayor de la que puede ser recibida o almacenada.

Procedimiento de control del enlace de datos a alto nivel

High-Level Data Link Control Procedure (HDLC)

El estándar X.25, encontrado particularmente en la capa de Enlace de Datos y en la capa de Red del modelo OSI, define los estándares para enlazar un dispositivo *DTE*, tal como una computadora, con un dispositivo *DCE*, tal como un modem utilizando *HDLC*.

"El *Bit stuffing* asegura que los datos dentro de un paquete no estarán equivocados para el control de bits. El protocolo HDLC está diseñado para manejar el intercambio de datos entre una computadora central de control y sus estaciones secundarias. La computadora central es responsable del chequeo de errores y de la asignación de los tiempos de trabajo de las estaciones secundarias. Cuando ésta recibe la señal de que una estación de trabajo tiene un mensaje para enviar, ésta envía un *pull bit*, que le permite responder a la estación, esta forma de trabajo es llamada *Modo de Respuesta Normal* (*Normal Response Mode - NRM*)" [2:pág. 51].

Un segundo modo de operación permite a todas las estaciones secundarias a enviar mensajes cuando ellas lo decidan, sin esperar por un poll bit de la computadora central. Este método es llamado *Modo de Respuesta Asíncrono* (*Asynchronous Response Mode-ARM*).

Control Síncrono de Enlace de Datos (Synchronous Data Link Control - SDLC)

Las computadoras de IBM que corren bajo su *Arquitectura de Sistemas de Red* (*Systems Network Architecture*) usan *SDLC*, un subconjunto de *HDLC*. Mientras éste contiene el mismo marco que el *HDLC* -consistente en banderas de inicio y término, con el mismo patrón de bits *HDLC*- existen algunas diferencias. Los campos de información del *SDLC* contienen datos que sólo pueden ser integrados por múltiples caracteres de 8 bits. Una diferencia igualmente significativa es que el *SDLC* tiene varios comandos y respuestas no encontrados bajo *HDLC*.

Estándares de red IEEE

Algunos comités IEEE han desarrollado estándares de LAN y métodos de acceso, utilizando un conjunto de estándares, de las capas del modelo OSI, como fundamento. Dentro de los estándares de la IEEE se encuentran: el estándar 802.2 (*LCC*), el 802.3 (el estándar de bus *CSMA/CD*), el 802.4 (el estándar *Token bus*) y el 802.5 (el estándar *Token ring*). Otro estándar, el 802.6, concierne con los estándares para las redes de área metropolitana.

La razón por la cual la IEEE desarrolló diferentes -y tan contradictorios- estándares, es que para 1980, el subcomité 802 determinó que aún existía un amplio rango de productos de red incompatibles. Algunos fabricantes habían optado por topologías bus mientras que otros habían optado por *Token Ring* o de estrella. Los fabricantes también habían adoptado métodos bastante divergentes para manejar problemas significativos en las capas de la red, como es el evitar las colisiones de datos entre los nodos de la red, que tienen información para enviar.

Muchos tipos diferentes de redes han proliferado debido a que una sola topología o método de acceso de datos no es la mejor para todas las aplicaciones de red. IBM ha ilustrado este hecho por medio de ofrecer una red (de PCs) con una topología de bus tan buena como la topología de red *Token Ring*, cada red ha sido diseñada conociendo las diferentes necesidades de los clientes.

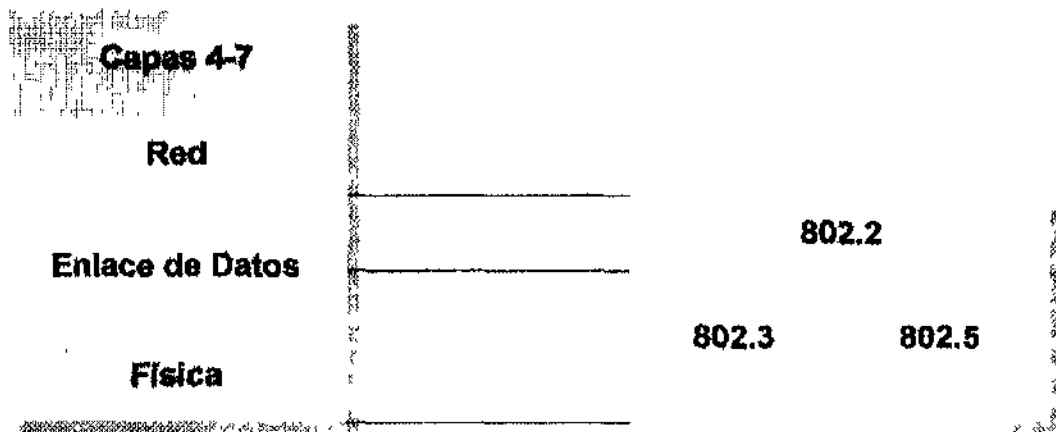
Para el usuario final, la mayor ventaja de los estándares 802 de la IEEE es que ellos eventualmente resultarán en la estandarización de las capas físicas y de enlace de datos.

del modelo OSI. Esto significa que diferentes fabricantes, que cumplan con diferentes estándares, producirán hardware que puede trabajar en un mismo sistema. Para trabajar con software de red, sin embargo, los fabricantes tendrán que seguir los estándares de las capas superiores del modelo OSI, pero esto tomará tiempo.

IEEE 802.2

El IEEE 802.2, también llamado *Logical Link Control (LLC)*, es un protocolo que provee una interface entre la capa de red y algunos mecanismos de acceso al medio de transmisión. También, controla el flujo de datos y maneja los errores de transmisión. El IEEE 802.2 corre sobre el IEEE 802.3 y el IEEE 802.5. IEEE 802.2 especifica la mitad superior de la capa de enlace de datos del modelo OSI. Tanto el IEEE 802.3 como el IEEE 802.5 especifican las capas inferiores de del modelo OSI, incluyendo a la capa Física. El estándar 802.2 es el estándar por default para los nuevos NetWare 3.12 y 4 X.

Tabla 3-3 Estándar IEEE 802.2



Fuente: Introduction to Networking Technologies

IEEE 802.3 / Ethernet

IEEE 802.3 y Ethernet (el sistema de red creado a fines de los 70s sobre el cual se basó el IEEE 802.3) son considerados protocolos simples, bastante robustos, razonablemente compatibles con otros protocolos y soluciones económicas de red. Juntos representan a los protocolos más populares de las capas inferiores de las LAN.

Cuando el comité 802 de la IEEE comenzó con sus deliberaciones, coincidieron con el *EtherNet Local Area Network* de Xerox, como el estándar por defecto. Para 1980 Intel y Digital Equipment Corporation trabajaron con Xerox en términos de que todos sus productos pueden ser compatibles con EtherNet. Lejos de que todas las LAN sigan los estándares EtherNet, un subcomité proporcionó el 802.3 como un estándar EtherNet-like aceptable.

Como se ha planteado anteriormente, el subcomité 802 desarrolló estándares basados en las tres primeras capas del modelo OSI. Por lo que dividieron a la capa de Enlace de Datos en dos subcapas. La subcapa de *Control de Enlace Lógico* (*Logical Link Control - LLC*) y la subcapa de *Control de Medio de Acceso* (*Media Access Control - MAC*). El estándar LLC es tal como el estándar HDLC, mientras que la subcapa MAC concierne a la detección de colisiones de datos. La siguiente tabla muestra la relación existente entre EtherNet y el estándar del IEEE 802.3.

Tabla 3-4 Especificaciones IEEE 802.3 & Ethernet

	Ethernet	IEEE 802.3
Topología	Bus	Bus, Estrella
Tipo de medio	Coaxial	Coaxial Par-trenzado
Método de acceso	Contention	Contention

Fuente: Introduction to Networking Technologies

Ambos, IEEE 802.3 y Ethernet utilizan el método de acceso contention (específicamente CSMA/CD) y dependiendo del tipo de implementación, pueden soportar velocidades arriba de 10 Mbps.

Ethernet soporta cable coaxial y especifica una topología de red, mientras que IEEE 802.3 permite varias topologías, dependiendo de cuál de las especificaciones físicas del IEEE 802.3 sea implementada. Quizás, la especificación física IEEE 802.3 más rápida y con mayor crecimiento es *10BaseT*, debido a que ésta combina los beneficios de una velocidad de datos alta (10 Mbps) y una topología de estrella. Además, *10BaseT* corre sobre el desprotegido par-trenzado (el más barato y común medio de cableado).

El Paquete de Datos Ethernet (The Ethernet Data Packet)

El estándar 802.3 de la IEEE describe a una LAN utilizando una topología de bus. Esta red usa cable coaxial *baseband* de 50 ohms, capaz de enviar datos a 10 Mbs. El paquete Ethernet empieza con un *PREAMBLE*, consistente en ocho bytes, utilizados para la sincronización. El *DESTINATION ADDRESS* puede ser simplemente la dirección de una workstation, de un grupo de workstations o de varios grupos de workstations. La *SOURCE ADDRESS* es crítica, ya que la estación de trabajo por medio de ésta reconoce de dónde provino el mensaje. El campo *TYPE* es importante porque éste designa cual es el tipo de formato que están utilizando los datos, sin esta información es imposible descifrar el paquete cuando éste llega. El campo *DATA* está limitado estrictamente, éste puede solamente mantener un mínimo de 64 bytes y un máximo de 1500 bytes de información. Finalmente, el campo *FRAME-CHECK SEQUENCE* asegura que los datos en los otros campos lleguen a su destino. En adición a la especificación del tipo de frame de datos y el tipo de cable que puede ser usado para enviar esta información, el comité también especificó la longitud máxima de un cable simple (1500 pies) y la forma en la cual los repetidores pueden ser utilizados para aumentar la señal a través de la red

Tabla 3-5 Formato del Frame Ethernet



Fuente: Understanding Local Area Networks

El Protocolo CSMA/CD

El subcomité 802.3 de la IEEE especificó la forma en la cual una LAN, usando una topología de bus, debe construir sus *frames* de información y enviarlos a través de la red con el fin de evitar las colisiones. Este protocolo es conocido como *Carrier-Sense Multiple Access with Collision Detection* (CSMA/CD). Para ilustrar la función del protocolo CSMA/CD, imaginemos a un usuario de red quien desea enviar un mensaje. En términos del modelo OSI (incorporado al estándar 802.3 de la IEEE) la capa física de la workstation del usuario genera una señal. Esta workstation escucha y detecta otra señal *carrier*. Si no es detectada otra señal, el mensaje del primer usuario es enviado

IEEE 802.3 10Base5

Cuando el comité 802 desarrolló su estándar para redes con topología de bus, el cableado de coaxial grueso fue la norma para Ethernet. Como resultado, algunas veces, el conjunto original de especificaciones *IEEE 802.3* es conocido como *10Base5*, debido a que éste describe una red de bus con un cableado de coaxial grueso *baseband*, que puede transmitir datos a 10 Mbs, a una distancia máxima de 500 metros.

IEEE 802.3 10Base 2

Muchos de los vendedores de redes han encontrado que es más fácil y menos caro usar un cableado coaxial delgado *baseband* cuando se instala una red de bus 802.3. Las especificaciones *IEEE 802.3 10Base2* describen a una red de bus compuesta por un cableado de coaxial delgado, que puede transmitir datos a 10 Mbs a una distancia máxima de 200 m.

IEEE 802.3 STARLAN

El comité IEEE 802.3 ha desarrollado un estándar para redes CSMA que usan una topología de estrellas agrupadas (*cluster star topology*) en la cual las estrellas están enlazadas entre sí. Algunas veces este estándar se conoce como *1Base5*, este conjunto de especificaciones describen a una red que puede transmitir datos a 1 Mbs a distancias de 500 metros, utilizando dos pares de alambres par-trenzado, sin recubrimiento 24 gauge.

IEEE 802.3 10BaseT

El conjunto de especificaciones *IEEE 802.3 10BaseT* combina las mejores características de una red de estrella y de una red de bus. Mientras la red es lógicamente un bus con datos que son transmitidos en toda la red, ésta físicamente está configurada como una estrella distribuida, utilizando alambres baratos de par-trenzado. Las redes basadas en las especificaciones *IEEE 802.3 10BaseT* pueden transmitir datos a 10 Mbs a una distancia máxima de 100 metros.

La razón por la cual el *10BaseT* es tan atractivo para los administradores de red es que las estaciones de trabajo son enlazadas a un hub, el cual contiene los diagnósticos interconstruidos. Cuando el hub reconoce que una de las estaciones de trabajo está fallando, éste puede evitar que la estación de trabajo altere a la red completa.

El token es actualmente un paquete de datos. Una workstation envía un token hacia la dirección de la estación de trabajo que ha sido designada para recibirlo. Esta estación copia el mensaje y después regresa el token hacia la estación que lo envió.

La red mantiene una tabla comprimida de direcciones de cada workstation. Estas direcciones no localizan físicamente a las estaciones en la red de bus; ellas indican el orden en el cual cada estación recibirá el token.

El token es pasado de una estación a la siguiente que contenga la dirección inmediata inferior. Por ejemplo, cuando una estación con la dirección 100 envía el token hacia la dirección 75, ésta se tiene que asegurar que el token ha sido recibido satisfactoriamente. Cuando una estación necesita utilizar más a la red que las otras estaciones, por lo que también requiere los tokens con mayor frecuencia, ésta puede aparecer listada varias veces en la tabla de direcciones de la red y así ésta recibirá los tokens más frecuentemente.

"Hay que recordar que el token es realmente un *patrón de bit*. Si una estación no recibe una replica desde la estación que ha enviado el token, ésta envía un segundo token. Si aún no hay una replica, la estación transmisora envía un mensaje especial bajo la red, requiriendo la dirección de la siguiente estación que debe recibir el token por medio de enviar lo que se conoce como *who follows*. Si éste falla al invocar una respuesta, la estación envía un requerimiento general a través de la red, preguntando a alguna estación que desee enviar un mensaje, y a su vez ésta responderá al recibir el token. Esto es conocido como un *frame solicit successor*. La estación de trabajo transmisora cambia la dirección del token, por la nueva dirección seleccionada y envía dicho token" [2: pág. 59].

Hay que hacer notar que, la topología del estándar 802.4 es un bus, ya que el paso del token es en forma de anillo lógico. Las últimas direcciones de estaciones que reciben el token lo envían hacia atrás, para empezar el proceso nuevamente. En un token bus lento, cada estación recibe el token, inserta la información que desea enviar y después envía ésta hacia su destino a través de la red.

IEEE 802.5 / Token Ring

IEEE 802.5 y Token Ring de IBM son esencialmente lo mismo. Ambos especifican un anillo token-passing. La especificación 802.5 deja algunos atributos, tal como el medio de transmisión, la topología del cableado y el número máximo de estaciones por anillo, por encima de la implementación.

El Token-Ring de IBM, por otro lado, especifica un par-trenzado desprotegido en una topología de estrella y un máximo de 260 estaciones por anillo.

IEEE 802.3/Ethernet Vs. IEEE 802.5/Token Ring

"IEEE 802.5 es más complicado que el 802.3/Ethernet. El 802.3/Ethernet esencialmente permite a los nodos transmitir siempre y cuando ellos estén listos (contention), IEEE 802.5/Token Ring adhiere un mecanismo complejo para que los nodos accesen al medio físico (token passing). Adicionalmente, el IEEE 802.5/Token Ring tiene algunos problemas de construcción, que el IEEE 802.3 no tiene" [16. unidad 3, sección 1, lección 1].

Como resultado del método de acceso del token-passing, las redes IEEE 802.5/Token Ring son llamadas determinísticas. Una *red determinística* es aquella en la cual el tiempo máximo, requerido para que la información fluya desde un nodo hacia otro, puede ser calculada. Cada uno de los nodos en una red Token Ring puede almacenar el token una determinada cantidad máxima de tiempo. A partir de que el número de nodos en el anillo es conocido, el tiempo máximo de transmisión de token puede ser calculado.

Las redes determinísticas son útiles en los ambientes en donde la demora debe ser siempre menor a un valor particular. Una línea de ensamble de un automóvil es un ejemplo de tal medio ambiente.

Las redes IEEE 802.5/Token Ring usan un método de prioridad compleja dando un tratamiento preferencial a ciertos nodos. Si el nodo con la prioridad más alta quiere monopolizar el token, éste puede hacerlo incrementando la prioridad del token. En este caso, el token no puede ser retenido por otros nodos con prioridades bajas.

ARCNET

"La *Attached Resource Computer NETWORK* (ARCNET) es una popular combinación de protocolos de la capa Física y de Enlace de Datos. Este fue originalmente creado por Datapoint Corporation a finales de los años 70, haciendo de éste una de las redes más viejas. A pesar de ser menos popular que el IEEE 802.3/Ethernet o que el IEEE 802.5/Token Ring, ARCNET ofrece varios beneficios: este es relativamente menos caro, fácil de instalar y de configurar, y confiable. ARCNET opera a una velocidad especificada, arriba de los 4 Mbps. ARCNET es generalmente utilizado en redes pequeñas de PCs" [16: unidad 3, sección 1, lección 4].

ARCNET es un protocolo flexible. Este puede utilizar múltiples topologías, incluyendo una estrella y un bus. Además, puede trabajar con múltiples tipos de medios de transmisión, incluyendo par-trenzado, cable coaxial, y fibra óptica. ARCNET utiliza una combinación de accesos de token-passing para determinar cuándo los nodos pueden transmitir. Cada nodo ARCNET tiene una dirección numérica. El token es pasado desde un nodo hacia otro en el mismo orden de las direcciones, desde la dirección inferior hacia la dirección superior.

Cuando una estación ARCNET entra o sale de la red, se lleva a cabo una auto-reconfiguración. La *auto-reconfiguración* es un proceso por el cual los nodos se insertan a sí mismos y ellos mismos se borran de el proceso del token-passing.

ARCNET Plus define a la nueva generación de ARCNET. Este ofrecerá una velocidad incrementada a 20 Mbps (versus 4 Mbps para la versión actual de ARCNET), la cual se comparará favorablemente con el Token Ring de IBM (16 Mbps) y Ethernet (10 Mbps). ARCNET es rentable para la variedad de necesidades de los usuarios. El token-passing de ARCNET es bastante simple, utilizando una ruta (path) low-to-high, determina cuál nodo recibirá el siguiente token. La auto-reconfiguración del sistema ARCNET permite a los nodos tener un *check in* y un *check out* automáticos en el proceso token-passing.

Local Talk

Local Talk es un protocolo de la capa Física y de Enlace de Datos propietario de Apple Computer. Este es un protocolo simple, diseñado para grupos de trabajo pequeños. Local Talk, el cual está construido dentro de todas las Macintosh de Apple, corre a 230.4 Kbps y utiliza cable par-trenzado desprotegido y una topología de Bus.

Tabla 3-7 Especificaciones del protocolo Local Talk

	Local Talk
Velocidad de los datos	230.4 Kbps
Tipo de medio	Par-trenzado desprotegido
Método de acceso	Contention (CSMA/CA)
Topología	Bus

Fuente: Introduction to Networking Technologies

Local Talk utiliza el método de acceso *Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)*. En el caso del Local Talk, CSMA/CA está implementado a través de diálogos de transmisión (múltiples frames que inician una conversación lógica). Para iniciar un diálogo de transmisión, la interface de red Local Talk detecta el canal para la transmisión. Si un envío es detectado, los nodos CSMA/CA esperan por un periodo de tiempo. Pero si el carrier no es detectado en el mismo momento en el cual la interface detecta al canal, los nodos LocalTalk envían un mensaje *Request-To-Send (RTS)* corto. El nodo receptor debe responder al mensaje RTS con un mensaje *Clear-To-Send (CTS)* dentro de un periodo de tiempo. Si el mensaje CTS no es recibido durante este periodo se asume una colisión.

Sin embargo el más interesante e inusual aspecto del LocalTalk es su procedimiento de asignación de direcciones. Las direcciones del IEEE 802 son asignadas por los fabricantes de tarjetas de interface de red (*Network Interface Card - NIC*) como parte del proceso de manufactura, este direccionamiento no cambia mientras se use la misma NIC. Por otro lado, los nodos LocalTalk, adquieren sus direcciones la primera vez que son activados. Esta asignación dinámica de direcciones previene los conflictos de direcciones y es fácil de administrar. Esta dirección es almacenada en PROM y utilizada cada vez que el nodo es activado, previniendo que la dirección no sea utilizada por otro nodo. Si la dirección está siendo utilizada, éste obtendrá una dirección distinta, que será almacenada en la PROM.

Protocolos de las capas superiores del Modelo de Referencia OSI

En la capa de Aplicación, OSI ofrece varios protocolos importantes. Por esta razón, muchos fabricantes están empezando a ofrecer aplicaciones OSI que se ejecutan por encima de varios protocolos *lower-layer* existentes (por ejemplo TCP/IP). Estas aplicaciones incluyen a X.400 (un sistema de transferencia de correo electrónico), *Common Management Information Protocol (CMIP)* y *File Transfer Access Management (FTAM)*.

X.400

X.400 es uno de los más populares protocolos de la capa de Aplicación del modelo OSI. Al igual que la mayoría de las especificaciones de correo electrónico existentes, X.400 provee solamente un sistema fundamental de transporte para la transferencia de mensajes; éste no especifica la interface con el usuario. Muchos de los fabricantes de sistemas de correo electrónico han asegurado que sus productos cumplen con las especificaciones X.400.

Protocolos administradores de red

CMIP es el protocolo administrador de red OSI. Actualmente, éste no ha sido implementado por muchos fabricantes. *Simple Network Management Protocol (SNMP)* y *Netview* son actualmente los protocolos de administración de red más populares. Debido a que los administradores de red son cada vez más populares, el nivel de aceptación de CMIP probablemente se incremente.

FTAM ofrece el equivalente de los servicios de aplicación de transferencia de archivos, más los nuevos servicios distribuidos de acceso de archivos (ésta es una aplicación bastante extensa).

Protocolos propietarios de las capas superiores

"*NetWare* es el nombre que se le ha dado a un grupo de protocolos de red y servicios relacionados, producido por Novell. La primera versión apareció a principios de los 80s, NetWare actualmente es el sistema de archivos de red más popular del mercado. Sin embargo éste fue diseñado originalmente para redes de PCs. El dominio de NetWare se ha extendido a través de los años incluyendo a los grandes sistemas de computadoras" [16: unidad 3, sección 3, lección 1].

Muchos de los protocolos de NetWare se derivaron de los protocolos de red *Xerox Network Systems* (XNS) producidos por Xerox Corporation. Los protocolo XNS han sido la base para muchos sistemas distribuidos de archivos, incluyendo Banyan VINES, Ungermann Bass NetOne, y 3Com (3+ y 3+Open).

Capítulo IV. Conjunto de protocolos TCP/IP

Dado el objetivo general de este trabajo que es el de mostrar que el sistema operativo UNIX es el sistema operativo más viable para ser base de la implementación de sistemas abiertos, en este capítulo se analizan los protocolos de comunicación relacionados con la interconexión de los sistemas abiertos

Introducción a TCP/IP

"TCP/IP (*Transmission Control Protocol/Internet Protocol*) es un sistema de transporte independiente que originalmente fue diseñado por El Departamento de Defensa de los Estados Unidos, a finales de los 70s. Este ha llegado a ser aceptado por la industria como el estándar de facto" [4:pág 183].

En la primera mitad de los años 70, la *Defense Advanced Research Projects Agency* [DARPA] requirió un nuevo protocolo de intercambio de paquetes (*packet-switching*) que pudiera permitir el crecimiento de la popularidad de diversos sistemas de comunicación adquiridos por el gobierno de EUA. Para satisfacer esta necesidad, la DARPA decidió fundar el desarrollo de un conjunto de protocolos con estas características. El conjunto llegó a ser conocido como el *Conjunto de Protocolos Internet*.

Tabla 4-1 Desarrollo de TCP/IP

1970	---	Inicio del desarrollo de Internet Protocol
1980	---	UNIX adoptó los protocolos Internet y se incrementa la popularidad del protocolo Internet
1990	---	Los protocolos Internet son ofrecidos por más de 200 organizaciones

Fuente: Introduction to Networking technologies

Fuera del gobierno de EUA y de algunas universidades, los protocolos Internet eran relativamente desconocidos hasta 1982, cuando una popular versión de UNIX adoptó los protocolos como su forma primaria de red. En los siguientes cinco años, los protocolos Internet llegaron a ser los protocolos más populares en las redes comerciales conectando diferentes tipos de sistemas de computadoras. Los protocolos Internet son actualmente ofrecidos por más de 200 organizaciones.

Transmission Control Protocol (TCP) e *Internet Protocol (IP)* son los dos miembros más conocidos del conjunto de protocolos Internet. TCP cubre completamente la funcionalidad especificada por la capa de Transporte del Modelo de referencia OSI, mientras que el IP cubre la funcionalidad de la capa de Red de OSI.

TCP es un protocolo de transporte típico. Este controla el flujo de datos, maneja los errores y asegura que los paquetes (conjuntos de información) sean recibidos confiablemente y en el orden correcto. *UDP (User Datagram Protocol)* es otro protocolo de la capa de Transporte. IP es un protocolo de la capa de Red que rutea la información a través de una Internetwork (serie conectada de segmentos de red). IP utiliza la información contenida en las tablas de ruteo para determinar las rutas óptimas a través de la Internetwork.

El conjunto de protocolos Internet incluye varias aplicaciones bien definidas. Por ejemplo, *TELNET* provee emulación de terminal clásica, *File Transfer Protocol (FTP)* una utilidad de transferencia de archivos, *Simple Mail Transfer Protocol (SMTP)* es un protocolo de transferencia de correo electrónico. Cada uno de éstos es una aplicación pura de red y todos se encuentran junto con la mayoría de las implementaciones de protocolo.

El Departamento de Defensa ha convenido transportar su *NDD (Network Defense Data)* hacia los protocolos OSI, anticipándose al hecho de que TCP/IP será respaldado por OSI en mediano término.

TCP/IP es utilizado para referirse a una familia completa de protocolos llamada *Conjunto de Protocolos Internet*. Existe una situación complicada en cuanto a algunos protocolos desarrollados por diferentes organizaciones, pero que no forman oficialmente parte de este conjunto, sin embargo existen más de 50 protocolos dentro del conjunto.

Transferencia de datos en la capa de Transporte

El mensaje transferido entre dos capas TCP se le llama *segmento*. Cuando se establece una sesión entre dos capas TCP, el tamaño del segmentos es negociado. Este es el tamaño máximo que cada TCP está preparado para aceptar. TCP es responsable de:

- La segmentación de mensajes
- La secuencia de los segmentos
- El reensamble de los segmentos recibidos en el mensaje original
- La respuesta de que se ha recibido el segmento
- Detección de los segmentos con errores, usando secuencias de números, tiempos y sumas de segmentos detectados
- Retransmisión de segmentos erróneos
- Control del flujo

Transferencia de datos en la capa de Red

Los mensajes transferidos entre dos capas IP son llamados *datagramas* (diagrama de dato). La función de IP es enviar un datagrama a su destino. IP utiliza las direcciones destino (direcciones Internet) para guiar al datagrama utilizando la ruta más apropiada y además maneja cada datagrama de forma individual, así cada datagrama de un segmento dado debe tomar una ruta distinta hacia el mismo destino. IP es responsable de:

- Rutear el datagrama a través de la red
- Detectar encabezados IP erróneos usando un analizador de encabezados. Esto se hace para asegurar que la dirección Internet no sea alterada durante la transmisión, de otra forma el datagrama podría enviarse a un destino incorrecto.
- Guiar al datagrama recibido hacia la capa superior correcta
- Fragmentar los datagramas
- Reensamblar los fragmentos en datagramas y enviarlos a la *dirección IP destino*.

Panorama sobre la arquitectura TCP/IP

TCP/IP es una arquitectura que permite la transferencia confiable de datos entre sistemas. A mediados de los 80s, todas las arquitecturas habían sido comparadas con el Modelo de Referencia para la Interconexión de Sistemas Abiertos (OSI)

Actualmente, TCP/IP es un conjunto de protocolos, el cual provee un medio para transferir datos entre sistemas heterogéneos. Dentro del desarrollo de los protocolos se han desarrollado tareas específicas. Estas incluyen.

- Acceso al mecanismo de transporte
- Ruteo de datos
- Reporte de errores asociados con el transporte de los datos
- La presentación de los datos
- Acceso a los datos una vez que alcanzan su destino

El conjunto de protocolos está organizado en cuatro capas: la capa de Aplicaciones, la capa de Protocolos de Servicio, la capa Internet y la capa de Red. Existen capas establecidas de Enlace de Datos y Físicas las cuales proveen la entrega de los datos y las conexiones físicas (las cuales forman el *backbone* o parte central de la red).

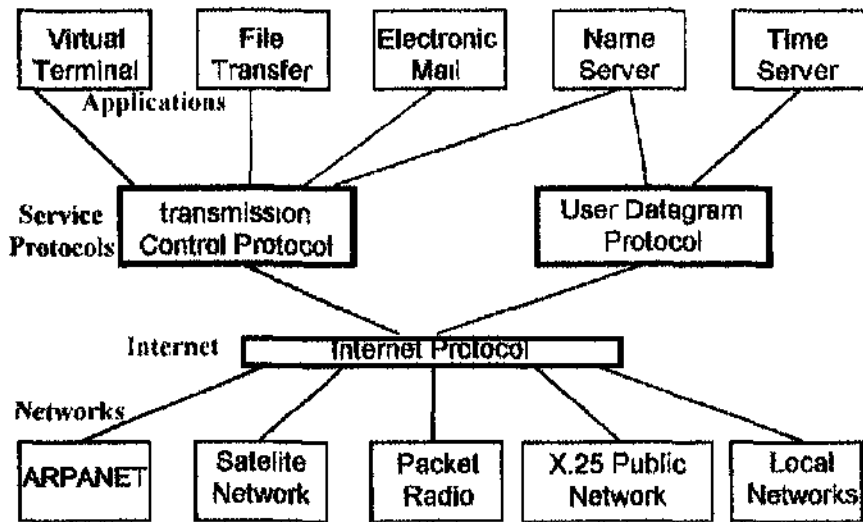
IP fue diseñado para proveer la función de ruteo de datos entre nodos de la capa de Red. El *ICMP* es implementado como parte del IP para reportar mensajes de error y control asociados con el ruteo de los datos. Por otro lado, TCP fue diseñado para proveer el servicio de transferencia confiable entre procesos de la capa de Transporte.

Los protocolos de aplicación fueron diseñados para direccionar las funciones de las tres capas superiores (Aplicación, Presentación y de Sesión). Las necesidades más comunes de estas capas son:

- Conexiones abiertas hacia un host remoto
- Login (ingresar) a un host remoto
- Identificar archivos en un host remoto
- Controlar la transmisión de un archivo hacia un host remoto

Entre los protocolos de aplicación que se han desarrollado se encuentran: *Simple Mail Transfer Protocol (SMTP)* el protocolo estándar de Internet para la transferencia de correo electrónico entre sistemas; *File Transfer Protocol (FTP)* el protocolo de alto nivel estándar de Internet, para la transferencia de archivos de un sistema a otro; *Telecommunications Network Protocol (TELNET)* el protocolo estándar de Internet para el servicio de conexiones de terminal remota.

Figura 4-1 Conjunto de Protocolos Internet



Fuente: TCP/IP and Related Protocols

Servicios del Protocolo Internet (IP)

El Protocolo Internet (*Internet Protocol - IP*) es un ejemplo de un servicio sin conexión. Este permite el intercambio de tráfico entre dos computadoras host sin ningún inicio de llamada (de alguna manera, estas dos computadoras usualmente comparten un protocolo común orientado al transporte). Debido a que el IP no tiene conexión, es posible que los datagramas puedan ser extraviados entre las dos estaciones de usuario final. Por ejemplo, el gateway IP fuerza una longitud máxima de cola, y si la longitud de la cola es rebasada, los buffers se sobrecargarán. En esta situación, los datagramas adicionales son descartados en la red. Por ésta razón, un protocolo de transporte de mayor nivel (como TCP) es esencial para recuperarse de estos problemas.

