

36
29.



Universidad Nacional Autónoma de México

**ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
ARAGON**

INGENIERIA EN COMPUTACION

**ADMINISTRACION DE UN CENTRO DE COMPUTO CASO
PRACTICO**

TESIS

**QUE PARA OBTENER EL TITULO DE
INGENIERO EN COMPUTACION**

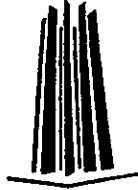
P R E S E N T A N

**MANUEL LOPEZ LUGO
LUIS MARTINEZ IBARRA**

**ASESOR DE TESIS:
Dr. ENRIQUE DALTABUIT GODAS**



ENEP



ARAGON

San Juan de Aragón, Edo. Mex. Mayo de 1998.

**TESIS CON
FALLA DE ORIGEN**

263054



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

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

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

A nuestros padres:

Por habernos dado todo lo mejor de ellos para que pudiéramos salir adelante, por esa confianza que han depositado en nosotros y por todo el apoyo y cariño que siempre hemos recibido de su parte, muchas gracias.

A nuestros hermanos:

Por toda la ayuda y confianza que nos brindaron para terminar la carrera.

A la universidad:

Por la puerta abierta a la cultura que nos permitió entrar al camino del conocimiento.

A nuestra escuela:

Por proveer todas las herramientas que hicieran posible que alcanzáramos la primera meta del camino.

A nuestros maestros:

Que nos abrieron las puertas al conocimiento y con su paciencia y dedicación compartieron con nosotros su sabiduría.

A nuestros amigos:

Quienes nos enseñaron el verdadero concepto de la amistad y nos hicieron disfrutar aun más nuestra carrera con su compañía.

A nuestro amigo:

Ing. Rafael Ramírez Otamendi por todo su apoyo, ayuda y motivación para la elaboración de la presente tesis.

A la D.C.A.A.

Por toda la sabiduría que deposito en nosotros durante nuestra estancia, a la Lic. Rosario Salinas Cuellar y a la Lic. Lorea San Martín Tejedo por todo el apoyo, confianza y motivación que nos brindaron para la realización de la presente tesis.

Gracias a todos:

Luis Martínez Ibarra
Manuel López Lugo

INDICE

ADMINISTRACION DE UN CENTRO DE CÓMPUTO CASO PRACTICO

1.- Antecedentes	3
1.1. Crecimiento de los Centros de Cómputo	3
1.2. Crecimiento del CCA (Centro de Ciencias de la Atmósfera).....	5
2- Situación inicial	11
2.1. Descripción del equipo	13
2.2. Problemas que se encontraron en un inicio en el Centro de Cómputo	16
2.3. Diagrama de la red en la situación inicial.....	17
3.- Estándares y requerimientos	21
3.1. Estándar	21
3.2. Estándar abierto	21
3.3. Arquitectura cliente-servidor	21
3.4. Definición de arquitectura cliente-servidor	22
3.5. Tipos de sistemas.....	24
3.5.1. Sistema servidor.....	24
3.5.2. Sistema standalone.....	25
3.5.3. Clientes diskless.....	25
3.5.4. Clientes dataless.....	25
3.5.5. Sistemas autoclient	25
3.6. Guía para seleccionar tipos de sistemas.....	25
3.6.1. Administración centralizada	26
3.6.2. El performance (Calidad de Operación)	26
3.6.3. El uso de disco	26
3.7. Sistema de archivos en el Sistema Operativo Unix	26
3.7.1. Tipos de sistemas de archivos.....	27
3.7.2. Sistemas de archivos basados en discos	27
3.7.3. Sistemas de archivos basados en red	27
3.7.4. Sistemas de archivos virtuales	28
3.8. Particiones de disco	28
3.9. Arreglo de las particiones con múltiples discos	29
3.10. Determinando que partición usar.....	29
3.11. Proceso de migración.....	30
3.11.1. Ventajas de migrar al ambiente del S.O. Solaris	30
3.11.2. Portabilidad, Escalabilidad, Interoperabilidad y Compatibilidad	31
3.11.3. Mejoras para los administradores de sistemas.....	32
3.11.4. Cambios en la instalación y configuración	32
3.11.5. Rasgos generales de la instalación del S.O. Solaris.....	33
3.12. Impresoras sobre red.....	34
3.12.1. Distribución de impresoras sobre red	34
3.12.2. Asignando servidores y clientes de impresión.....	35

3.13. TCP/IP, Protocolo de Control de Transmisión/Protocolo de Internet, (Transmission Control Protocol/Internet Protocol)	36
3.13.1. Características de TCP/IP	37
3.13.2. Niveles TCP/IP	38
3.13.3. Direccionamiento	38
3.13.3.1. Direccionamiento Físico	39
3.13.3.2. Direccionamiento Internet	39
3.13.4. Mapeo de direcciones	41
3.13.5. Mapeo de direcciones Internet a direcciones Físicas	41
3.13.6. Servidor de Nombres de Dominio (DNS: Domain Name System)	41
3.13.6.1. Mapeo entre nombres y direcciones IP	43
3.13.6.2. Servidores de nombres	43
3.13.7. Protocolo de Internet (IP: Internet Protocol)	44
3.13.8. Protocolo de Control de Transmisión (TCP) y Protocolo de Datagramas de Usuario (UDP)	46
3.14. Fundamentos del administrador	47
3.14.1. Actividades del administrador del sistema	48
3.14.2. Respaldos	50
3.14.2.1. Estrategias para hacer respaldos	51
3.14.2.2. Respaldos remotos	53
3.14.3. Sistemas de Archivos en Red (NFS: Network File System)	53
3.14.4. Cuotas	55
4.- Propuesta de solución para el Centro de Ciencias de la Atmósfera	59
4.1. Problemas que se encontraron en un inicio en el Centro de Cómputo	59
4.2. Realización de respaldos	60
4.3. Compartir recursos en red	61
4.4. Cuotas	62
4.5. Estandarización de los Sistemas Operativos	63
4.6. Instalación del disco optomagnético externo (Vertex)	67
4.7. Servidores de impresión	68
4.8. Instalación de software para despliegue de imágenes postscript	70
4.8.1. PostScript	70
4.8.2. PDF (Formato de Documento Portable)	71
4.8.3. Ghostscript	71
4.8.4. Ghostview	72
4.9. Instalación de software de seguridad	73
4.9.1. PASSWD+	74
4.9.2. COPS (Computer and Password System)	74
4.9.3. TCP-Wrapper	75
5.- Implementación	81
5.1. Realización de respaldos	81
5.2. Compartir archivos a través de NFS	83
5.3. Cuotas	84

5.4. Estandarización de los Sistemas Operativos	86
5.5. Instalación del disco optomagnético externo (Vertex)	90
5.6. Servidores de impresión	90
5.7. Instalación de software para despliegue de imágenes PostScript	91
5.8. Seguridad	91
5.8.1. Buenos passwords	92
5.8.2. Malos passwords	93
5.8.3. Restringiendo el comando su	94
5.8.4. Sistemas de archivos en UNIX	95
5.8.5. Umask	96
5.8.6. Permisos en directorios	96
5.8.7. Herramientas de seguridad	97
5.8.7.1. PASSWD+	97
5.8.7.2. COPS	98
5.8.7.3. TCP-Wrapper	98
Resultados y Conclusiones	103
Apéndices	107
A Instalación del Sistema Operativo Solaris 5.x	109
Preinstalación	109
Requerimientos de hardware	110
Instalación	111
Notas y tips de instalación	115
Posinstalación	116
B Diferencias de SunOS 4.1.X y Solaris 5.X	119
Diferencias en los comandos de administración	119
Diferencias en los archivos de administración SunOS 4.1.X y Solaris 5.X	122
Glosario	125
Bibliografía	141
Lista de productos utilizados	143

Introducción.

La actividad del ser humano se basa en la información y esta época se caracteriza por el crecimiento acelerado de los volúmenes de la misma. Para que dicha información tenga utilidad de alguna manera tiene que utilizarse y moverse, de este hecho se deriva la creciente importancia de los sistemas de comunicación. Estos sistemas con el paso del tiempo han sufrido modificaciones radicales debido a las innovaciones en el campo de las comunicaciones.

Durante la última década, las computadoras y las redes han producido en nuestra sociedad un impacto de enormes consecuencias. Se dice que hemos entrado en la "Era de la información". Lo cierto es que estas herramientas revolucionarias han multiplicado la productividad y eficiencia del trabajo, tanto para las empresas como para los usuarios individuales. Día a día, infinidad de usuarios acuden a las redes para atender sus necesidades privadas o comerciales, y esta tendencia se acentúa a medida que las empresas y los usuarios van descubriendo la potencia de estos medios.

Conforme avanza la tecnología, descubrimos que el uso de la computadora se va aplicando a situaciones y a objetivos nunca antes imaginados. El empleo de la computadora en universidades, instituciones públicas y privadas, en el hogar, etc., continúa creciendo; pero un beneficio mayor se presenta en cualquier lugar en el que se tengan dos o más computadoras enlazadas en red.

Las computadoras se van acoplando a nuestra vida diaria, cada vez las usamos más para resolver nuestros problemas; éstas son capaces de hacer muchas cosas desde ayudarnos a crear nuevos programas de aplicación, realizar simulaciones de procesos industriales, hasta cosas tan sencillas y cotidianas como ayudarnos a escribir un texto y darle presentación. Sin embargo, consideramos las capacidades adicionales que estarían disponibles si conectara su computadora a otras y desplegara la información contenida en ellas. La puerta se abriría hacia un mundo de mayor información.

Es importante mencionar que el objetivo de las redes es compartir elementos tales como equipo periférico, impresoras, información, etc., con la implantación de una red sabemos que podremos contar con enlaces de comunicación con computadoras o redes remotas.

La sociedad actual requiere un constante intercambio de información que sea oportuna y segura en cualquier parte del mundo. Para ello se plantea la necesidad del uso de las redes de comunicación que vienen a ser la infraestructura que soporta y hace posible dicho intercambio de información.

En el presente trabajo encontrará el desarrollo de los temas que fueron necesarios para mejorar la administración de la red del Centro de Cómputo del CCA (Centro de Ciencias de la Atmósfera), perteneciente a la Universidad Nacional Autónoma de México.

Capítulo 1 “Antecedentes” En este capítulo se describirá el crecimiento de los Centros de Cómputo de la UNAM y en especial el crecimiento que ha tenido el Centro de Ciencias de la Atmósfera.

Capítulo 2 “Situación Inicial”. En este capítulo se menciona la situación inicial del Centro de Cómputo, con el equipo con que se cuenta y se detectaran los problemas iniciales de dicho Centro, con el fin de tener un parámetro en la línea de investigación para la realización de esta tesis.

Capítulo 3 “Estándares y Requerimientos” Aquí se analizarán los estándares y requerimientos que nos ayudarán a implementar una política de administración de los equipos, con el fin de proponer posibles soluciones para ayudar a resolver los problemas detectados en el capítulo 2.

Capítulo 4 “Propuesta de Solución” El objetivo de este capítulo es dar propuestas que solucionen los problemas descritos en el capítulo 2, se describirá el problema y la solución planteada sobre la base de las investigaciones hechas en el capítulo 3.

Capítulo 5 “Implementación” Es este capítulo se describirá la puesta en marcha de las soluciones sobre la base de los planteamientos realizados en el capítulo 4; además se describirán los resultados obtenidos.

Al final de la tesis podrá encontrar dos apéndices; en el primero se describe una breve explicación del proceso de instalación del Sistema Operativo Solaris Sun 5.X, el cual fue utilizado para el proceso de instalación del Sistema Operativo en las estaciones de trabajo, y en el segundo se describe las principales diferencias entre las versiones de SunOS (Sistema Operativo desarrollado por Sun Micro Systems) 4.1.X y Solaris 5.X, las cuales nos fueron de gran ayuda en el proceso de migración de los Sistemas Operativos de las estaciones de trabajo descrito en la presente tesis.

También al final encontrara un glosario de términos más utilizados en esta área del cómputo, y las fuentes de información que han sido utilizadas para la sustentación que se presenta en esta tesis.

Esperamos que con este breve panorama del contenido del presente trabajo, que conjunta tanto al aspecto teórico como el practico sea útil en la consulta acerca del tema de la administración de redes de cómputo.

Justificación

A manera de justificación del presente trabajo cabe mencionar la tendencia actual de los sistemas de cómputo, a trabajar en un entorno de red, para obtener un alto índice de rendimiento y rentabilidad de los equipos así configurados y operados.

Una de las influencias más profundas en el desarrollo de las redes de cómputo, ha sido la adopción de estándares de diseño y administración de redes de computadoras y centros de cómputo (estándares que incluso los gigantes de la industria encuentran difícil de pasar por alto).

El propósito más importante de este trabajo es lograr la buena funcionalidad de esta red de cómputo ya que no es admisible que si la función de un centro de cómputo es simplificar las labores administrativas, ésta termine por ser más complicada, además la falta de administración nos lleva a un desperdicio de los recursos de cómputo, tanto humanos como materiales.

La interconexión de dispositivos se debe hacer conforme a estándares coherentes y políticas de administración. El objetivo de la interconexión y la administración de los dispositivos de la red es asegurar la eficiencia global de la red, la disponibilidad de recursos y la productividad de los usuarios sin importar donde se encuentren.

Así como una computadora vacía, es como una mente también vacía, de poca o ninguna utilidad para nadie, incluyendo a su propietario. Si cada computadora debe ser llenada en forma diferente y a mano, entonces el trabajo se vuelve menos (no más) eficiente.

En el desarrollo de la era de la informática es importante, que la tecnología ayude a las personas a reducir la cantidad de la información a niveles manejables y a mejorar la calidad de dicha información.

Objetivo General

- Analizar el estado actual del centro de cómputo.
- Detectar los principales problemas que aquejan a este centro, con el fin de dejarlo trabajando a su máxima capacidad para que los investigadores desarrollen día con día nuevas aplicaciones.
- Que el sistema de red sea íntegro y confiable para el usuario final, sin que este tenga que ver nada en cuanto a la administración, ni resolución de los problemas que antes él tenía que resolver, y se dedique a desarrollar las tareas que él sabe hacer sin tener que pensar en la red de cómputo como un problema más en su trabajo sino como una herramienta que le ayude a simplificar y mejorar sus labores cotidianas.

Objetivo Particular

La red de cómputo en su fase inicial tiene problemas referentes a la administración y al mantenimiento de los equipos, en particular de las estaciones de trabajo, PC's y equipos periféricos en los cuales enfocaremos la realización de la presente tesis.

A lo referente a cableado y la infraestructura de red instalada actualmente no presenta ningún problema, ya que dicha red fue realizada conforme a las normas de cableado estructurado para edificios comerciales (Norma EIA/TIA 568/B), por lo tanto el desarrollo de esta tesis no se enfocará a los problemas referentes al cableado. Para conocer más acerca del diseño de redes en cuanto a cableado se recomienda consultar manuales para diseño de redes en los que se describe los fundamentos básicos que se deben tener en cuenta en el diseño de cualquier tipo de red de área local, no solamente a un tipo específico ni particular.

1

Antecedentes

1.- Antecedentes	3
1.1. Crecimiento de los Centros de Cómputo.....	3
1.2. Crecimiento del CCA (Centro de Ciencias de la Atmósfera).....	5

Capítulo 1

Antecedentes.

Cuando se habla del uso de la red en los centros de cómputo se piensa en los dispositivos que son necesarios para la red, y si funcionan no hay problema, pero no se piensa en lo que hay atrás de esto: ¿quién es el responsable de administrar la red?, si el administrador actual es el mismo que analizó y diseñó la red, los pasos a seguir para su puesta en marcha, si se basó en los estándares actuales o si solo lo hizo a "sentimiento", ¿por qué uso ese software?, ¿Cómo lo configuro?, etc. y si al terminar documento todo.

En la administración de un centro de cómputo se pueden encontrar muchos problemas debido a que éstos jamás fueron planeados, por ejemplo si se necesita un punto de red, sólo tienden el cable y ya, si se necesita un equipo nuevo le habla al proveedor, y este vende lo que quiere, si se necesita instalar un software en el servidor, se instala no importa dónde ni cuántas veces se intente sólo lo hacen y ya, y al final lo que obtenemos es un crecimiento que no fue planeado ni documentado, problemas con los equipos por que no eran los requeridos, problemas con la conexión de red, y al final se dan cuenta que el costo de tener a un ingeniero en la materia hubiera salido más barato que hacer modificaciones, parches y cambios de equipo, etc.

1.1. Crecimiento de los Centros de Cómputo.

En los centros de cómputo, las conexiones, los servidores (las computadoras centrales), las estaciones de trabajo, etc., ofrecen el medio para permitir que el poder de cómputo disponible, sea utilizado a su máxima capacidad. Otros aspectos generan intereses en el centro, incluyendo el deseo de las personas de tener independencia en las operaciones de cómputo, la necesidad de contar con una computadora en todos y cada uno de los departamentos y la economía de una LAN.

Pero no es sólo el pensar en los componentes del centro de cómputo el que lo hace que sea óptimo para los objetivos que se persigan, sino además otros son los factores que se complementan para tener un centro que realmente sea el adecuado y este es el personal que lo opera, ya que sin un personal calificado el centro tendrá más problemas que resolver.

Los centros de cómputo día con día crecen y tienen cambios en su infraestructura ya sea en sus conexiones internas, en sus servidores, en sus estaciones de trabajo o en equipos PC's, etc. y con un personal que no tuvo cuidado en realizar un diseño y mucho menos una planeación, por muchas razones como son tiempo, conocimiento, presupuesto, negligencia, etc, el centro seguirá modificándose más por lo que sólo recibirá parches para corregir la situación y no el problema desde la raíz.

Actualmente el principal problema que tiene el administrador de una red de cómputo es que la mayoría de dichos centros nunca fue documentado, planeado, ni diseñado, ya que

el crecimiento de la mayoría de las redes se va dando indistintamente de acuerdo al avance tecnológico, y al crecimiento que este vaya teniendo a través del tiempo.

Muchas preguntas salen por la ignorancia o por la mala documentación, como ¿cuál es el servidor de archivos?, ¿cuál es el servidor de correo?, ¿cuál es el servidor de impresión?, ¿de dónde proviene este cable?, ¿en dónde esta instalada la licencia de algún lenguaje?, ¿porqué no hay servicio de red externo solo interno?. Son muchas las preguntas o factores que retrasan y obstaculizan la labor de un administrador de redes ya que en la mayoría de las veces el crecimiento que llega a tener su red ha sido anárquico.

El crecimiento que han tenido los centros de cómputo en los últimos 5 años, ha sido de gran relevancia, ya que han podido descentralizar sus operaciones para así contar con su propia capacidad de cómputo para desarrollo de nuevas aplicaciones. De esta manera no dependerá de alguien en específico que le brinde este servicio y mucho menos esperar respuestas para la realización de alguna actividad.

Pero este crecimiento no ha sido sólo del centro de cómputo de Ciencias de la Atmósfera, sino que ha sido adoptado por muchas empresas y organizaciones de varios sectores económicos que antes no pensaban en tener su propia capacidad de cómputo, incluso las mismas empresas pequeñas empiezan a tener interés en optar por estas nuevas tecnologías para ayudar a mejorar su productividad.

Hace algunos años algunas personas aun veían lejos el poder tener una capacidad de cómputo propia que les pudiera resolver sus problemas de productividad utilizando equipos de alta tecnología como las redes de computadoras. Si nos remontamos a unos 5 años atrás el número de centros de cómputo que en México existían eran muy pocos, solo se podían mencionar unos cuantos en Universidades y empresas privadas (de gran capacidad) teniendo en ese entonces una gran demanda en cuanto a usuarios en espera de ser atendidos de manera eficaz, e incluso hemos visto que el uso de la INTERNET ha ido creciendo en los últimos años de manera exponencial, llegando a que la adopción de la INTERNET en la mayoría de las empresas mexicanas es ya una realidad. Nosotros recordamos que hace unos años ningún anuncio en televisión del sector público o privado hacia referencia a su dirección de correo electrónico o su página del WEB.

Hoy muchas empresas han optado por implementar las herramientas de Cómputo para el crecimiento de la productividad de sus empresas y actividades personales dándose casos como desarrollos de proyectos a distancia o el editar artículos, libros o resolver problemas de distintos géneros e incluso tener educación a distancia sin estar físicamente en el mismo lugar y que jamás vamos a conocer a la gente que nos esta ayudando a resolver un problema, comprando o vendiendo un producto. ¿Cuántas personas han escrito o resuelto problemas juntos a través de INTERNET y no haberse conocido sino meses después de haber escrito la primera letra de un correo electrónico?.

Pero, ¿a qué nos lleva esto?. Nos lleva a comprar equipos y diseñar nuestras propias redes de cómputo como la empresa y las necesidades vayan creciendo, un crecimiento

acelerado pero rara vez planeado y sobre todo administrado de manera correcta. Ya que la mayoría de estos diseñadores no cuentan con una capacitación o conocimiento acerca del área en cuestión, solo conocen lo que el vendedor les dice y desafortunadamente la mayoría de los vendedores tienen estas mismas interrogantes.

Algunas expresiones que continuamente se escuchan a menudo en los centros de cómputo y que obligan a los usuarios a pensar en alguna persona que les pueda dar respuesta a sus problemas son palabras como:

- ¡Este habrá sido el servidor que nosotros necesitábamos!
- ¿Cómo puedo hacer para que todos podamos ver la misma información?
- ¡Otra vez se perdió la conexión!
- ¡Ya no hay red!
- ¿Quién me desconecta la impresora?
- ¡Se acaba de perder toda la información!
- ¡Acabamos de comprar un disco de gran capacidad y ya está lleno !
- ¿Cómo puedo prevenir mi futuro crecimiento?
- ¿Qué necesito hacer para que mi red funcione de manera optima?
- Habla a la persona que nos vendió el equipo para que venga a restaurar el servicio nuevamente. ¡ Pero nos va a volver a costar 100 dólares el servicio.....!
- Háblale a tu amigo el güru sí, ese el que me cae bien gordo, para que nos ayude a resolver el problema.
- ¿Alguien se volvió a introducir al sistema?

1.2. Crecimiento del CCA (Centro de Ciencias de la Atmósfera).

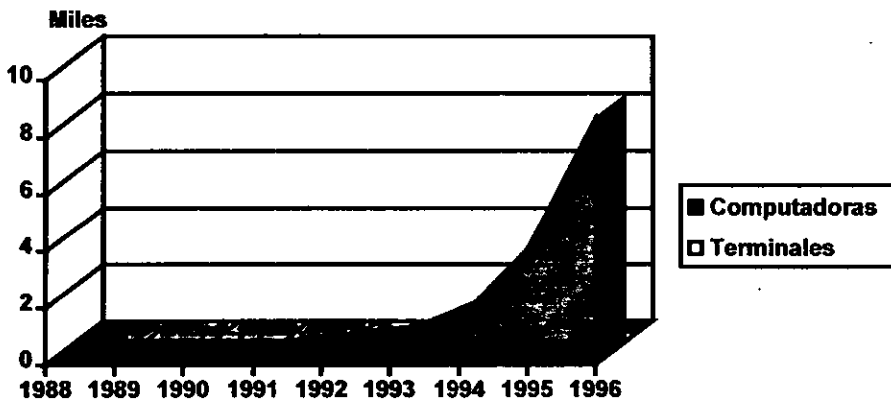
El centro de cómputo del CCA (Centro de Ciencias de la Atmósfera) es aún joven, su crecimiento fue acelerado con el avance de la tecnología y por supuesto con el cómputo que se ha convertido en una herramienta indispensable en nuestros días.