IP esconde la subcapa de red al usuario final. En este contexto, crea una *red virtual* hacia el usuario final. Este aspecto de IP es atractivo debido a que permite a diferentes tipos de redes conectarse a un gateway IP. Como resultado, IP es razonablemente simple de instalar, y debido a su diseño sin conexiones, es bastante robusto.

Debido a que IP es un protocolo de tipo datagrama, no tiene mecanismos de confiabilidad. No provee recuperación de errores de la subcapa de red y no tiene mecanismos de control de flujo. Los datos del usuario (datagramas) pueden ser extraviados, duplicados, o aún llegar fuera de orden. No es el trabajo del IP tratar con esos problemas.

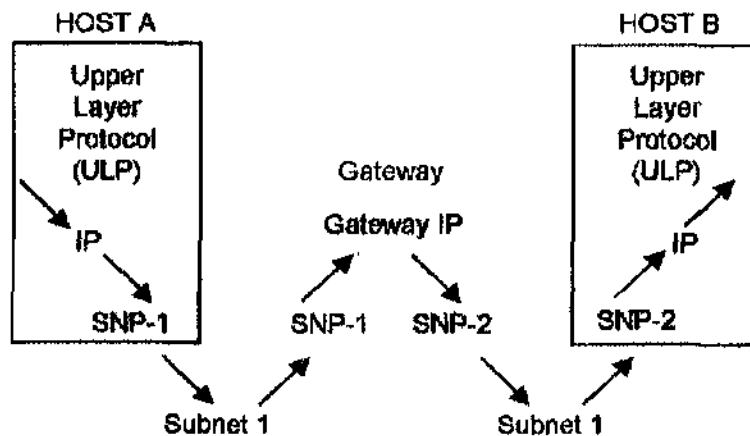
IP soporta operaciones de fragmentación. El término *fragmentación* se refiere a una operación en la cual una unidad de datos del protocolo (*PDU*) es dividida o segmentada en pequeñas unidades. Esta característica puede ser muy útil debido a que todas las redes utilizan distintos tamaños de *PDU*. Por ejemplo, las WAN basadas en X.25 típicamente emplean un *PDU* con un campo de datos de 128 octetos. Algunas redes permiten cambios mayores o menores en el tamaño del *PDU*. El estándar Ethernet limita el tamaño de un *PDU* a 1500 octetos.

Sin el uso de la fragmentación, un gateway podría atarearse demasiado tratando de ajustar tamaños de *PDUs* incompatibles entre redes. El IP resuelve el problema estableciendo las reglas para la fragmentación en el gateway y reensamblando en el host que recibe

El IP y las Sub-redes

El IP está diseñado para residir en la cima de la subcapa de red de la manera más transparente posible. Esto significa que el IP asume algunas características de las subcapas de red. Desde el punto de vista del diseño ésto es bastante atractivo para los ingenieros ya que ésto mantiene la sub-red relativamente independiente del IP.

Figura 4-2 El modelo IP



Fuente. TCP/IP and Related Protocols

Como es de esperarse, la transparencia es lograda por medio de encapsulación. Los datos enviados por la computadora host son encapsulados dentro de un datagrama del IP. El encabezado del IP identifica la dirección de la computadora host que recibe. El

datagrama y el encabezado del IP son también encapsulados dentro del protocolo específico de tránsito de red. Por ejemplo, un tránsito de red puede ser una red X.25 o una LAN Ethernet.

Después de que el tránsito de red ha entregado el tráfico a un gateway IP, su control de información se desecha. El gateway entonces usa la dirección destino en el encabezado del datagrama para determinar hacia donde rutear el tráfico. Típicamente, éste pasa después el datagrama hacia una sub-red invocando a un protocolo de acceso a la sub-red (por ejemplo, Ethernet en una LAN, y X 25 en una WAN). Este protocolo es utilizado para encapsular el encabezado del datagrama y los datos del usuario dentro de los contenedores que son usados por la sub-red. Este proceso es repetido en cada gateway, y eventualmente el datagrama llega a su destino final, donde es entregado a la estación que recibe.

Debe enfatizarse que un gateway IP no está completamente separado del protocolo de acceso de una sub-red conectada. No hay nada extraordinario acerca del IP, el gateway debe conocer cómo acceder a sus redes conectadas. Consecuentemente, algunas formas de comunicación deben ocurrir entre el gateway y las sub-redes conectadas. El punto importante es que un módulo IP no se preocupa de las operaciones dentro de las redes.

El datagrama IP

Para poder analizar el IP primero se deben examinar los campos en el datagrama IP (PDU).

El campo *version* identifica la versión del IP en uso. La mayoría de los protocolos contienen este campo debido a que algunos nodos de red pueden no tener la última versión disponible del protocolo.

El campo *header lenght* contiene 4 bits de un valor que indica la longitud del encabezado del datagrama. La longitud es medida en palabras de 32 bits. Típicamente, un encabezado sin opciones QOS contiene 20 octetos. Por lo tanto, el valor en el campo es usualmente 5.

El campo *type of service (TOS)* puede ser usado para identificar varias funciones QOS provistas para Internet.

El campo *total length* especifica la longitud total del datagrama del IP. Esta es medida en octetos e incluye la longitud del encabezado y los datos. El IP substrahe el campo *header length* del campo *total length* para calcular el tamaño del campo *data*. La longitud máxima posible de un datagrama es 65,535 octetos.

El protocolo IP utiliza tres campos en la fragmentación y reensamble del datagrama desde el encabezado hasta el control. Estos campos son: *Identificador (identifier)*, *banderas (flags)* y el *desplazamiento de fragmentación (fragmentation offset)*. El campo *identifier* es usado para identificar únicamente a todos los fragmentos de un datagrama original. Este es usado con la dirección origen en el host receptor, para identificar el fragmento. Las *flags* contienen bits para determinar si el datagrama debe ser fragmentado. Si éste puede ser fragmentado, uno de los bits debe ser puesto en el último fragmento del datagrama. El campo *fragmentation offset* contiene un valor, el cual especifica la posición relativa del fragmento en el datagrama original. El valor es inicializado a cero y es subsecuentemente puesto a un número apropiado cuando el gateway fragmenta los datos. El valor es medido en unidades de 8 octetos.

El parámetro *time-to-live (TTL)* es usado para medir el tiempo que un datagrama ha estado en el Internet.

El campo *protocol* es usado para identificar el protocolo del siguiente nivel, el cual va a recibir a el datagrama al final del host destino.

El *header checksum* se utiliza para detectar una distorsión que puede haber ocurrido en el encabezado. Los chequeos no son realizados en los datos del usuario.

El IP lleva dos direcciones en el datagrama. Estas están etiquetadas como *source* y *destination address* y conservan el mismo valor a través de toda la vida del datagrama.

El campo *options* es usado para identificar a varios servicios adicionales. El campo *options* no es utilizado en cada datagrama. La mayoría de las implementaciones usan este campo para administración y diagnósticos de la red.

El campo *padding* puede ser usado para tener la certeza de que el encabezado del datagrama se alinea en un límite exacto de 32 bits

Finalmente, el campo *data* que contiene los datos del usuario. El IP estipula que la combinación del campo *data* y el encabezado no pueden exceder de 65,535 octetos

Tabla 4-2 El Datagrama IP (*n*-no. de bits)

Version (4)	Header Length (4)
Type of Service (8)	
Total Length (16)	
Identifier (16)	
Flags (3)	Fragment Offset (13)
Time to Live (8)	
Protocol (8)	
Header Checksum (16)	
Source Address (32)	
Destination Address (32)	
Options and Padding (variable)	
Data (Variable)	

Fuente: TCP/IP and Related Protocols

Servicios Mayores del IP

Internet header check routine

Cuando un gateway recibe el datagrama, checa el encabezado para determinar el tipo de tráfico que está procesando. Si el tráfico es un datagrama Internet, se pasa el datagrama hacia la rutina de chequeo del encabezado Internet. Este módulo realiza un numero de pruebas de edición y validación en el encabezado del datagrama del IP. Los siguientes chequeos son realizados en el encabezado:

- Longitud del encabezado del IP válida
- Número de versión del IP apropiada
- Longitud del mensaje del IP válida
- Chequeo del encabezado del IP válido
- Validación de que el campo *live* sea diferente de cero

Si los chequeos son realizados y no aprobados, el datagrama es descartado. Si los chequeos son realizados y aprobados, la dirección Internet destino es examinada para determinar (a) si el datagrama está direccionado hacia este gateway, o (b) si el datagrama está destinado para otro gateway. Si no está destinado para este gateway, el datagrama es pasado hacia la rutina de avance del IP para un siguiente ruteo

Ruteo fuente del IP

El IP puede usar un mecanismo llamado *source routing* (*ruteo origen*) como parte de su algoritmo de ruteo. El source routing permite a un protocolo de una capa superior (*ULP - Upper Layer Protocol*) determinar cómo los gateways del IP rutean los datagramas. El ULP tiene la opción de pasar una lista de direcciones de Internet hacia el módulo del IP. La lista contiene los nodos del IP intermedios a ser transitados durante el ruteo de los datagramas al destino final. La última dirección en la lista es el destino final de un nodo intermedio

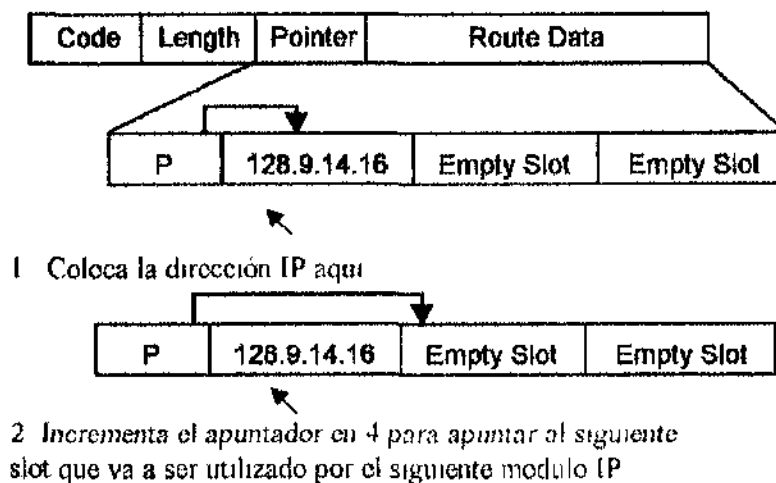
Cuando el IP recibe un datagrama, usa las direcciones en el campo source routing para determinar el siguiente salto intermedio. El IP usa un campo apuntador para aprender acerca de la siguiente dirección IP

Si un chequeo al apuntador y a la longitud del campo indican que la lista ha sido completada, el campo source address IP es usado para el ruteo. Si la lista no está terminada, el módulo IP usa la dirección IP indicada por el apuntador.

El módulo IP entonces reemplaza el valor en la lista *source routing* con su propia dirección. Por supuesto, debe incrementar el apuntador en una dirección (4 bytes) para el siguiente salto y recuperar la siguiente dirección IP en la ruta. Con esto, el datagrama sigue la ruta origen dictada por el ULP y graba la ruta a lo largo del camino

La siguiente gráfica provee un ejemplo del uso del grabado de ruta. En el primer paso, el IP usa el apuntador para localizar la siguiente dirección en el campo *route data* (datos de ruta). En éste ejemplo, localiza la dirección 128.2.3.4 y toma una decisión de ruteo basado en ésta dirección. En el segundo paso, pone su propia dirección en el campo *route data* en la misma localización de la dirección de destino actual. En el tercer paso, incrementa el valor del apuntador para habilitar el siguiente modulo IP para determinar el salto siguiente (o final) en la ruta.

Figura 4-4 Grabación de la Ruta



Fuente: TCP/IP and Related Protocols

Operaciones de ruteo

El gateway IP toma decisiones de ruteo basadas en la lista de ruteo. Si el host destino reside en otra red, el gateway IP debe decidir como rutear hacia la otra red. Ciertamente, si múltiples saltos están involucrados en el proceso de comunicaciones, entonces cada gateway debe ser cruzado y el gateway debe tomar decisiones acerca del ruteo.

Cada gateway mantiene una tabla de ruteo que contiene el siguiente gateway en el camino hacia la red de destino final. Estas tablas pueden ser estáticas o dinámicas, sin embargo las tablas dinámicas son más comunes. El módulo IP toma una decisión de ruteo en todos los datagramas que recibe.

La tabla de ruteo contiene una dirección IP por cada red alcanzable y la dirección de un gateway vecino (esto es, un gateway directamente conectado a esta red). El gateway

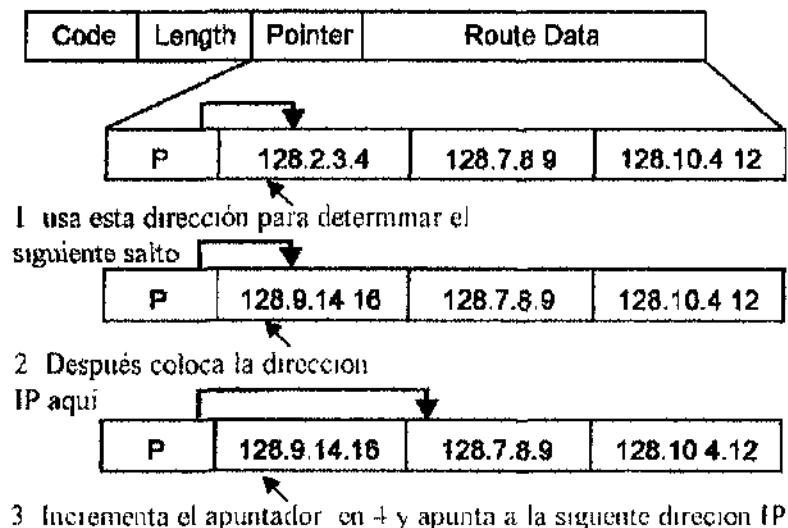
vecino es la ruta más corta hacia la red destino. Es decir, el gateway IP lógico establece que el gateway esté directamente conectado a esta red.

El ruteo IP está basado en un concepto llamado *distancia métrica (distance metric)*. Este valor es usualmente el número menor de saltos entre el gateway y el destino final. El gateway consulta su tabla de ruteo e intenta hacer coincidir la dirección de la red destino contenida en el encabezado del IP con una entrada de red contenida en la tabla de ruteo. Si no se encuentra alguna coincidencia, descarta el datagrama y construye un mensaje ICMP (*Internet Control Message Protocol*) para enviarlo de regreso hacia el origen del IP. Este mensaje podría contener un código de *destino inalcanzable*. Si una coincidencia es encontrada en la tabla de ruteo, el gateway entonces la usa para determinar el puerto de salida.

Ruteo de pérdida

La opción de grabado del ruteo opera de la misma manera que el ruteo de origen, con la característica de grabación. Esto significa que cualquier módulo IP que recibe un datagrama debe adicionar su dirección a una lista de grabación de ruta.

Figura 4-3 Ruteo Fuente (Source Routing)



Para la operación de grabación de ruta, el módulo IP receptor usa los campos *pointer* y *length* para determinar si hay espacio disponible para grabar la ruta. Si la lista de grabación de ruta está llena, el módulo IP simplemente avanza el datagrama sin insertar su dirección. Si no está llena, el apuntador es utilizado para localizar el primer slot de octeto vacío, la dirección es insertada, y el módulo IP entonces incrementa el apuntador hacia el siguiente slot IP.

La opción *timestamp*

Otra opción bastante útil del IP es la provisión de pegado de la hora (*timestamping*) al datagrama conforme cruza cada módulo IP a través del Internet. Esta idea permite a un administrador de red no sólo determinar la ruta del datagrama a través de la red sino también el tiempo en el cual cada módulo IP procesó el datagrama. Esto puede ser bastante útil para determinar la eficiencia de los gateways y los algoritmos de ruteo.

Al igual que las opciones previas, los campos *length* y *pointer* son usados para identificar el slot apropiado, en el cual poner una dirección IP y el timestamp relacionado a ésta dirección. Por lo tanto, el apuntador se incrementa a través de una dirección IP y el timestamp para la dirección. El campo *overflow* se utiliza únicamente cuando un módulo IP no puede registrar un timestamp debido a una falta de recursos o a un campo opción muy pequeño. Este valor es incrementado por cada módulo en el cual se encuentra este problema.

Un campo bandera de 4 bits es usado para proveer una guía a cada módulo IP acerca de las operaciones timestamp. Los valores actualmente establecidos son:

- 0: Timestamps de sólo escritura y almacenados en palabras de 32 bits
- 1: Para cada timestamp precedido por la dirección IP del módulo relevante
- 3: Para las direcciones IP especificadas por el originador cuando el gateway está atareado con el grabado del timestamp en su área de dirección IP relevante.

El tiempo usado con el timestamp está basado en milisegundos (ms) usando el tiempo universal (el viejo meridiano de Greenwich). Obviamente, el uso del tiempo universal no garantiza completamente la exactitud de los timestamps entre máquinas, debido a que los relojes de las máquinas pueden variar ligeramente.

Fragmentación y reensamble

Un datagrama IP puede cruzar a través de varias redes que utilicen diferentes tamaños de *PDU*. Todas las redes tienen un tamaño máximo de *PDU*, llamado la *unidad máxima de transmisión (MTU - Maximum Transmission Unit)*. Por lo tanto, el IP contiene procedimientos para dividir (fragmentar) un datagrama grande en pequeños datagramas. Esto también permite al ULP estipular si la fragmentación debe ocurrir o no. Por supuesto, debe utilizarse un mecanismo de reensamble en el destino final, el cual coloca los fragmentos de vuelta en el orden en que fueron transmitidos originalmente.

Cuando el módulo de un gateway IP recibe un datagrama el cual es demasiado grande para ser transmitido por la sub-red de tránsito, utiliza sus operaciones de fragmentación. Este divide el datagrama en dos o más piezas (con alineación en límites de 8 octetos). Cada una de las piezas fragmentadas tiene colocado un encabezado conteniendo identificación, direccionamiento y todas las opciones pertenecientes al datagrama original. Los paquetes fragmentados además tienen información adherida a ellos definiendo la posición del fragmento dentro del datagrama original, y una indicación de si este fragmento es el último.

El IP maneja cada operación de fragmento independientemente. Esto es, los fragmentos pueden cruzar diferentes gateways hacia su destino final, y pueden estar sujetos a mayores fragmentaciones si pasan a través de redes que usen unidades de datos más pequeñas. El siguiente gateway usa el valor de desplazamiento de los datagramas fragmentados. Si se hacen mayores fragmentaciones en otro gateway, el valor de desplazamiento del fragmento es establecido hacia la colocación en la que este fragmento cabe relativamente en el datagrama original y no en el paquete fragmentado anterior.

¿Existe reensamble en los gateways?

Los gateways sin conexión usando ruteo dinámico (tal como el IP) no reensamblan datagramas. La tarea es imposible porque todos los fragmentos pertenecientes al datagrama original pueden no ser procesados por los mismos gateways. Como consecuencia, el gateway no conoce cómo calcular los valores de desplazamiento para fragmentos que no recibe. En contraste, los gateways orientados a la conexión pueden realizar reensamble intermedio ya que por la naturaleza del sistema, todos los PDUs pasan a través del mismo gateway.

Se asume que los fragmentos descartados son retransmitidos por un protocolo de una capa más alta. El tráfico es fragmentado (nuevamente) por el originador y enviado hacia el receptor. Sin embargo, debe evitarse enfocar al IP hacia las características orientadas hacia la conexión.

Tablas de Dirección y Ruteo del IP

Tabla de dirección

La Tabla de Actividades Internet (*IAB - Internet Activities Board*) ha publicado en el RFC 1213 la definición para la tabla de direcciones IP. Esta consta de cinco columnas y de 1 a n renglones. Cada renglón pertenece a una dirección IP de una entidad (un host, un gateway, etc.). Puede haber más de un renglón si la máquina tiene más de una dirección IP. Los contenidos de esta tabla son los siguientes:

El *Entry Address* contiene la dirección IP para la interface de la entrada. El *Entry If Index* contiene el número de interface (número de puerto) perteneciente a esta conexión de la entidad hacia una sub-red. La columna *Entry Net Mask* contiene la máscara de la sub-red asociada con la dirección IP en la columna entry address. El *Broadcast Address* contiene un valor para el bit menos significativo en la dirección broadcast IP. Este es usado para el envío de datagramas en la interface local y está asociado con la dirección IP de éste renglón. El *Maximum Size of Datagram* representa el tamaño máximo de un datagrama que puede ser procesado por este módulo IP.

Tabla 4-3 Tabla de direcciones IP

	Entity Address	Entity If Index	Entity Net Mask	Broadcast Address	Maximum Size of Datagram
Address Entity 1					
Address Entity 2					
Address Entity n					

Fuente: TCP/IP and Related Protocols

Tabla de ruteo

Hasta 1990, una tabla de ruteo IP era diseñada en base a una percepción individual de un proveedor. Con la publicación de la Base de Información de Administración de Internet (*MIB - Management Information Base*), una definición más formal de la tabla de ruteo IP está disponible ahora. Cada renglón de la tabla de ruteo IP contiene una entrada para cada ruta conocida, para que el módulo IP almacene esta tabla. Las columnas representan la información disponible en cada ruta. Una breve descripción de cada columna es la siguiente:

La entrada *Destination* contiene la dirección IP del destino de esta ruta. Si esta columna es codificada como 0.0.0.0, la ruta es considerada una ruta por defecto.

La entrada *IfIndex* contiene el índice de la interface. Este identifica la interface local (más comúnmente conocida como un puerto físico) a través de la cual el siguiente salto en la ruta puede ser alcanzado.

Las siguientes cinco columnas están etiquetadas como *Metric*. Las entradas *Metric* contienen información acerca de la medida del costo usada para determinar la ruta. Con la mayoría de los sistemas, la *medida del costo* es el número de saltos para alcanzar el destino. De cualquier forma, con la evolución de protocolos descubridores de rutas más sofisticados, es posible que más de una medida de costo pueda ser usada para calcular una ruta. Como la tabla indica, pueden ser almacenadas hasta cinco medidas de costo.

La entrada *Next Hop* contiene la dirección IP identificando el siguiente salto para esta ruta. La siguiente columna en la tabla es el *Route Type*. Aquí se establece uno de cuatro valores para proveer la siguiente información:

- 1 : Ninguno de los siguientes
- 2 : Una ruta inválida
- 3 : Una ruta o sub-ruta directamente conectada
- 4 : Indirecta (una conexión indirecta para alcanzar este destino).

La siguiente columna está etiquetada como *Routing Protocol*. Esta entrada identifica el protocolo que define las rutas. La columna *Route Age* es un valor, en segundos, desde que la ruta fue actualizada o verificada.

El siguiente campo en la tabla contiene la *Route Mask* (Máscara de Ruta) para la ruta actual. Esta máscara es un AND lógico con la dirección destino en el datagrama IP antes de ser comparado con la columna 1 en esta tabla (etiquetada como *Destination*).

La última columna, etiquetada *Route Information*, permite una referencia a una definición *MIB* perteneciente a un protocolo particular de ruteo. Su valor depende del tipo de protocolo de ruteo utilizado en este renglón de entrada.

Tabla 4-4 Tabla de Ruteo IP

	Destination	If Index	Metric 1	Metric 5	Next hob	Route Type	Routing Protocol	Route Age	Routing Mask	Route Information
Route 1										
Route 2										
Route 3										
Route n										

Fuente: TCP/IP and Related Protocols

He aquí un ejemplo de los valores con los cuales podría llenarse la tabla

Destination	= 14 0 0.0
Interface (port) Index	= 3
Metric 1	= número de saltos (las columnas metric restantes están vacías)
Next Hop	= 13.0.0.2
Route Type	= indirect (4)
Routing Protocol	= egp (5)
Route Age	= 5 seconds
Route Mask	= several options
Route Information	= value that depends on routing protocol entry

Definiciones y primitivas del Servicio IP

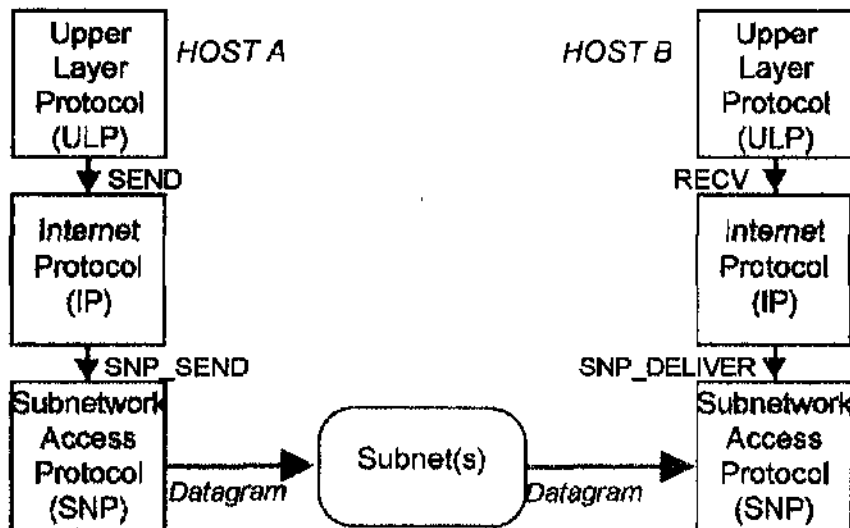
Primitivas UP/ULP

El IP usa dos primitivas para definir los servicios que provee al ULP (*Upper Layer Protocol*) adyacente. El ULP transmitiendo utiliza la primitiva *SEND* (enviar) para solicitar los servicios del IP. En cambio, el IP usa la primitiva *DELIVER* (entrega) para notificar al ULP destino el arribo de información. La interface del IP con la capa superior es simple, debido a que el IP está diseñado para operar con diversos ULPs.

Estas definiciones de servicio (implementadas con primitivas) son de alguna manera algo abstractas para permitir que sean modificadas para el sistema operativo de un host específico. Por ejemplo, los servicios *SEND* y *RCV* en un sistema basado en UNIX pueden ser implementados con llamadas a las librerías del sistema UNIX.

La relación del IP y el ULP se muestra en la siguiente figura, la cual representa al host A enviando información al host B. Las flechas se invierten si el host B envía información al host A.

Tabla 4-5 Las Primitivas IP



Fuente: TCP/IP and Related Protocols

Los parámetros asociados con las primitivas informan al IP y al ULP acerca de la operación solicitada desde el ULP (SEND) y la realizada por el IP (RECV).

Los parámetros SEND también son usados para crear el encabezado IP. Consecuentemente, ellos se correlacionan con los campos del encabezado IP de un datagrama transmitido, mostrado en la gráfica anterior. De la misma manera, los parámetros en la primitiva RECV se correlacionan con los parámetros del datagrama recibido.

Primitivas IP/SNP

Las primitivas entre el IP y el protocolo de acceso a la sub-red (*SNAP - Subnetwork Access Protocol*) son similares a las primitivas del IP/ULP. Las operaciones del IP/SNP invocan dos primitivas. La primitiva SNP_SEND es usada por el IP para invocar a un servicio del SNP; la primitiva SND_DELIVER es usada por el SNP para entregar un datagrama al módulo IP. La primitiva SNP_SEND contiene la siguiente información.

- *Local destination address*: Dirección de la sub-red destino
- *TOS indicators*: precedencia, confiabilidad, demora y traspaso
- *Length of datagram*
- *The datagram*

La primitiva SNP_DELIVER contiene los indicadores del datagrama y de error (éste último es opcional y no está definido en el estándar).

Primitivas de la capa de red/LLC

Las primitivas IP/SNP explicadas anteriormente no están diseñadas para la interface de Control de Enlace Lógico (*LLC - Logical Link Control*). De cualquier forma, si una implementación sólo hace uso del servicio de transferencia de datos sin conexión del LLC, la interface es simple.

Dos primitivas son usadas para transferir datos sin conexiones. Ellas transmiten entre el LLC y su protocolo de la capa superior ULP (el cual puede ser el IP o algún otro módulo). Estas dos primitivas son.

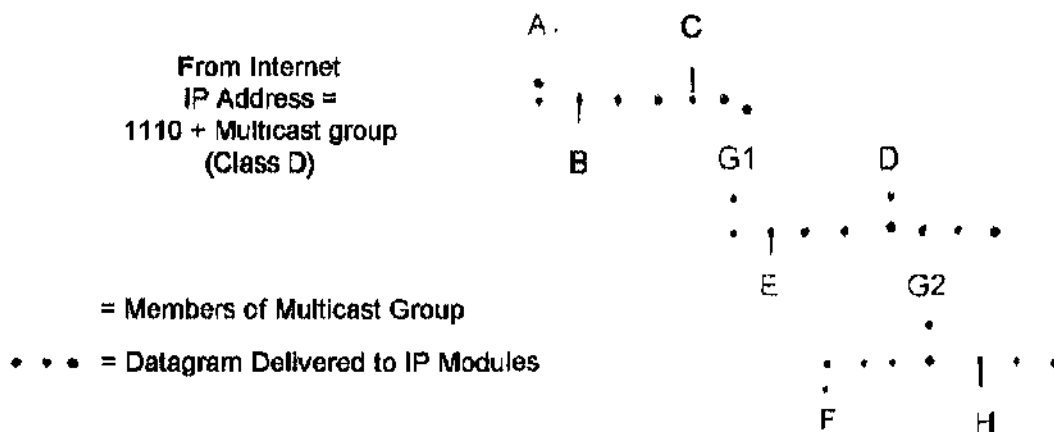
- *DL-UNITDATA.request* (dirección origen, dirección destino, datos, prioridad)
- *DL-UNITDATA.indication* (dirección origen, dirección destino, datos, prioridad)

La primitiva *request* es pasada desde la capa de red hacia el LLC para solicitar que una unidad de datos del servicio de enlace (*LSDU - Link Service Data Unit*) sea enviada hacia un punto de acceso de servicio remoto de enlace. Los parámetros de dirección son equivalentes a una combinación del LLC SAP y las direcciones *MAC (Media Access Control)*. El campo prioridad es pasado al MAC e implementado (excepto para el 802.3, el cual no tiene mecanismo de prioridad). La primitiva *indication* es pasada desde el LLC hacia la capa de red para indicar el arribo de una *LSDU* desde una entidad remota.

Multicasting

Al igual que la capa Física, la capa de Red Internet permite el uso de PDUs *multicasting* (multidestinos). El concepto es similar a las LAN multicasting, en las cuales un sólo *PDU* (en este caso un datagrama IP) es enviado a más de un host. El conjunto de hosts forman un grupo multicast. El IP multicasting permite a los host operar en una o múltiples redes físicas. Un host debe pertenecer a más de un grupo multicast y a un grupo multicast permanente, o debe dinámicamente entrar y salir de grupos según las necesidades. Además, un host no tiene un miembro del grupo multicast para enviar datos hacia el grupo. El multicasting es completado a través del uso de la dirección del IP clase D. La siguiente gráfica muestra cómo opera el multicasting del IP. El Gateway 1 (G) recibe un datagrama IP de otra parte de una Internet. El gateway es responsable de interpretar las direcciones multicast y avanzar hacia el host apropiado y hacia otros gateways participantes multicast. En este ejemplo, los hosts A, C, y E son miembros del mismo grupo multicast. Los host G2 y F son también miembros.

Tabla 4-5 Operaciones Multicasting



Fuente: TCP/IP and Related Protocols

Protocolo de Administración de Grupo Internet

El Internet Group Management Protocol (IGMP) permite a los gateways y hosts informarse a uno y otro acerca de las operaciones multicasting, tales como conectarse o salir de grupos multicast. Adicionalmente, permite a las máquinas comunicar mensajes de status acerca de la información multicast. El *IGMP* trabaja de forma similar al Protocolo de Control de Mensajes Internet (ICMP). Un datagrama IP es usado para transportar el mensaje IGMP entre las máquinas.

El IGMP tiene algunas similitudes con el protocolo de LAN token bus, en cómo una máquina es adicionada como un miembro a un grupo. Primero, cuando un host desea unirse a un grupo multicast, éste debe enviar un mensaje (tal como, en un token bus, una estación de LAN envía un conjunto de mensajes solicitantes). Este mensaje es una dirección multicast de todos los host en la cual el host establece que es un miembro de un grupo multicast. El mensaje IGMP es recibido por el gateway local multicast que realiza las operaciones necesarias para rutear el tráfico hacia otros gateways multicast a través de un Internet.

Una vez que esas operaciones han sido realizadas, el gateway multicast debe periódicamente preguntar al host para determinar si dicho host sigue siendo miembro de un grupo. Si la pregunta no obtiene una respuesta del host, entonces el gateway multicast es requerido para detener los mensajes para ese host hacia otros gateways multicast.

El formato para el mensaje IGMP es simple y se ilustra en las siguiente gráfica. El mensaje consiste de cinco campos:

- El campo *version* proporciona la versión actual del protocolo, la cual hasta el momento es 1.
- El campo *type* identifica el campo como una pregunta con un valor de 1 o a una respuesta con un valor de 2.
- Lógicamente el campo *unused* no se utiliza.
- El campo *checksum* es usado para checar si hay errores.
- El cálculo usa el mismo algoritmo de los protocolos IP y TCP.
- El campo *group address* contiene la dirección del grupo para que los hosts reporten su membresía en el grupo multicast. Este campo no tiene significado para un mensaje de pregunta

Tabla 4-5 Formato del mensaje IGMP

Version (4)
Type (4)
Unused (8)
Checksum (8)
Group Address (32)

Fuente: TCP/IP and Related Protocols

Servicios del Protocolo de Control de Transmisión (TCP)

Anteriormente se mencionó que el Protocolo Internet (IP) no está diseñado para recuperarse de ciertos problemas, o no garantiza la entrega de tráfico. El IP está diseñado para descartar datagramas que no están actualizados o que han excedido el número de saltos de tránsito permisibles en una Internet.

Ciertas aplicaciones del usuario requieren asegurarse de que todos los datagramas han sido entregados a salvo en su destino. Además, el usuario que transmite puede necesitar saber que el tráfico ha sido entregado al host receptor. El mecanismo para lograr estos servicios importantes reside en el Protocolo de Control de Transmisión (TCP/ Transmission Control Protocol).

El trabajo del TCP puede ser complejo. Debe ser capaz de satisfacer un amplio rango de requerimientos de aplicaciones, igualmente importante es que debe ser capaz de adaptarse a un ambiente dinámico dentro de una Internet. Debe establecer y administrar sesiones (asociaciones lógicas) entre sus usuarios locales y remotos.

Panorama de TCP

El TCP reside en la capa de transporte (del modelo convencional de siete capas) y está situado sobre el IP y debajo de las capas superiores. TCP está diseñado para residir en la computadora host o en una máquina que está atareada con la integridad end-to-end (punto a punto) de la transferencia de la información del usuario. En la práctica, el TCP es usualmente puesto en la máquina host del usuario.

TCP está diseñado para correr sobre el IP. Debido a que el IP es una red sin conexión, las tareas de confiabilidad, control de flujo, secuencio, abrir, y cerrar son dadas al TCP. De hecho el TCP y el IP están tan unidos que son usados en el mismo contexto "TCP/IP", el TCP además soporta otros protocolos. Por ejemplo, otro protocolo sin conexión, tal como el ISO 8473 (*Connectionless Network Protocol* - CLNP), podría operar con TCP (con ajustes hacia la interface entre los módulos). En adición, los protocolos de aplicación, tal como el Protocolo de Transferencia de Archivos (*File Transfer Protocol* - FTP) y el Protocolo de Transferencia de Correo Simple (*Simple Mail Transfer Protocol* - SMTP), dependen en mucho de los servicios del TCP.

Muchos de las funciones del TCP (tal como el control de flujo, confiabilidad, y secuencio) podrían ser manejados dentro de un programa de aplicación. Más aún, los programadores de aplicaciones no están usualmente familiarizados con la detección de errores y operaciones de flujo de control. El alcance preferido es desarrollar software generalizado que provee funciones comunitarias aplicables a un amplio rango de aplicaciones, y luego invocan esos programas desde el software de aplicación. Esto permite al programador de aplicaciones concentrarse en resolver el problema de la aplicación y separar al programador de los cambios y problemas de las redes.

Características mayores del TCP

El TCP provee los siguientes servicios a las capas superiores:

- Administración de datos orientada a la conexión
- Transferencia de datos confiable
- Transferencia de datos orientada al stream
- Funciones *push*
- Resecuencio
- Control de flujo (ventanas deslizantes)
- Multiplexamiento
- Transmisión full duplex
- Precedencia y seguridad
- Cerrado cuidadoso (*graceful close*)

TCP es un protocolo *orientado a la conexión*. Este término se refiere al hecho de que TCP mantiene información del estado de cada stream de datos del usuario fluyendo dentro

y fuera del módulo TCP. El término utilizado en este contexto además, significa que TCP es responsable de la transferencia de datos end-to-end a través de una red o múltiples redes hacia una aplicación receptora (o el siguiente protocolo de la capa superior). El TCP debe asegurarse que los datos son transmitidos y recibidos entre los dos hosts a través de varias redes.

Debido a que TCP es un protocolo orientado a la conexión, es responsable por la *transferencia confiable* de cada uno de los caracteres pasados a él desde una capa superior (los caracteres son llamados también bytes u octetos). Consecuentemente, éste usa secuencias de números y códigos de reconocimiento (acknowledgments). El término asociado con estos aspectos de un protocolo orientado a la conexión es un *circuito virtual* (*virtual circuit*).

Un número de secuencia es asignado a cada octeto transmitido. El módulo receptor TCP usa una rutina checksum para checar si los datos fueron dañados durante el proceso de transmisión. Si los datos son aceptables, TCP regresa un acknowledgment positivo (ACK) hacia el módulo TCP emisor. Si los datos están dañados, el TCP receptor descarta los datos y usa el número de secuencia para informar al TCP emisor acerca del problema. Como muchos otros protocolos orientados a la conexión, el TCP se asegura de que el lapso de tiempo no sea excesivo antes de que las medidas correctivas sean tomadas, ya sea para la transmisión de acknowledgments desde el lugar receptor y/o la retransmisión de los datos en el lugar de transmisión.

TCP recibe los datos desde un protocolo de una capa superior (Upper Layer Protocol ULP) en una forma *orientada al stream*. Esta operación está en contraste a muchos protocolos en la industria. Los protocolos orientados al stream están diseñados para enviar caracteres individuales y no bloques, frames, datagramas, etc. Los bytes son enviados desde un ULP basado en un stream, byte por byte. Cuando arriban a la capa del TCP, los bytes son agrupados dentro de segmentos de TCP. Estos segmentos son pasados al IP (o a otro protocolo de capa inferior) para su transmisión hacia el siguiente destino. La longitud de los segmentos es determinada por el TCP, sin embargo un sistema implementador puede además determinar como TCP toma esta decisión.

Los implementadores de TCP, quienes han trabajado con sistemas orientados al bloque, tal como los sistemas operativos de IBM, tienen que hacer algunos ajustes en sus pensamientos concernientes al desempeño del TCP. TCP permite el uso de segmentos de longitud variable debido a su naturaleza orientada al stream. Por lo tanto, las aplicaciones que normalmente trabajan con bloques modificados de datos no pueden confiar en el TCP para presentar este bloque modificado al receptor. Algunas acciones deben ser tomadas en el nivel de aplicación para delinear los bloques dentro de los streams de TCP.

TCP además chequea si hay datos duplicados. En el evento en que el emisor TCP retransmite los datos, el TCP receptor descarta los datos redundantes. Los datos redundantes deben ser introducidos dentro de una Internet cuando la entidad TCP receptora no reconozca el tráfico de una manera oportuna, en tal caso la entidad TCP emisora retransmite los datos.

"En armonía con la capacidad de transferencia de streams, TCP además soporta el concepto de una función *push*. Esta operación es usada cuando una aplicación quiere tener la certeza de que todos los datos que han pasado hacia la capa inferior TCP han sido transmitidos. Haciendo esto, gobierna la administración del buffer de TCP. Para obtener esta función, el ULP usa un comando *send* hacia TCP con un parámetro *push* establecido a 1. La operación requiere a TCP para dirigir todo el tráfico almacenado en el buffer en la forma de un segmento o de segmentos hacia el destino" [4 pág. 263]

En adición al uso de números de secuencia para el reconocimiento, TCP los usa para *resecuenciar* los segmentos si arriban al destino final fuera de orden. Debido a que TCP descansa sobre un sistema sin conexión, es posible que datagramas duplicados puedan ser creados en una Internet. TCP además elimina segmentos duplicados.

El módulo TCP del receptor, es además capaz de *controlar el flujo* de los datos del emisor, lo cual es una herramienta muy útil para prevenir la sobrecarga del buffer y una posible saturación de la máquina receptora. El concepto usado con TCP es de alguna manera inusual entre los protocolos de comunicación. El transmisor tiene permitido enviar un número especificado de bytes dentro de una ventana de salida, después de lo cual la ventana debe ser cerrada y el transmisor debe detener el envío de datos.

TCP además tiene una facilidad muy útil para multiplexar varias sesiones de usuarios dentro de una sola computadora host sobre los ULPs. Esto está acompañado a través de algunas simples convenciones de nombres para puertos y sockets en los módulos TCP e IP. TCP provee una transmisión *full duplex* entre dos entidades TCP. Esto permite transmisiones en dos sentidos simultáneas sin tener que esperar por una señal de retorno, lo cual es requerido en una situación *half duplex*.

TCP además provee al usuario con la capacidad de especificar niveles de *seguridad* y *precedencia* (nivel de prioridad) para la conexión. Sin embargo, estas características no están implementadas en todos los productos TCP, sino que ellas están definidas en el estándar TCP.

TCP provee un cerrado cuidadoso a un circuito virtual (la conexión lógica entre dos usuarios). Un cerrado cuidadoso se asegura que todo el tráfico ha sido reconocido antes de que el circuito virtual sea removido.

Puertos y Sockets

El TCP de la capa superior de un usuario en una computadora host es identificado por un *puerto de dirección* (*port address*). El puerto de dirección está concatenado con la dirección Internet del IP para formar un *socket*. Esta dirección debe ser única a través de la Internet. Un par de sockets únicamente identifican cada punto final de la conexión. Por ejemplo:

Socket del emisor = dirección IP origen + número de puerto origen

Socket del receptor = dirección IP destino + número de puerto destino

Sin embargo el mapeo de puertos hacia procesos de capas superiores pueden ser manejadas internamente en un host, la Internet publica números y valores para procesos de capas superiores frecuentemente usados.

Aperturas Pasivas y Activas

Dos formas de establecimiento de conexión son permitidas con puertos TCP. El modo de *apertura pasiva* permite al ULP (por ejemplo, un servidor) decirle al TCP y al sistema operativo del host que espere el arribo de solicitudes de conexión desde el sistema remoto en lugar de sacar una apertura activa. Una vez recibida esta solicitud, el sistema operativo

del host asigna un número de puerto a esta orilla. Esta característica podría ser usada para acomodar comunicaciones de usuarios remotos sin ir a través de la espera de una apertura activa.

Los procesos de las aplicaciones solicitando la apertura pasiva deben aceptar una solicitud de conexión de cualquier usuario. Si cualquier llamada puede ser aceptada, el número del socket foráneo es puesto en ceros. Sockets foráneos no especificados son permitidos sólo en aperturas pasivas.

La segunda forma de establecimiento de conexión es el modo de *apertura activa*. En esta situación, el ULP específicamente designa otro socket a través del cual una conexión será establecida. Típicamente, la apertura activa es dada a una apertura pasiva para establecer un circuito virtual.

TCP soporta un escenario en el cual dos aperturas activas son dadas al mismo tiempo de una a la otra. TCP hará la conexión. Esta característica permite a las aplicaciones realizar una apertura en cualquier momento sin importar que otra aplicación haya realizado una apertura

TCP provee convenciones estrictas de cómo las aperturas pasivas y activas deben ser usadas juntas. Primero, una apertura activa identifica un socket específico tan bien como su precedencia y niveles de seguridad dados. TCP otorga una apertura si el socket remoto tiene una apertura pasiva coincidente o si ha sacado una apertura activa coincidente. Mas aún, TCP define dos tipos de apertura pasivas:

Aperturas pasivas totalmente especificadas. La dirección destino en la apertura pasiva y en la activa son las mismas. Por lo tanto, la operación de la apertura pasiva local tiene totalmente especificado el socket foráneo. Además, el parámetro de seguridad en la apertura activa está dentro del rango del parámetro de seguridad de la apertura pasiva.

Apertura pasiva no especificada. Las direcciones no necesitan coincidir, pero el parámetro de seguridad debería estar dentro de un rango aceptable

El Bloque de Control de Transmisión

Debido a que el TCP debe recordar varias cosas acerca de cada conexión virtual, éste almacena la información en un Bloque de Control de Transmisión (*Transmission Control Block - TCB*). Entre las entradas almacenadas en el TCB están los números locales y remotos, apuntadores para enviar y recibir buffers, apuntadores hacia la cola de retransmisión, los niveles de seguridad y precedencia para la conexión, y el segmento actual. El TCB además contiene varias variables asociadas con el número de secuencia de envío y recepción.

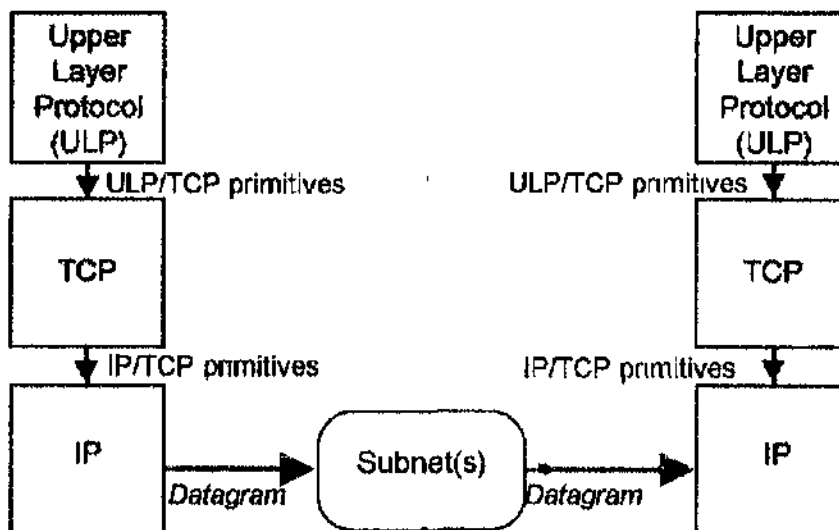
Operaciones de Retransmisión

TCP tiene una forma única de conteo de tráfico en cada conexión virtual. A diferencia de otros protocolos, no tiene un *reconocimiento negativo* (*negative acknowledgment - NAK*). En vez de eso, confía en la entidad de transmisión para sacar una señal de tiempo terminado y retransmitir datos para los cuales no ha recibido un reconocimiento positivo.

TCP y las interfaces del usuario

TCP trabaja con el concepto/definición de servicio hacia una interface con un usuario de una capa superior. La interface es lograda con varios comandos y mensajes.

Tabla 4-6 Relación entre UPL, TCP e IP



Fuente: TCP/IP and Related Protocols

Las definiciones del servicio entre TCP y su capa inferior no están especificadas en el estándar TCP. TCP espera que la capa inferior especifique esta interface. Esta interface (de la capa inferior) está definida en la especificación IP.

Consideraciones en el uso de TCP

Como se ha visto, el stream de datos del TCP es reconocido por el receptor basado en bytes (no en PDUs). El número de reconocimiento, regresado por el receptor, se refiere al byte más alto en stream de datos que ha sido recibido. El software de TCP emisor guarda una copia de los datos hasta que han sido reconocidos. Una vez reconocidos, apaga un reloj de retransmisión y borra la copia del segmento de una cola de retransmisión. Si es necesario, retransmitirá datos perdidos o con errores.

Capítulo V. UNIX

Dado el objetivo principal de este trabajo que es el de mostrar que el sistema operativo UNIX es el sistema operativo más viable para ser base de la implementación de sistemas abiertos, se presentan en este capítulo los conceptos básicos y fundamentales que hacen de UNIX el sistema operativo líder para la interconectividad de sistemas pertenecientes a distintas plataformas.

Introducción

El Right-sizing y los sistemas abiertos son dos términos de los que actualmente se habla mucho en la industria de cómputo de hoy. Su uso, de alguna manera, indica un cambio mayor en la forma en la cual negocios e individuos direccionan y administran sus necesidades de procesamiento de datos.

Históricamente el procesamiento de datos fue originalmente manejado en grandes sistemas de cómputo llamados mainframes. Estos sistemas evolucionaron para proveer un sistema centralizado que manejara grandes cantidades de usuarios. El ambiente de los mainframes era estable, seguro y capaz de soportar grandes aplicaciones críticas de negocios y bases de datos masivas. Esto era caro, no amigable y atrapaba a los usuarios dentro de un producto propietario, haciendo más caro el cambiar hacia una solución perteneciente a otra compañía.

Los 80s trajeron consigo a la computadora personal. En muchas formas ésta fue la antítesis de los mainframes. Ésta era relativamente fácil de usar, barata, y había disponibles sistemas compatibles provenientes de una amplia variedad de proveedores, una solución abierta. Las mejoras continuas en el microprocesador y la tecnología del sistema operativo han creado dos oportunidades significativas en el mercado de hoy.

- Un desplazamiento hacia las soluciones de cómputo distribuido, lo cual permite transportar aplicaciones desde los mainframes y minicomputadoras hacia las redes de PCs.

- Actualizarse desde un sistema operativo tradicional de PC hacia sistemas operativos avanzados de propósito general, para proveer sistemas más capaces para los negocios.

Estas tendencias han creado una gran oportunidad de mercado para productos que pueden proveer capacidades de sistemas avanzados, operar en las plataformas estándar de hardware de la industria, soportar tecnología de punta para redes, y proveer de una amplia variedad de aplicaciones de software fáciles de usar y administrar.

Sistemas operativos de 32 bits

Abundan las aplicaciones para DOS y Windows, relativamente baratas que satisfacen las necesidades del usuario. Sin embargo, DOS y Windows son entornos operativos de 16 bits que no aprovechan los procesadores de 32 bits dentro de los sistemas. Ni DOS ni Windows proveen una operación de modo protegido, un modelo de memoria plana, multitareas reales o apoyo para múltiples hilos de ejecución (Windows 95 promete proveer todo lo anterior, pero aún no está terminado). Desde hace tiempo existen muchas alternativas para superar estas limitaciones, pero éstas son famosas por su falta de estabilidad, específicamente en Windows, o muy exclusivas.

Características de los sistemas operativos de 32 bits

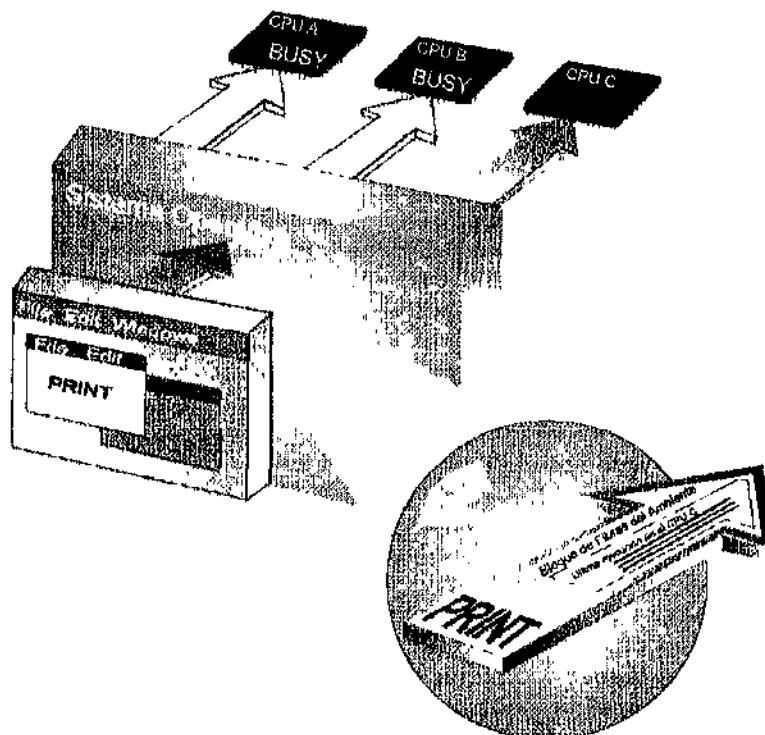
Los sistemas operativos de 32 bits ofrecen características que aprovechan la verdadera potencia de los altamente evolucionados procesadores de Intel. Una de las más importantes es la *operación en modo protegido*. Esta es la habilidad del sistema operativo de aprovechar el esquema de protección del hardware incluido en los procesadores de Intel desde el 80286. El sistema operativo implementa una serie de reglas de protección que impiden que los programas del usuario interfieran con los elementos importantes del sistema. Por ejemplo, cuando una aplicación se traba ésta no puede afectar al sistema operativo.

Los sistemas operativos de 32 bits también administran la memoria de una manera más simple y efectiva que DOS. El acceso a la memoria ocurre en un modelo "plano", un espacio unificado de 4 GB. Así se eliminan los problemas con la memoria alta, la memoria extendida, la memoria expandida, los administradores de memoria añadidos y todas las vicisitudes que han sufrido los programadores y los usuarios durante años.

Otra característica estándar de todos los sistemas operativos de 32 bits, es la habilidad de realizar *multitareas con prioridad*. Un planificador del sistema operativo es responsable de dividir el tiempo del procesador entre todas las tareas que el sistema operativo necesita manejar. Este sistema equitativo contrasta con las multitareas cooperativas de Windows 3.1 donde la propia aplicación es responsable de devolver el control. Obviamente, una aplicación que no devuelva el control puede parar todo el sistema.

"Los *múltiples hilos de ejecución* son otra ventaja importante de los entornos operativos de 32 bits. Las aplicaciones están escritas en hilos, definidos como las unidades más pequeñas de código ejecutable independiente. El sistema operativo puede operar con multitareas a nivel de hilos para que las aplicaciones puedan trabajar con varias tareas independientemente. Los hilos de ejecución pueden mejorar significativamente el rendimiento de los servidores de bases de datos y otras aplicaciones de peso" [7:pág. 99].

Figura 5-1 Los hilos de ejecución y el multiprocesamiento de los sistemas operativos de 32 bits

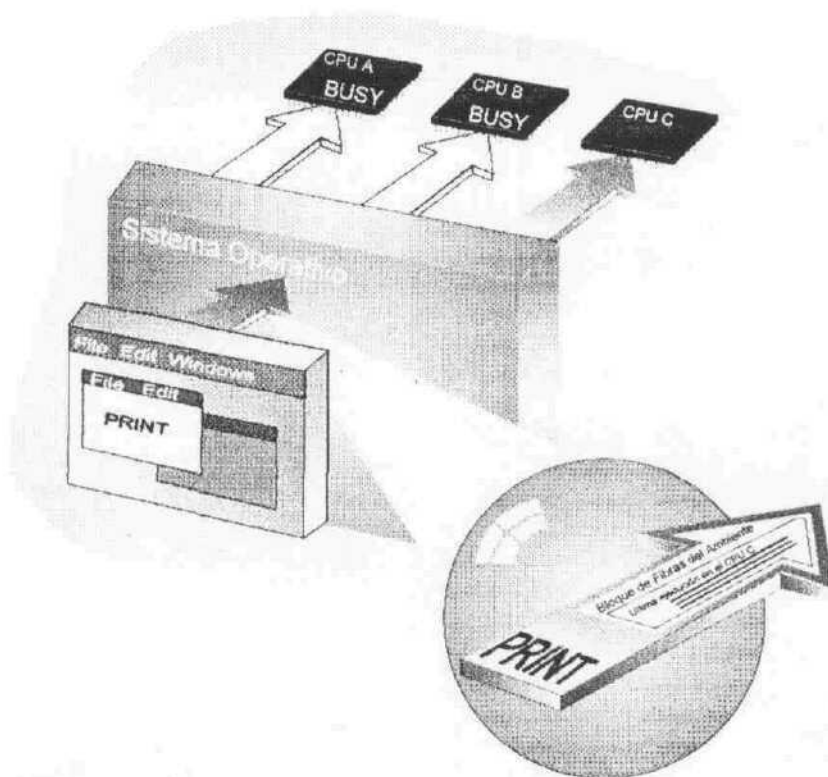


Fuente: PC Computing

Otra característica estándar de todos los sistemas operativos de 32 bits, es la habilidad de realizar *multitareas con prioridad*. Un planificador del sistema operativo es responsable de dividir el tiempo del procesador entre todas las tareas que el sistema operativo necesita manejar. Este sistema equitativo contrasta con las multitareas cooperativas de Windows 3.1 donde la propia aplicación es responsable de devolver el control. Obviamente, una aplicación que no devuelva el control puede parar todo el sistema.

"Los *múltiples hilos de ejecución* son otra ventaja importante de los entornos operativos de 32 bits. Las aplicaciones están escritas en hilos, definidos como las unidades más pequeñas de código ejecutable independiente. El sistema operativo puede operar con multitareas a nivel de hilos para que las aplicaciones puedan trabajar con varias tareas independientemente. Los hilos de ejecución pueden mejorar significativamente el rendimiento de los servidores de bases de datos y otras aplicaciones de peso" [7: pág. 99].

Figura 5-1 Los hilos de ejecución y el multiprocesamiento de los sistemas operativos de 32 bits



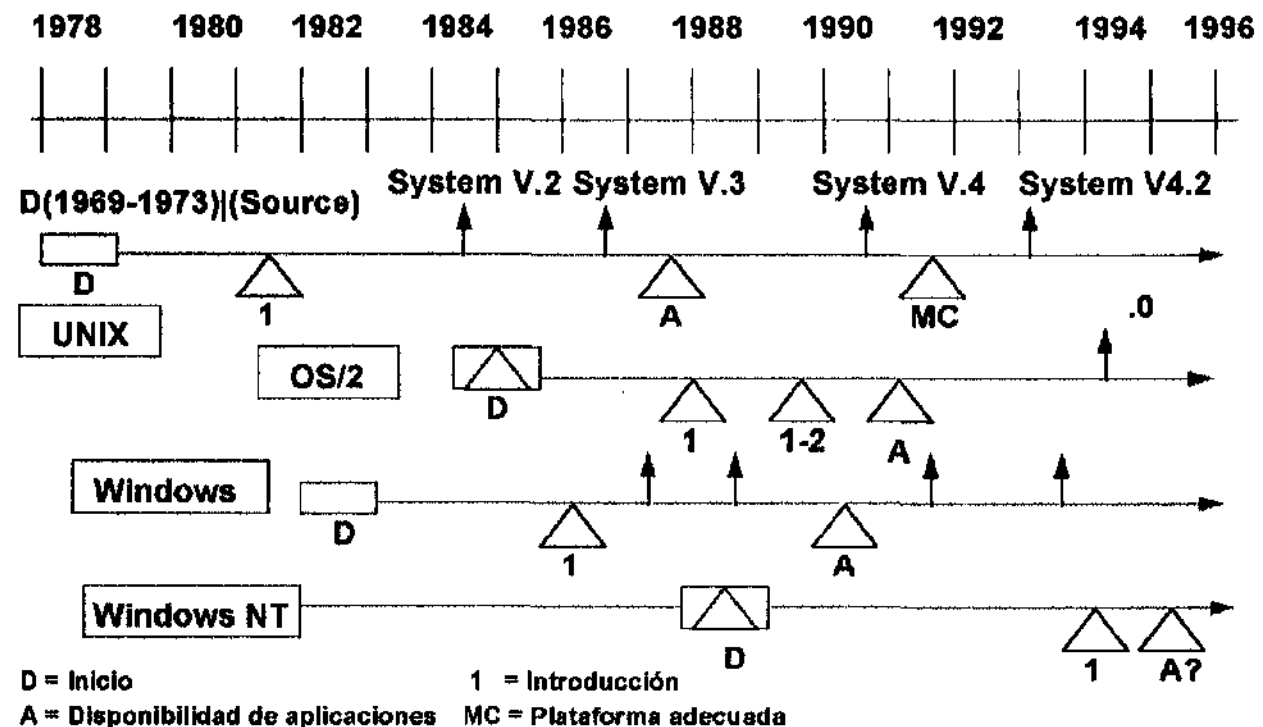
Fuente: PC Computing

Muchos sistemas operativos de 32 bits también apoyan al "multiprocesamiento simétrico", la habilidad del sistema operativo de trabajar con más de un procesador en la misma computadora. El sistema operativo realiza esta función dividiendo los hilos de ejecución dentro de los procesadores que tenga disponibles. Cuando aumentan sus necesidades de procesamiento, simplemente puede añadir otro procesador" [19:pág. 116].

Por último estos sistemas frecuentemente se pueden transportar a otras arquitecturas de procesadores. Las corporaciones pueden considerar importante usar un sólo sistema operativo en sistemas de Alpha, Intel, MIPS, SPARC y muy pronto, POWERPC. Muchos de los sistemas operativos actualmente residen en varias plataformas de hardware

La siguiente figura muestra el ciclo de vida de algunos sistemas operativos de 32 bits que actualmente se encuentran disponibles en el mercado. La figura contempla el inicio y desarrollo de cada uno de estos sistemas operativos

Figura 5-2 Ciclo de vida de los sistemas operativos de 32 bits



Fuente: UNIX Marketing Course

Análisis comparativo

La familia de productos UNIX esta enfocada principalmente a solventar los requerimientos de la empresa a menudo asociados con los esfuerzos down-sizing o righth-sizing. Al realizar la comparación de UNIX contra otros productos alternativos, estos productos han sido evaluados de acuerdo a la solución que proveen en áreas clave incluyendo:

- Conectividad hacia un ambiente NetWare existente y/o integración en un ambiente NetWare.
- Poderosas aplicaciones de servidor a nivel empresa para clientes de red
- Clientes poderosos ejecutando aplicaciones críticas
- Conectividad hacia otros sistemas UNIX.
- Conectividad hacia host u otras redes y servicios corporativos.
- Sistema operativo maduro y estable basado en la tecnología estándar de la industria.

Alternativas

Varias compañías ofrecen el sistema operativo UNIX en estaciones de trabajo basadas en Intel. "UnixWare es muy similar al Open Desktop de SCO (ODT) y al Solaris 2.0 de SunSoft, los tres productos son verdaderas soluciones de 32 bits basadas en UNIX para los microprocesadores Intel. La integración con NetWare, el journaling file system y lo último en la tecnología UNIX (estándar), distingue a UnixWare de los dos, el ODT y Solaris" [13:pág. 25].

Windows NT y OS/2 son ambos sistemas propietarios no Unix los cuales tienen o prometen capacidades similares de multitareas y avanzadas redes cliente/servidor

La siguiente sección presenta un análisis comparativo entre estos sistemas operativos, que actualmente compiten por el liderazgo en el mercado de la industria de cómputo. Cada uno de estos sistemas operativos es analizado a partir de distintos ángulos, los cuales comprenden desde sus orígenes y desarrollo hasta un panorama sobre su arquitectura interna, lo cual nos permitirá seleccionar a uno de estos sistemas operativos como la mejor alternativa para la interconectividad de los sistemas abiertos

UNIX y otros sistemas operativos

Grupo de Evaluación: aquí cubrimos los sistemas operativos de 32 bits actualmente disponibles para los procesadores de Intel. Limitamos nuestra selección a los sistemas operativos que se distribuyen con una interface gráfica para el usuario y que tienen apoyo para multitareas y múltiples hilos de ejecución.

En el lado del Unix, evaluamos a Novell UnixWare versión 1.1; entre los sistemas no Unix evaluamos a OS/2 versión 3.0 (WARP) de IBM y a Microsoft Windows NT versión 3.1. También analizamos las características de la próxima versión de Windows NT 3.5 (proyecto Daytona)

Panorama de Microsoft Windows NT

"Microsoft, con sus cuatro líneas de productos (Productividad Personal, Aplicaciones, Productos de Red y Sistemas Operativos), es el gigante de la industria del software con ganancias de \$2.8 billones para el año fiscal de 1993, de las cuales aproximadamente el 36% provinieron de sistemas y lenguajes, el 51% de aplicaciones, y el 13% de otros (hardware, consultoría, etc.)" [13:pág. 27]. Lo anterior demuestra que Microsoft no está enteramente enfocado hacia los sistemas operativos o redes.