El Centro de Ciencias de la Atmósfera hizo uso en sus primeros años de las computadoras B-6700, B-6800, B-7800 y A-12, que proporcionaban servicio de cómputo a investigadores, en este sentido siempre hubo una dependencia hacia instituciones como el Programa Universitario de Cómputo (PUC) ahora DGSCA (Dirección General de Servicios de Cómputo Académico), Centro de Investigación en Matemáticas Aplicadas y en Sistemas (CIMAS), etc. hasta el año de 1987, cuando se adquiere una microcomputadora modelo TITÁN propia.

Durante esta primera etapa las computadoras eran de gran tamaño, extremadamente caras y muy difíciles de usar. Estas enormes máquinas ocupaban normalmente amplias salas y eran gestionadas por el usuario desde una consola, único medio de acceder a dicha computadora; también los problemas de administración y manejo de estas computadoras eran ajenos a este centro debido a que solo eran usuarios de los servicios que les proporcionaban. Pero aún así había problemas para los usuarios, como son el manejo de algún software o el diseño de algún programa por lo que ellos recibían asesorías.

Lo que ocurre a finales de los 80's y a principios de los 90's y hasta la fecha dentro de la UNAM es una revolución en las comunicaciones, la adquisición masiva de computadoras personales (véase la fig. 1.1. y fig. 1.2.), y su interconexión en redes de área local, lo cual permitió desarrollar la infraestructura de comunicaciones con fibra óptica, par trenzado y establecer más enlaces satelitales. Con esto último, se estableció en definitiva el final de la era del teleproceso, para dar paso a las redes de computadoras y sus enlaces de fibra óptica.

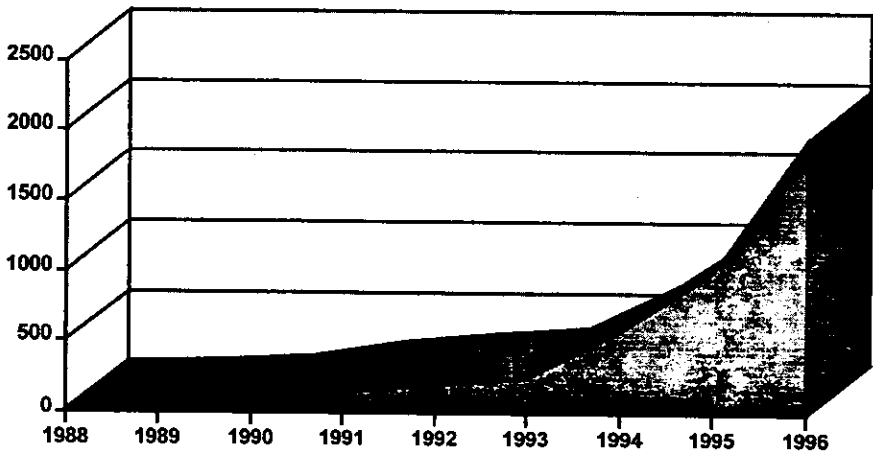
CRECIMIENTO DE LA RED UNAM DGSCA 1988-1996



Fuente DGSCA 1996

Figura 1.1

ESTACIONES DE TRABAJO DGSCA 1988-1996



Fuente DGSCA 1996

Figura 1.2.

Sin lugar a duda el campo que más se ha transformado en los últimos años en nuestro país y en nuestra Universidad ha sido el desarrollo tecnológico en informática, en particular en el área de cómputo y telecomunicaciones que sustenta los programas académicos de vanguardia que desarrolla DGSCA (Dirección General de Servicios de Cómputo Académico), apoyando los sistemas administrativos y proporcionando infraestructura de telecomunicaciones, lo que ha permitido que nuestra institución se coloque al mismo nivel que las instituciones del primer mundo.

El centro de cómputo del CCA no fue la excepción en la participación de estos cambios que trajeron muchos progresos pero también grandes problemas. Como se mostró en las gráficas anteriores el crecimiento ha sido tan acelerado que organizaciones que antes no tenían una infraestructura de cómputo sólida o centros de enseñanza que se mostraban ajenos al mundo de la computación ahora lo ven como una necesidad cotidiana en sus ámbitos de trabajo.

Los problemas que trajo este tipo de situaciones en la mayoría de los nuevos centros de cómputo que se empezaron a crear como el CCA, fueron que el mismo personal empezara a tomar decisiones sobre equipos de cómputo sin saber si realmente estaban haciendo lo correcto, o instalar y configurar equipo sin tener algún conocimiento de cómputo; lo peor de todo hacer compras sugeridas por personal de ventas que jamás tuvo una cultura informática para dar ese tipo de asesoría. Lo que nos daba como resultado una

forma de trabajo empírica y una falta de normalización en el crecimiento y compatibilidad del equipo.

Como consecuencia este centro se enfrenta a otro reto más, después de haber instalado su red y adquirir su propio equipo de cómputo, el problema ya no van a ser sólo los usuarios, ahora es cómo comenzar a operar los equipos, configurarlos, administrarlos y algo más interesante, cómo optimizar su rendimiento, y aprovechar los recursos actuales.

2

Situación Inicial

2- Situación inicial	11
2.1. Descripción del equipo	13
2.2. Problemas que se encontraron en un inicio en el Centro de Cómputo	16
2.3. Diagrama de la red en la situación inicial.....	17

Capítulo 2

Situación Inicial.

El cómputo del Centro de Ciencias de la Atmósfera ha evolucionado desde el año de su fundación hasta nuestros días de la siguiente forma:

En los primeros años, (1977) se realizaba procesamiento informático en computadoras Burroughs B-6700 a través de tarjetas perforadas, lo cual marcaba los inicios del cómputo en dicho Centro, para los años 80's los trabajos de cómputo se realizaban en equipos Burroughs B-6800 con graficador de plumas e impresoras de matriz de puntos.

Para 1986 el centro adquiere su propio equipo de cómputo:

1 Microcomputadora Titán la cual nunca opera a su máxima capacidad, computadoras Apple las cuales eran utilizadas para el procesamiento de texto, además se usaban los equipos que proporcionaba el Programa Universitario de Cómputo (PUC) actualmente Dirección General de Servicios de Cómputo Académico (DGSCA).

Para los principios de los años 90's el Centro contaba con el siguiente equipo:

- Una Microcomputadora MICROVAX II: con 100 Mbytes en disco, 2 Mbytes en memoria central y un controlador de 90 Mbytes, mas terminal maestra, esta última fue subutilizada en un principio.
- Dos computadoras Ohio Scientific (C2 y C3).
- Dos computadoras Apple II.
- 11 Computadoras personales compatibles con IBM, PC. (Distribuidas en diversas áreas del Centro).
- 13 Impresoras distribuidas en el Centro.
- 2 Graficadoras.
- 1 Unidad de cinta.
- 1 Controlador de 6 puertos para 6 terminales conectadas a la computadora Burroughs del PUC.

En lo que respecta a los equipos PC's, desde 1986 hasta nuestras fechas, el Centro ha ido evolucionando desde equipos 80286, 80386, 486, hasta Pentium en sus distintos modelos y marcas.

En 1993 se da un gran salto en el desarrollo de cómputo del Centro, ya que se adquiría la primera estación de trabajo SUN-Sparc 10 "Belenos" para uso de las actividades del Centro de cómputo y ha ido cada año creciendo aceleradamente como se ve en la figura 2.1.

Crecimiento del Centro de Cómputo

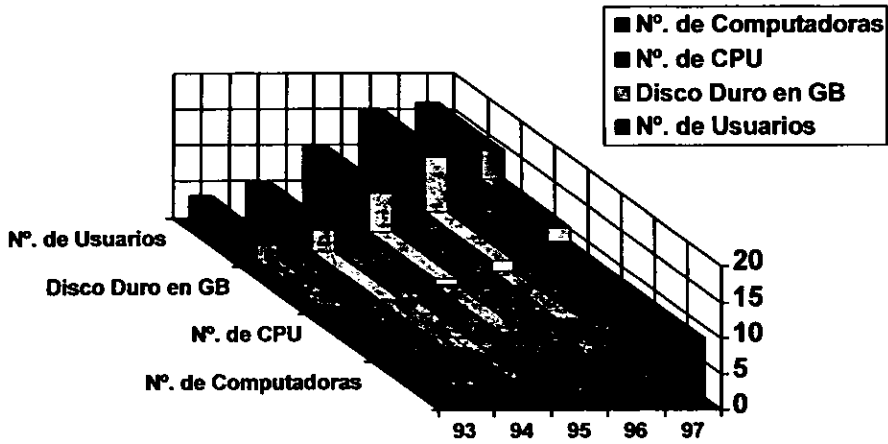


Figura 2.1.

De 1994 a 1995, el Centro empieza el uso general de las estaciones de trabajo en dos ramas distintas, como se muestra en la figura 2.2.



Las estaciones de trabajo que son utilizadas con Sistema Operativo VMS y las estaciones de trabajo que son utilizadas con Sistema Operativo UNIX, dentro de estas dos ramas una parte tuvo tendencia al crecimiento con equipo Sun bajo el sistema Operativo Solaris Unix y otra fue la de crecimiento con equipo de trabajo Digital en las dos versiones de sistema operativo: VMS y Unix, de Digital.

Para la realización del presente trabajo nosotros nos enfocaremos al crecimiento de las estaciones de trabajo Sun, y sólo mencionamos los equipos Digital para casos de comparación.

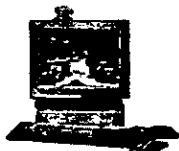
2.1. Descripción del equipo.

BELENOS: SUN SPARCstation 10



Sistema Operativo:	Solaris B.S.D 4.1.3.
Memoria:	96 MB.
CPU'S:	1
Disco Duro:	1.5 GB.
Dispositivos:	Unidad de Cinta de Respaldo de 8mm Exabyte 8505XL Unidad Interna de Disco Flexible de 3 ½".

CCAO2: SUN SPARCstation 5



Sistema Operativo:	Solaris B.S.D 4.1.3.
Memoria:	64 MB.
CPU'S:	1
Disco Duro:	2.5 GB.

VORTICE: SUN SPARCstation 5



Sistema Operativo:	Solaris 2.4
Memoria:	64 MB.
CPU'S:	1
Disco Duro:	2.5 GB.
Dispositivos:	CD-ROM externo 2x.

Equipos personales.

4 Digital 575 Pentium.
Disco Duro de 848 MB
16 MB en RAM.
Tarjeta de Red 3Com.

2 Digital 466.
Disco duro de 540 MB.
16 MB en RAM.
Tarjeta de Red 3Com.

Unidades de cinta.

Unidad de cinta EXABYTE 8500 DE 8mm.
Unidad de Cinta de 8mm IBM.

1 Multiplexor.

Unidades de CD-ROM.

Una unidad Externa.
Una unidad Interna

Impresoras.

1 HP laserJet IIP Plus.
1 DeskJet 1200C/PS Color. PostScript
1 NewGen Imager Plus PostScript.
1 Servidor de Impresión Multiprotocolo AXIS NPS550 RISC

Equipo que será utilizado para pruebas de instalación y configuración del mismo

Borola: SUN UltraSPARC 2.



Ultra 2 / Creator 3D

Sistema Operativo:
Memoria:
CPU'S:
Disco Duro:
Dispositivos:

Solaris 2.5.1.
128 MB.
2
4 GB.
Unidad Interna de CD-ROM 6X

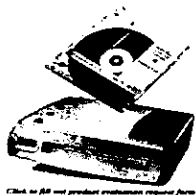
Regino: SUN UltraSPARC 1



Sistema Operativo:
Memoria:
CPU'S:
Disco Duro:

Solaris 2.5.1.
96 MB.
1
3 GB.

Otros dispositivos.



Unidad de Disco optomagnético de 5 1/4".
Capacidad de 1 GB por lado.

En un inicio la red de cómputo cuenta con el equipo antes mencionado (véase fig. 2.3.) el cual tiene algunos problemas referentes a la administración y al mantenimiento; el cableado y la infraestructura de red instalada actualmente no presentan ningún problema. En esta red se tienen identificados todos los puntos de red, así como los concentradores y la ubicación de cada uno de ellos. Es importante hacer notar que las mayores fallas en las redes de cómputo se presentan por fallas en el cableado, ya que este no ha sido planeado y diseñado correctamente.

Situación Inicial del Equipo en el Centro de Cómputo.

Estación	Modelo Sun	Disco del Sistema Operativo	Aplicaciones Compartidas en red	Sistema Operativo	Impresión en Red	Realización de Respaldos
Belenos	SPARCstation 10	No	No	SunOS 4.1.3	No	No
CCA02	SPARCstation 5	No	No	SunOS 4.1.3	No	No
Vórtice	SPARCstation 5	No	No	Solaris 2.4	No	No
* Borola	Ultra 2	Si	No	Solaris 2.5.1	No	No
* Regino	Ultra 1	No	No	Solaris 2.5.1	No	No

Figura 2.3

* Estos equipos serán utilizados para realizar pruebas de instalación y configuración de dispositivos y software.

Los problemas que se identificaron en un inicio en la red de cómputo fueron los siguientes:

2.2. Problemas que se encontraron en un inicio en el Centro de Cómputo.

1. No se tiene compartida la información utilizada.
2. Duplicidad de información.
3. No se cuenta con respaldos de información de ningún servidor.
4. No se cuenta con un servidor de impresión para las estaciones de trabajo sólo para los equipos PC's.
5. El proceso de impresión en las PC's es realizado con la ayuda de un multiplexor el cual es un proceso muy molesto para los usuarios.
6. Cada estación de trabajo trabaja en forma independiente.
7. El ambiente gráfico de comunicación de las PC's hacia las estaciones de trabajo no puede desplegar imágenes PostScript.
8. Cada estación de trabajo cuenta con un sistema operativo distinto.
9. No se cuenta con los discos de los sistemas operativos instalados en las estaciones de trabajo.
10. No existen cuotas para los usuarios.
11. Los sistemas no son muy confiables ya que, no reciben un mantenimiento constante.
12. Instalación de nuevo software para el desarrollo de nuevas aplicaciones.

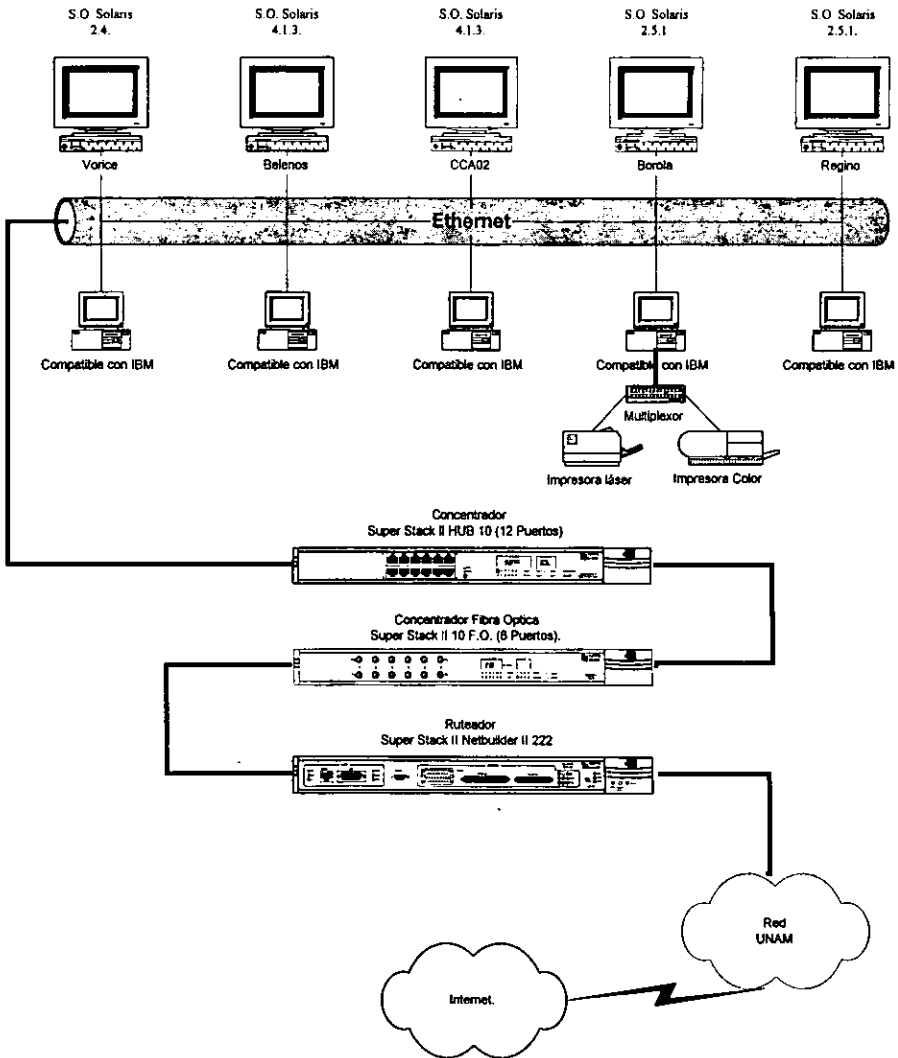
Estos son los problemas que nos enfocaremos a resolver en el presente trabajo.

Para la resolución de los problemas antes descritos se propone el siguiente procedimiento en base, al orden de importancia de las tareas a realizar y que son de mayor prioridad en el centro de cómputo:

- I - Realización de respaldos.
- II- Compartición de recursos en red.
- III- Asignación de cuotas.
- IV- Estandarización de los sistemas operativos.
- V- Instalación del disco optomagnético (VERTEX).
- VI- Servidores de Impresión.
- VII- Instalación de Software para despliegue de imágenes PostScript.
- VIII- Instalación de Software de Seguridad.

2.3. Diagrama de la red en la situación inicial.

SITUACIÓN INICIAL DEL CENTRO DE CÓMPUTO



3

Estándares y Requerimientos

3.- Estándares y requerimientos	21
3.1. Estándar	21
3.2. Estándar abierto	21
3.3. Arquitectura cliente-servidor	21
3.4. Definición de arquitectura cliente-servidor	22
3.5. Tipos de sistemas.....	24
3.5.1. Sistema servidor.....	24
3.5.2. Sistema standalone.....	25
3.5.3. Clientes diskless.....	25
3.5.4. Clientes dataless.....	25
3.5.5. Sistemas autoclient	25
3.6. Guía para seleccionar tipos de sistemas.....	25
3.6.1. Administración centralizada	26
3.6.2. El performance (Calidad de Operación)	26
3.6.3. El uso de disco	26
3.7. Sistema de archivos en el Sistema Operativo Unix.....	26
3.7.1. Tipos de sistemas de archivos.....	27
3.7.2. Sistemas de archivos basados en discos	27
3.7.3. Sistemas de archivos basados en red	27
3.7.4. Sistemas de archivos virtuales	28
3.8. Particiones de disco	28
3.9. Arreglo de las particiones con múltiples discos	29
3.10. Determinando que partición usar.....	29
3.11. Proceso de migración.....	30
3.11.1. Ventajas de migrar al ambiente del S.O. Solaris	30
3.11.2. Portabilidad, Escalabilidad, Interoperabilidad y Compatibilidad	31
3.11.3. Mejoras para los administradores de sistemas.....	32
3.11.4. Cambios en la instalación y configuración	32
3.11.5. Rasgos generales de la instalación del S.O. Solaris.....	33
3.12. Impresoras sobre red.....	34
3.12.1. Distribución de impresoras sobre red	34
3.12.2. Asignando servidores y clientes de impresión.....	35
3.13. TCP/IP, Protocolo de Control de Transmisión/Protocolo de Internet,	

(Transmission Control Protocol/Internet Protocol)	36
3.13.1. Características de TCP/IP	37
3.13.2. Niveles TCP/IP	38
3.13.3. Direccionamiento	38
3.13.3.1. Direccionamiento Físico	39
3.13.3.2. Direccionamiento Internet	39
3.13.4. Mapeo de direcciones	41
3.13.5. Mapeo de direcciones Internet a direcciones Físicas	41
3.13.6. Servidor de Nombres de Dominio (DNS: Domain Name System)	41
3.13.6.1. Mapeo entre nombres y direcciones IP	43
3.13.6.2. Servidores de nombres	43
3.13.7. Protocolo de Internet (IP: Internet Protocol)	44
3.13.8. Protocolo de Control de Transmisión (TCP) y Protocolo de Datagramas de Usuario (UDP)	46
3.14. Fundamentos del administrador	47
3.14.1. Actividades del administrador del sistema	48
3.14.2. Respaldos	50
3.14.2.1. Estrategias para hacer respaldos	51
3.14.2.2. Respaldos remotos	53
3.14.3. Sistemas de Archivos en Red (NFS: Network File System)	53
3.14.4. Cuotas	55

Capítulo 3

Estándares y Requerimientos.

3.1. Estándar. En computación, conjunto de reglas o especificaciones que, en conjunto, definen la arquitectura de un dispositivo de hardware, programa o sistema operativo.

3.2. Estándar abierto. Es un conjunto de reglas y especificaciones, que en conjunto describen las características de diseño u operación de un programa o dispositivo, que se publica y ofrece libremente a la comunidad técnica. Los estándares abiertos pueden contribuir a un rápido crecimiento del mercado si fomentan la interoperabilidad (la capacidad de un dispositivo creado por un fabricante para funcionar con un dispositivo creado por un fabricante distinto). Lo opuesto a un estándar abierto es un estándar patentado, impulsado por una compañía que espera que su estándar, y no otro, llegue a dominar el mercado.

Ventajas:

- Maneja un conjunto limitado y preciso de términos
- Incrementa la compatibilidad y conectividad
- Facilita el intercambio de información
- Aumenta la productividad y la eficiencia
- Crean una base para sustentar nuevas tecnologías
- Permite mantener un control mundialmente ideal de tecnología.

3.3. Arquitectura cliente-servidor.

Existen diversas Arquitecturas, que obedecen a la idea de cómo deseamos resolver los problemas, básicamente podríamos hablar de tres tipos: la Arquitectura Centralizada, la Arquitectura Peer-to-Peer (uno a uno) y la Arquitectura cliente-servidor.

En el primer caso, Arquitectura Centralizada, todo el trabajo y toda la información se realiza y reside en una sola máquina, que habitualmente son los grandes MainFrame, y de hecho manejan también un Sistema Operativo monolítico con una nula interfaz con los usuarios, en este caso, el usuario manda ejecutar sus trabajos a través de unas terminales tontas en modo de lote.