Con su éxito en las aplicaciones de productividad personal y el mercado de los sistemas operativos, Microsoft está haciendo esfuerzos por introducirse a los mercados de redes y sistemas operativos avanzados. Microsoft en combinación con IBM, introdujo en 1987 a OS/2, el cual fue rápidamente abandonado por Microsoft en favor de Windows, su interface personal gráfica para el usuario basada en MS-DOS. Al mismo tiempo Microsoft pretendió nuevamente en unión con IBM entrar al mercado de redes de PC con LAN Manager, que solo pudo obtener el 2% del mercado y 7.5% incluyendo a las versiones OEM.

Pretendiendo nuevamente introducirse al mercado de los sistemas operativos de alto rendimiento, Microsoft ha lanzado una serie de diferentes productos todos bajo el nombre de "Windows" (Windows for Workgroups, Windows, y LAN Manager for Windows), con un solo conjunto de interfaces de programación de aplicaciones llamado *Windows Open Services Architecture (WOSA)*, quien agrupa a todos estos productos, facilitando el desarrollo de aplicaciones para la plataforma Windows.

Windows NT es el nuevo producto propietario de la estrategia de Microsoft. Windows NT está diseñado para ofrecer casi todas las características comúnmente asociadas con los sistemas operativos avanzados:

- Extensibilidad
- Facilidad de transporte
- Fiabilidad
- Compatibilidad
- Rendimiento
- Multiproceso y facilidad de ampliación
- Proceso distribuido
- Conformidad con POSIX

Windows NT es un verdadero sistema operativo multitareas con prioridad que apoya las aplicaciones de múltiples hilos de ejecución y que tiene capacidades que rivalizan con las de UNIX y OS/2. No es de sorprender que también provee una compatibilidad casi total con las aplicaciones de DOS, MS Windows y OS/2 2 X. Algunas características especialmente notables incluyen su apoyo para múltiples procesadores, una fuerte capacidad de conectividad, y portabilidad a varias plataformas.

La nueva versión de Windows NT presenta una nueva variante, Windows NT Server y Windows NT Workstation, un programa común pero con dos variantes que se adapte a las necesidades de red que tengan los usuarios. "NT Workstation está construido en un diseño de microkernel portátil, para migrarlo a máquinas con diferentes procesadores" (Bill Gates, 1994).

Sin embargo, las aplicaciones nativas de Windows NT todavía son escasas, casi todas las aplicaciones disponibles actualmente son para tareas de negocios en mercados especializados, aunque Lotus, Microsoft, Novell y otros fabricantes están transportando o planean transportar aplicaciones importantes a Windows NT.

Breve historia de Windows NT

La historia de Microsoft en el negocio del funcionamiento en red comienza con la versión 3.1 de MS-DOS. Esta versión de MS-DOS añadía al sistema de archivos FAT las extensiones necesarias sobre el cierre de archivos y el cierre de registros, que permitían

que más de un usuario accediera a los archivos de MS-DOS. Con la liberación de Windows 3.1 en 1984, Microsoft también liberó un producto denominado Microsoft Networks, al que se hace referencia de manera informal como MS-NET.

MS-NET estableció algunas tradiciones que aún perduran en LAN Manager y ahora en Windows NT. Por ejemplo, el redirector, aunque completamente rediseñado y más sofisticado. Otras partes de MS-NET que se han conservado en Windows NT y son: su protocolo de mensaje de servidor (Server Message Block - SMB) y el servidor de red. El protocolo SMB de MS-NET es una especificación de alto nivel para formatear mensajes y enviarlos a través de la red, en tanto que el servidor de MS-NET era un software que residía en una computadora remota, transformándola en un servidor de archivos y de impresión dedicado. El software simplemente monitorizaba la conexión con la red y esperaba la llegada de los SMB.

El software de funcionamiento en red que actualmente forma parte de Windows NT incluye un servidor de red básico que habla el protocolo SMB (haciéndolo compatible con MS-NET y LAN Manager), este hecho hace que Windows NT pueda cargar otros servidores de red y ejecutarlos junto a su servidor interno, por lo que podrá transformar una workstation de red en un avanzado servidor de dominio. También proporciona características avanzadas, como por ejemplo, discos tolerantes a fallas. Estas capacidades que Windows NT ha adquirido permiten que pueda soportar las necesidades de grandes redes empresariales.

Requerimientos de Windows NT

"Windows NT 3.1 requiere al menos 16 Mb de RAM para un rendimiento aceptable. Por su parte, Windows NT 3.5 (Daytona) es tres veces más rápida que su predecesor, consume menos memoria (de 4 a 8 Mb menos que NT 3.1) y ofrece conectividad a NetWare de Novell y a las redes que se comunican vía TCP/IP. Además puede correr en procesadores Intel, MIPS Computer Systems y Digital Equipment (y a finales de 1995 IBM soportará a NT 3.5 en su línea de estaciones de trabajo PowerPC)" [18:pág. 66].

NT 3.1 necesita cerca de 50 Mb de espacio libre en disco duro, con 20 a 30 Mb reservados para memoria virtual. Microsoft NT 3.1 trabaja con la mayoría de los procesadores

386 pero es lento, en cambio en un procesador 486 o Pentium es más veloz y es compatible con casi todos los subsistemas SCSI y unidades de CD-ROM.

Por su parte, Windows NT Server requiere como mínimo una 386 a 25 MHz, 16 MB de memoria RAM, CD-ROM, tarjeta adaptadora de red y 90 Mb disponibles en disco, aunque para sistemas RISC requiere un espacio mayor en disco (110 Mb)

Windows NT es compatible con los sistemas FAT de DOS, HPFS (High Performance File System) de OS/2 y NTFS (New Technology File System) de Windows NT. NTFS puede hacer retroceder las operaciones de entrada salida (I/O) fallidas, y apoya nombres de archivos de hasta 254 caracteres.

Tabla 5-1 Requerimientos de Windows NT

	NT Workstation	NT Server
Espacio libre en disco duro	75 Mb (X86 ó Pentium) 92 Mb (Proc. RISC)	90 Mb (X86 ó Pentium) 110 Mb (Proc. RISC)
Memoria RAM	12 Mb (X86 ó Pentium) 16 Mb (Proc. RISC)	16 Mb (con X86 y RISC)
Procesador	386 en adelante ó Sistemas con procesador RISC	Min. 386 a 25Mhz ó Sistemas con procesador RISC
Unidad de CD - ROM	Solo con procesadores RISC	Con procesadores X86 o RISC

Estructura de Windows NT

"La estructura de Windows NT puede dividirse en dos partes: la porción de *modo usuario* del sistema (los subsistemas protegidos de Windows NT, o servidores) y la porción de *modo kernel* (el ejecutor de NT)" [7: pág. 26]. Esta estructura está representada en forma detallada en la figura 5-3.

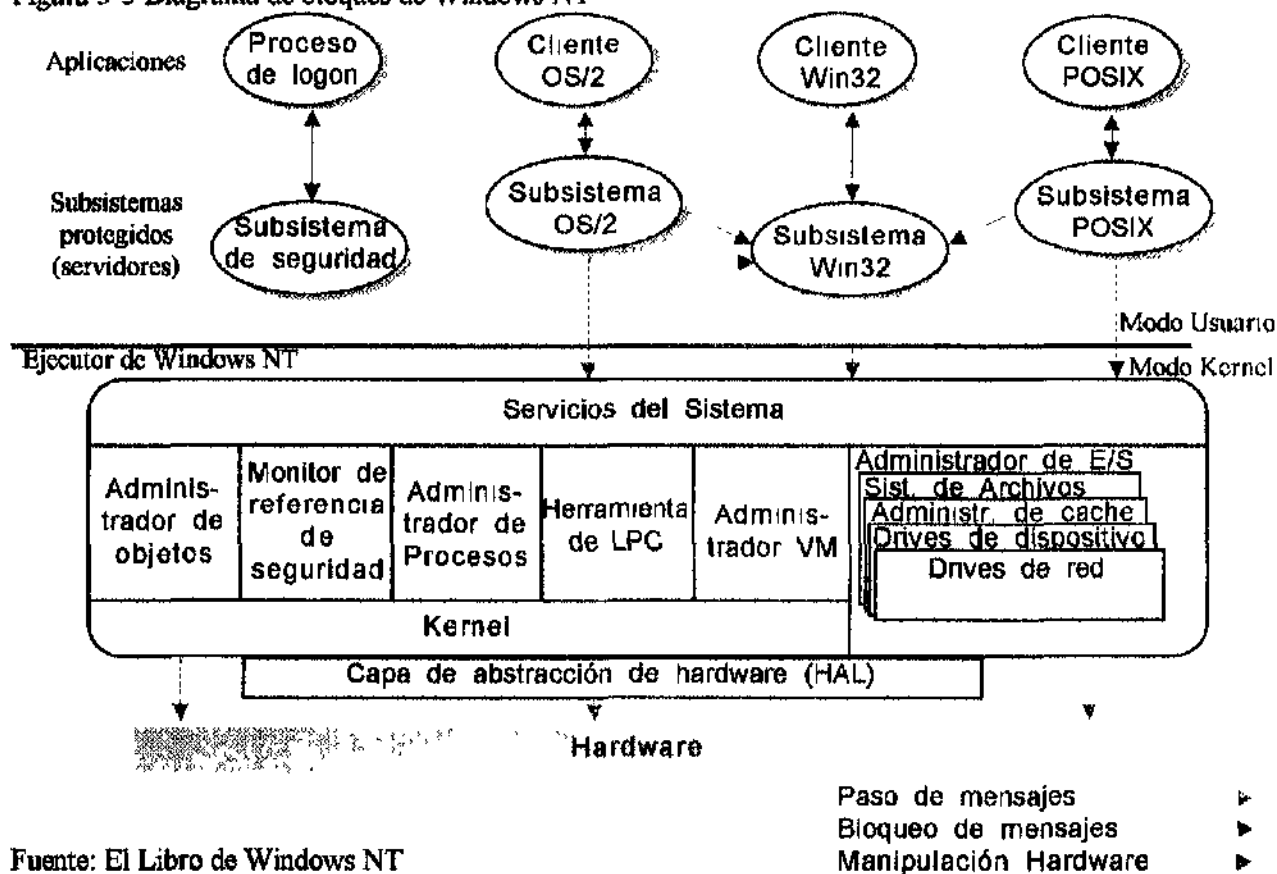
El subsistema de conectividad de Windows NT está diseñado sobre el estándar *Network Device Interface Specification (NDIS)*, versión 3.0. NDIS simplemente es un grupo de capas de API que apoyan varias actividades en la red. La *Transport Driver Interface*

(TDI) puede conectar varias aplicaciones e interfaces de la capa de Presentación usando manejadores de protocolos individuales independientemente de la red.

Windows NT también utiliza el *protocolo de Streams* originado en UNIX para proveer soporte de IPX/SPX, TCP/IP, NetBEUI y DLC. Usando el protocolo IPX/SPX, Windows NT puede actuar como un cliente de NetWare. Windows NT también soporta las operaciones FTP y TelNet de los sistemas UNIX. Para la conectividad con IBM, Windows NT actúa como un cliente SNA. Windows NT 3.5 (Daytona) también incluye una implementación modificada de TCP/IP.

"Los servidores de Windows NT se denominan *subsistemas protegidos* porque cada uno reside en un proceso independiente cuya memoria está protegida de otros procesos por el sistema de memoria virtual del ejecutor de Windows NT. Puesto que los subsistemas no comparten memoria automáticamente, se comunican por medio del paso de mensajes" [7:pág. 26].

Figura 5-3 Diagrama de bloques de Windows NT



Fuente: El Libro de Windows NT

En la figura 5-3 las líneas continuas representan los caminos que pueden tomar los mensajes que van entre clientes y servidores o entre dos servidores. Todos los mensajes pasan a través del ejecutor, pero para simplificar la figura dichos caminos no se muestran

"El *ejecutor* de NT es como una máquina del sistema operativo capaz de soportar cualquier número de procesos del servidor. Los servidores dan al ejecutor de NT sus interfaces de usuario y de programación y proporcionan entornos de ejecución para diversos tipos de aplicaciones" [7: pág. 28].

Los procesos son una división fundamental del trabajo y los recursos en Windows NT. Permiten al sistema operativo dividir su labor en unidades funcionales, para lograr una utilización eficiente del procesador. "Windows NT divide sus procesos en unidades ejecutables denominadas hilos. Los hilos permiten que un único proceso ejecute concurrentemente diferentes partes del programa y logre una mejor utilización del procesador, especialmente en unidades multiprocesador" [7: pág. 98]. Un proceso consta de un espacio de direcciones y un conjunto de recursos, que todos sus hilos comparten en cuanto se ejecutan.

Subsistemas protegidos

Debido a que el término *servidor* implica a cada subsistema protegido que proporciona un API que puede ser utilizado por los programas. Cuando una aplicación (u otro servidor) llama a una rutina o función de un API, se envía un mensaje al servidor que implementa la rutina del API a través de la herramienta de llamada de procedimientos locales (*Local Procedure Call - LPC*) del ejecutor de NT, que es un mecanismo optimizado para el paso de mensajes locales. El servidor contesta enviando un mensaje de retorno al que ha realizado la llamada.

"Windows NT tiene dos tipos de subsistemas protegidos: *Subsistemas de entorno* y *Subsistemas integrales*. Un *subsistema de entorno* es un servidor en modo usuario que proporciona un API específico para un sistema operativo. Cuando una aplicación llama a una rutina del API, la llamada se envía a través del mecanismo del LPC al subsistema de entorno. Este subsistema ejecuta la rutina del API y devuelve el resultado al proceso de la aplicación enviando otra LPC" [7: pág. 27].

El subsistema de entorno más importante de Windows NT es **Win32**, que suministra los API de Windows de 32 bits de Microsoft a los programas de aplicación. Además Win32 proporciona la interface gráfica del usuario (GUI) de Windows NT y controla todas las E/S de la aplicación. Windows NT también proporciona un subsistema de entorno *POSIX*, un subsistema de entorno OS/2, un subsistema de entorno para Windows de 16 bits, así como un subsistema MS-DOS. Estos subsistemas proporcionan sus propios API a los programas de aplicación, pero emplean el subsistema Win32 para recibir entradas del usuario y mostrar las salidas por pantalla.

El resto de los subsistemas protegidos (*subsistemas integrales*) son servidores que realizan funciones importantes dentro del sistema operativo. Algunos subsistemas integrales han ido apareciendo durante el desarrollo de Windows NT, pero uno ha permanecido siempre, el *subsistema de seguridad*. Este sistema se ejecuta en modo usuario y almacena las normas de seguridad activas en la computadora local. El subsistema de seguridad mantiene una base de datos acerca de las cuentas de los usuarios incluyendo, los nombres de las cuentas, palabras clave y cualquier conjunto de privilegios especiales que posea el usuario. También acepta información de petición de conexión (logon) del usuario e inicia su identificación" [7:pág. 28].

Algunos de los componentes de red de Windows NT están implementados como subsistemas integrales. Vale la pena destacar a dos de ellos: el *servicio de workstation* y el *servidor*. Cada uno de estos servicios, llamados a menudo subsistemas de red, es un proceso en modo usuario que implementa un API para acceder y gestionar al redirector de red y el servidor de red LAN Manager, respectivamente. El redirector es el componente de la red responsable de enviar (redireccionar) solicitudes de E/S a través de dicha red cuando el archivo y el dispositivo al que se solicita acceso no es local, el servidor se sitúa en la máquina remota y recibe tales solicitudes remotas. El redirector y el servidor de LAN Manager están implementados como controladores (drivers) del sistema de archivos, es decir, como parte del sistema de E/S de NT.

Arquitectura Abierta

Puesto que el servidor de red está integrado en Windows NT, podría parecer que está "cableado" ahí, pero no lo está. El objetivo de conectividad inmediata de Dave Thompson dictaba que Windows NT fuera capaz de enlazarse a una gran variedad de redes. Por lo

tanto no solo el redirector, el servidor y los drives de transporte tienen que cargarse y descargarse dinámicamente, sino que deben poder coexistir muchos de estos componentes. Windows NT soporta redes distintas de LAN Manager de varias formas.

- Proporciona acceso a sistemas de archivos que no son de Microsoft, para la conexión de recursos e inspección en red, para E/S a archivos y dispositivos remotos a través del API común Win32.
- Permite que estén cargados al mismo tiempo múltiples drivers para protocolos de transporte de red y que los redirectores llamen a una interface única y común para acceder a ellos.
- Proporciona una interface y un entorno para drives de tarjetas de red que permiten acceder a los drives de transporte de Windows NT, y para tener portabilidad hacia sistemas MS-DOS futuros.

Funcionamiento en Red

La proliferación de grandes redes de ordenadores y la necesidad de los usuarios de comunicarse y compartir bases de datos centralizadas de información, ha elevado el software de red desde la esfera de la utilidad a la esfera de la necesidad. Participando en una o más redes, un sistema operativo puede incrementar su potencia de proceso y características de almacenamiento, permitir a los usuarios que se comuniquen y que compartan datos, y proporcionar un conjunto más rico de posibilidades a sus aplicaciones de lo que podría ofrecer si estuviera solo.

Para proporcionar estas ventajas de una forma eficiente, el software de red de Windows NT forma parte de él, operando en la misma base que el resto del ejecutor de Windows NT. Aunque estén integrados, los componentes de red no están cableados en el sistema. Los flexibles modelos de *DLL* y el sistema de E/S de Windows NT permiten al software ser añadido y eliminado dinámicamente del sistema operativo.

Windows NT proporciona varias interfaces de red que le permiten enlazarse a diferentes tipos de redes e interactuar con distintas clases de sistemas de computadoras. La interface del proveedor permite a los fabricantes, distintos de Microsoft, enlazarse al Win32 y a los API de E/S de archivos; la capa *TDI* permite a los redirectores de red y a los servidores acceder y utilizar cualquier driver de transporte disponible sin modificar su código; la capa *NDIS* permite a los drives de transporte acceder a cualquier tarjeta de red

y dar la portabilidad de drivers de red desde sistemas Windows NT al entorno de driver del dispositivo virtual de Windows.

Las prestaciones de las aplicaciones distribuidas, incluyendo la *RPC* y los mecanismos de comunicación interprocesos, permiten a los desarrolladores de aplicaciones explotar a las computadoras en red al mandar trabajos intensivos a otras máquinas o accediendo a recursos remotos como si fueran locales. Además, LAN Manager para Windows amplía las posibilidades de red del sistema Windows NT estándar para hacer frente a grandes redes con características de seguridad y administración distribuidas

Portabilidad y Escalabilidad

Cada aplicación, incluyendo DOS, Win32 y el subsistema de Windows NT, se ejecuta en su propio espacio de memoria o *máquina virtual (Virtual Machine - VM)*. Si está ejecutando una aplicación de DOS o Win32 en una VM, y otra aplicación se traba en otra VM, esto no parará todo el sistema. Las aplicaciones de Windows 3.1 actualmente se ejecutan en una sola VM que ejecuta a Windows 3.1, y una aplicación de Windows de mal comportamiento puede trabar a todo el subsistema de Windows (pero no todo el sistema operativo). La versión Daytona de Windows NT remediará esta situación permitiendo ejecutar aplicaciones de Windows 3.1 en espacios de memoria separados. Daytona permitirá crear enlaces DDE y OLE entre estas VMs. Esto se maneja mediante una capa de conversión de 16 a 32 bits que también puede manejar enlaces OLE entre programas de Windows 3.1 y Windows NT.

La edición Daytona de Windows NT añadirá una mejora significativa a sus recursos gráficos con OpenGL, el API gráfico de 3-D creado por Silicon Graphics. Ninguno de los objetos GUI de Windows NT aprovechará el Open GL, pero las aplicaciones que llamen a las estructuras de OpenGL podrán utilizar las bibliotecas de OpenGL. Esto coloca a Windows NT como una plataforma seria para el trabajo gráfico de alto nivel. "*Windows NT tiene el poder de una estación de trabajo, maneja gráficos tridimensionales gracias a OpenGL, multiprocesamiento simétrico, multiprocesamiento de tareas, está construido en un diseño de microkernel portátil (para migrarlo a máquinas con diferentes procesadores) y proporciona mayores niveles de seguridad en la información*" (Bill Gates, 1994) .

Windows NT puede ejecutar todas las aplicaciones de DOS y Windows usando el emulador de DOS incluido en el subsistema de Windows 3.1. A diferencia de muchos emuladores de Windows basados en UNIX, Windows NT puede ejecutar aplicaciones estándares de Windows en modo mejorado. Hasta ahora no se ha encontrado una aplicación de DOS o Windows que Windows NT no pueda ejecutar, aunque las aplicaciones de DOS parecen ejecutarse un poco más lento bajo Windows NT.

Programación de Aplicaciones

Aunque Microsoft ofrece un Windows NT SDK, para una programación seria, probablemente harán falta herramientas separadas como Borland C++ 4.0, o Microsoft Visual C++, edición 32 bits. Las aplicaciones nativas de Windows NT están escritas usando Win32, API que está bastante bien documentado. Microsoft provee una documentación excelente con todos los productos de Windows NT, y la asistencia técnica está disponible por teléfono en el servicio en línea de CompuServe o la red Internet.

Windows NT puede competir con UNIX en su propio terreno y su capacidad rivaliza a la de OS/2. El apoyo para múltiples procesadores y las múltiples plataformas de Windows NT son características de vanguardia que deben ser importantes en los años venideros. La falta de aplicaciones nativas lo hacen una solución menos ideal en estos momentos, pero si las promesas de una compatibilidad binaria entre Windows 95 y Windows NT se hacen realidad, el número de aplicaciones crecerá dramáticamente y en poco tiempo.

Ventajas de Windows NT

Windows NT es la base de un sistema operativo de multiproceso simétrico que soporta múltiples entornos de sistemas operativos. Posee una interface gráfica de usuario (GUI) de Windows y ejecuta programas basados en Win32, Windows de 16 bits, MS-DOS, POSIX y OS/2. Emplea principios avanzados de sistemas operativos, como la memoria virtual, la multitarea real, el tratamiento estructurado de las excepciones, y la incorporación del concepto de objetos del sistema operativo. Es seguro, potente, fiable y flexible.

Desventajas de Windows NT

Windows NT fue anunciado en mayo de 1993 y un año después Microsoft anunció las versiones cliente y servidor de Windows NT. Este producto ha sido llamado la versión 3.11 para estar acorde con Windows 3.1, pero Windows NT es un producto nuevo. Mientras éste

aprovecha la interface más familiar (la de Windows 3.1), la arquitectura interna es nueva, esto pone en desventaja a Windows NT frente a los sistemas operativos que cuentan con una amplia experiencia empresarial. Además, se debe hacer notar que las aplicaciones de Windows existentes son de 16 bits comparadas con las aplicaciones de 32 bits de Windows NT. Sin embargo, existe un gran esfuerzo involucrado en la migración de aplicaciones existentes. Mientras Microsoft logra esto, *UnixWare toma ventaja en lo que se refiere al soporte para las aplicaciones Windows.*

Panorama de OS/2

El sistema operativo OS/2 utiliza las capacidades y poder de la familia de procesadores Intel 80386 y 80486. Actualmente OS/2 es un sistema operativo prometedor de IBM. Un verdadero sistema de 32 bits, tal como UNIX, este utiliza las capacidades de la multitarea de los procesadores Intel. En adición a las diferencias fundamentales entre OS/2 y MS-DOS, OS/2 tiene otras implementaciones significativas incluyendo un eficaz sistema de archivos y soporte para el trabajo en red.

Para este relativamente nuevo sistema operativo desafortunadamente hay pocos usuarios a pesar del soporte que provee para aplicaciones de MS-DOS y Windows.

Breve Historia de OS/2

Para poder entender mejor cómo es que OS/2 soporta la multitarea, es necesario entender acerca de sus orígenes. A pesar de que mucha gente considera a OS/2 como un sistema operativo nuevo, el desarrollo de OS/2 empezó en 1984 cuando IBM introdujo la IBM PC-AT. Las primeras versiones de este sistema operativo multitarea estuvieron basadas en los microprocesadores 80286, el cual tenía defectos significativos

Para soportar las aplicaciones de DOS, el procesador tenía que cambiar los modos de operación. La única forma de cambiar los modos de operación para regresar al modo DOS era un reset del procesador, la cantidad de tiempo que tomaba el reset hacía que el desempeño disminuyera significativamente. Sin embargo, a través de programas escritos para el nuevo sistema operativo este pudo trabajar bien por sí solo, con un desempeño bajo comparado con las aplicaciones DOS. La versión multitarea de OS/2 tuvo que soportar a las aplicaciones existentes de DOS con dificultades

Hasta 1987 IBM y Microsoft produjeron la primera versión de OS/2 (versión 1.0) que contaba con una interface no gráfica para el usuario y no tenía un soporte para mouse, y solo podía trabajar en discos duros de más de 32 MB. Además, con los altos precios de las memorias de las computadoras, los 4 MB de memoria mínima que requería el sistema era un recurso bastante costoso. Muchos desarrolladores y usuarios decidieron esperar la disponibilidad de una interface gráfica y un soporte directo del procesador 80386.

IBM esperó repetir el éxito de DOS, resultado de su unión con Microsoft, cuando descubrió el nombre de OS/2, en abril de 1987, el mismo día en que se introdujo la serie PS/2. Desde el momento en que las relaciones entre IBM y Microsoft se habían disuelto, OS/2 no logró crear el impacto en el mercado que IBM hubiera deseado, vendiendo solo 2 millones de unidades desde su introducción en diciembre de 1987.

En noviembre de 1988, la versión 1.1 de OS/2 fue distribuida con la interface *Presentation Manager*. En 1989, la versión 1.2 incluyó el nuevo *High Performance File System* y el lenguaje de comandos por lotes REXX. OS/2 podía soportar múltiples sesiones de DOS, sin embargo sus ventas aún eran bastante pobres. A principios de 1991, IBM lanzó la versión 1.3 de OS/2, una versión similar del OS/2 anterior con un soporte *built-in* para una nueva tecnología de tipos de letra llamada *Adobe Type Manager*, de Adobe System.

Después de repetidas versiones de mantenimiento y mucha disputa pública, IBM y Microsoft cambiaron su acuerdo, resultando en que IBM esencialmente tomó todas las responsabilidades de desarrollo de OS/2. Después de repetidas esperas IBM introdujo la primera versión de 32 bits, OS/2 2.0, en abril de 1992. A pesar de las nuevas alianzas tal como la unión *Taligent* con Apple para desarrollar una nueva tecnología orientada a objetos (*Pink*), IBM permanece enfocado hacia OS/2 como parte clave de su estrategia SAA (*System Application Architecture*).

IBM ha establecido a OS/2 como el ambiente operativo de desktop en sus operaciones mainframe y agresivamente intentará ganar usuarios de DOS y Windows. Debido a la amplia aceptación de NetWare en los ambientes IBM y el soporte para clientes OS/2, IBM ha recomendado NetWare como una solución de red y revende NetWare con el logo compartido "Blue Box".

Como parte del incrementado énfasis de IBM hacia el software, OS/2 continuará siendo mejorado con la nueva tecnología de IBM tal como el *Mach kernel* y la tecnología de objetos de Taligent

A pesar de que OS/2 puede ser un servidor con la instalación de LAN Server o el OS/2 LAN Manager, IBM ha colocado a OS/2 en primer lugar como un cliente para soportar aplicaciones *high-end* y como una plataforma integradora de aplicaciones DOS, Windows y OS/2, manteniendo el lema "Mejor DOS que DOS y mejor Windows que Windows". La implementación de servidores tiende a ser ligada hacia soluciones altamente específicas de IBM y están basadas en NetBEUI, limitándolas a no más del 7.5% de los ambientes de redes de PC existentes. El acierto de IBM de revender NetWare indica su conciencia acerca de la importancia de NetWare para el éxito de su negocio comercial.

Por toda la atención que IBM ha dado para soportar las aplicaciones Windows, éstas se ejecutan bien bajo OS/2. De alguna manera, la capacidad para ejecutar programas Windows incrementa las posibilidades de selección de programas de aplicación.

Las mejores características de OS/2 son:

- Soporte para las aplicaciones de 32 bits
- Soporte para las PCs basadas en microprocesadores Intel 80386 y 80486
- Soporte para aplicaciones DOS y Windows
- Manejador de arranque (Boot Manager) para arrancar con múltiples sistemas operativos
- Multitareas
- Demanda de memoria virtual paginada
- Workplace shell, una evolución de la interface gráfica para el usuario de Presentation Manager

Muchas de las características asociadas con el cómputo en redes empresariales tales como la seguridad, la administración, el trabajo en red y el sistema de archivos no fueron originalmente diseñadas como parte del sistema operativo. Éstas fueron proporcionadas por el LAN Manager/LAN Server o han sido gradualmente introducidas

como productos *add-on* separados para OS/2, tal como el OS/2 Crash Protection, el cual previene que sesiones de DOS y Windows colapsen el sistema cuando éstas fallen.

Es importante hacer notar que *la mayoría de estas características son estándares en UNIX*. IBM gasta esfuerzos significativos en el desarrollo de nombres vistosos para los servicios del sistema operativo que *son estándares en UNIX* y lo han sido por un largo tiempo.

Soporte de OS/2 para DOS

OS/2 soporta aplicaciones de DOS por medio de emular una computadora completa MS-DOS, y manejar esta emulación como una sesión de OS/2. En OS/2 se puede trabajar con una sesión de pantalla completa y ejecutar programas de DOS, tal y como sucediera si DOS estuviera trabajando por sí solo. Debido a que los programas de DOS varían ampliamente en la forma en que utilizan a la computadora, OS/2 provee variados parámetros para ajustar la forma en que el sistema OS/2 provee la sesión de DOS. Las áreas que se pueden ajustar incluyen:

- Soporte y colocación de memoria convencional, extendida, expandida y alta
- Interacciones del sistema de video
- Opciones del sistema de archivos
- Interfaces de periféricos del sistema
- Información de la versión DOS
- Opciones de acceso desde el teclado
- Generación de sonido

Se debe considerar la forma en que OS/2 provee la sesión de DOS para poder ejecutar programas de DOS. Primero, los programas de DOS se ejecutan más lentamente bajo OS/2 que bajo MS-DOS. OS/2 crea la sesión de DOS como un programa ejecutándose bajo OS/2 (sin embargo los programas de DOS no lo saben) y OS/2 continúa ejecutándose junto con otros programas que se hayan iniciado antes de abrir la sesión de DOS. Cada uno de los otros procesos toma una fracción de tiempo de las sesiones de DOS y causa que los programas de DOS se ejecuten más lentamente. Segundo, algunos programas

DOS no corren bajo OS/2. Los programas que tiene problemas caen en las siguientes categorías:

- Juegos
- Programas de diagnóstico de disco
- Programas de comunicaciones DOS
- Programas Gráficos
- Cualquier programa que utilice las características avanzadas de multitareas de los procesadores 80286, 80386 u 80486

Después de todo, el soporte para los programas de DOS bajo OS/2 es bueno. Si se ejecutan sólo aplicaciones DOS, existen mejores formas para hacer multitareas con ellos

Soporte de OS/2 para Windows

IBM, a través de un acuerdo con Microsoft, incluye una versión modificada de Windows en cada copia de OS/2. Las únicas restricciones para ejecutar programas de Windows son que Windows solo puede ejecutarse en modo estándar bajo OS/2, y si se tiene una aplicación que requiere Windows en modo extendido, no se puede ejecutar ésta bajo OS/2. Como con las aplicaciones DOS, OS/2 provee varios parámetros que se pueden ajustar para hacer que una aplicación específica de Windows se ejecute de la mejor manera posible. Estos parámetros son para ajustar los iconos de programas individuales de Windows.

OS/2 utiliza todo el poder del procesador 80386 en su soporte de una arquitectura interna de 32 bits. Las aplicaciones que fueron escritas para OS/2, pueden operar más rápido que las aplicaciones escritas para sistemas operativos de 16 bits, tal como MS-DOS.

Utilizando las capacidades del procesador 80386, OS/2 cumple la promesa de soportar múltiples aplicaciones de DOS, Windows, y OS/2 ejecutándose al mismo tiempo. Utilizando la multitarea *timeslice*, las aplicaciones pueden ejecutarse sin preocuparse de que no poseen el sistema entero. OS/2 ha cumplido la meta de soportar aplicaciones que actualmente son populares y que se ejecutan bajo DOS y Windows. También provee un sistema operativo base, poderoso para ser utilizado en futuros desarrollos de aplicaciones

Las bases de OS/2 sobre una arquitectura enfocada al objeto son consistentes con los paradigmas actuales de programación, tal como el uso de C++ como un lenguaje de desarrollo de aplicaciones.

El *Workplace Shell* provee un ambiente sofisticado para los usuarios de PC. Después de aprender a utilizarlo, éste provee una simple y sofisticada interface para controlar el sistema.

Soporte de red en OS/2

Las capacidades de multitarea de OS/2 y su capacidad de utilizar la totalidad del espectro de memoria sin restricciones hacen fácil su uso en el mundo de las redes. Diseñado para soportar totalmente operaciones de red, OS/2 tiene muchas facetas que soportan el trabajo en red directamente y muchas formas de incluir estaciones de trabajo basadas en OS/2, en las redes existentes. Comparado con el DOS, OS/2 mantiene una ventaja distintiva para las aplicaciones de red. *Comparado con Windows o UNIX, OS/2 no es mucho más útil, en la práctica, para aplicaciones de red*

OS/2 tiene muchas ventajas como un sistema operativo para desarrolladores de sistemas de red. Para los usuarios, la ventaja más grande sobre DOS es que OS/2 no está restringido por el límite de 640 KB de memoria convencional como lo está DOS. Debido a que el trabajo en red de Windows está sólo comenzando a utilizar todo el potencial de la memoria disponible para todas las aplicaciones Windows, la mayoría de las redes bajo Windows están también al límite de los 640 KB.

Con OS/2, no existe preocupación acerca del tamaño de los programas de red o de cómo cargarlos en memoria alta, lo cual se debe de hacer con MS-DOS. OS/2 trata toda la memoria de igual forma y puede acceder a la memoria sin la división entre la memoria convencional, alta, expandida y extendida.

Ventajas de OS/2

OS/2 es un moderno sistema operativo que provee muchas ventajas sobre sistemas tales como MS-DOS. Para los usuarios que existen en un ambiente de cómputo dominado por IBM, OS/2 provee un ambiente de estación de trabajo PC consistente con las filosofías y direcciones estratégicas de IBM.

Desventajas de OS/2

Numerosos factores han hecho que los creadores de paquetes de software se desplacen lentamente hacia el uso de OS/2 como un sistema operativo líder. Sin embargo, muchas aplicaciones continúan estando disponibles para ejecutarse bajo OS/2, los desarrolladores generalmente escriben primero la versión para Windows y después migran hacia OS/2 y UNIX.

El tamaño y complejidad de OS/2, así como la carencia de aplicaciones han causado que los clientes se muevan muy lentamente hacia OS/2. La competencia con Windows, Windows NT y UNIX, quienes proveen a los clientes muchas opciones de sistema operativo, hace difícil justificar el cambio hacia OS/2.

El nuevo *Workplace Shell* es una ventaja y una desventaja para el OS/2. La desventaja de la orientación a objetos y de las nuevas formas de hacer las cosas con OS/2 hacen que los usuarios familiarizados con Windows y otras versiones anteriores de OS/2 tengan problemas de aprendizaje en lo que se refiere al uso de OS/2.

"IBM continúa desarrollando versiones adicionales de OS/2 que incorporan funciones avanzadas, tales como el multiprocesamiento simétrico. La última versión de OS/2, WARP, integra las instalaciones existentes de Windows en el ambiente OS/2. Esta integración permite utilizar a Windows y a sus aplicaciones, en la forma acostumbrada, pero con la ventaja de usar el manejo de multitareas y su espacio lineal de memoria, para independizar a cada una de las aplicaciones activas" [20.pág. 76].

Es evidente que IBM ha invertido tiempo y esfuerzo para hacer de OS/2 (incluyendo a WARP), un sistema operativo optimizado, fácil de instalar y utilizar, sin embargo, a pesar de que IBM ha intentado que el Workplace shell orientado a objetos sea más fácil de utilizar, éste requiere un cierto cambio de paradigma para ser usado, especialmente por los usuarios experimentados de Windows.

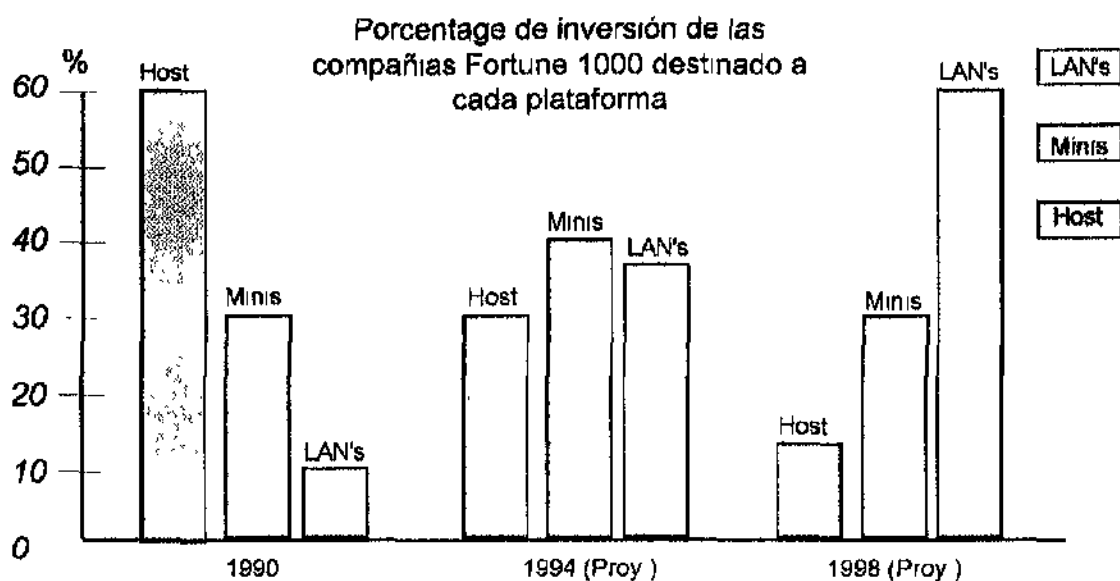
Panorama sobre UNIX

"Los sistemas operativos basados en UNIX, en las PCs de la industria, están proyectados a crecer en una tasa considerable. Por ejemplo

- La tasa anual de crecimiento componente (CAGR) crecerá el 67% desde 1991 hasta 1996.
- El mercado para las avanzadas computadoras UNIX de escritorio crecerá desde 69,000 unidades hasta 1,000,000 de unidades para 1996.
- Los sistemas multiusuario UNIX crecerán desde 242,000 hasta 500,000 unidades para 1996.
- Las estaciones de trabajo UNIX crecerán desde 420,000 unidades hasta casi 1.5 millones de unidades, uno de los segmentos de más rápido crecimiento en el mercado de cómputo.
- Alrededor del 65% de las compañías del Fortune 1000 están investigando, probando u operando sistemas UNIX " [13:pág 3].

Este crecimiento está siendo impulsado hacia la tendencia conocida como *right-sizing*. Esto significa que los negocios se están desplazando hacia la implementación de soluciones basadas en el modelo de cómputo cliente/servidor. La mayoría de las empresas están actualmente implementando este modelo o evaluando su uso en los negocios.

Figura 5-4 Cambios en los ambientes de cómputo

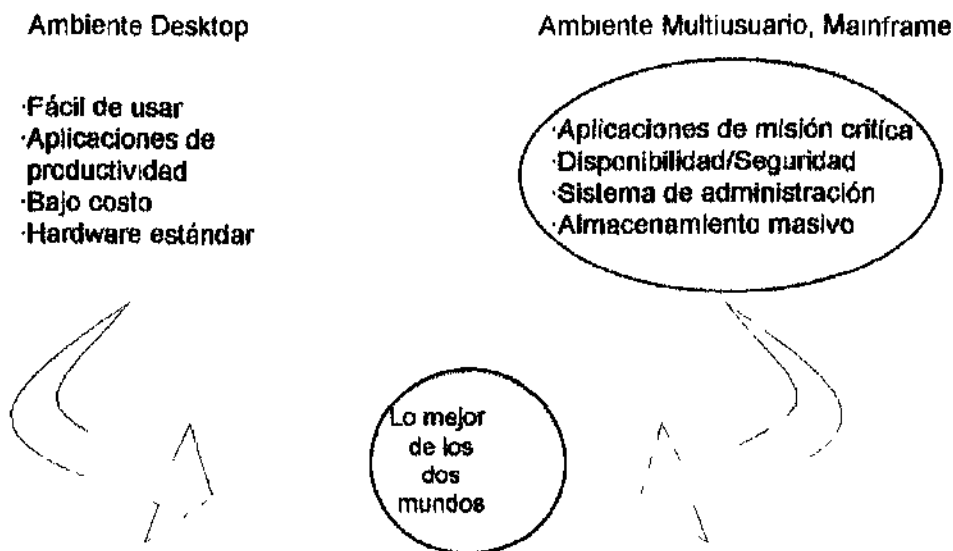


Fuente: Forrester Research (1992), Datamation and Cowen (1992)

Es importante hacer notar la diferencia entre un ambiente de cómputo distribuido y un ambiente multiusuario. Un *ambiente distribuido* o *cliente/servidor* es uno en el cual un sistema de servidor de archivos está conectado vía una red a computadoras inteligentes en el escritorio del usuario (el cliente). La carga de cómputo es por lo tanto compartida (o distribuida) a través de la red entre el cliente y el servidor. Un *ambiente multiusuario* es uno en el cual un solo sistema de cómputo es accesado por terminales de caracteres o gráficas sobre una red. Todo el cómputo es realizado por un solo sistema. UnixWare puede proporcionar soluciones en cualquiera de esos dos ambientes.

Cada compañía con equipo de cómputo mayor se está desplazando para encontrar una solución en este mercado en expansión tan veloz. El ganador en esta batalla controlará el escritorio y con ésto controlará el ambiente de cómputo corporativo. Los clientes están tomando decisiones hoy en día que afectarán sus compras de la década venidera.

Figura 5-5 Right-sizing



Fuente: UnixWare Sales Guide, Novell

Muchos de los clientes actualmente emplean redes para conectar sus sistemas de cómputo y compartir efectivamente recursos. El sistema operativo de red líder es NetWare con más de dos terceras partes del mercado. Un estudio de investigación reportó que, "NetWare es tan popular entre los usuarios, integradores de sistemas, revendedores con

valor agregado y vendedores de software independiente y aún otros vendedores, que ha cimentado virtualmente su lugar como *el sistema de arquitectura de red del mundo de las LANs*" [13;pág. 5]. Debido a ésto, la conectividad entre un sistema operativo avanzado y el ambiente NetWare será un requerimiento para el éxito en una topología de right-sizing

Reseña histórica del sistema operativo UNIX

Durante los últimos años, UNIX ha adquirido una popularidad sin precedentes. En esta sección se presenta una breve historia del sistema operativo UNIX en la que se explica el motivo de su popularidad.

El sistema operativo UNIX se desarrolló en los Laboratorios *Bell de Murray Hill*, en Nueva Jersey, uno de los centros de investigación más grandes del mundo. Son muchas las personas que han aportado ideas al sistema desde el diseño y la estructuración originales de *Ken Thompson* en 1969.

Cuando se desarrolló el sistema operativo UNIX, muchas computadoras todavía ejecutaban trabajos individuales en un proceso por lotes. Debido a que estas computadoras no servían más que a un usuario a la vez, no se aprovechaban al máximo la capacidad y velocidad de la computadora. Es más, ese ambiente de trabajo aislaba a los programadores entre sí y no era fácil compartir programas y datos, como tampoco promovía la cooperación entre las personas que trabajaban en un mismo proyecto. El sistema UNIX de tiempo compartido introdujo dos ventajas importantes respecto a los sistemas por lotes, de un solo usuario:

- Permitir que dos o más personas compartieran la computadora al mismo tiempo (el sistema operativo UNIX es *multiusuario*)
- Admitir la comunicación directa con la computadora a través de una terminal (es *interactivo*)

Sin embargo, UNIX no fue el primer sistema multiusuario e interactivo, un sistema operativo llamado *Multics*, se utilizó durante algún tiempo en los laboratorios Bell antes de la creación de UNIX. En Europa se había desarrollado el Sistema de Acceso Múltiple de Cambridge (*The Cambridge Multiple Access System*) y también se empleó durante varios años el CTCS (Sistema de Tiempo Compartido Compatible). Los diseñadores de UNIX

aprovecharon el trabajo hecho con éstos y con otros sistemas operativos para combinar las mejores características de cada uno.

UNIX fue desarrollado por investigadores que necesitaban un equipo de herramientas de computación modernas que les ayudaran en sus proyectos; el UNIX hizo posible que grupos de personas, que trabajaban en un mismo proyecto, compartieran determinados tipos de información y programas, sin perder confidencialidad en otros

Las universidades y escuelas superiores desempeñaron un papel importante en el fomento de la popularidad del UNIX mediante el efecto de *los cuatro años*. Cuando empezó a distribuirse normalmente el UNIX, en 1975, los laboratorios Bell lo ofrecieron a instituciones educativas a un costo mínimo. Las escuelas, a su vez, lo usaron en sus cursos de computación, asegurando así que todos los estudiantes de las ciencias de computación se familiarizaran con él. Como quiera que sea, UNIX es un sistema de desarrollo avanzado, los estudiantes se acostumbraron a un medio de programación óptimo, por lo que al graduarse y empezar a trabajar en la industria, estos estudiantes esperaban encontrarse en un ambiente igualmente avanzado. Con el ascenso de un número cada vez mayor de estudiantes en el mundo comercial, el sistema operativo UNIX se abrió camino en la industria.

El departamento de ciencias de la computación de la Universidad de California en Berkeley, además de enseñar a los estudiantes a usar el sistema, introdujo en él cambios y aportaciones tan significativas que en la actualidad existe una versión denominada sistema operativo *Berkeley UNIX*. Algunas de las características desarrolladas en Berkeley aparecieron en las versiones posteriores de los Laboratorios Bell y en varias versiones de empresas de software especializadas en la adaptación del sistema para diversas computadoras. Es esta herencia -el desarrollo en un ambiente de investigación y su enriquecimiento en el ambiente universitario- lo que ha hecho de UNIX, una herramienta de tanta utilidad para el desarrollo de software.

Hacia mediados de la década de los 70s, las minicomputadoras empezaron a constituir un reto para los equipos grandes. Los fabricantes de minicomputadoras demostraron que, en muchas aplicaciones, sus equipos podían realizar las mismas funciones que los grandes, pero a un costo mucho menor. Hoy, las microcomputadoras

representan el mismo reto contra las minicomputadoras. En la actualidad las potentes computadoras, las memorias más amplias y baratas, y el bajo precio del almacenamiento en discos duros de gran capacidad, han permitido a los fabricantes instalar sistemas operativos multiusuario en microcomputadoras. El costo y rendimiento de estos equipos está rivalizado con las minicomputadoras.

De acuerdo con lo anterior, los avances en la tecnología de hardware crearon la necesidad de un sistema operativo que aprovechara el poder disponible del hardware. Con la caída de los precios del hardware, los fabricantes no pueden darse el lujo de desarrollar y mantener sistemas operativos propios. De igual manera, quienes producen software de aplicación tampoco pueden modificar sus productos para que funcionen con sistemas operativos distintos, sino que deben reducir el precio de sus productos, en línea con el hardware.

Los fabricantes de hardware requieren un sistema operativo genérico que pueda adaptarse con facilidad a sus equipos, desean ofrecer un medio receptivo al software de terceros; en tanto que los fabricantes de software necesitan un sistema operativo genérico, como ambiente común para sus productos.

El sistema operativo UNIX satisface ambas necesidades. Dado que inicialmente se desarrolló para minicomputadoras, su estructura de archivos aprovecha al máximo los discos duros grandes y rápidos. Además, UNIX se desarrolló desde un principio como un sistema multiusuario y no como otros sistemas que fueron adaptados posteriormente para servir a varios usuarios. Por último, debido a que UNIX se ideó como un sistema de desarrollo, éste proporciona un ambiente ideal para una empresa de software.

La aparición de un sistema operativo estándar legitimizó el nacimiento de la industria del software. Ahora las casas de software pueden ofrecer una versión de un producto disponible para muchos equipos distintos. Los fabricantes que ofrecen una computadora con UNIX cuentan ya con el apoyo de software de terceros para el nuevo equipo. Por otro lado, un sistema operativo que puede ejecutarse en muchos equipos distintos, se denomina *portátil*. Cerca de 95% del sistema operativo UNIX está escrito en lenguaje de programación C, y el C es portátil debido a que está escrito en lenguaje de alto nivel independiente de la máquina (ya que el mismo compilador de C está escrito en C).

En un principio Ken Thompson escribió el sistema operativo UNIX en lenguaje ensamblador de la PDP - 7. Este es un lenguaje dependiente de la máquina; los programas escritos en lenguaje ensamblador funcionan solamente en un equipo, o en el mejor de los casos, en una familia. Por este motivo, el primer sistema operativo UNIX no era fácil de transportar a otros equipos.

Para que el sistema operativo UNIX fuera portátil, Thompson desarrolló el sistema de programación B, que no dependía de la máquina. Dennis Ritchie desarrolló el lenguaje C modificando el B, y junto con Thompson reescribió el sistema UNIX en C. Como resultado de esto pudo transportarse con facilidad para ser ejecutado en otras máquinas

Y así comenzó el C; conociendo las circunstancias de su creación, se comprenden algunas de las razones que lo convierten en un instrumento tan eficaz. C puede usarse para escribir programas independientes de la máquina. Un programa ideado para ser portátil, escrito en C, puede transportarse con facilidad a cualquier computadora que tenga un compilador de C. A medida que aumente la popularidad del UNIX y del C, habrá más computadoras con compiladores de C.

El C es un lenguaje de sistemas modernos; en él puede escribirse un programa o un sistema operativo. Es muy estructurado, pero no es necesariamente un lenguaje de alto nivel. El C permite al programador manipular bits y bytes, tal y como se necesita para escribir un sistema operativo, pero también tiene estructuras de alto nivel que permiten realizar una programación modular eficiente.

El C se está haciendo cada vez más popular por las mismas razones que el UNIX; es portátil, estándar y potente. Posee características de alto nivel que lo hacen flexible y es posible emplearlo en programación de sistemas. Estas características lo convierten en un sistema útil y práctico.

Con más de 20 años de evolución, UNIX ha llegado a ser el sistema operativo más avanzado y mejorado disponible hoy en día. Su amplia aceptación y uso lo han hecho también la solución líder de los sistemas abiertos o no propietarios. UNIX es hoy el tercer sistema operativo más vendido después de DOS y Macintosh.

Versiones de UNIX

En la actualidad, las empresas que encabezan el mercado de los sistemas operativos UNIX para la plataforma de Intel son The Santa Cruz Operation (SCO), NeXT Computer, Univel, SunSoft, HP e IBM.

Sistemas UNIX de SCO

SCO domina el 65% del mercado, el sistema operativo UNIX de SCO constituye una plataforma de sistemas abiertos que corre en todas las computadoras 386 y 486 estándares. Se trata de un núcleo de 32 bits multiusuarios, de recorrido múltiple con memoria virtual.

Open Desktop Personal System (ODPS)

ODPS es un sistema avanzado de SCO, con interface gráfica basada en los estándares de OSF/Motif y X Window. Permite que los usuarios presenten y controlen programas tanto locales como a distancia.

Open Server Network System (OSNS)

OSNS integra un sistema operativo con capacidades para su funcionamiento en red. Sirve para armar aplicaciones importantes para los negocios y que puedan manejarse en red.

SCO Open Desktop Server System (ODSS)

Con ODSS los usuarios combinan todo el poder de un sistema gráfico UNIX, servicios de red e interoperabilidad DOS para ejecutar aplicaciones distribuidas de 32 bits en el esquema cliente/servidor.

LAN Manager for UNIX

LAN Manager (de Microsoft) para sistemas UNIX corre en los sistemas operativos de SCO Open Desktop o en SCO Unix System, basados en Intel 80X86. Los usuarios pueden integrar los servidores UNIX o SCO Open Desktop en una LAN con una combinación de los sistemas de Clientes SCO Open Desktop, SCO Unix System, MS-DOS y OS/2.

SunSoft Solaris

“El sistema operativo Solaris está destinado a las 1000 compañías principales de Fortune para desarrollar labores fundamentales en sistemas operativo de alto nivel, dentro

de ambientes heterogéneos. [Shernaz Daver, vocero de SunSoft, 1994] SunSoft se puede utilizar para manejar toda una empresa y es ideal para manejar el proceso del right-sizing

HP-UX

HP-UX de Hewlett-Packard es una modalidad del sistema operativo UNIX que corre en estaciones de trabajo HP-9000 Series 700 y Series 900. Provee la capacidad de funcionar en máquinas desprovistas de disco.

AIX PS/2

El sistema operativo AIX PS/2 de IBM para CPU Intel es un sistema multiusuarios, multitareas con memoria virtual que da soporte hasta a 16 usuarios al mismo tiempo. AIX es una variedad de 32 bits del sistema operativo IBM AIX/RT, e incluye extensiones seleccionadas del sistema operativo Unix Berkeley 4.3 BSD, el estándar en la industria

Nextstep

El sistema operativo Nextstep de NeXT computer brinda una interface gráfica de usuario, conectividad, acceso a bases de datos, enlace de información, arquitectura orientada a objetos, todos ellos para PC basadas en Intel y estaciones de trabajo.

Nextstep está basado en el núcleo del sistema Mach y de Berkeley 4.3 BSD. Fue diseñado para integrarse con la mayoría de LAN y WAN, incluyendo NSF y Novell. Asimismo, Nextstep brinda acceso a los sistemas de archivos de Macintosh, MS-DOS y OS/2.

UnixWare

Se podría decir que Novell controla el mercado puesto que es dueña de la tecnología (es la que otorga las licencias). Sin embargo, en 1993 Novell transfirió la propiedad de la marca Unix de USL a X/OPEN Company Ltd., una organización internacional independiente que promueve aplicaciones abiertas de múltiples proveedores.

Univel, la empresa conjunta de Novell y USL, se formó con la idea de prestar más atención al usuario final dentro del sistema UNIX, tomando en cuenta que ya no había problema con la distribución.

UnixWare de Novell hace posible que los usuarios de UNIX ejecuten aplicaciones en hardware estándar a través de redes NetWare. UnixWare se empezó a distribuir a principios de 1993. Con él Novell tiene planeado desempeñar un papel importante en la computación corporativa. *"La escalabilidad de UNIX hará que Univel baje al nivel de las máquinas de escritorio gracias a su fuerza, su madurez y su vigor"* [Jeff Byrne, vocero de Univel, 1994]. Estudios de Univel muestran que en todo el mundo habrá una inversión de entre \$60,000 y \$70,000 millones de dólares en el sistema operativo UNIX. La mayor parte correrá en sistemas patentados, en las minicomputadoras más grandes o en procesadores RISC. Debido a que Univel quiere estar en todas las plataformas.

Características principales de UNIX

UNIX es una plataforma ideal para el desarrollo de aplicaciones de misión crítica y de soluciones de computo distribuidas y multiusuario, debido a que proporciona una amplia funcionalidad, propia de un sistema operativo avanzado y de múltiples características. Algunas de las características avanzadas de UNIX incluyen: multitareas, soporte de aplicaciones multiusuario gráficas y en modo texto, procesamiento en tiempo real, sistema de arquitectura de 32 bits, características mejoradas de seguridad, un robusto sistema de manejo de archivos y un poderoso ambiente de desarrollo.

Tabla 5-2 Características y Beneficios de UNIX (UNIX System V Release 4.2)

Característica	Beneficio
Ambiente poderoso de desarrollo	- Amplia selección de herramientas y utilerías disponibles - Rápido desarrollo de aplicaciones propias y a la medida
Módulos cargables dinámicamente	- Instalación de dispositivos mientras el sistema está en funcionamiento - Dispositivos removibles durante el funcionamiento del sistema, mantienen el kernel pequeño y eficiente
Interface de aplicación binaria	Soporta muchas aplicaciones UNIX existentes
Modularidad del kernel	Provista para una fácil actualización del sistema operativo
Sistema de archivos VERITAS (VFS)	- Provee un sistema de archivos reforzado - Integridad de los archivos en caso de interrupción eléctrica
Soporte de SNMP, PPP y SLIP	Provee soporte para línea serial estándar, administración de protocolos móviles y de red

Característica	Beneficio
Arquitectura de sistema de 32 bits	- Uso total de las capacidades de procesamiento de los procesadores de 32 bits - Aplicaciones de alto desempeño - Soporte para la migración hacia sistemas estándar de 32 bits
Funcionalidad Multitarea	- Soporte de procesamiento de aplicaciones en capas - Procesamiento en background
Procesamiento en tiempo real	- Agenda de proceso controlado por el usuario - Ideal para ambientes de producción y manufactura
Capacidades Multiusuario	- Soporte para múltiples terminales de usuario - Ruta de migración para aplicaciones actuales de multiusuario
MoOLIT GUI	Los usuarios pueden seleccionar entre el Look-and-Feel de Motif o el de OPEN LOOK
Desktop Manager	- Intuitivo, fácil de usar para los usuarios principiantes - Tiempo reducido para varios usuarios UNIX
X Window System	- Manipulación rápida de ventanas - Actualización rápida de pantallas para todas las aplicaciones - Acceso remoto de UNIX, DOS y Windows
Funciones poderosas de red	- Comunicaciones de STREAMS y TLI - Funciones de transporte independientes - Soporte simultáneo de múltiples pilas (IPX/SPX & TCP/IP)

Fuente: UnixWare Sales Guide, Novell

UNIX es un avanzado sistema operativo de propósito general para los sistemas estándares de la industria de cómputo basados en Intel. Como resultado de esto, UNIX proporciona varias capacidades que no son comunes en sistemas operativos especializados o menos sofisticados. Estas características hacen que UNIX represente una solución ideal para soportar aplicaciones críticas de negocios.

Emulación de UNIX para DOS y Windows

En OS/2 y Windows NT, la emulación de DOS y Windows 3.1 están incorporadas en el sistema operativo. Tanto OS/2 como Windows NT pueden ejecutar múltiples aplicaciones Windows de 16 bits en el modo mejorado, y el rendimiento en ambos productos es bastante razonable.

Los entornos de UNIX utilizan productos de emulación de DOS como el SoftPC de Insignia Solutions, Advanced Merge de Locus Computing Corp. y VPix de Phoenix Technologies. Hay aplicaciones de UNIX que emulan el entorno de DOS, haciendo pensar a las aplicaciones que realmente están trabajando bajo DOS. Sin embargo, en el rendimiento pueden haber limitaciones, tales como la inhabilidad de configurar una sesión de DOS con memoria extendida.

Hay varias estrategias de emulación de Windows en UNIX. La más común es ejecutar el código de Microsoft Windows bajo un emulador de DOS y luego ejecutar las aplicaciones de Windows bajo Windows. Aquí el rendimiento sufre y por lo general estará limitado a la operación de Windows en modo estándar. Algunos sistemas toman una ruta diferente, evitando a DOS y a Windows y convirtiendo las llamadas del API de Windows directamente a un API que el sistema operativo UNIX pueda entender, en este caso X Window. Un ejemplo es la *WABI* (*Windows Application Binary Interface*) de SunSelect que se distribuye con Solaris para X86 y Solaris SPARC, pero solamente puede apoyar a 13 aplicaciones de Windows.

Otra variación de la emulación en un entorno mixto de DOS y UNIX es equipar a los clientes de Windows para que ejecuten programas de X Window. Hay varios productos de emulación de X Window disponibles que pueden realizar esta tarea. Se piensa que los usuarios de Windows se confundirán con la apariencia de X Window, pero con Wintif de SCO, ahora en pruebas preliminares, las aplicaciones de X Window tendrán la apariencia de Windows.

Conectividad

Los sistemas operativos avanzados fueron creados para la conectividad. Muchos de los sistemas operativos de 32 bits están listos para conectarse a la mayoría de las LAN existentes incluyendo a Novell NetWare y TCP/IP nativo de UNIX. En casos donde la

conectividad no viene incluida en el sistema básico, existen excelentes opciones de conectividad (como productos añadidos)

UNIX se destaca en otra forma de conectividad que OS/2 y Windows NT no pueden manejar: La *conectividad de múltiples usuarios*. UNIX puede conectar hasta 512 usuarios simultáneos mediante conexiones asíncronas a terminales, al igual que una minicomputadora. Los sistemas UNIX de múltiples usuarios son excelentes en tareas como las terminales de punto de venta, sistemas de contabilidad, y otras aplicaciones para procesar transacciones donde la belleza y la gracia se sacrifican a favor de un punto de vista práctico, la estabilidad, y el bajo costo. Algunas versiones de UNIX también tienen colecciones enormes de aplicaciones empresariales para usar en este tipo de ambientes.

Soporte de UNIX para las redes

El sistema operativo UNIX puede ofrecer muchas capacidades a la gente que sabe como utilizarlo y administrarlo. Con la adición de interfaces gráficas del usuario, UNIX se ha vuelto agradable aún para los usuarios casuales. UNIX provee una capacidad robusta de multitareas que es importante para los sistemas operativos de las LAN, y puede ser un servidor de propósitos múltiples que cumpla con las necesidades de los usuarios de terminales y de LANs.

El trabajo en red con UNIX es una característica relevante, basado en la historia del sistema operativo en su soporte para usuarios remotos y conexiones UNIX punto a punto. El soporte de redes bajo UNIX siempre ha sido una de las ventajas del sistema operativo. Desde las capacidades básicas del UUCP hacia TCP/IP, NFS, y RFS, UNIX provee una variedad de formas para compartir información y recursos entre sistemas. Además de servir a redes de área local, UNIX lo hace mejor con redes de área amplia. La red más grande a lo largo del mundo, Internet, es un sistema host basado en UNIX.

UNIX provee una característica clave que los sistemas operativos de LAN necesitan, el pre-vaciado de multitareas. Esta capacidad habilita a UNIX a soportar cientos de procesos paralelos y simultáneamente servir a las solicitudes de cientos de usuarios.

Compartir archivos remotos (*RFS - Remote File Sharing*) y compartir archivos en red (*NFS - Network File Sharing*) son dos formas de habilitar a los sistemas UNIX a compartir

archivos. AT&T diseñó el RFS para facilitar el cómputo distribuido con UNIX System V. Sun Microsystems desarrolló NFS para su versión de UNIX. NFS es ampliamente utilizado ahora y está disponible en numerosos sistemas no-UNIX, incluyendo PCs con MS-DOS. RFS y NFS proveen muchas características en común, con pequeñas diferencias en sus estructuras.

Existen varias ventajas clave para usar UNIX en aplicaciones de red, incluyendo una herencia de soporte para redes, un sistema multitareas robusto, y un sistema operativo estable que ha estado operando por muchos años en una variedad de plataformas.

UUCP

UUCP, que significa *UNIX to UNIX Copy* (Copia de UNIX a UNIX), es una colección de programas diseñados para habilitar a los sistemas UNIX para intercambiar información sobre líneas telefónicas utilizando modems. Varios archivos y programas forman el paquete UUCP, incluyendo estas tres capacidades primarias:

- Transferencia remota de archivos
- Ejecución remota de comandos
- Transferencia de correo electrónico entre sistemas

El protocolo UUCP, el cual es tan viejo como UNIX, es un protocolo relativamente simple. Con él, se pueden enviar y recibir archivos desde y hacia otros sistemas UNIX, ejecutar programas en sistemas UNIX remotos, así como enviar y recibir correo con sistemas UNIX remotos. La posibilidad de ejecutar programas en un sistema remoto es estrictamente controlada por razones de seguridad.