La ventaja de estos equipos es que su capacidad de procesamiento es muy superior a cualquier máquina y la capacidad de almacenamiento es enorme, su desventaja es que si en dado momento fallara el MainFrame se pararía el trabajo totalmente. Hay que mencionar que esta Arquitectura así como las MainFrame están en proceso de desaparecer. Aunque las grandes instituciones que necesitan gran capacidad de cálculo y almacenamiento, como los bancos y compañías de seguros lo utilizarán y en algunos casos lo siguen utilizando.

La Arquitectura Peer to Peer, es en la que ambas máquinas realizan procesos y guardan información sin que ninguna de ellas lleve a cabo más trabajo que la otra, en general esta arquitectura es la que se utiliza en aplicaciones de escritorio para estar comunicados y puedan compartir información sin que por ello dependan la una de la otra.

La Arquitectura cliente-servidor es en la que hay una máquina Servidor que atiende solo a peticiones de clientes que están perfectamente formuladas y le regresan respuestas a sus peticiones, las computadoras clientes por su parte se encargan de dar la interfaz al usuario para interactuar con ellos. Además esta es la Arquitectura que empieza a dominar al cómputo y por lo cual nos enfocaremos más en ella.

La Arquitectura cliente - servidor, esta formada por uno o más clientes y uno o más servidores, que junto con el sistema operativo y los protocolos de comunicación, conforman el ambiente que permite y facilita el cómputo distribuido.

La idea o filosofía del cómputo distribuido nos permite utilizar todos los recursos de todas las máquinas de una manera mas cooperativa y sin sobrecargar ni depender de un solo equipo.

En una aplicación basada en esta Arquitectura existen dos procesos independientes, en lugar de uno solo. De esta forma se puede repartir el trabajo a través de varias computadoras en una red. Estos dos procesos, cliente y servidor, se comunican mediante un protocolo bien definido. Esta técnica permite la comunicación entre distintas computadoras (servidores de archivos, estaciones de trabajo de alta resolución en gráficos), para que cada una de ellas se dedique a realizar el trabajo que hace mejor.

De manera introductoria, se puede decir que un servidor es una computadora con un sistema o un programa que provee de algún servicio a otros Sistemas a través de una red. Un ejemplo típico es un *servidor de archivos, que permite el acceso a información remota a cualquier usuario a través de la red*. Un cliente es un sistema que requiere y recibe alguna acción de un servidor.

Esta filosofía de cómputo, es la que más auge tiene en la actualidad y es la que más futuro tiene, por diversas causas y razones, y es a la que nos enfocaremos, dado que es la que presenta más ventajas que desventajas. Por eso nos falta definir varios conceptos que son muy importantes para comprender mejor la Arquitectura Cliente/Servidor.

3.4. Definición de arquitectura cliente-servidor.

La Arquitectura cliente-servidor es una forma de cómputo de red en la que ciertas funciones solicitadas por clientes son servidas por los procesos adecuados.

Un servidor es un administrador de recursos. Un recurso puede ser identificado como algo físico o abstracto, como una base de datos. Un cliente es un usuario de los recursos que administra el servidor.

Bajo este esquema, se reparte el proceso de una aplicación entre un **front end** y un **back end**. En el estándar de la ciencia de la computación, un proceso es un programa corriendo en el procesador (back end).

De manera general, para que se inicie la comunicación entre un cliente y un servidor es necesario establecer una sesión. Por lo tanto, el servidor debe estar esperando que algún cliente trate de establecer una sesión. Esto quiere decir que un cliente puede hablar pero si no es escuchado, la comunicación va a fracasar. Es muy posible que, por algún momento el servidor también hable y que el cliente escuche, pero esto solo se hará cuando el servidor así lo indique al cliente.

Un servidor se reserva también el derecho de mantener uno o mas clientes. Así el servidor se encargara de atender a cada cliente y establecer los mecanismos que seguirá para la distribución de sus servicios. Un servidor define operaciones que son exportadas a los clientes. Los clientes invocan estas operaciones para que el servidor controle el manejo de datos.

Típicamente una aplicación comenzara una transacción, ejecutara una o varias operaciones en el servidor y terminara la transacción. Lógicamente los servidores están estructurados como un ciclo infinito. El servidor simplemente recibe los requerimientos de los clientes para invocar operaciones en favor de esas transacciones. Para implantar las operaciones que exporta, el servidor puede requerir de otro servidor o puede manipular sus propios datos.

Servidor. Es un sistema que provee servicios a otros sistemas (clientes) a través de la red. Existen servidores de archivos, servidores de arranque (boot), servidores de bases de datos, servidores de impresión, servidores de instalación y servidores de aplicaciones particulares. Este término es comúnmente usado para describir a los servidores que proveen sistemas de archivos y software de instalación para otros sistemas a través de la red.

Los principales beneficios de los servidores, es proveer software y servicios de uso común para que otros sistemas puedan trabajar. El soporte que estos incluyen son:

- Ayudar a que un sistema pueda ser conocido por la red, por ejemplo proporcionándole la información de su nombre y dirección.
- Proveer servicios de instalación de sistemas remotos.
- Proveer servicio de sistema operativo para equipos con capacidades limitadas.

Cliente. Es un sistema que usa servicios remotos que le proporciona un servidor. Algunos clientes tienen limitaciones de capacidad de almacenamiento o quizá no tengan ninguna capacidad de almacenamiento en lo absoluto y ellos tienen que utilizar los de un servidor que les proporcione este servicio, algunos ejemplos de estos clientes son los que son sin discos y sin datos (Diskless y Dataless).

Otros clientes utilizan servicios remotos (como software de instalación) de un servidor, pero ellos realmente no dependen de este servidor para otras operaciones. Un sistema Standalone puede tener en su disco duro, sus propios sistemas de archivos y trabajar de forma independiente.

¿Qué significa proveer? Proveer soporte para un sistema, significa proporcionar software y servicios para ayudar a que otros sistemas funcionen. El soporte puede incluir entre otros servicios:

- Hacer que el sistema sea conocido por la red. (Por ejemplo proporcionar el nombre y la dirección IP a una máquina).
- Proporcionar servicios de instalación para arrancar desde un sistema remoto.

3.5. Tipos de sistemas.

Los tipos de sistemas son básicamente definidos en como ellos accesan los sistemas de archivos root (/) y /usr (usuarios) incluyendo el área de swap. Por ejemplo un sistema Standalone y un Servidor pueden montar estos sistemas de archivos en su disco local, mientras que los clientes de Diskless y Dataless tienen que instalar estos sistemas de archivos remotamente, de un servidor que les provea dichos servicios. La siguiente tabla muestra las diferencias entre cada tipo de sistema.

Tabla de tipos de sistemas UNIX

Tipo de Sistema	Sistemas de Archivo locales	Swap local	Sistemas de Archivos Remotos	Uso de Red	Performance Relativo
Servidor	root (/) /usr /opt /export/home /export/swap	Si	-ninguna-	media	Alta
Standalone	root (/) /usr /export/home	Si	-ninguna-	baja	Alta
Cliente Dataless	root (/)	Si	/usr /home	media	media
Cliente Diskless	-ninguna-	No	root(/) swap /usr/ /home	alta	baja
AutoClient	Cache root (/) Cache /usr	Si	/var /home	baja	alta

3.5.1. Sistema servidor. Un servidor cuenta con los siguientes sistemas de archivos:

- Sistemas de archivos de root (/) y /usr, más espacio de swap.

- Sistemas de archivos de /export, /export/swap y /export/home, para dar soporte y proveer directorios de home para los usuarios.
- El sistema de archivo de /opt para almacenar las aplicaciones de software.
- Los servidores también pueden contener software para dar soporte a otros sistemas.
- Imágenes de CD (S.O. Solaris) y de software para inicializar o instalar a través de la red.

3.5.2. Sistema standalone. Este sistema puede trabajar por sí sólo, por que es dueño de su propio disco duro que contiene los sistemas de archivos root (/), /usr, /home y espacio de swap. Así el Sistema Standalone tiene acceso local al software, espacio de memoria virtual y crear archivos para los usuarios. Un Sistema Standalone en red puede compartir información con otros sistemas dentro de la misma, sin que este se vea afectado por un aislamiento de la red en caso de que esta falle, ya que tiene la capacidad de seguir trabajando por sí solo.

3.5.3. Clientes diskless. Un cliente diskless no tiene disco duro y depende de un servidor para que le proporcione todo el software y espacio de disco. Un cliente diskless monta remotamente las particiones de sus sistemas de archivos de root (/), /usr, y /home de un servidor que le proporcione el servicio. Un cliente diskless genera tráfico sobre la red ya que continuamente realiza peticiones de software y espacio de memoria virtual a través de la red.

3.5.4. Clientes dataless. Un cliente Dataless tiene almacenamiento local como los sistemas de archivos de root (/) y espacio de swap. Los clientes Dataless no pueden funcionar si son desconectados de la red, por que sus ejecutables (/usr) y sus archivos están localizados a través de la red en un servidor de disco.

3.5.5. Sistemas autoclient. Un sistema Autoclient es casi idéntico a los clientes Diskless en términos de administración e instalación. Sus características son:

- Requiere 100 Megabytes de disco local de cache y swap para los sistemas de archivos de root (/) y /usr del servidor.
- Cuenta de un servidor para acceder a otros sistemas de archivos y aplicaciones de software.
- No contiene datos permanentes.

3.6. Guía para seleccionar tipos de sistemas.

Para seleccionar que tipo de sistema es más conveniente para las necesidades del Centro hay que realizar comparaciones de cada tipo de donde se toman en cuenta las siguientes características:

3.6.1. Administración centralizada.

- ¿Puede el sistema ser reemplazado por otro? Esto significa que si el sistema llega a fallar puede ser rápidamente reemplazado por otro sin que se realice alguna operación de respaldo o recuperación sin tener una pérdida de datos.
- ¿El sistema necesita ser respaldado? Grandes costos en términos de tiempo y recursos pueden ser asociados con largos respaldos de información sobre sistemas centrales.
- ¿Puede el sistema de datos ser modificado sobre el servidor central?
- ¿Puede el sistema ser instalado sobre el servidor central, rápido y fácilmente?

3.6.2. El Performance (Calidad de Operación).

- ¿Esta configuración se ejecuta mejor en servidores?.
- ¿La adición de sistemas afecta el performance de otros sistemas instalados sobre la red?.

3.6.3. El Uso de disco. Cuánto espacio de disco es requerido para tener una configuración óptima.

La siguiente tabla describe en términos de puntuación la mejor descripción para cada sistema, en escalas del número 1 que indica que es el más eficiente hasta el número 4 que es el menos eficiente.

Tabla de comparación de tipos de sistemas.

Standalone	4	1	4
Diskless	1	4	1
Dataless	3	3	2
Autoclient	1	2	2

3.7. Sistema de archivos en el Sistema Operativo Unix.

Un sistema de archivos es una estructura arbórea de directorios usados para organizar y almacenar archivos. El término "Sistemas de Archivos" o "File System" es usado en distintos casos:

- Para describir un tipo particular de un sistema de archivos: basado en disco, en red o virtual.

- Para describir un árbol de archivos en orden descendente sobre el directorio de root.
- Para describir una porción del sistema de archivos que fue instalada en un punto del árbol de archivos principal, de manera que esta porción sea accesible.

3.7.1. Tipos de sistemas de archivos.

El Sistema Operativo Solaris soporta tres tipos de sistemas de archivos:

- Basado en discos. "Disk Based"
- Basado en Red. "Network Based"
- Virtual.