Los programas como UUCP también existen para PCs basadas en DOS, y el código fuente para un programa llamado UUPC está disponible en varios sistemas de cómputo de universidades y en sistemas comerciales de boletines electrónicos. Con UUPC se puede conectar una PC (con MS-DOS) a una red UNIX (con UUCP).

Adaptabilidad de UNIX al hardware

Ningún otro sistema operativo puede correr en tantas plataformas de hardware como UNIX debido a un constante desarrollo de UNIX en lo que se refiere a la adaptabilidad al hardware, conservando su identidad y funcionalidad básicas.

Muchos proveedores de UNIX distribuyen versiones idénticas de UNIX que operan a través de un amplio rango de velocidades de procesadores y aún de múltiples procesadores. Debido a que UNIX opera en varias plataformas de hardware y a que existen varias versiones de UNIX, el código fuente para aplicaciones a menudo es gratis, o disponible a un costo mínimo. Si se desea tener un mantenimiento a largo plazo de una aplicación vertical, la mejor garantía es poseer el código fuente.

Con la introducción de la serie de estándares POSIX, los desarrolladores están en posibilidades de escribir aplicaciones que puedan ser desplazadas fácilmente hacia muchas plataformas y versiones de UNIX diferentes.

UNIX & Intel

"La tecnología de Intel depende mucho de la tecnología de Unix. En lo que se refiere a la reingeniería de diseño, tal vez Intel sea, actualmente, el mayor usuario de UNIX en toda la industria. UNIX constituye el *soporte fundamental* de los microprocesadores Intel. Todas las herramientas que Intel ha desarrollado internamente para la fabricación y el desarrollo de sus microprocesadores están basadas en UNIX" [21: pág. 47]

Intel depende de una red de estaciones de trabajo UNIX que actúan como servidores. Para 1995, la empresa habrá estado involucrada en la fabricación de 10,000 máquinas de escritorio, 3500 estaciones de trabajo ingeniería de diseño y 4000 computadoras que se utilizan en procesos de manufactura. Todas estas máquinas estarán basadas en el sistema operativo UNIX.

Consideraciones de programación

No se debe seleccionar un sistema operativo sin investigar las herramientas disponibles para crear aplicaciones. Por ejemplo, Windows NT está bien apoyado por excelentes herramientas de Borland, Microsoft, Symantec y Watcom. La mayoría de ellas no sólo incluyen a compiladores de C y C++, sino entornos gráficos de programación integrados (IDEs), extensos marcos de trabajo y generadores de códigos sofisticados para crear interfaces para el usuario, o automatizar tareas como la programación de OLE 2.0. OS/2 tiene disponibles herramientas similares de Borland, IBM y Watcom, pero éstas carecen de algunas características especiales.

En el lado de UNIX, la mayoría de los fabricantes incluyen u ofrecen una opción de sistema de programación para cada sistema operativo. Si se está cambiando de herramientas de programación de último modelo para DOS o Windows, probablemente se encontraran bastante modestos los entornos de programación para UNIX.

Aplicaciones

Probablemente la característica más importante de cualquier sistema operativo es la disponibilidad de aplicaciones de buena calidad y precio razonable. Se debe verificar la existencia de aplicaciones estándares para la oficina, aplicaciones poderosas para servidores tales como bases de datos SQL, y programas empresariales especializados. La mezcla variará significativamente de un entorno a otro.

En el lado de UNIX, las aplicaciones estándares para la oficina son escasas por lo general, mientras que las aplicaciones empresariales especializadas y las bases de datos abundan. Es importante notar que algunos entornos de UNIX, como *Interactive UNIX* y *SCO Open Desktop*, pueden intercambiar aplicaciones.

Desventajas del uso de UNIX

UNIX es el sistema operativo ideal, pero se deben considerar varias cosas antes de colocar a UNIX como el sistema operativo primario para el servidor de LAN o para estaciones de trabajo.

Una de las desventajas de UNIX es la variedad de versiones con las que cuenta. Se pueden obtener versiones de UNIX de muchas compañías diferentes, y aplicaciones que están lejos de ser compatibles a través de las diferentes versiones. Debido a la variedad de versiones de UNIX se debe trabajar exclusivamente con un sólo proveedor para soportar la instalación de UNIX.

El mercado para el software de UNIX indudablemente no es tan grande como el mercado para los programas Windows y probablemente será afectado por el mercado para el nuevo sistema operativo Windows NT. Basado en simple economía, un programa de mercado masivo costará más para un sistema UNIX que para un sistema Windows. Este costo incluye el sistema operativo. Sin embargo se puede comprar una copia de OS/2 por menos de US\$200 y MS-DOS por menos de US\$100, un sistema base de UNIX cuesta al

menos US\$700 y tal vez tanto como US\$7000, dependiendo en quien suministre el sistema y cuántos usuarios soporte. Esto constituye otra desventaja para los ambientes UNIX.

No se puede dejar de hablar de que la original simplicidad y elegancia de UNIX se ha ido. UNIX es ahora un sistema operativo grande y poderoso que puede ser tan difícil de mantener como su grandeza. Sin embargo los usuarios pueden ser aislados de la complejidades de UNIX por medio de interfaces gráficas para el usuario, sólo que alguien debe ser el responsable de mantener el sistema ejecutándose sin problemas. UNIX puede no ser la elección apropiada para *una compañía pequeña en crecimiento, con la única necesidad de un sistema operativo de red.*

Ventajas de UNIX

Las ventajas de UNIX sobre otros sistemas operativos que actualmente compiten con él en el mercado, se encuentran sintetizadas en las siguientes dos tablas. En la primera tabla se encuentran las ventajas de UNIX sobre Windows NT y en la segunda las ventajas sobre OS/2.

Tabla 5-3 Comparación entre UnixWare y Windows NT

	UnixWare	Windows NT
Estabilidad / Madurez	20 años, 5 generaciones	Nuevo
Base de App. Inst.	UNIX, DOS, Windows	Windows, DOS
Adaptabilidad con el medio existente	Cliente/Servidor Multiusuario, Peer-to-Peer	Cliente/Servidor Peer-to-Peer (no multiusuario)
Tipo de aplicaciones	Cliente, Productividad Personal y grupal	Productividad personal
Redes Privadas	NetWare, TCP/IP	TCP/IP

Fuente: UnixWare Sales Guide, Novell

Tabla 5- X Comparación entre UnixWare y Windows NT

	UnixWare	OS/2
Estabilidad / Madurez	20 años, 5 generaciones	Kernel de 16bits/32bits
Crecimiento	Estándares en S. A.	Nuevo microkernel?
Compatibilidad Futura	UI roadmaps, X/Open	Productos Apple / IBM-Taligent
Soporte de Redes	UNIX, NetWare	LAN server
Enfoque de aplicaciones	Cliente/Servidor Multiusuario	Multiusuario

UNIX en la implementación de los Sistemas Abiertos

El ambiente común del software abierto

(*Common Open Software Environment -COSE*)

El 17 de marzo de 1993 seis proveedores líderes de sistemas UNIX, incluyendo a Univel, HP, IBM, SunSoft, Unix System Laboratories y SCO, anunciaron su intento de desarrollar un proceso de sistemas abiertos para proveer estándares comunes para las plataformas del sistema UNIX. Este proceso, conocido como el proceso COSE, está intentado proveer especificaciones para varias áreas del ambiente de cómputo incluyendo el desktop y la multimedia. Las especificaciones de desktop, por ejemplo, proveen un look -and-feel consistente, para usuarios de desktop y provee a los desarrolladores un conjunto común de APIs para escribir sus aplicaciones. Con ésto los usuarios se beneficiarán en varias formas:

- Una base más amplia de plataformas UNIX estandarizadas atraerá inversiones de proveedores de software independientes de alto nivel, para proveer a los usuarios de nuevas soluciones UNIX.
- Compartir tecnologías lo cual significará software para sistemas UNIX de más alta calidad, disponible pronto por parte de la mayoría de los proveedores.
- Un ambiente común creará una mayor interoperabilidad entre diferentes sistemas UNIX de distintos fabricantes y reducirá los costos de los clientes, tales como el mantenimiento y entrenamiento de empleados.

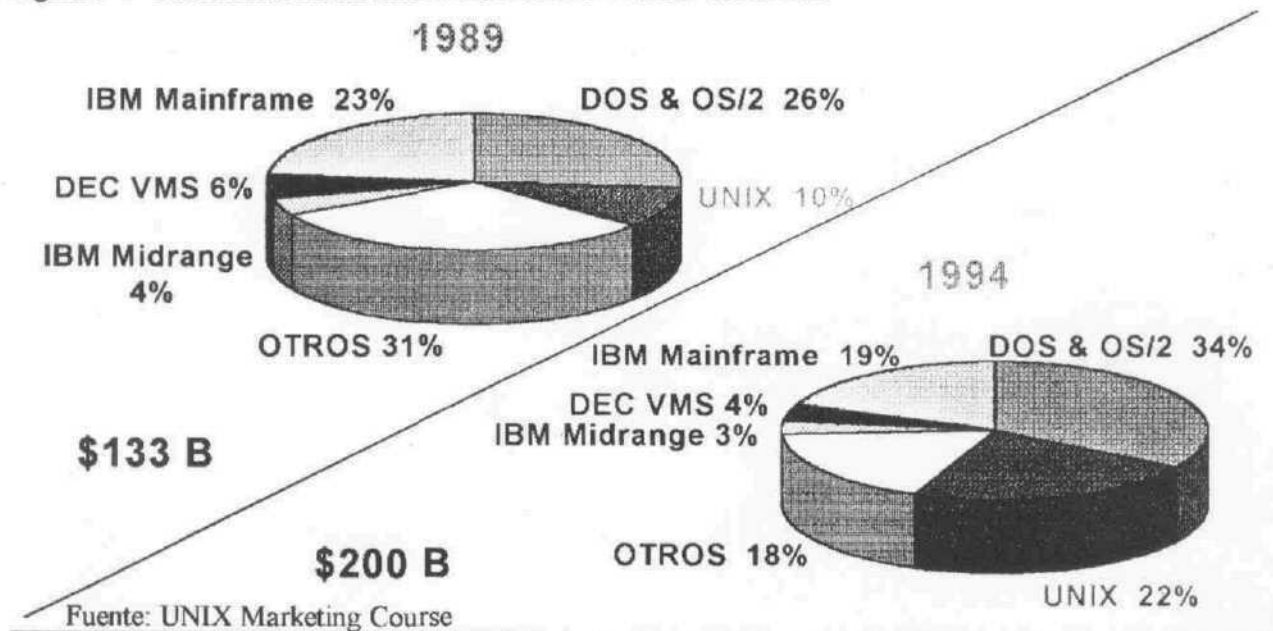
El anuncio del proceso COSE también incluye un reaseguramiento hacia los clientes que están adquiriendo UnixWare hoy UnixWare ya incluye mucha de la tecnología desktop anunciada, por ejemplo, y proveerá un compatibilidad completa y una clara ruta de actualización para el futuro.

Para crear los ambientes comunes, los fabricantes de UNIX participantes compartirán previamente la tecnología propietaria uno con otro Para el *Common Desktop Environment*, por ejemplo Hewlett-Packard proveerá su Visual User Environment GUI y SunSoft hará disponible sus utilidades productivas DeskSet.

Como parte de esta contribución Novell ha acordado redirigir la especificación para el cliente NetWare UNIX hacia *X/Open* (un cuerpo de estándares líderes independiente). *X/Open* pondrá la especificación para el cliente Netware UNIX a disposición de todos los fabricantes de UNIX participantes. Todos los fabricantes de UNIX participantes han acordado ofrecer la funcionalidad del cliente Netware de UNIX con sus sistemas. Esta funcionalidad es actualmente una característica estándar de UnixWare.

Novell se benefició desde este anuncio, ya que su enfoque en la arquitectura de Intel los provee con un mercado sustancial de desktop, el cual no está siendo atacado por los proveedores de RISC (HP, IBM, Sun). La integración del NetWare para UNIX legitima a UnixWare en el mercado. Finalmente, este esfuerzo de ingeniería cooperativa da a los fabricantes de UNIX un arma poderosa en contra de Microsoft y Windows NT, y en particular habilita a UnixWare para competir aún más efectivamente por el mercado de desktop avanzado.

Figura 5-6 Crecimiento de los sistemas abiertos al rededor del mundo



Ninguna plataforma soportará las miles de aplicaciones que están disponibles en los sistemas UNIX, ni proveerán la escalabilidad de Unix desde una laptop hasta una supercomputadora. Otros sistemas operativos (como Windows NT y OS/2) requieren mayor rearquitectura cuando la empresa lleva sus aplicaciones personalizadas o semipersonalizadas hacia el downsizing desde mainframes o minicomputadoras, debido

a que Windows NT y OS/2 carecen de las características de funcionabilidad de multiusuarios de estas aplicaciones y de UNIX. Además, estos productos no ofrecen un sistema de gráficas distribuido (X Window).

Diferentes ambientes UNIX

Por muchos años, la única forma de usar un sistema UNIX era a través del *shell* de UNIX: el prompt de comandos. En años recientes, se han desarrollado ambientes gráficos, basados en el sistema X Window System. Usuarios y grupos de la industria han extendido la funcionalidad básica del X Window System para proveer un aspecto común para las interfaces gráficas. Las dos interfaces más comunes son *Motif* y *Open Look*.

X Window System

El X Window System, o sólo X, fue creado en el Instituto de Tecnología de Massachusetts (MIT) en 1984. Para enero de 1986, Digital Equipment Corporation anunció el primer uso comercial de X en su VAXstation-II/GPX. Debido a que otras compañías se vieron envueltas, muchas contribuyeron con comentarios y kits de herramientas para la distribución de X Window. Más tarde en 1986, Digital contribuyó con recursos significativos de personal al proyecto X, y X fue reescrito hasta la versión 11. Durante 1987, el MIT y nueve corporaciones se unieron para crear el Consorcio X, fundado por las compañías participantes, encargado de soportar y controlar el desarrollo y evolución del X. El código fuente del X está disponible públicamente.

X y la biblioteca de funciones básicas, *xlib*, forman el fundamento para un ambiente de procesamiento distribuido. Este consiste en una definición de protocolo y un conjunto de funciones de bajo nivel. La mayoría de aplicaciones escritas para X están escritas usando una de las dos interfaces estándares líderes para X, *Motif* y *Open Look*.

La interface del usuario Open Look es similar en operación a *Motif*, sin embargo las pantallas se ven un tanto diferentes. Estos dos estándares mayores existen con Open Look, soportado por UNIX System Laboratories y Sun Microsystems, y *Motif* impulsado por la Open Software Foundation. Los programas escritos para una sola interface estándar no corren en el otro estándar.

La última versión de UNIX del UNIX System Laboratories (USL) para el mercado de las estaciones de trabajo basadas en procesadores Intel, llamado UnixWare, soporta ambas interfaces Open Look y Motif. Esta versión está siendo producida por UNIVEL, una unión entre USL y Novell.

La interface Motif

Afortunadamente para los usuarios de computadoras, todas las interfaces gráficas del usuario (GUIs) para OS/2, MS-DOS, y UNIX tienen un alto grado de similitud. Si se ha usado Windows, no habrá problema para usar un ambiente Motif. Si se ve el desktop básico de Motif, se puede observar que incluye los menús de persiana (drop-down), las ventanas del administrador de programas, y los iconos que representan archivos y programas. (Diferentes versiones de UNIX, aún aquellas que compartan la interface Motif, pueden usar diferentes iconos para representar tipos de archivos, tales como archivos de datos y de programas).

Las interfaces GUI de UNIX difieren significativamente en términos de su organización, la funcionalidad de interfaces es constante. Así como en Windows y OS/2, se presentan una serie de ventanas e iconos seleccionables a través del mouse. Una ventana de administrador de archivos permite maniobrar alrededor del sistema de archivos de UNIX.

Unix International & Open System Fundation

USL es la organización que implementa las definiciones de tecnología como las previstas por Unix International (UI). UI es una conglomeración de un número de proveedores, de los cuales ninguno controla actualmente a la organización. En este sentido, UI y OSF son organizaciones paralelas. UI ha especificado un plan de desarrollo a 5 años para UNIX y eso es algo a lo que todos los miembros de UI se han adherido. OSF no tiene una estrategia clara de desarrollo para el sistema operativo.

Apesar de que la mayoría de los sistemas UNIX en los últimos años fueron vendidos en los ambientes técnicos, en la actualidad cada vez más organizaciones han implementado UNIX para aplicaciones comerciales.

Es cierto que existen muchas versiones de UNIX, por lo que no se pueden mover aplicaciones UNIX del sistema de un fabricante al de otro fácilmente, debido a que estas

aplicaciones fuerón propietarias. También es cierto que UNIX proporciona toda la protección a la inversión y el acceso al software de aplicación que se solicite.

Algo que no debe olvidarse es que para poder implementar una LAN de PCs, se debe elegir un sistema operativo de red propietario, tal como Novell. Si se usa UNIX se está al menos considerando un sistema operativo abierto.

Sistemas Abiertos y Sistemas Distribuidos

Las inversiones hechas en un sistema central son para proveer las aplicaciones necesarias. Para implementar un sistema distribuido es necesaria una inversión adicional. Un sistema distribuido es mucho más efectivo que expandir el sistema central por muchas razones, incluyendo el bajo costo de la tecnología distribuida, la fácil disponibilidad de aplicaciones y la estructura de soporte simplificada que se necesita. La implementación de un sistema distribuido basado en UNIX trae consigo las siguientes ventajas:

- Aplicaciones de terceros
- Flexibilidad
- Reducir futuros costos mediante un crecimiento modular

Se han instalado sistemas distribuidos para resolver el problema de obtener información necesaria de una colección de aplicaciones de PCs y mainframes. Se usan ambientes estándares y estaciones de trabajo amigables a el usuario, para integrar información de muchas fuentes diferentes. Los usuarios ven toda esta información en un formato común en la pantalla. Esta es una de las razones que nos conducen hacia la implementación de sistemas abiertos.

UNIX está directamente involucrado en los procesos de down-sizing y de right-sizing su presencia en estos dos procesos hace posible el migrar aplicaciones desde tecnologías propietarias caras, hacia tecnologías abiertas más accesibles económicamente para la empresa.

Conclusión

Los usuarios exigen confiabilidad, efectividad a bajo costo y apoyo para le usuario final. Quieren aplicaciones empresariales basadas en UNIX para trabajar consistentemente, sin importar la marca o modelo del hardware en que estén instaladas, con el propósito de proteger sus inversiones relativas a la optimización de los procesos de negocios y a la capacitación del usuario final

La plataforma de UNIX desempeñará un papel relevante en el proceso llamado down-sizing a medida que los administradores de sistemas de información se den cuenta de todos los beneficios que brinda un sistema operativo que ha demostrado su utilidad por más de 20 años.

En el futuro el sistema operativo Windows competirá con UNIX en el mercado de los sistemas operativos multiprocesadores y multiusuarios, pero la tecnología de Windows NT tardará en madurar .

En base a las tendencias que siguen los sistemas operativos respecto a nuevas aplicaciones, UNIX muestra una presencia importante en toda una variedad de plataformas de hardware, particularmente en PC's de alcance medio y en máquinas conectadas a una red. Pero incluso en las PC autónomas, que es un sector en el que DOS y Windows ejercen una presión considerable, UNIX mantiene un porcentaje de usuarios notable

Otro factor del éxito de UNIX es que, mientras otros sistemas operativos han tenido serios problemas en su evolución (como lo es OS/2), UNIX lleva ya varios años trabajando con éxito en el área empresarial.

UNIX es un sistema multiusuarios y multiprocesos, mientras que Windows no es un sistema multiusuarios. OS/2 tampoco es un sistema multiusuario, aunque tiene un buen desempeño en el área de multitareas. Otro aspecto que favorece a UNIX es que existen aplicaciones para DOS y Windows que están disponibles para servidores UNIX.

A medida que los usuarios abandonen los servicios y las aplicaciones en sistemas centrales de minicomputadoras o mainframes, o que elaboren nuevas aplicaciones fundamentales para los negocios, se irán trasladando a la plataforma de UNIX.

Es muy importante que haya estándares en la industria para ofrecer garantía de interoperabilidad, escalabilidad y compatibilidad en las aplicaciones.

UNIX se ha incorporado a la corriente principal del ambiente corporativo y ha demostrado su utilidad y eficiencia para realizar labores delicadas. UNIX es realmente un sistema operativo abierto: maduro, estable y bastante probado.

La mayoría de los expertos coinciden en que el mercado se orienta en esa dirección y en que UNIX aumenta su presencia en las máquinas de escritorio, particularmente con aplicaciones de Lotus, Novell, Borland, Oracle y Corel.

Kirzne afirma que "En nuestros días, los consumidores no se fijan en el sistema operativo. Están más interesados en el servicio, el apoyo, las aplicaciones y los estándares en que se basan los sistemas".

De acuerdo con Schwark, de Novell, "El ser diferente ya no representa una cualidad", ya que los proveedores que antes ofrecían productos únicos o patentados ya cambiaron de enfoque, ya que UNIX se ha colocado en primer plano.

Capítulo VI. Implementación de un sistema abierto

Dado el objetivo principal de este trabajo, que es el de mostrar que el sistema operativo UNIX es el sistema operativo más viable para ser base de la implementación de sistemas abiertos, en este capítulo se describen los pasos necesarios para implementar un sistema abierto, basado en UNIX, incluyendo la interconexión de hardware y la instalación del software necesario para comunicar a los diferentes sistemas operativos que residen en cada una de las computadoras que forman parte del sistema.

Aquí se describe la forma en que se puede implementar un sistema abierto, estableciendo todas las características que debe cumplir tanto el hardware como el software de cada estación de trabajo que forma parte del sistema abierto

El sistema abierto que se implementa aquí consta de varios componentes que son

- Un servidor de archivos NetWare 3.12
- Un servidor de archivos UnixWare 1.1
- Una estación de trabajo OS/2 2.11
- Una estación de trabajo MS-DOS 6.2 / Windows 3.11

Estos equipos estarán interconectados entre sí en una topología de bus, utilizando cable coaxial delgado con conectores BNC, siguiendo las especificaciones del estándar Ethernet.

Especificación de los requerimientos para la implementación del sistema abierto

Dentro de los requerimientos que deben cumplirse para la implementación de un sistema abierto, se deben tomar en cuenta por separado.

- Los requerimientos de hardware y*
- Los requerimientos de software.*

Los requerimientos de hardware

La parte más importante de un sistema abierto y de cualquier red de computadoras es el *servidor* (*server*). El proceso de determinar cual servidor se debe adquirir debe iniciar tan pronto como se haya elegido un sistema operativo. La adquisición del hardware apropiado para albergar el sistema operativo seleccionado, determina directamente el éxito en la implementación del sistema abierto.

Antes de seleccionar el hardware del servidor, se debe determinar el tipo de servidor de archivos: un servidor de archivos o un servidor de base de datos. La distinción clave entre las implementaciones es que las estaciones de trabajo generalmente desempeñan un procesamiento de servidor de archivos, y el servidor tiene los trabajos de procesamiento en un servidor de base de datos. Cuando se busca un "servidor de archivos", se debe dedicar mucho tiempo a la búsqueda de los componentes del canal apropiado de LAN, tal como la topología, la tarjeta de interface de la red (NIC), y los drives de disco. Si el servidor está destinado a ser un "servidor de base de datos", se debe considerar el desempeño y la confiabilidad (poder de procesamiento, diseño del bus, y la tolerancia general a fallas, tales como fuentes de poder, drives de disco, y el servidor).

El sistema operativo y las aplicaciones que se seleccionen ayudarán a distinguir entre las diferentes implementaciones de servidores. El software del servidor de base de datos a menudo puede tomar ventaja del poder del procesamiento simétrico, por ejemplo, y la mayoría de las aplicaciones del servidor de archivos no pueden.

La importancia de hardware de alta calidad

La importancia de implementar hardware de alta calidad para el servidor puede no estar suficientemente enfatizada, especialmente en caso de situaciones desastrosas como caídas del sistema o pérdidas de datos. Algunas personas confían en un proveedor específico y creen que éste hace hardware perfecto; otras no creen aún que el hardware perfecto exista. Para llegar a una solución, el hardware debe ser visto desde la perspectiva de costo versus desempeño versus calidad. Se debe comparar esta perspectiva contra las funciones e importancia de la máquina. Después de considerar las restricciones presupuestales y cuánto tiempo de caída de la red puede tolerar el ambiente, se puede decidir cuánta calidad es necesaria.

Confiabilidad, desempeño, y calidad, todas tienen un lugar definido en el ambiente de red. Mucha gente erróneamente descarta las máquinas de bajo costo porque asumen que las máquinas son de menor calidad. En una red de una preparatoria, por ejemplo, en la cual los estudiantes usan las computadoras en un laboratorio, las aplicaciones de misión crítica no son utilizadas. Por lo tanto, si la red se cae sólo hay que encenderla de nuevo.

Más importante aún, es el error común de usar hardware de baja calidad en ambientes de misiones críticas. Se debe considerar el costo de la calidad, y por último, el costo del tiempo de caída.

Por lo anterior, se puede afirmar que *un sistema abierto requiere de hardware de alta calidad*, debido a que la mayoría de las aplicaciones que en él se ejecutarán, serán de misión crítica.

Debido a que el servidor es la base de cualquier red o sistema abierto, la red o sistema abierto pueden ser sólo tan buenas como el servidor sea. Si el servidor se cae en un ambiente de un sólo servidor, la red se caerá. Además, un servidor de calidad es sólo tan bueno como un sólo componente: si el disco duro falla, el sistema falla; si la fuente de poder se muere, el sistema se muere. Como la importancia del tiempo de trabajo del sistema crece, por lo tanto, la importancia de adquirir una máquina con componentes de calidad crece exponencialmente. Si se adhiere a este concepto la inversión de tiempo y el esfuerzo de compra de una base confiable (el servidor), el tiempo de caída se vuelve la menor de las preocupaciones.

Los servidores basados en procesadores Intel

El desempeño del servidor es una porción vital de la duración y la productividad del sistema abierto. Dos de los más importantes factores determinantes del desempeño en un servidor, son el bus de E/S y el procesador. Para ser eficiente, esos dos componentes deben estar bien balanceados (teniendo un procesador rápido y un bus de E/S lento, por ejemplo, se crea un cuello de botella y disminuye el desempeño del servidor)

Selección del procesador

El procesador es el corazón del servidor. Si éste tiene un buen “corazón”, es un servidor fuerte; de la misma manera, si el “corazón” es débil, el servidor es débil. En

situaciones de bases de datos pesadas, un segundo corazón comúnmente es adicionado para descargar algo del trabajo. Este proceso es comúnmente llamado *procesamiento discreto, o simétrico*. Algunas máquinas soportan este tipo de diseño, y otras están diseñadas alrededor de este concepto, el sistema operativo, de cualquier manera, determina la capacidad para usar esas mejoras de desempeño.

Debido a que algunos de los sistemas operativos que pueden usarse en un sistema abierto son de 32-bits, se requiere al menos un procesador de 32-bits para poder utilizar esos sistemas operativos. Cuando se habla de procesadores de 32-bits se debe usar un vocabulario totalmente nuevo: verdadero pre-vaciado de multitareas, multihilos, y administración de memoria virtual.

Se describen a continuación los procesadores para servidores, y se da una explicación técnica de por qué los procesadores difieren y en cuáles situaciones se deben o no usar.

Intel 80386 SX

El Intel 386 SX, el procesador de 32-bits más pequeño, es el requerimiento mínimo para la mayoría de los sistemas operativos de red. El término "mínimo" ciertamente define este procesador debido a que el 386 SX fue diseñado como un chip de estrategia de mercado para reemplazar los viejos procesadores 286. El 386 SX tiene sus propias capacidades limitadas, específicamente, puede manejar memoria en sólo un modo de 16 bits y puede direccionar un total de sólo 16 Mb de memoria. El ambiente de servidor de 32-bits tiene muy poco espacio para el 386 SX como un servidor.

Intel 80386 DX

El procesador 386 DX, es un verdadero procesador de 32-bits capaz de manejar una ruta de datos de 32-bits, 4 Gb de memoria física, y 64 Mb de memoria virtual. En términos más simples, el 386 de 32-bits hace posible el procesamiento concurrente de red. El procesamiento concurrente de red consiste de varias conexiones (estaciones de trabajo) que simultáneamente pueden usar diferentes porciones del procesador del servidor. Los procesadores 386 DX de Intel son útiles en el mercado de servidores y llenan el nicho de servidores de nivel menor.

Intel 80486 SX

El 486 es ofrecido en cinco modelos: SX, DX, DX2, DX4 y OverDrive. El 486 SX fue lanzado después de las versiones DX y, como el 386 SX, es el nivel menor de la familia 486. El procesador 486 SX tiene el mismo conjunto de instrucciones optimizado y el caché interno como la línea DX lo tiene; debido a que la unidad de punto flotante (FPU) o porción del coprocesador ha sido deshabilitado, ha sido nombrado el *procesador disminuido*.

A diferencia del 386 SX, el chip 486 SX tiene lugar en el mercado de los servidores. Un servidor bien diseñado, basado en el chip 486 SX, provee un compromiso para sistemas con restricciones de presupuesto. Un servidor 486 SX es más rápido que un servidor 386 DX, pero el costo entre un 486 SX y un 486 DX es mínimo. Por lo tanto, si es posible, se debe adquirir un verdadero servidor 486 DX, es definitivamente más rápido.

Intel 80486

Los sistemas operativos sofisticados pueden detectar que están trabajando sobre un CPU 486 y automáticamente tomar ventaja del conjunto de instrucciones especiales que el 486 ofrece. Su interface de memoria se beneficia por un controlador de caché y 8 Kb de caché interno. El caché interno, localizado dentro de la arquitectura, incrementa la velocidad a la cual procesa comandos, especialmente comandos de 32-bits. Un caché de 486 usa una asociación de conjuntos de cuatro formas, un modo de transferencia de datos explosivo que habilita al procesador para enviar cuatro instrucciones de 32-bits en cinco ciclos de reloj. (En el mejor de los casos, el 386 tarda ocho ciclos de reloj). El controlador de caché, el caché interno, la transferencia explosiva, el coprocesador interconstruido, y 1.2 millones de transistores, hacen al chip 486 el preferido sobre el procesador 386 como un servidor de red.

Pentium (Anteriormente P5 y 586)

Es difícil comparar el chip P5 (el equivalente de un 586) con otros procesadores. El P5, medido en millones de instrucciones por segundo (MIPS) en lugar de MHz, sobrepasa cinco veces o más la velocidad de los procesadores 486 más veloces.

Intel involucró a varios proveedores líderes en el proceso de desarrollo de su procesador Pentium. El Pentium incluye un bus de datos de 64-bits (el doble del de un 486) y soporta la nueva generación de memorias RAM dinámicas de diez nanosegundos.

La siguiente lista muestra algunas de las características del Pentium:

- Opera a 66 MHz. (su velocidad oficial es 100 MIPS)
- Tiene 16 Kb de caché interno
- Tiene un conjunto de instrucciones de 32-bits
- Usa una ruta de datos de 64-bits

Requerimientos de hardware de los sistemas operativos

Los sistemas operativos que se integrarán al sistema abierto que se va implementar, requieren ciertas configuraciones de hardware para instalarse y trabajar adecuadamente

En la siguiente sección se describen las características que deben poseer las estaciones de trabajo, para poder albergar los sistemas operativos del sistema abierto

IBM OS/2

La versión de OS/2 que se va utilizar en este sistema abierto es la 2.11, la cual necesita los siguientes requerimientos de hardware:

- Computadora con procesador Intel 386 SX o superior
- 4.0 Mb de memoria RAM (mínimo), IBM recomienda al menos 6.0 Mb
- Drive de 3½ pulgadas
- Monitor a color VGA o de resolución superior
- Disco duro con al menos 20 a 40 Mb libres
- Mouse

Microsoft Windows

La versión de Windows que se va a instalar para este sistema abierto es la 3.11 para Trabajo en Grupo la cual necesita los siguientes requerimientos:

- Computadora con procesador Intel 386 SX o superior
- 3.0 Mb de memoria RAM (mínimo), Microsoft recomienda al menos 4.0 Mb
- Drive de 3½ pulgadas
- Monitor a color VGA o de resolución superior
- Disco duro con al menos 10.5 Mb libres, Microsoft recomienda 15.5 Mb
- Mouse

Novell NetWare 386

La versión de NetWare que se va a instalar como uno de los servidores en este sistema abierto es la 3.12 la cual necesita los siguientes requerimientos:

- Computadora con procesador Intel 386 SX o superior
- 4.0 Mb de memoria RAM (mínimo), Novell recomienda calcular la memoria según el número de volúmenes en el servidor
- Drive de 3½ pulgadas
- Disco duro con la capacidad suficiente para albergar todas las aplicaciones que se deseen tener en la red.

Novell UnixWare 1.1

La versión de UnixWare que se va a instalar como uno de los servidores en este sistema abierto es la 1.1 Personal Edition la cual necesita los siguientes requerimientos.

- Computadora con procesador Intel 386 SX o superior
- 8.0 Mb de memoria RAM (mínimo)
- Drive de 3½ o 5¼ pulgadas para bootear UnixWare
- Disco duro con un mínimo de 80 Mb
- Disco duro adicional con un mínimo de 40 Mb (opcional)
- Mouse
- Un mínimo de 10 a 20 Mb de espacio en disco libre por cada producto adicional add-on.
- Drive de CD-ROM

Nota: En todos los sistemas operativos anteriormente mencionados, se requiere que el equipo cuente con una tarjeta de interface de red (NIC), que cumpla con los estándares Ethernet para conectarse en red, es decir, para formar el sistema abierto.

Los requerimientos de software

La posibilidad de compartir aplicaciones de software es una de las razones primarias por la que la gente instala redes y sistemas abiertos. La selección de aplicaciones de red es un poco más compleja que la elección de paquetes para un ambiente de un sólo usuario. El conocer qué es lo que se debe buscar cuando se compra, es la clave para encontrar un producto que beneficie a los usuarios. Esta lista muestra algunos puntos a considerar

- Conciencia de la red
- Interoperabilidad de la red
- Soporte multiusuario
- Documentación específica de red
- Soporte para redes de las aplicaciones
- Opciones de licencia

No se deben olvidar las dos reglas más importantes para elegir una aplicación. Primero, ésta debe cumplir las necesidades de los usuarios. Si no lo hace, es la elección incorrecta para la red, no importa que tan fácil es de usar y cuántas características tenga. Segundo, se debe asegurar que el hardware es lo suficientemente poderoso para el software que se está considerando.

Cuando se busca software para correr en la red, se debe elegir un producto que sea para red. Esto se hace, porque las aplicaciones que son para red, corren mejor en una red que una versión stand-alone. Estas aplicaciones tienden mucho menos a caerse, y por lo tanto, a causar problemas. Cuando se busquen paquetes de software, se deben recordar las tres categorías básicas de las aplicaciones:

- Network-blind
- Network-aware
- Network-inherent

Estas categorías están basadas en el artículo de Michael Rockwell, en el *Windows-DOS Developer's Journal* de diciembre de 1991.

Las aplicaciones network-blind (ciegas de la red) no están conscientes de que están corriendo en una red. Estos paquetes, diseñados para el uso en red, pueden trabajar en una LAN, pero no hacen nada para protegerse en un ambiente multiusuario. Por ejemplo, se instala una aplicación de hoja de cálculo network-blind en la red, pero ésta no lo sabe. Un usuario ejecuta el programa y le pide que cargue una hoja de cálculo. Este lo hace, y luego otro usuario entra en la red, ejecuta la aplicación, y carga la misma hoja de cálculo. Momentáneamente la aplicación actúa confusamente, despliega la hoja de cálculo en la pantalla del segundo usuario. El primer usuario cambia algunos números en la hoja de cálculo, guarda su trabajo, y hace alguna cosa más. El otro usuario también hace algunos

cambios y guarda el archivo. Ahora se tiene un escenario "last one wins" (el último gana). La versión que fue guardada al último sobrescribe los cambios que cualquier otro más hizo mientras el archivo estuvo abierto.

Las aplicaciones network-aware (conscientes de la red) tienen algunos controles básicos interconstruidos para bloqueo de archivos: las aplicaciones no deben cuidar dónde están o en qué tipo de red se encuentran, pero ellas saben cuántos usuarios las están usando simultáneamente. Por ejemplo, se tiene una aplicación de hoja de cálculo la cual es network-aware. El primer usuario ejecuta la aplicación y abre una hoja de cálculo, y la aplicación muestra el archivo en la pantalla. El segundo usuario carga la aplicación de nuevo y abre la misma hoja de cálculo. La aplicación despliega el mensaje "Acceso Denegado". La mayoría de las aplicaciones probablemente se encuentren dentro de esta categoría.

Para que una aplicación sea clasificada como network-inherent (natural de red), debe tener fuertes lazos con el sistema operativo y manejar sus funciones de una forma parecida a la red. Los servidores de bases de datos, por ejemplo, hacen uso de la semejanza de la red cliente-servidor a través de métodos de procesamiento distribuido. Para una base de datos grande o un paquete de contabilidad, a menudo se debe dedicar una máquina al manejo de grandes cantidades de datos. Este tipo de máquina es llamada el *servidor de base de datos (database server)*. Cuando se hace una consulta a la base de datos desde cualquier máquina, el servidor de base de datos usa su propio procesador para procesar la solicitud y envía a través del cable de la red sólo los datos que se solicitaron, lo cual acelera la operación notablemente.

Implementación de un servidor NetWare

Para la implementación de un servidor NetWare se debe contar con un equipo que cuente con las características mencionadas en los requerimientos de hardware para el Novell NetWare 386.

- I. Se debe tener el equipo completamente instalado y con la interface de red instalada, y debe contar al menos con una estación de trabajo para poder instalar el software de aplicación al servidor.

Para instalarlo se debe contar con lo siguiente:

- Una copia de la hoja de trabajo del servidor de archivos (File Server Worksheet) que viene al final del manual de instalación (Installation and Upgrade).
- Copias de trabajo de los diskettes de instalación del NetWare 386 v3 12
- Copia de los diskettes de drivers de hardware de terceros (como el driver para la interface de la red)

II. Se debe calcular la memoria que necesita el servidor, para lo cual se debe hacer lo siguiente:

1. Se requieren al menos 4 Mb para cargar el sistema operativo, los drivers de disco y tarjetas, y el INSTALL.NLM.
2. Multiplicar la cantidad de espacio en disco del sistema (en Mb) por 0.008 y añadir este número a los 4 Mb iniciales
3. Adicionar de 1 a 4 Mb para un buffer de memoria Caché para optimizar el desempeño.

III. Se debe usar la copia de la hoja de trabajo (File Server Worksheet) para grabar la siguiente información acerca del servidor de archivos:

- Servidor de archivos: nombre, fabricante, y modelo
- Tamaño de memoria
- Tarjetas de red: drivers de LAN asociados, número de red, dirección de I/O, dirección de memoria, interrupción, o dirección de estación
- Otras tarjetas que no sean de red: tipos y configuraciones
- Drive de diskettes: tamaño del diskette y tamaño del almacenamiento
- Discos internos: fabricante, modelo, y capacidad de almacenamiento
- Tarjetas coprocesadoras de disco (DCB): drivers DCB y dirección I/O
- Sub-sistema de disco: número de drives, tipos de drives, tamaño de almacenamiento, número de cabezas y cilindros

IV. Se debe decidir dónde poner los archivos de arranque del servidor, ya que se puede arrancar el servidor desde un diskette de arranque o desde una pequeña partición de

DOS en un disco duro interno. Las ventajas de cada uno son las siguientes:

Ventajas del diskette de arranque.

- La creación de diskettes de arranque es más rápido que crear particiones de DOS en los discos duros.
- El disco duro entero puede ser usado para una partición de NetWare.
- Los discos de arranque pueden ser almacenados aparte del servidor de archivos para evitar accesos no autorizados.

Ventajas del disco duro:

- Después de la instalación, el arranque del servidor de archivos es más rápido.
- El riesgo de falla del disco es mucho menor.
- Si se desea tener los drivers, los módulos de ayuda y el sistema operativo se deben tener libres al menos 4 Mb de espacio en disco.

Nota: Las máquinas que no cuentan con discos duros conectados a una controladora interna de bus estándar deben arrancar con un diskette de boot

Si se elige arrancar desde un diskette se debe hacer lo siguiente

a. Cargar el DOS

b. Crear el diskette de arranque del servidor

- Formatear un diskette de alta densidad como disco del sistema
- Copiar del diskette *System-1* al diskette de arranque los siguientes archivos:

SERVER.EXE

NUT.NLM

NWSNUT NLM

c. Copiar el driver del disco para el sistema del diskette *System_2*

d. Crear el archivo *autoexec.bat* en el directorio raíz del diskette de arranque con la siguiente línea.

SERVER

Si se elige arrancar desde un disco duro se debe hacer lo siguiente:

- a. Insertar el diskette INSTALL en el drive a: y reiniciar la computadora, o cambiarse al drive a: y teclear INSTALL.
- b. Seleccionar la opción "Install new NetWare v3.12" del menú "Select an Installation Option"
- c. Determinar los requerimientos de la partición del disco para DOS.
Se recomienda crear una partición DOS de un mínimo de 5 Mb.
- d. Seleccionar la opción "Create a new DOS partition".
- e. Seleccionar "Create a DOS partition".
- f. Introducir el tamaño (en MB) de la nueva partición
- g. Formatear la partición recién creada de DOS.
- h. Nombrar el servidor de archivos. Dar al servidor un nombre único utilizando las siguientes reglas:
 - El nombre puede tener entre 4 y 298 caracteres
 - Caracteres legales incluyen cualquier caracter alfanumérico, subrayado, y guiones.
 - El nombre no puede contener un punto (.).
 - Los espacios no están permitidos.
- i. Asignar un número IPX interno de red
- j. Presionar <ENTER> para copiar los archivos de arranque del servidor hacia el disco duro. Durante el proceso de copia se solicitará que se inserten los diskettes de NetWare.
- k. Introducir el Country Code, el Code Page, y el Keyboard Mapping y presionar <F10>
- l. Seleccionar el formato para los archivos DOS.
- m. Adicionar SERVER.EXE al archivo AUTOEXEC.BAT
- n. Insertar el diskette INSTALL y presionar <ENTER>.

Se debe usar la hoja File Server Worksheet para guardar el nombre del servidor de archivos y el número interno de red

V. Cargar los NLM (NetWare Loadable Module) para los drives de disco

1. Cargar el driver del disco

• Para cargar el driver del disco se debe teclear lo siguiente.

LOAD *[ruta] driver_disco*

Se debe reemplazar *ruta* por la letra del drive local que contiene el driver del disco. Se debe reemplazar *driver_disco* con IDE, ya que este es el caso del sistema abierto a instalar.

2. En los servidores de arquitectura estándar, se debe introducir el puerto de dirección I/O.

VI. Crear tablas de partición de disco NetWare.

Una vez que los drives de disco han sido cargados se debe utilizar INSTALL.NLM para crear una partición NetWare en el disco duro.

1. Para cargar el INSTALL se debe teclear lo siguiente:

LOAD *ruta* INSTALL

Se debe reemplazar *ruta* con la ruta del directorio de INSTALL NLM

2. Del menú "Installation Options", seleccionar "Disk Options"
3. Del menú "Available Disk Options", seleccionar "Partition Tables".
4. Del menú "Partition Options", seleccionar "Create NetWare Partition".
5. Aceptar o decrementar el tamaño de la partición NetWare.
6. Aceptar o cambiar el tamaño del área de datos o de la Hot Fix redirection area.
7. Presionar <ESC> y seleccionar "Yes" para crear la partición
8. Presionar <ESC> para regresar al menú "Available Disk Options".

Nota: Un disco duro interno puede contener una partición DOS y una partición NetWare. Los discos duros externos pueden tener sólo particiones NetWare. Los volúmenes de NetWare son creados en las particiones NetWare.

- Se selecciona la opción "Disk Options" del menú "Installation Options".
- Seleccionar "Partition Tables" del menú "Available Disk Options".
- Si se tiene más de un disco, seleccione el disco que se necesite particionar de los listados en el menú "Available Disk Drives"

- Seleccionar "Create NetWare Partition" del menú "Partition Options"
NetWare sólo permite una partición NetWare por disco. Al crear una partición NetWare se despliega la pantalla "Partition Information", la cual muestra el espacio en la partición NetWare y los bloques separados para el área de datos y de redirección.
- Para decrementar el tamaño de la partición (si no se quiere usar toda la partición para NetWare), se debe cambiar el campo "Partition Size:", e introducir un número más pequeño.
- Para cambiar el tamaño de las áreas del "Hot Fix Information:" se debe cambiar alguno de los campos, introduciendo el nuevo número de bloques y NetWare calcula el espacio sobrante en el otro campo.
- Se debe presionar <ESC> y seleccionar "Yes" cuando se pregunte si se debe crear la partición.
- Si se tiene más de un disco, se debe seleccionar el siguiente disco de la pantalla "Available Disk Drives" y repetir los pasos del 4o. al 7o. para cada disco.
- Presionar <ESC> para regresar al menú "Available Disk Options".

Crear volúmenes

Con NetWare 386, el servidor de archivos puede operar desde 1 hasta 64 volúmenes.

- Seleccionar "Volume Options" del menú "Installation Options".
- Presionar <Insert> en la pantalla "Volumes". Si se tiene más de un disco duro (listado como una partición local), se debe seleccionar el disco duro donde se desea colocar el primer volumen de los listados en la pantalla "Free Space Available for Volume Segments". NetWare automáticamente introduce al volumen SYS como el primer volumen en la pantalla "Volume Information" Su tamaño por default es la partición entera.
- Presionar <ESC> y responder "Yes" a la pregunta "Create volume" para crear el volumen.
- Para crear otro volumen se debe presionar <ESC> hasta que se pueda presionar <Insert> en la pantalla "Volumes" y repita los demás pasos.

Montar volúmenes.

- Seleccionar el volumen a montar de la listas "Volumes".
- Presionar <Down-Arrow> para llegar al campo "Status".
- Presionar <Enter> para llegar a la pantalla "Volume Status".
- Seleccionar "Mount Volume".
- Para montar otros volúmenes, presionar <ESC> dos veces, y se deben repetir los pasos.

Copiar los archivos SYSTEM y PUBLIC

INSTALL automáticamente carga el sistema operativo NetWare y los archivos de utilerías en los directorios SYS:PUBLIC y SYS:SYSTEM del servidor de archivos.

- Regresar al menú "Installation Options".
- Seleccionar "System Options".
- Con el diskette NETWARE 386 OPERATING SYSTEM-2 en el drive A, seleccionar "Copy System and Public Files" desde el menú "Available System Options".
- Se deben insertar los demás diskettes a petición de INSTALL.
- Presionar <Alt><ESC> para regresar al prompt de la consola.

Cargar los drivers de LAN y los tipos de Frame

Una vez que los archivos System y Public son copiados, se deben seleccionar los drivers de LAN para el sistema de cableado y las tarjetas de red que se utilicen.

1. Cargar los drivers con el tipo de frame 802.2 Teclar :

LOAD LAN_DRIVER

Donde LAN_DRIVER debe ser cambiado, en el caso de este sistema abierto, por EXP16ODI el cual se refiere a una tarjeta de red Intel Etherexpress 16.

2. Responder a las preguntas de direcciones e interrupciones, de acuerdo a la información que se introdujo en la File Server Worksheet.

Conectar el protocolo al LAN Driver

El paso final de la instalación es conectar el protocolo al LAN Driver NetWare v3.12 permite a los protocolos diferentes de IPX funcionar en la red. Los pasos siguientes utilizan IPX para enlazar a cada LAN Driver en el servidor de archivos:

1. Para enlazar IPX a cada driver de LAN, teclear

BIND IPX TO LAN_DRIVER

Donde *LAN_DRIVER*, en el caso de este sistema abierto, es EXP16ODI.

2. Asignar la dirección de red que identifica el sistema de cableado que usa para comunicarse con drivers de LAN similares en el sistema abierto. Es un número hexadecimal que consta de 1 a 8 dígitos.

Creación del los archivos de boot del servidor de archivos

Crear el archivo AUTOEXEC.NCF.

El archivo AUTOEXEC NCF provee al servidor de archivos con comandos para completar el proceso de arranque después de que el SERVER.EXE y el STARTUP.NCF son ejecutados. Debido a que el AUTOEXEC.NCF es guardado y corre desde SYS:SYSTEM, se deben poner la mayoría de los comandos de arranque. Los comandos elegibles para este archivo son los siguientes:

- Nombrar el servidor de archivos.
- Asignar el número interno de red para el servidor de archivos.
- Cargar los drivers de LAN para el servidor de archivos y asignar el número de red.
- Unir los drivers de LAN al protocolo registrado del servidor de archivos.
- Montar los volúmenes.

- a. Seleccionar "Create AUTOEXEC NCF" en el menú "Available System Options" Seleccionando la opción "Create", el sistema operativo

automáticamente recopila la información que se introduzca en el prompt de la consola para el archivo. El contenido del archivo AUTOEXEC.NCF es el siguiente:

```
FILE SERVER NAME SISTEMAS
IPX INTERNAL NET 1994BEDD
LOAD EXP16ODI PORT=300 INT=3
LOAD INSTALL
LOAD MONITOR
BIND IPX TO EXP16ODI NET=1994ABCD
MOUNT ALL
```

Crear el archivo *STARTUP.NCF*.

Este archivo puede contener comandos para cargar los drivers del disco para el servidor de archivos

- a. Si se está usando un diskette de arranque para arrancar el servidor de archivos, debe estar en el drive A.
- b. Seleccionar "Create *STARTUP.NCF* File" desde el menú "Available System Options".
- c. Introducir la letra del drive apropiado en la pantalla "Path For *STARTUP.NCF* File". Usar <Backspace> para asegurar que el drive sea:
 - C: si se arranca desde el disco duro,
 - A: si se arranca desde el drive A.
- d. Presionar <Enter>.
- e. Presionar <ESC> para guardar el archivo.
- f. Salir de *INSTALL*.

Ejemplo:

```
LOAD ISADISK PORT=1F0 INT=E
```

Con todo lo anterior se tendrá un servidor de archivos de NetWare 386 listo para ser accesado desde cualquier estación de trabajo.

Implementación de un servidor UnixWare

Para la implementación de un servidor UnixWare se debe contar con un equipo con las características mencionadas en los requerimientos de hardware para el Novell UnixWare versión 1.1.

La Edición Personal de UnixWare versión 1.1 trae tres diskettes de arranque para instalarse en una computadora local directamente, o tres diskettes de arranque y un diskette Network Install set up para instalarse desde un Servidor de Aplicaciones en la red

Se deben seguir los siguientes pasos para arrancar la computadora.

1. Insertar el diskette de arranque 1.

a. Encender o reiniciar la computadora.

Nota: Cuando aparezca el logo de Univel, no debe presionarse ninguna tecla ya que esto interrumpirá el proceso de instalación.

b. Remover el diskette 1 cuando se pida.

c. Insertar el diskette IHV HBA (Host Bus Adapter) y cualquier otro diskette de drivers si se requiere.

2. Insertar el diskette de arranque 2

Identificar el tipo de monitor en la pantalla "Monitor Type Selection" si se requiere

3. Seleccionar el tipo de teclado

La pantalla "Introduction" es desplegada seguida por la pantalla "Keyboard Setup". El tipo de teclado por default es U S. ASCII.

4. Establecer la fecha y hora actual.

La pantalla "Configure Date and Time" es desplegada.

5. Seleccionar el continente de ubicación Seleccionar el país y el área que representa el ambiente de trabajo.

6. Particionar el disco duro primario

Si el disco duro en la computadora se encuentra particionado, la información es desplegada en la parte media alta de la pantalla. Si se desea aceptar el esquema de particionamiento desplegado, seleccionar **Cancel** y avanzar al paso 7.

Si el disco duro no se encuentra particionado, un esquema de particionamiento por default es establecido automáticamente. Si se desea aceptar el esquema de particionamiento desplegado, seleccionar **Cancel** y avanzar al paso 7.

Si el esquema de particionamiento no es aceptable, se usan las opciones de la parte media baja de la pantalla para reparticionar el disco duro.

a. Para particionar el disco duro, existen varias opciones en pantalla que son:

- *Overwrite system master boot code:* con esta opción se puede sobrescribir el código de boot si la computadora no arranca con UnixWare.

Si la computadora tenía un sistema operativo existente, tal como OS/2, antes de iniciar la instalación de UnixWare, debe contener un código de boot que es incompatible con UnixWare. Si éste es el caso, se debe seleccionar esta opción.

- *Crear una partición:* con esta opción se selecciona el tipo de partición a crear. Esta opción no permite seleccionar cilindros, sólo porcentajes.

Partition Type: seleccionar el sistema operativo que se desea. Usar las flechas derecha e izquierda para seleccionar

Percentage of disk: escoger el porcentaje de disco que esta partición usará.

- *Change active (boot from) partition.* con esta opción se puede cambiar la partición activa. Solo una partición puede estar activa a la vez y UNIX debe ser la partición activa antes de instalar UnixWare

- *Delete a partition:* con esta opción se puede remover una partición de un disco duro.

- *Exit (update disk configuration and exit).* con esta opción se puede actualizar cualquier cambio en la partición y salir.

-Cancel (exit without updating disk configuration): con esta opción se puede continuar al siguiente paso sin realizar ningún cambio a las particiones.

b. Particionar el disco duro secundario (opcional)

7. Seleccionar realizar una instalación destructiva o detener la instalación.

Este paso determina si se quiere sobrescribir los archivos existentes. Si se desea esto, se debe seleccionar la instalación destructiva, si no, se debe cancelar esta instalación.

8. Seleccionar la instalación automática o manual.

El método sugerido es la instalación automática ya que UnixWare detectará el hardware existente y asignará los valores que se adapten mejor a ese hardware.

9. Cuando se requiera, remover el diskette de arranque 2 e insertar el diskette de arranque 3. Varios mensajes de status son desplegados

10. Remover el diskette 3 cuando se requiera.

11. Instalar los archivos y directorios de la Edición Personal.

a. Insertar el CD-ROM.

b. Seleccionar los paquetes que se desea instalar.

c. Escoger la instalación de los paquetes automática o manual. Se recomienda seleccionar la instalación automática ya que existen paquetes que son indispensables

12. Introducir el nombre de la computadora.

13. Seleccionar el país soportado para el Soporte al Lenguaje Europeo (ELS) en la pantalla "Locale Setup". None (USA) es el default.

Seleccionar cualquier país relacionado que se quiera soportar en el campo *additional support*:

-Install support for related countries: el soporte de install para cualquier país que comparta el mismo lenguaje o similares

-install support for all countries available. el soporte de install para todos los países en la lista.

Si se está instalando la Edición Personal desde CD-ROM, los archivos se están ahora cargando y construyendo, un proceso que toma cerca de una hora y media

Implementación de una estación de trabajo OS/2

Para la implementación de una estación de trabajo OS/2 se debe contar con un equipo con las características mencionadas en los requerimientos de hardware para el IBM OS/2 2.11.

El sistema operativo OS/2 puede instalarse en un equipo que no tenga ningún otro sistema operativo, o también puede compartir el disco duro con otros sistemas operativos como DOS.

Si se desea que OS/2 comparta el disco duro con DOS, se debe instalar primero el DOS y luego el OS/2. La estación de trabajo que se implementará tendrá el OS/2 como único sistema operativo en el disco duro.

Para iniciar la instalación del sistema operativo, se debe realizar lo siguiente

1. Insertar el *Diskette de Instalación* en la unidad A.
2. Iniciar o reiniciar el sistema.
3. Extraer el *Diskette de Instalación*.
4. Insertar el *Diskette 1*, y presionar <Enter>.

En varios momentos de la instalación, se solicitará que se extraiga el diskette de la unidad A para insertar otro. Se debe asegurar que el diskette permanezca en la unidad A hasta que se indique que se sustituya o se extraiga. Se sustituirán algunas veces los diskettes para copiar la información al disco duro.

5. A medida que se visualiza la información, se puede aceptar o modificar.

Si se desea configurar el sistema por omisión, se debe aceptar la opción que aparece seleccionada en cada pantalla presionando <Enter>.

Durante esta parte de la instalación se solicitará si se desea aceptar la partición de instalación por omisión o bien especificar una partición propia. Si se acepta la partición por omisión, ésta abarcará todo el disco duro

6. Si se está llevando a cabo una instalación en un sistema nuevo o bien si se decide formatear una partición existente, se solicitará seleccionar un sistema de archivos. Se puede seleccionar el HPFS de OS/2 o el FAT de DOS/OS/2

Se deben seguir las indicaciones que se ven en pantalla. Después de cambiar diskettes varias veces, se solicitará que se reinicie el sistema extrayendo el diskette y presionando <Enter>.

Una vez reiniciado el sistema, aparecerá la ventana *Configuración e Instalación de OS/2*. En esta ventana se debe seleccionar las opciones correspondientes a las funciones del sistema operativo que se desee instalar. Las opciones son las siguientes:

- *Instalar las funciones preseleccionadas.* Si se selecciona este conjunto predeterminado de funciones OS/2, se necesitarán aproximadamente 32 Mb de espacio total en disco duro para el sistema operativo y sus funciones.
- *Instalar todas las funciones.* Si se seleccionan todas las funciones, se necesitarán aproximadamente unos 40 Mb de espacio total en disco para el sistema operativo y sus funciones.
- *Seleccionar funciones e instalar.* Si se decide seleccionar desde un menú las funciones que se desean instalar, se necesitarán de 20 a 40 Mb de espacio en disco duro para el sistema operativo y sus funciones.

Después de seleccionar la opción de instalación aparecerá la ventana *Configuración del sistema*, la cual describe la configuración del país y el soporte de dispositivos.

Debido a que el programa de instalación detecta los tipos de dispositivos que están conectados al sistema, la mayor parte de las opciones serán correctas.

Se deben establecer los valores correctos para todas las opciones mostradas en pantalla, y al terminar se debe presionar el botón [Bien]

Después de haber copiado la mayor parte de los archivos del sistema operativo en el disco duro, aparecerá la ventana *Opciones avanzadas*. Desde esta ventana, se pueden seleccionar las siguientes opciones:

- *Instalar Diskette de Soporte de Dispositivo*: Se utiliza si se desea instalar hardware del cual se tenga el diskette de configuración para OS/2
- *Migrar aplicaciones*: Con esta opción se puede colocar una copia de programas de DOS o Windows en carpetas del escritorio de OS/2.
- *Configurar el Escritorio de WIN-OS/2*: Se utiliza para copiar el escritorio de Windows que ya existe o bien para crear uno nuevo.
- *Migrar CONFIG SYS/AUTOEXEC.BAT*: Sirve para copiar lo referente a la personalización de una versión anterior del sistema operativo a OS/2 2.11.

Cuando se termine de efectuar selecciones en la ventana *Opciones avanzadas*, se solicitará que se inserte el *Diskette 1 de controladores de impresora*

A continuación, se indicará que se inserte uno de los diskettes de *controladores de pantalla* para que el programa de instalación del OS/2 pueda instalar el soporte para los dispositivos de pantalla.

Una vez que el sistema operativo esté instalado, se solicitará que se reinicie el sistema. Luego de una demora, aparecerá la ventana *Guía de Aprendizaje del OS/2*.

Con lo anterior, el sistema operativo OS/2 quedará instalado en la estación de trabajo, sólo resta crear el soporte de NetWare para estaciones de trabajo OS/2.

Instalación de NetWare para estaciones de trabajo OS/2

Para instalar el software de estaciones de trabajo NetWare se debe checar lo siguiente:

- Si se está usando LAN Server, LAN Requester o Extended Services, se debe asegurar que están ya instalados en la estación de trabajo.
- Se deben tener copias de trabajo de los archivos de las estaciones de trabajo NetWare.

Cuando se instala el software de estación de trabajo NetWare sucede lo siguiente

- Un directorio es creado en la raíz del drive desde donde se arrancó el OS/2.
- Todos los archivos de estación de trabajo para OS/2, son copiados al directorio especificado durante la instalación.
- Los archivos de configuración de OS/2 y NetWare son creados o modificados
- Un ícono llamado "Novell" es creado en la ventana Desktop

Para instalar el software se debe seguir el siguiente procedimiento

1. Insertar el disco etiquetado *WSOS2_1* en algún drive.
2. Elegir el ícono "Drive-A" en el desktop.
3. Seleccionar el ícono "Drive-A" de la "Drive-A Tree-View".
4. Seleccionar el ícono "INSTALL.EXE" para cargar el programa de instalación
5. Seleccionar "Requester on workstation..." del menú "Installation".
6. Seguir las instrucciones en pantalla.

Al finalizar, la estación de trabajo NetWare estará instalada y lista para entrar (login) en un servidor de archivos NetWare.

Implementación de una estación de trabajo Windows

Para la implementación de una estación de trabajo Windows se debe contar con un equipo con las características mencionadas en los requerimientos de hardware para el Microsoft Windows para Trabajo en Grupo versión 3.11

Para instalar Windows para Trabajo en Grupo se debe:

1. Introducir el disco 1 de Instalar en una unidad de diskettes.

2. A continuación del símbolo del sistema, escribir la letra de la unidad que esté utilizando seguida de dos puntos(.) y presionar <Enter>

3. Escribir Instalar y presionar <Enter>

4. Seguir la instrucciones que aparecen en pantalla.

Se debe elegir el método de instalación de los dos posibles: instalación rápida y personalizada.

Si se va a utilizar una red, independientemente de que se elija cualquier instalación, se deben conocer los datos siguientes:

- El tipo de red que se quiere utilizar con Windows para Trabajo en Grupo.

Si aún no se ha instalado un software de red en la computadora, el programa Instalar puede configurar el software de Red de Microsoft Windows

Si ya se tiene instalada una red, Windows para Trabajo en Grupo quedará configurado para trabajar con ella. Entre las redes que puede utilizar en lugar de (o conjuntamente con) la Red de Microsoft Windows se encuentran Novell NetWare y Banyan VINES.

- El tipo de tarjeta de interface (adaptador) de red que se va a utilizar.

Si se utiliza la Instalación rápida, bastará con que se escriba el nombre del usuario, y que se contesten algunas preguntas (como el tipo de impresoras y de tarjeta de interface de red) e introducir los diskettes cuando el programa Instalar lo solicite. Este es el método más recomendado.

Implementación de una estación de trabajo MS-DOS/Windows

Para la implementación de una estación de trabajo MS-DOS/Windows se debe contar con un equipo PC de preferencia con procesador 386 o mayor y al menos 2 Mb de memoria RAM para poder trabajar dentro de la red NetWare.

La computadora debe contar con MS-DOS y además debe tener instalada una tarjeta de red y el cableado necesario para conectarla con el servidor NetWare

Instalación de NetWare para estaciones de trabajo DOS y Windows

Las estaciones de trabajo DOS y Windows comparten el mismo programa de instalación, el cual se ejecuta desde DOS.

Para instalar el software de estaciones de trabajo NetWare se debe checar lo siguiente:

- Se debe cerrar Windows antes de cargar el programa de instalación, ya que éste hace modificaciones a algunos archivos de Windows
- Se deben tener copias de trabajo de los archivos de las estaciones de trabajo NetWare.

Cuando se instala el software de estación de trabajo NetWare sucede lo siguiente

- Un directorio es creado en la raíz del drive desde donde se arrancó el DOS.
- Todos los archivos de estación de trabajo para DOS y Windows son copiados al directorio especificado durante la instalación.
- Los archivos de configuración de DOS, Windows y NetWare son creados o modificados.
- Un grupo llamado "NetWare User Tools" es creado en el Administrador de archivos de Windows.

Para instalar el software se debe seguir el siguiente procedimiento:

1. Insertar el disco etiquetado *WSDOS_1* en algún drive.

2. Cambiarse al drive que contiene el diskette *WSDOS_1*.
3. Teclear *INSTALL*.
4. Seguir las instrucciones de la pantalla.