3.7.2. Sistemas de archivos basados en discos. Los sistemas de archivos basados en discos son almacenados sobre medios físicos como discos duros, CD-ROM's y disquetes. Los sistemas de archivos basados en discos pueden ser escritos en diferentes formatos. Los formatos disponibles son:

- **UFS.** Unix File System. Es el sistema de archivo usado por default en los sistemas con software SUNOS.
- **HSFS.** High Sierra File System e ISO 9600. High Sierra es el primer sistema de archivos sobre CD-ROM's. ISO 9600 es la versión standard oficial, de sistemas de archivos High Sierra. Los sistemas de archivos HSFS son usados sobre CD-ROM y son sistemas de archivos de sólo lectura.
- **PCFS.** PC File System. Permite accesos de lectura y escritura para datos y programas escritos para computadoras personales sobre discos formateados en DOS.

Es acostumbrados asociar cada tipo de sistemas de archivos basado en disco con un particular tipo de medio.

- **UFS** con discos duros.
- **HSFS** con CD-ROM.
- **PCFS** con discos (3.5").

La asociación de estos no son restrictivas. Por ejemplo, los CD-ROM y disquetes pueden tener sistemas de archivos que tengan UFS puestos sobre ellos.

3.7.3. Sistemas de archivos basados en red. Los sistemas de archivos basados en red son sistemas de archivos accedidos sobre la red. Típicamente, residen sobre un sistema

de archivos y son accedidos por otros sistemas a través de la red. NFS (Network File System) es el único sistema de archivos basado sobre la red.

NFS es el sistema de archivos distribuido por default por Solaris. El administrador de sistemas distribuye los sistemas de archivos para exportarlos y montarlos sobre sistemas individuales.

3.7.4. Sistemas de archivos virtuales. Los sistemas de archivos virtuales son sistemas basados en memoria, que proveen acceso especial a la información del kernel. La mayoría de los sistemas de archivos virtuales no utilizan espacio de disco. Sin embargo los sistemas de archivos con cache usan el sistema de archivos sobre disco para mantener al cache y algunos sistemas de archivo virtuales, como los sistemas de archivos temporales usan espacio de swap sobre el disco.

3.8. Particiones de disco.

Sobre sistemas SPARC, Solaris define ocho particiones de disco y determina a cada una un uso convencional. Estas particiones son numeradas del la 0 a la 7. A continuación se explicará el contenido de cada partición.

Tabla de particiones de disco

Partición	Sistema de archivos	Usualmente encontrada en una estación de trabajo como cliente o como servidor	Función
0	Root	ambos	Contiene los archivos y procedimientos que activan al servidor
1	Swap	ambos	Provee memoria virtual o espacio de swap. Swap es espacio usado cuando se corren programas demasiado grandes en la computadora y estos son puestos en el área de swap
2	-----	ambos	Por convención se refiere a el disco entero. Este es definido automáticamente por el comando format de Sun y los programas de instalación de Solaris. El tamaño de la partición no puede ser cambiado.
3	/export	Solamente en el servidor	Es contenido en versiones alternativas de sistemas operativos. Estas alternativas son requeridas por los sistemas clientes, cuyas arquitecturas difieren a la del servidor. Los clientes con arquitecturas semejantes a las del servidor obtienen archivos ejecutables los sistemas de archivos /usr que se encuentra usualmente sobre la partición 6.
4	/export/swap	Solamente en el servidor	Provee a los clientes espacios de memoria virtual.
5	/opt	ambos	Contiene software de aplicación que será instalado en el sistema.
6	/usr	ambos	Contiene comandos del sistema operativo

			conocidos como archivos ejecutables diseñados para ser corridos por los usuarios. Esta partición también contiene documentación, programas del sistema y librerías del sistema.
7	/home o /export/home	ambos	Contiene todos los archivos creados por los usuarios.

3.9. Arreglos de las particiones con múltiples discos.

Aunque un sólo disco sea lo suficientemente grande para contener todas las particiones y sus correspondientes sistemas de archivos, dos o más discos son comúnmente usados para contener las particiones y sistemas de archivos.

Un simple disco puede contener los sistemas de archivos de root (/), área de swap y /usr, mientras que otro disco separado puede contener los sistemas de archivos de /export/home el cual contendrá los datos de los usuarios, este tipo de ejemplo es comúnmente utilizado por los administradores de sistemas ya que si existe alguna falla en algún otro disco que no sea el del sistema, este puede ser reparado sin que el equipo sea dado de baja para un mantenimiento.

En múltiples arreglos de discos, el disco que contiene el software del sistema operativo y el área de swap (que es el disco que contiene los sistemas de archivos de root (/) y /usr) es llamado disco del sistema, y los otros discos son llamados discos secundarios.

3.10. Determinando que partición usar.

Cuando se seleccionan los sistemas de archivos, no sólo se selecciona el tamaño de cada partición, sino también qué particiones usar. Las decisiones de qué particiones se deben de usar dependen de la configuración del sistema y el software que se desea instalar sobre el disco.

Cada configuración del sistema requiere del uso de distintas particiones, que son descritas a continuación:

Partición	Servidor	Cientes Diskless	Sistemas Standalone	Cientes Dataless	Sistemas AutoClient.
0	Root	sobre el servidor	root	root	root
1	Swap	sobre el servidor	swap	swap	swap
2	-----	-----	-----	-----	-----
3	/export	-----	-----	-----	-----
4	/export/swap	-----	-----	-----	-----
5	/opt	sobre el servidor	/opt	/opt	Sobre el servidor
6	/usr	sobre el servidor	/usr	Sobre el servidor	Sobre el servidor
7	/export/home	sobre el servidor	/home	Sobre el servidor	Sobre el servidor

3.11. Proceso de migración.

El propósito de este subcapítulo es obtener una apreciación global de las diferencias entre los sistemas operativos SunOS versión 4.x y SunOS versión 5.5, para hacer su transición de una forma más eficiente y las ventajas que se ofrecen con la migración hacia la versión SunOS versión 5.5. En este tema sólo presentamos algunos puntos, los más importantes, ya que el sistema operativo Solaris refuerza el ambiente de trabajo sobre su sistema agregando herramientas con capacidades más gráficas.

El UNIX estándar, SVR4, abarca las principales variantes de UNIX (System V, BSD, SunOS y Xenix), uniendo la mayoría de la base instalada de usuarios de sistemas UNIX. El ambiente de operación de Solaris, basado en SVR4, da a los diseñadores de software, administradores de sistema, y a los usuarios finales los beneficios de un sistema operativo normal incluyendo una amplia compatibilidad, un buen crecimiento y un tiempo reducido de comercialización. También proporciona un poder y funcionalidad en el producto reflejado por años de refinamiento. Entre las muchas ventajas que el ambiente del sistema operativo provee encontramos la portabilidad, interoperabilidad, escalabilidad y compatibilidad.

Aunque el ambiente del sistema operativo Solaris se basa en el estándar SVR4, SunSoft ha agregado funcionalidad extensiva en áreas como el multiprocesamiento simétrico, con multitareas, multiusuario, funcionalidad en tiempo real, incremento en la seguridad y mejoras en la administración del sistema.

3.11.1. Ventajas de migrar al ambiente del S.O. Solaris.

- Solaris versión 5.5 es un sistema operativo de 32 bits basado sobre el estándar System V versión IV (SVR4).
- Práctica funcionalidad para correr sobre procesadores SPARC, Intel 386, 486, Pentium y otras arquitecturas compatibles con DOS.
- Los estándares de la industria incluyen SVR4 (System V Release 4) como un familia de protocolos para las redes.
- Interfaces Gráficas para el usuario. (Graphical User Interface GUI) en el manejador de ventanas OPEN LOOK.
- Herramientas de escritorio de uso personal y herramientas para grupos de trabajo incluyendo correo electrónico con multimedia, manejador de archivos, herramientas de impresión, imágenes y otras.
- File Manager que provee un gráfico e intuitivo camino para navegar dentro de los sistemas de archivos locales y remotos.
- Image Tool es una herramienta para despliegue de imágenes de hasta 40 formatos distintos.
- OPEN LOOK Admintool es la base para la administración local.
- Arquitectura avanzada que incluye un completo multiprocesamiento y una sofisticada multilectura.
- Network Information Services Plus (NIS+).

Con NIS+ se pueden manejar cuentas de usuarios de forma centralizada, de manera que la información de las cuentas importantes de usuarios, como nombres de usuarios, no tengan que ser duplicadas sobre cada sistema en la red.

NIS+ como su nombre lo indica es un servicio de información de red, el cual almacena información que los usuarios, estaciones de trabajo y aplicaciones deben tener para comunicarse a través de la red. Si no cuenta con un servicio de información de la red, cada workstation debe contar con su propia información para poder mantener comunicación con la red.

- Multimedia mail. Correo electrónico con multimedia, simplifica el envío de mensajes incorporando audio, gráficas, incluyendo archivos.
- Audio Tool. Graba y reproduce sonidos de mensajes hablados, ellos pueden ser conectados a un correo electrónico.

3.11.2. Portabilidad, Escalabilidad, Interoperabilidad y Compatibilidad.

- **Portabilidad.** Es portable ya que múltiples vendedores soportan esta plataforma. Mientras es realizada una aplicación o un nuevo software, todos los vendedores de sistemas trabajan sobre una misma arquitectura de microprocesador. Esto implica que los desarrolladores de software tengan un costo reducido en el desarrollo de nuevas aplicaciones y brinden sus productos hacia el mercado a bajo costo rápidamente, y den oportunidad a los usuarios a actualizar su hardware mientras retienen sus aplicaciones de software y minimizan los costos de conversión.
- **Escalabilidad.** Conforme avanza el tiempo las aplicaciones llegan a ser más extensamente usadas y requieren del apoyo de sistemas más poderosos. Al operar en un ambiente de trabajo creciente, se debe de correr software con un amplio poder además de tomar las ventajas adicionales del poder de procesamiento. Los sistemas operativos SunSoft's corren sobre máquinas de todos los tamaños, desde Laptop's hasta Supercomputadoras.
- **Interoperabilidad.** Los ambientes de cómputo heterogéneos son una realidad ahora. Los usuarios compran sistemas de muchos vendedores para implementar las necesidades que ellos necesitan. La estandarización y las interfaces claras son críticas para ambientes heterogéneos, ya que dejan que los usuarios desarrollen sus estrategias de comunicación a través de su red. Los sistemas Solaris pueden interoperar con cada sistema popular sobre el mercado de hoy y las aplicaciones que corren sobre UNIX pueden comunicarse fácilmente.
- **Compatibilidad.** La tecnología de cómputo continúa avanzando rápidamente, pero las necesidades para tener equipo, requiere que los vendedores minimicen sus costos y maximicen sus inversiones. SunSoft asegura que la introducción de nueva tecnología y la inversión en un software existente es preservada. Los usuarios pueden tomar las

ventajas de las soluciones de ahora y poder tener compatibilidad con la tecnología del mañana.

3.11.3. Mejoras para los administradores de sistemas.

Para los administradores de Sistemas, Solaris ofrece una variedad de nuevas utilerías para simplificar las tareas de administración, estas incluyen:

- **Información de Dispositivos.** Los administradores pueden usar las utilerías opcionales para obtener información acerca de los dispositivos instalados incluyendo nombres de dispositivos, atributos, y accesibilidad.
- **Administración de Sistemas de Archivos.** Estas utilidades habilitan a los administradores para crear, copiar, montar, depurar, reparar y desmontar sistemas de archivos.
- **Información del Sistema.** Estas utilerías reportan la memoria y configuración del sistema. El administrador del sistema puede usar estas utilerías para cambiar los nombres de los sistemas y el nodo de la red.
- **Manejador de Procesos.** Esta utilería controla las tareas del sistema. Usando esta utilería el administrador puede generar reportes sobre el performance, los usuarios, accesos a disco, etc. En adición el administrador puede cambiar de nivel de sistema, matar procesos activos etc.
- **Manejador de Usuarios y Grupos.** Con estas utilerías el administrador de sistemas puede crear y borrar entradas a bases de datos asignando un password, especificado por default.
- **Contabilidad del Sistema.** Las utilerías de contabilidad ayudan a los administradores a monitorear el uso del sistema, procesador, usuarios, paquetes recibidos, errores etc.
- **Admintool.** El Admintool puede correrse bajo el ambiente OpenWindows y provee facilidades para el manejo del sistema, es de gran ayuda para agregar hosts, manejo de la red y muchas otras tareas cotidianas en el sistema local.