Después de esto aparecerán en pantalla 5 pasos a seguir para completar la instalación del software para cliente NetWare

Paso 1. Teclear el nombre del directorio destino para la instalación del cliente
C:\NWCLIENT

Paso 2. La instalación del cliente requiere "LASTDRIVE=Z" en el archivo CONFIG.SYS y "CALL STARTNET.BAT" adicionado a AUTOEXEC.BAT. Install hará copias de respaldo. ¿Permite los cambios? (Y/N): Yes

Paso 3. ¿Desea instalar el soporte para Windows? (Y/N): Yes
Windows Subdirectory: C:\WINDOWS

Paso 4. Presionar <Enter> para instalar el driver para su tarjeta de red. Debe usar las teclas del cursor para encontrar el nombre de la tarjeta. Presione <Enter> para ver la lista.

Paso 5. Presione <Enter> para instalar.

Se deben usar las teclas del cursor para moverse entre los pasos. Se debe presionar <Enter> para modificar un campo.

Al finalizar los cinco pasos la estación de trabajo NetWare estará instalada y lista para entrar (login) en un servidor de archivos NetWare.

La representación de la conexión del sistema abierto se encuentra ilustrada en el apéndice A.

Análisis de las comunicaciones establecidas dentro del sistema abierto

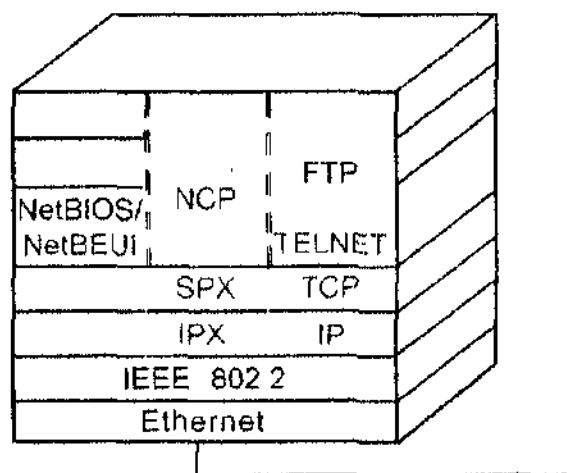
El sistema abierto utiliza distintos protocolos de comunicación para empaquetar la información, enviarla desde una fuente, y entregarla hacia un sistema destino. Esto permite establecer una comunicación entre dos o más end-points.

Para establecer las **conexiones a nivel lógico** los protocolos de transporte están implementados como *drivers* que pueden cargarse o descargarse del sistema

En términos de comunicaciones de red, el sistema operativo de red debe ser capaz de soportar concurrentemente múltiples pilas de protocolos en el servidor. Esta capacidad es necesaria debido a los diferentes protocolos que actualmente se utilizan.

La ventaja de utilizar más de un protocolo en una workstation, es que *ésto habilita a los usuarios para acceder a varios tipos de recursos en la red*. Al cargarse la pila de protocolo IPX/SPX y los protocolos TCP/IP en la workstation DOS, por ejemplo, se puede acceder a un servidor de archivos NetWare y simultáneamente ejecutar una sesión de terminal con UNIX.

Figura 5-1 Soporte de múltiples pilas de protocolos concurrentemente



Fuente: LAN Operating Systems

Los protocolos nativos involucrados en el sistema abierto son protocolos de red específicos de las workstation y servidores, los cuales son:

- Protocolos IPX/SPX (NetWare)
- Protocolos TCP/IP (UNIX)
- Transporte NetBIOS y NetBEUI (OS/2)

IPX/SPX

El protocolo IPX/SPX de NetWare está basado en protocolos *Xerox Network Services* (XNS) desarrollados al mismo tiempo que TCP/IP. Los dos protocolos, IPX/SPX y TCP/IP, comparten muchas similitudes conceptuales. *IPX (Internetwork Packet eXchange)* es el protocolo de comunicación de Novell que crea, mantiene, y termina las conexiones entre dos dispositivos de red (workstations, file servers, ruteadores, etc.). IPX direcciona y rutea los paquetes de datos a través de la red, y además, lee las direcciones asignadas de los datos regresados y direcciona los datos hacia el área apropiada en el sistema operativo de la workstation o del servidor de archivos.

IPX está enlazado con otros programas y rutinas que ayudan en los procesos de transmisión de datos en la red. El shell de NetWare (NetWare DOS Requester) prepara los paquetes de datos, antes de ser manejados por IPX, con el fin de que sean entendibles para el destino. IPX utiliza los servicios de la rutina del driver de LAN para controlar a la tarjeta de red de la workstation, y así poder entregar los datos. IPX también utiliza los servicios del protocolo SPX, el cual monitorea las transmisiones asegurando que la entrega sea correcta.

Debido a que *IPX es un protocolo de datagramas*, no tiene interconstruido un acknowledgment. IPX, es por lo tanto un protocolo "best-effort"; ya que hace el mejor esfuerzo para entregar un paquete, pero no puede garantizar la entrega de ese paquete. Este tipo de garantía puede sólo ser dado por un protocolo acknowledgment

La mayoría de las aplicaciones NetWare utilizan IPX por las siguientes dos razones

1. *IPX rara vez falla al entregar un paquete*
2. *IPX es un protocolo de bajo nivel. El servidor puede enviar y recibir paquetes IPX ejecutando realmente pocas instrucciones de máquina.*

Los paquetes IPX siempre contienen un encabezado de 30 Bytes y un campo de datos de cero o más bytes. Los servidores de NetWare 3.X tienen la capacidad de establecer paquetes de IPX más grandes en cada cliente, si el medio de transmisión fundamental de la red soporta paquetes más grandes. Esta capacidad es llamada soporte LIP (Large Internet Packet), y el tamaño del paquete puede ser de hasta 69 Kb.

SPX

Un protocolo de comunicación que monitorea la transmisión en la red para asegurar una entrega exitosa. SPX se deriva del Internetwork Packet Exchange (IPX) de Novell utilizando el protocolo Sequenced Packet de Xerox. SPX mejora el protocolo IPX debido a que proporciona un servicio para supervisión de los datos enviados a través de la red. SPX puede dividir la transmisión de los datos en una serie de paquetes separados.

SPX es un protocolo de entrega garantizada, construido sobre IPX. SPX utiliza a IPX para enviar y recibir paquetes, pero además, provee un servicio de acknowledgment y garantiza que los paquetes serán recibidos por su nuevo destino en el mismo orden en el cual su nodo origen los envió.

TCP/IP

Para tener un mejor funcionamiento de grandes redes, es mejor utilizar a TCP/IP como protocolo de red. Con TCP/IP es posible dividir una red en piezas manejables y mantener un alto nivel de desempeño a través de la red.

Un beneficio de TCP/IP es que ha sido diseñado especialmente para ser ruteable. Esto significa que con TCP/IP es posible conectar varias redes por medio de utilizar dispositivos que permiten manejar el tráfico en la red.

TCP/IP ha comprobado ser extremadamente efectivo y ha sido adaptado exitosamente a las nuevas tecnologías y actualmente está implementado en una gran variedad de sistemas de computadoras, desde las computadoras personales basadas en DOS hasta mainframes IBM y desde workstations RISC basadas en UNIX hasta supercomputadoras Cray.

Transporte NetBIOS

IBM LAN Server y Microsoft Windows NT están basadas en SMBs para soportar la compartición de archivos e impresoras. La NetBIOS API, una interface de programación de alto nivel, constituye una parte integral de los protocolos de red.

NetBIOS no es realmente un protocolo, éste es una interface para un conjunto de comandos que habilitan a las aplicaciones de red para desempeñar las siguientes funciones.

- Establecer sesiones de comunicación entre aplicaciones
- Enviar y recibir datos
- Nombrar objetos en la red

Actualmente, la mayoría de los fabricantes soportan NetBIOS y SMBs sobre TCP/IP y el transporte NetBEUI/LLC 802.2, esto incluye a LAN Manager, LAN Server, Windows NT, y Windows for Workgroups. En un principio, NetBIOS sobre TCP/IP llegó a ser un ingrediente importante para redes LAN Manager y LAN Server debido a las limitaciones en el transporte NetBEUI básico.

Bajo NetBIOS, un nombre consiste en 16 bytes que deben incluir al menos algunos caracteres ASCII de 8 bits, imprimibles o no-imprimibles. Un nodo puede también tener múltiples nombres o grupos (nombres de grupos) con los cuales éste se asocia. La primera máquina de la red debe grabar algunos de los nombres que seleccionó, previniendo que otros nodos posteriores utilicen este nombre. Mientras el direccionamiento dinámico es conveniente en una LAN pequeña, éste llega a ser problemático en una LAN grande.

Transporte NetBEUI

El transporte NetBEUI (NetBIOS Extended User Interface) es un protocolo de transporte de área local desarrollado para operar bajo la interface de red NetBIOS de Microsoft.

Desarrollado por Microsoft e IBM a mediados de los 80s, el protocolo NetBEUI no es ruteable. Este depende del grabado de un nombre de 16 bytes, en el nodo local, el cual no puede ser único de sesión en sesión. Cuando es necesaria una WAN y un ruteo, NetBEUI

depende de paquetes NetBIOS encapsulados (a menudo llamados tunneling) dentro de los paquetes TCP/IP, típicamente necesitando ambas pilas de protocolos NetBEUI y TCP/IP.

NetBEUI es una extensión de NetBIOS para hacer de éste un protocolo de red completo con características y servicios adicionales. Es importante hacer notar que NetBEUI está diseñado para correr en una LAN sencilla, debido a que es difícil de rutear a través de los diferentes segmentos de red.

NetBEUI no contiene una provisión para rutear o para pasar información hacia redes distintas. Afortunadamente, debido a que el NetBIOS corre sobre el transporte TCP/IP, esto soluciona algunas de estas diferencias. El ruteo es manejado todavía con dificultades en la mayoría de las circunstancias debido a que un archivo LMHOSTS debe ser mantenido para mapear los nombres NetBIOS a una dirección IP. Actualmente, NetBIOS 3.0 es la interface estándar para servidores y estaciones de trabajo OS/2.

Algunos fabricantes soportan a **NetBIOS** directamente o a través de un emulador. Un emulador trabaja aceptando un comando de NetBIOS y colocándolo a éste en el paquete de datos del protocolo, lo que se conoce como encapsulación. Novell provee un emulador para su implementación de NetBIOS.

El comando NetBIOS es encapsulado en un paquete IPX y éste es transmitido a través de la red, por medio del protocolo nativo de Novell. Esta encapsulación no tiene efecto en la interface NetBIOS.

NetBIOS es capaz de proveer una sesión orientada a la conexión con el fin de transferir un STREAM de datos. NetBIOS incluye un servicio sin conexión que puede transferir datagramas a través de la red. Debido a que NetBIOS es una interface de aplicación en la capa de sesión, por lo tanto, ésta no puede proveer un servicio de ruteo (que normalmente reside en la capa de red del modelo OSI). Esta incapacidad de ruteo hace difícil utilizar NetBIOS para construir internetworks.

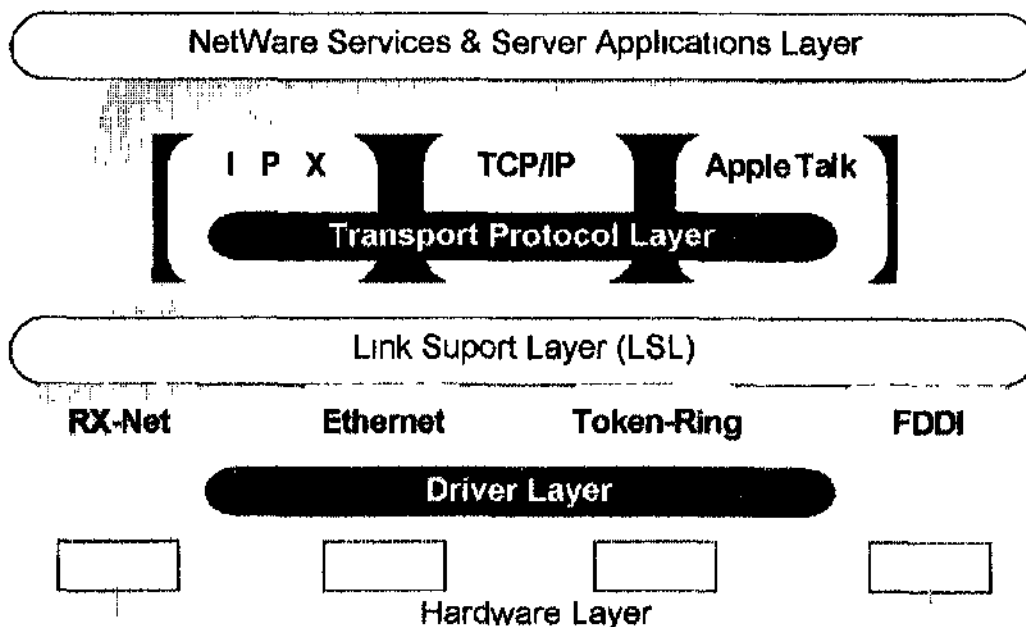
El entorno STREAMS del sistema abierto

Dentro del ambiente de comunicación del sistema abierto se encuentran varios elementos que hacen posible establecer una comunicación entre los distintos sistemas operativos. Entre estos elementos se encuentran los drivers de STREAMS, que son un entorno de desarrollo de drivers para UNIX que permite a los drivers de transporte lograr un alto grado de portabilidad de un sistema operativo a otro. Este entorno permite que muchos drivers de transporte basados en STREAMS que ya existen, puedan conectarse de un protocolo a otro con pocas o ninguna modificación. Los drivers de transporte como IPX/SPX y otros pueden ser implementados como drivers basados en STREAMS.

Para lograr que el protocolo de transporte sea transparente al sistema operativo de red, los STREAMS permiten proveer a través de la red un mismo conjunto de servicios, sin que éste pueda notar qué protocolo de transporte está usando.

El servidor NetWare v3.12 del sistema abierto, implementa STREAMS como NLMs (NetWare Loadable Modules). Los NLMs proveen una interface común entre NetWare y los protocolos de transporte (IPX/SPX y TCP/IP) que necesitan enviar datos hacia NetWare para ser procesados.

Figura 6-2 Funcionamiento del entorno STREAMS



Fuente: Novell NetWare [Concepts]

EL NLM *TLI* (*Transport Level Interface*) es una interface de programación de aplicaciones que reside entre STREAMS y las aplicaciones del usuario, *permitiendo la comunicación con los protocolos de nivel de transporte tales como IPX/SPX o TCP/IP*

Por otro lado, *Windows NT* proporciona una interface de programación denominada *Transport Driver Interface* (*TDI*), para redirectores y otros drivers de red de alto nivel. El *TDI* es una interface asíncrona independiente del transporte, que implementa un mecanismo de direccionamiento genérico y un conjunto de servicios y bibliotecas. Cada driver de transporte proporciona una interface en su capa más alta, de manera que los redirectores puedan llamarlo sin importar qué transporte está utilizándose por debajo de la interface.

Aunque LAN Manager utiliza comunicaciones orientadas a la conexión, el software *IPX* de Novell emplea comunicaciones no orientadas a la conexión, el *TDI* soporta retransmisiones orientadas a la conexión (*circuito virtual*) y transmisiones no orientadas a la conexión (*datagrama*).

Habilitación de múltiples pilas de protocolos dentro del sistema abierto

La **conexión física** la proporciona una tarjeta de red que, o está integrada, o se añade a una ranura de expansión de la máquina. Cada tarjeta de red (a veces denominadas adaptadores de red) es capaz de comunicarse a través de un tipo particular de cable, utilizando una topología concreta de red.

Para utilizar estos drivers de dispositivo simultáneamente con múltiples pilas de protocolos, ambos, la pila de protocolos y los drivers de dispositivo deben estar relacionados uno con otro. En otras palabras, ellos necesitan una interface común con la cual comunicarse e intercambiar datos en la computadora de la red. Dos especificaciones competentes soportan múltiples pilas de protocolos en las estaciones de red.

- *Open Data-Link Interface* (*ODI*) de Novell
- *Network Driver Interface Specification* (*NDIS*) de Microsoft

Ambas especificaciones soportan funciones similares y desempeñan su tarea por medio de separar el driver de dispositivo del adaptador de red, a partir de los protocolos de las capas superiores. El protocolo de las capas superiores puede ser alguno de los

mencionados, tal como IPX/SPX o TCP/IP. El único requerimiento es que la pila de protocolos y los drivers de dispositivos de LAN deben estar de acuerdo con la interface definida en la especificación. Cuando ésta se completa de forma correcta, múltiples pilas de protocolos pueden coexistir en la estación de red.

Network Driver Interface Specification (NDIS)

NDIS (Network Driver Interface Specification) de 3Com y Microsoft habilita a múltiples pilas de protocolos para compartir la misma tarjeta de interface de red por medio de proveer una interface públicamente definida para tarjetas de red. Windows NT proporciona la interface **NDIS** que aísla a los drivers de red de los diferentes protocolos de transporte, y viceversa. La interface NDIS representa la capa más alta de un driver de red aislado. Esto permite que cualquier driver de protocolo dirija sus peticiones de red hacia la tarjeta de red llamando a su interface. De esta forma, un usuario puede comunicarse a través de una red TCP/IP y una NetBEUI utilizando una tarjeta de red y un único driver de red.

Cada driver de red NDIS es responsable de enviar y recibir paquetes a través de su conexión de red, y de gestionar la tarjeta física en nombre del sistema operativo. En su nivel más bajo el driver NDIS, se comunica con la tarjeta o con las tarjetas a las que sirve, utilizando rutinas NDIS para acceder a ellas. El driver NDIS pone en marcha la I/O en las tarjetas y recibe las interrupciones de ellas. Llama a los drivers de protocolos superiores para indicar que ha recibido datos y para advertirles de la terminación de una transferencia de datos. NDIS permite que los drivers de red sean portables sin que sea necesario que tengan conocimiento del procesador o del sistema operativo bajo el cual se están ejecutando. Los drivers de red pueden llamar a rutinas NDIS para aislarse así mismos de información específica de la plataforma, de manera que puedan moverse fácilmente de un sistema a otro.

Open Data-Link Interface (ODI)

El sistema abierto está basado en ODI de Novell. ODI es una interface de tarjetas de red que consta de dos partes:

- El nivel de soporte de enlace (*Link Support Layer - LSL*)
- El controlador de interface de enlaces múltiples
(*Multiple Link Interface Driver - MLID*)

El módulo LSL actúa como un director de paquetes entre el controlador de transporte TCP/IP y los controladores ODI. LSL también permite a múltiples pilas de protocolo, como TCP/IP e IPX, funcionar al mismo tiempo, en una misma tarjeta de red. Los controladores ODI se conectan a una tarjeta de red por lo general, se requiere un controlador diferente para cada tipo o versión de la tarjeta de red.

Los *Dedicated IPX Drivers* son archivos IPX.COM creados con WSGEN. Estos drivers trabajan solo con el protocolo IPX. Para utilizar otros protocolos, tales como TCP/IP, se necesita llamar a los drivers **ODI**

Habilitación del la pila de protocolo TCP/IP

NetWare además de su protocolo nativo IPX/SPX, provee un ambiente open-ended para soportar diferentes protocolos de transporte de red como son:

- TCP/IP
- NetBIOS

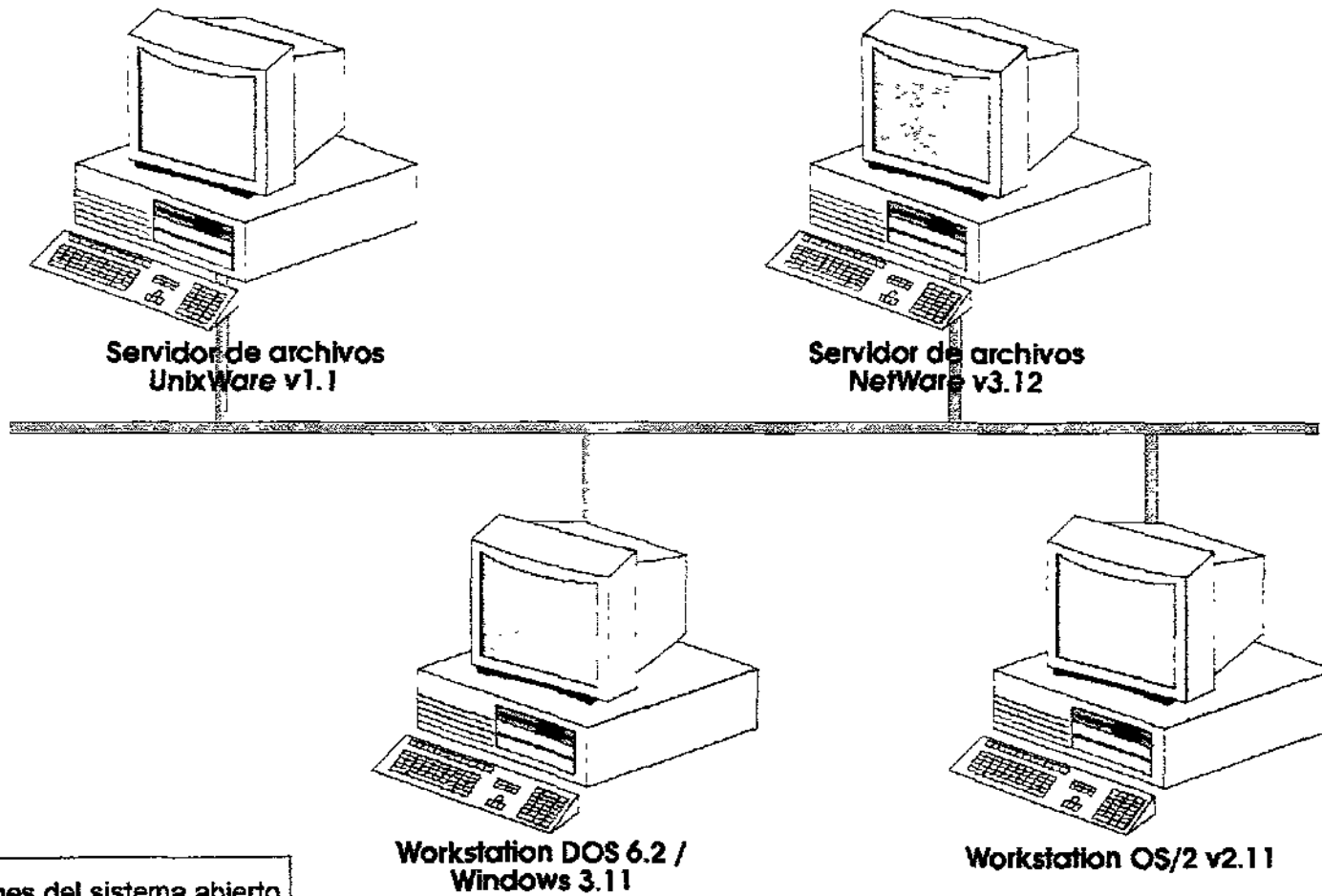
Cuando se carga **TCP/IP** en un servidor NetWare, por medio del subsistema de transporte TCP/IP, incluido en el sistema operativo (archivos .NLM) el servidor además de soportar el protocolo TCP/IP actúa como un *ruteador IP Full-Fledged*.

Para que las estaciones de trabajo conectadas al servidor NetWare puedan acceder al anfitrión UnixWare, se requieren las utilerías de LAN WorkPlace. El software TCP/IP de LAN WorkPlace funciona con cualquier controlador ODI. LAN WorkPlace proporciona el software compatible con ODI que se requiere para tener acceso a NetWare, desde el DOS y Windows.

Para poder ejecutar TCP/IP e IPX al mismo tiempo en la estación de trabajo DOS/Windows, se debe modificar la sección *Link Driver* del archivo NET.CFG.

La representación de la conexión del sistema abierto se encuentra ilustrada en la gráfica siguiente.

Representación del sistema abierto



Especificaciones del sistema abierto

Topología: Bus
Conectores: BNC
Medio: Cable coaxial delgado
Estándar: Ethernet

Conclusión

Para mantener funcionando de forma eficaz un sistema abierto es necesaria una administración y configuración continua con el fin de brindar mantenimiento a las diferentes arquitecturas de red, lo cual requiere niveles elevados de pericia técnica. También se requieren administradores para trabajar en dos plataformas distintas (LANs de PCs y UNIX), lo que puede incurrir en un aumento en el costo del manejo de la información. Pero a pesar de esto, la conectividad PC-UNIX ofrece beneficios potenciales. Algunos de los principales beneficios que UNIX ofrece son: *un acceso rápido al monitoreo de las actividades en la red y un excelente manejo de archivos*.

Por otro lado, los beneficios de la compartición de recursos PC-UNIX han hecho que se incluya la pila de protocolos TCP/IP y software de conectividad adicional a las PC (DOS, MS Windows, OS/2). La pila de protocolos TCP/IP ofrece una posibilidad de conectividad remota con UNIX.

Con la adición de los protocolos PC-LAN, los sistemas UNIX probablemente llegarán a ser los servidores líderes de la industria para fines de la década de los 90s. Y TCP/IP podría llegar a ser el estándar en el desktop de las PCs, y éste proporcionaría una viabilidad a largo plazo a los protocolos de LAN de PCs.

La nueva generación de sistemas operativos (Windows NT, Windows 95, OS/2 3.0 y System 7.5) pueden soportar varios protocolos de red de forma transparente. Esto viene a disminuir el costo y las decisiones de administración. Debido a todo lo anterior es posible esperar un crecimiento dramático en el uso de los protocolos TCP/IP, y por lo tanto, *el paso hacia una conectividad transparente basada en UNIX llegará a ser un hecho.*

Glosario de Términos y Acrónimos

Device Driver. Software que sirve como enlace entre el sistema operativo y los dispositivos físicos conectados a la computadora, por ejemplo, CD-ROMs, impresoras, mouse, etc.

Drive Mapping. Un apuntador a una localidad en la estructura del directorio, representado como una letra asignada a una ruta de directorio en un volumen.

Hilo. Entidad ejecutable que pertenece a un proceso (y sólo a uno) Comprende un contador de programa, una pila de modo usuario, una pila de modo kernel y un conjunto de valores de registro. Todos los hilos de un proceso tienen igual acceso al espacio de direcciones de un proceso, a los handles del objeto, y a otros recursos. Los hilos se implementan como objetos.

Hub. Un dispositivo que modifica las señales de transmisión permitiendo a una red alargarse o expandirse con workstation adicionales.

Internetwork. dos o más redes conectadas por un ruteador interno o externo.

LAN driver. Una rutina de software que interpreta y controla la estructura física de una tarjeta de red.

Log in. Inicializar los derechos de seguridad del usuario y su ambiente usando el comando LOGIN, para establecer la comunicación con el servidor de la red.

Log out. Romper la conexión servidor/workstation y borrar cualquier drive mapping al servidor utilizando la utileria LOGOUT.

Memoria virtual (Virtual memory - VM). Visión lógica de la memoria que no se corresponde necesariamente con una estructura física de la memoria.

Modo Kernel. Modo de procesador privilegiado en el cual se ejecuta el código de acceso de Windows NT. Un hilo que se ejecuta en modo kernel tiene acceso a la memoria del sistema y al hardware.

Modo usuario. Modo de procesador no privilegiado en el cual se ejecuta el código de una aplicación. Un hilo que se ejecuta en modo usuario sólo puede conseguir acceso al sistema llamando a los servicios del sistema.

NDR (NetWare DOS Requester). La porción de software de NetWare v3.12 para las workstation DOS. El NetWare DOS Requester está compuesto de varios módulos llamados *Virtual Loadable Modules* (VLMs). Estos VLM son la clave de la modularidad del NetWare DOS Requester.

NLM (NetWare Loadable Modules). Programa que se puede cargar y descargar de la memoria del servidor mientras éste está en funcionamiento. Los NLMs enlazan los disk drivers, los LAN drivers y otros, utilerías de administración y mejoramiento del servidor de archivos al sistema operativo.

NTFS (New Technology File System). Sistema de archivos de avanzado diseño para ser utilizado específicamente con el sistema operativo Windows NT. Soporta la recuperación del sistema de archivos, medios de almacenamiento extremadamente grandes, y diversas características para el subsistema POSIX. También soporta aplicaciones orientadas a objetos al tratar a todos los archivos como objetos con atributos definidos por el sistema y atributos definidos por el usuario.

ODI (Open Data-Link Interface). Una arquitectura que permite que múltiples LAN drivers y protocolos coexistan. ODI soporta comunicaciones independientes del medio y del protocolo, proviendo una interface estándar que permite a los protocolos de transporte compartir una sola tarjeta de red sin conflicto.

POSIX. Conjunto común de estándares de interface para UNIX creado por organizaciones internacionales de estándares. Estos estándares proveen un nivel común de soporte de programación a través de varios sistemas operativos UNIX.

Proceso. División lógica de la labor de un sistema operativo. En Windows NT, comprende un espacio de direcciones virtuales, un programa ejecutable, uno o más hilos ejecución, algunas partes de las cuotas de recursos del usuario, y los recursos del sistema, que el sistema operativo ha reservado para los hilos del proceso.

Redirector. Software de red que acepta peticiones de E/S para archivos remotos, filtros con nombre, o buzones de correos, y las envía (redirige) a un servidor de red de otra máquina.

Router (ruteador). Una workstation o servidor de archivos corriendo software que administra intercambio de información (en la forma de paquetes de datos) entre sistemas de cableado de red. Los ruteadores, a diferencia de los bridges tradicionales, hacen más que transferir paquetes de datos entre redes que utilizan el mismo protocolo de comunicaciones. Un router conecta dos diferentes sistemas de cableado, y además, rutea los paquetes utilizando la mejor ruta.

SCSI (Small Computer System Interface). Un estándar de la industria que establece reglas para conectar dispositivos periféricos y sus controladoras a un microprocesador. Las computadoras de dispositivos y periféricos diseñados para cumplir las especificaciones SCSI tienen un alto grado de compatibilidad.

VLM (Virtual Loadable Module). Un programa modular ejecutable que corre en cada workstation DOS y habilita la comunicación con el servidor NetWare.

Bibliografia

- [1] **Halsall, Fred (Data Communications, Computer Networks and Open Systems)**
3rd. Edition
Addison-Wesley

- [2] **Schatt, Stan (Understanding Local Area Networks)**
3rd. Edition
SAMS

- [3] **Varios, (LAN Operating Systems)**
1st. Edition
New Riders Publishing

- [4] **Watt, Jim (TCP/IP and related protocols)**
2nd. Edition
McGraw Hill

- [5] **Unisys (TCP/IP Protocol Suite)**
Unisys Institute of Technology (UIT)

- [6] **Unisys (UNIX TCP/IP Implementation and Support)**
Unisys Institute of Technology (UIT)

- [7] **Custer, Helen (El libro de Windows NT)**
1ra. Edición
Microsoft Press/McGraw-Hill

- [8] **Novell (NetWare Versión 3.12 Concepts)**
Novell
- [9] **Novell (NetWare Versión 3.12 Installation)**
Novell
- [10] **Novell (UnixWare Installation Handbook)**
Novell
- [11] **Microsoft (Windows para Trabajo en Grupo Manual del usuario)**
Microsoft
- [12] **IBM (OS/2 Utilización del sistema operativo)**
IBM
- [13] **Novell (UnixWare Sales Guide)**
September 1993
Novell
- [14] **Unisys (UNISIZING)**
UNIX Marketing Course
Unisys
- [15] **Unisys (UNIX)**
UNIX Marketing Course
Unisys
- [16] **Novell (Introduction to Networking Course)**
Novell 1994.

Publicaciones Periódicas

- [17] PC Magazine en español**
Volúmen 5, Número 9
Septiembre de 1994
Ziff Communications/Edit. América

- [18] PC Computing en español**
Mayo de 1994
Ziff-Davis

- [19] BYTE México**
Año 8, Número 82
Noviembre de 1994
EDICOBISA

- [20] Aberdeen Group (Market View Point)**
Volume 3, Number 3
February, 1994
Aberdeen Group

- [21] Personal Computing México**
Año 5, Número 73
Junio de 1994
Sayrols