Para ver los comandos que mejoran la administración véase el apéndice B o revise el manual de usuario "System Administration Guide, Volume I y II by Sun Microsystems Inc."

3.11.4. Cambios en la instalación y configuración.

La instalación de la versión de Solaris 2.5 introduce un número de cambios en la manera en que los administradores instalan el software sobre sistemas existentes y en la adición de sistemas sobre la red.

- La versión de S.O 5.5 es solamente distribuida en disco compacto CD-ROM. Esto significa que se debe tener acceso a una unidad de CD-ROM antes de instalar el software. Sin embargo se puede seleccionar el modo de instalación a través de la red, si es que no se cuenta con una unidad de CD-ROM.
- La versión de S.O 5.5 es instalada dentro de módulos llamados paquetes. Se puede seleccionar los paquetes relevantes para el sistema y controlar la cantidad de espacio que requiere cada instalación o especificar las aplicaciones que deben de ser disponibles sobre los sistemas individuales.
- La versión de S.O 5.5 también contiene grupos de software fijos, que son grupos de paquetes de software y clusters para usuarios típicos. Se puede seleccionar un grupo de software para hacer funcionar los sistemas, sin seleccionar paquetes y clusters individuales. Esto puede ser útil cuando se instala por primera vez el sistema operativo para pruebas en ambientes limitados. Se puede agregar o remover paquetes más adelante cuando se tenga más experiencia con los sistemas.

La migración del sistema operativo SunOS versión 4.x a Solaris 2.5 consiste en un proceso de tres fases que incluyen:

- Pre-instalación. (Planear y respaldar los datos).
- Instalación. (Instalar Solaris).
- Post-instalación (Restauración de Datos).

Los tres pasos del proceso de migración son los mismos, sólo hay diferencias en las tareas que se realizan de un tipo de sistema a otro cuando se instala el software, y estas diferencias son discutidas en el apéndice B al final de la tesis.

3.11.5. Rasgos generales de la instalación del S.O. Solaris.

Lo que se necesita hacer antes de instalar el software de Solaris.

- Salvar la configuración de la información, conociendo las particiones de los discos y los sistemas de archivos.
- Salvar la información de los sistemas de archivos y los nombres de los dispositivos.
- Decidir qué sistemas de archivos salvar, incluyendo aplicaciones, productos, software instalado y archivos de administración que SunOS 4.x necesita para recrear sus variables y reconocer después estos archivos y aplicaciones.
- Realizar respaldos.
- Instalar el software de Solaris

La instalación de SunOS 5.5 es realizada usando las instrucciones de instalación, descritas paso a paso en el apéndice A.

- ¿Qué hacer después de la instalación del software de Solaris?.

- Si el sistema es un servidor, seleccionar el tipo de servicio que será instalado, el tipo de servicio que este proporcionará.
- Restaurar los datos de los usuarios de la versión SunOS 4.x.
- Instalar las nuevas aplicaciones.

3.12. Impresoras sobre red.

El punto principal de instalar impresoras sobre red, es dar a los usuarios acceso a una o más impresoras que son utilizadas por otros usuarios. En esta sección describiremos la distribución de las impresoras a través de la red para lograr la mejor eficiencia tanto de los servidores como de los clientes de impresión.

El software para clientes de impresión SunSoft ofrece la mejor solución para manejo y selección de impresoras sobre la red. El software SunSoft soporta servicios de nombres, que habilita la administración centralizada de la red.

3.12.1. Distribución de impresoras sobre red.

Un administrador debe decidir como conectar las impresoras y determinar si cada impresora podría ser mejor utilizada si está dedicada en un sistema o disponible para muchos sistemas y usuarios. En ambientes de red, se trabaja usualmente mejor con impresoras distribuidas sobre varios servidores de impresión. La ventaja de seleccionar varios servidores de impresión, es que cuando un servidor de impresión tiene problemas, se pueden redirigir los trabajos de impresión hacia otra impresora.

Si se usa una configuración de impresión centralizada, se puede controlar las impresoras conectadas para los usuarios, por conveniencia de mejorar la respuesta de trabajo hacia ellos. Una impresora que es conectada a un usuario de sistema esta disponible para otros usuarios sobre la red.

En la figura 3.1. muestra como se puede tener una configuración de impresión centralizada y tener conectada una impresora de un usuario del sistema.

Como Distribuir Impresoras sobre la Red

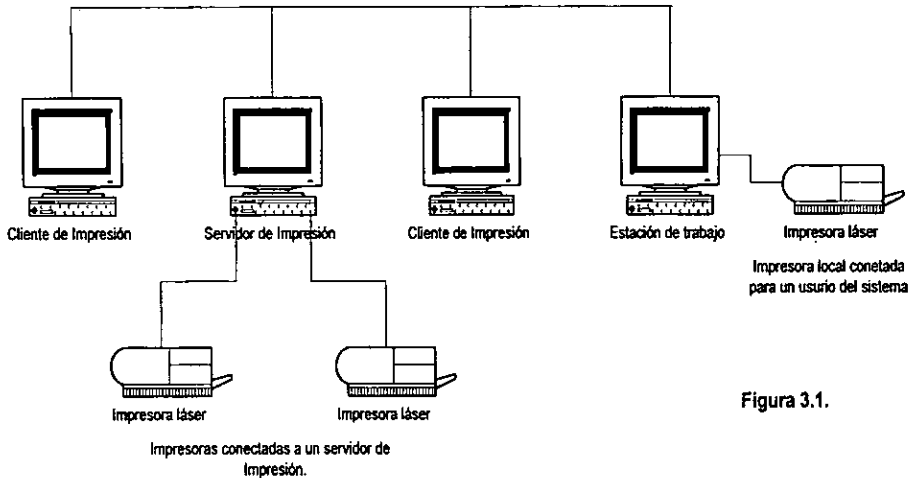


Figura 3.1.

3.12.2. Asignando servidores y clientes de impresión.

El administrador debe decidir cual servidor debe tener las impresoras físicamente conectadas y cuales sistemas podrían usar las impresoras sobre otros equipos. Un servidor que tiene conectada una impresora local y ésta es compartida con otros sistemas sobre la red es llamado *servidor de impresión*. Un servidor que envía sus trabajos de impresión hacia un servidor de impresión es llamado *cliente de impresión*.

Los servidores y clientes de impresión pueden correr distintas versiones de sistemas operativos. Sistemas que corren con sistemas operativos Solaris 5.X pueden imprimir hacia servidores con el sistema operativo SunOS 4.X, y los servidores que tengan el sistema operativo SunOS 4.x pueden imprimir hacia servidores que estén con sistema operativo Solaris 5.x. véase figura 3.2.

Ejemplo de Configuraciones de Impresión Sobre SunOs 4.X y Solaris 5.X

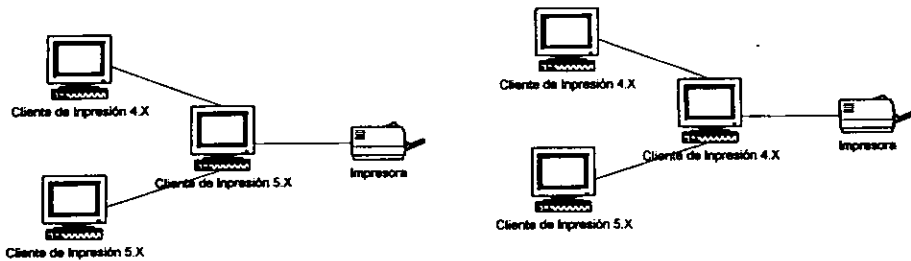


Figura. 3.2.

3.13. TCP/IP, Protocolo de Control de Transmisión/Protocolo de Internet, (Transmission Control Protocol/Internet Protocol).

La agencia de gobierno DARPA (Defense Advanced Research Projects Agency) comenzó sus investigaciones a mediados de 1970 y ya para 1978 se tenían definidos los principales protocolos y la arquitectura, los cuales se emplearon en una red experimental llamada Arpanet. El conjunto de protocolos definidos se le llamo TCP/IP en honor a los dos principales protocolos de esta tecnología.

Para 1980 Arpanet fue el backbone sobre el cual se unieron más redes y a la nueva red resultante se le llamó Internet.

Una de las estrategias utilizadas para difundir esta tecnología fue poner a disposición de las universidades una implementación a bajo costo, además de que se realizó una implementación de TCP/IP para su uso con el sistema operativo Unix desarrollado en la Universidad de Berkeley. Esto integró a Internet a muchas universidades y centros de desarrollo de los E.U.A.

TCP/IP es el nombre de un protocolo de conexión de redes. Un protocolo es un conjunto de reglas a las que se tienen que atener todas las compañías y productos de software con el fin de que todos sus productos sean compatibles entre ellos. Estas reglas aseguran que una máquina que ejecuta la versión TCP/IP de Digital Equipment pueda hablar con un PC Compaq que ejecuta TCP/IP. Los sistemas abiertos hacen referencia al hardware y al software no específico: aquellos en que los detalles de la operación se publican y están disponibles para todo el mundo. TCP/IP es un protocolo abierto, lo que significa que se publican todos los aspectos concretos del protocolo y cualquiera los puede implementar.

TCP/IP son las siglas de *Transmission Control Protocol/Internet Protocol*, Protocolo de Control de Transmisión/Protocolo de Internet, que son dos protocolos diferentes. TCP/IP no es un producto único, como piensa mucha gente, sino que TCP/IP hace referencia a una familia completa de protocolos relacionados entre sí, diseñados todos ellos para transferir información a través de una red y para proporcionar información de estado sobre la misma red. TCP/IP está diseñado para ser un componente de una red, principalmente la parte del software. Todas las partes de la familia del protocolo TCP/IP tienen unas tareas asignadas como enviar correo electrónico, proporcionar un servicio de acceso remoto, transferir archivos, asignar rutas a los mensajes, o gestionar caídas de la red. TCP/IP no está limitado a Internet. Se trata del protocolo de software de conexión de redes más ampliamente utilizado en el mundo.

3.13.1. Características de TCP/IP.

Desde el punto de vista de un usuario la Internet es una serie de programas de aplicación que utilizan la red para comunicarse. Las principales aplicaciones dentro de Internet son:

- Correo electrónico
- Transferencia de archivos
- Conexión a un sistema remoto

Desde el punto de vista de un programador de aplicaciones, la Internet provee dos tipos de servicio sobre los cuales trabajan las aplicaciones:

- **Connectionless Packet Delivery Service.**
Connectionless Delivery es una forma de envío de datos a través de la red, en la cual TCP/IP rutea el mensaje de una máquina a otra con base en la información de direccionamiento incluida en el mensaje. Al enviar este servicio, cada parte del mensaje de manera independiente, no garantiza que llegue en un orden adecuado. Trabaja de una forma más estrecha con el hardware, lo que lo hace muy eficiente.
- **Reliable Stream Service.**
A pesar de la eficiencia del servicio anterior, muchas aplicaciones requieren más que un servicio de entrega de mensajes. Necesitan tener una conexión confiable con métodos de recuperación de errores, capacidad de retransmisión, etc. Este tipo de servicio cubre con estas necesidades.

Permite que una aplicación establezca “una conexión” con la aplicación en el otro equipo, y enviar un gran volumen de datos a través de ella; como si fuera un enlace dedicado entre ambas.

Estas características son comunes a distintas redes y protocolos, sin embargo las características que distinguen a TCP/IP son:

- Independencia de la tecnología de red sobre la que trabaje.

- Interconexión universal, a cada computadora se le asigna una dirección única y que la identifica a través de toda la red.
- End-to-end acknowledgments, los protocolos de comunicación proveen un sistema de acknowledgments (acuse de recibo) entre la máquina origen y la destino, en lugar de que esto ocurra entre las diferentes máquinas a las que pueda llegar el paquete de información durante su viaje.
- Protocolos estándar para las aplicaciones de usuario como lo son la transferencia de archivos y el correo electrónico.

3.13.2. Niveles TCP/IP.

Aplicación	Principales aplicaciones: Telnet, FTP, NFS, SMTD
Transporte	Principales protocolos: TCP, UDP
Internetwork	Principales protocolos: IP, ICMP
Subnetwork	Esta definida con ciertos protocolos para tipos de red como X.25, Ethernet, FDDI, etc.

Subnetwork: capa que no se encuentra definida por TCP/IP, simplemente hace referencia a los protocolos de comunicación específicos empleados en cada tecnología de red en particular.

Internetwork: provee las funciones necesarias para conectar redes y gateways en un sistema coherente. Esta capa es responsable de la entrega de datos de su origen hasta su destino final. Los principales protocolos en esta capa son IP e ICMP junto con otros protocolos que los apoyan para realizar las labores de ruteo y mapeo de direcciones físicas.

Capa de transporte: se encarga de la comunicación end-to-end es decir, sólo de la comunicación entre la máquina origen y la destinataria de la información, no importando por que máquinas pase dentro de su viaje por la red. Los principales protocolos son TCP que además ofrece mecanismos que garantizan la entrega de datos, y el protocolo UDP.

Capa de aplicación: en esta capa se encuentran todos los protocolos que definen las diferentes aplicaciones dentro de la red, como el correo electrónico, la transferencia de archivos, etc.

3.13.3. Direccionamiento.

Una de las características especiales de TCP/IP es la interconexión universal, es decir, la capacidad que tiene un nodo de la red de llegar o comunicarse con otro cualquiera no importando la distancia que los separe. Esto se logra al definir una forma de direccionar la información hacia ese nodo en particular a través de la asignación de un identificador único de cada uno de los elementos que conforman la red.

3.13.3.1. Direccionamiento Físico.

Es importante hacer una distinción entre el direccionamiento físico y el utilizado por TCP/IP. Una dirección física es aquella asignada al dispositivo físico de red, por ejemplo, en una red Ethernet, tenemos a la dirección MAC. Esta dirección identifica de manera única a la interfaz de red conectada al equipo y es a través de ella que los protocolos de las capas hacen llegar la información de un equipo a otro. Sin embargo, cuando hablamos de la interconexión de redes de distinta naturaleza, el formato de esta dirección física cambia. Por lo que no podemos hacer un direccionamiento directo entre dos equipos conectados a esas redes. Aquí es donde entra TCP/IP, quien hace transparente para el usuario esas diferencias al definir una dirección lógica a cada una de las máquinas.

3.13.3.2. Direccionamiento Internet.

La red Internet la podemos definir como una red virtual, es decir, a la vista del usuario es una red única, a pesar de estar constituida por una multitud de diferentes redes.

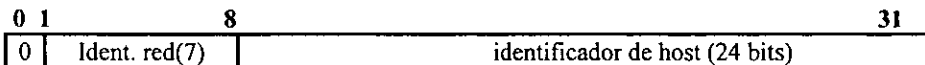
Con el objeto de identificar de manera única a cada uno de los hosts o máquinas dentro de esta gran red virtual se definió un identificador universal llamado dirección Internet.

La dirección Internet está formada por 32 bits agrupados en 4 grupos de 8 bits cada uno. De manera conceptual una dirección está formada por una parte que identifica la red y por otra que identifica el host. El organismo llamado NIC (Network Information Center) es el encargado de hacer las asignaciones de estas direcciones. Se realiza una asignación inicial de una dirección de red a partir de la cual la organización a la que se le da podrá ir asignando los números de hosts correspondientes. Por conveniencia y facilidad utilizamos una notación decimal, por lo que las direcciones quedarían de la siguiente forma:

132.248.10.190

Las direcciones IP se clasifican en cuatro formatos de acuerdo al tipo de red que sean asignadas, para identificar cada tipo de dirección nos basamos en los bits más significantes.

Clase A: las direcciones clase A utilizan los 8 primeros bits para identificar la red y los 24 bits restantes para identificar a cada host dentro de ella. Dentro de estos 8 bits el más significativo de ellos siempre es cero, lo cual nos deja 7 bits para identificar a la red, como podemos observar en esta figura:



el rango de números permisible para estas direcciones es de la 0 a la 127 (las direcciones 0 y 127 están reservadas para un uso especial, por lo que en total tenemos 126 direcciones de

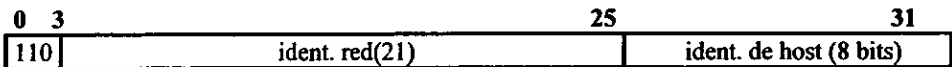
red pertenecientes a la clase A. Una dirección IP perteneciente a esta clase es: 119.200.30.100

Clase B: las direcciones clase B utilizan los 16 primeros bits para identificar la red y los 16 bits restantes para identificar a cada host dentro de ella. Dentro de estos 16 bits los dos más significantes son 0 y 1, lo cual nos deja 14 bits para identificar a la red, como podemos observar en esta figura:



Una dirección de esta clase es 132.248.27.10

Clase C: utiliza los primeros 24 bits para identificar la red y 8 para identificar el host y tenemos el siguiente formato:



Una dirección perteneciente a esta clase es 190.248.63.5

Clase D: utiliza el siguiente formato y esta reservada para un uso especial llamado multicasting.



De acuerdo a esto tenemos que de acuerdo al valor del primer número de la dirección IP podemos identificar a que clase pertenece.

0 - 127	Clase A
128 - 191	Clase B
192 - 223	Clase C
224 - 254	Clase D

El máximo número de redes y hosts que se pueden definir dentro de cada clase es el siguiente:

	REDES	HOSTS
Clase A	126	16,777,124
Clase B	16,384	65,534
Clase C	2,097,152	254

Direcciones especiales:

132.248.0.0	dirección que identifica a una red
127.0.0.1	dirección de loopback
255.255.255.255	dirección de broadcast
132.248.255.255	broadcast a los hosts de la red 132.248.0.0

3.13.4. Mapeo de direcciones.

¿Por qué el mapeo de direcciones? Para que dos máquinas dentro de una misma red puedan comunicarse deben conocer la **dirección física** de la otra máquina. Las direcciones IP nos sirven para identificar una máquina dentro de esta gran red pero cuando la información es enviada a través de la red física debemos conocer dirección física de la máquina destino para que esta puede llegar. Como se ve es necesario implementar un método que permita que a partir de una dirección IP pueda identificar la dirección física asignada a un host.

3.13.5. Mapeo de direcciones Internet a direcciones Físicas.

Existen dos formas de realizar esto, una es a través de un mapeo directo, la otra es dinámica a través de la red.

En el caso de mapeo de directo la dirección física puede ser incluida dentro de la dirección IP, por ejemplo en una red token ring llamada proNET-10 las direcciones físicas asociadas a cada tarjeta son números pequeños que pueden ser incluidos en la dir. IP; por ejemplo una máquina con dirección física **10** puede tener la dirección 132.248.27.10 y nuestro método de resolución se simplifica a través de una función de conversión muy sencilla.

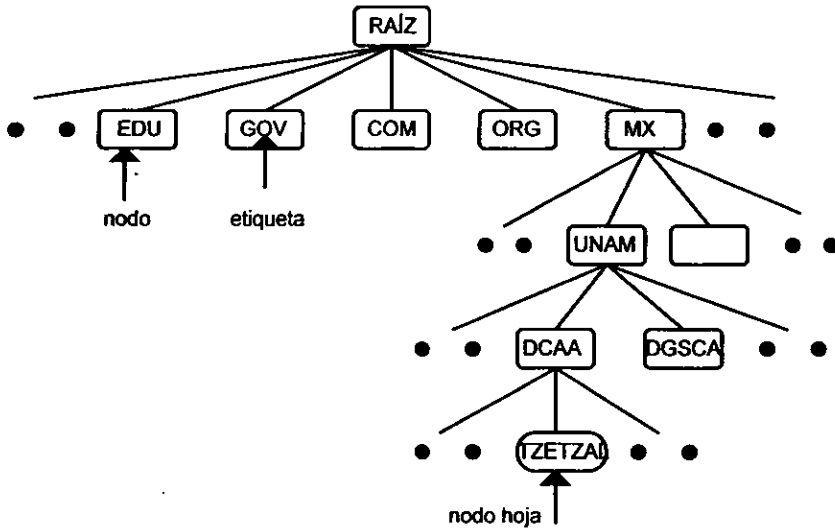
3.13.6. Servidor de Nombres de Dominio (DNS: Domain Name System).

Para un usuario es difícil recordar las direcciones IP de los hosts con los que desea trabajar, por lo que se emplea en su lugar un término con sentido y fácil de recordar. El mapeo entre dichos nombres y su dirección IP correspondiente se mantenía en un archivo llamado *hosts.txt* en una computadora del NIC¹, el cual tenía que ser accedido por todas las computadoras.

Sin embargo con el crecimiento de Internet resultó imposible mantener actualizada la información de este archivo además del gran tamaño que estaba adquiriendo. De esta forma en 1983 surge DNS (Domain Name System) que se basa en un esquema jerárquico para poder descentralizar la información. Este esquema se muestra en la figura 3.3.

¹Network Information Service

Figura 3.3. Esquema Jerárquico de DNS



DNS se encuentra organizado como una estructura de árbol, el cual consiste de nodos a los cuales se les identifica a través de etiquetas. Estas etiquetas deben ser únicas dentro de un mismo nivel del árbol. Un nodo hoja es aquel que ya no tiene subdivisiones.

Esta estructura permite que el nivel más alto delegue autoridad a cada división y que esa división se responsabilice por la asignación de nombres dentro de ella; a su vez cada una puede dividirse y delegar nuevamente responsabilidad hasta que la última división sea manejable.

El "domain name" o nombre del host consiste en una secuencia de etiquetas separadas por un punto, que se obtiene al recorrer el árbol de arriba hasta un nodo hoja; cualquier parte de esta secuencia es conocida como dominio. Por ejemplo tomemos la ruta del nodo hoja llamado tzetzal, el cual representa a un host. Su *domain name* es: tzetzal.dcaa.unam.mx

En el ejemplo anterior el nivel de dominio más bajo es dcaa.unam.mx (el dominio perteneciente a la DCAA en la UNAM), el segundo nivel es unam.mx (el dominio para la UNAM) y el último nivel es mx (el dominio asignado al país México).

La Internet ha definido los siguientes dominios en el nivel más alto, los que se muestran a continuación:

- | | |
|------------|--------------------------------------|
| com | Organizaciones comerciales |
| edu | Instituciones educativas |
| gov | Instituciones gubernamentales |

mil	Grupos militares
net	Centros de soporte a redes
org	Otro tipo de organizaciones

código	país	Asignación de acuerdo al país, por ejemplo:
jp	Japón	
uk	Reino Unido	
mx	México	

A una organización se le puede asignar su nivel de dominio alto de acuerdo a una ubicación geográfica o de acuerdo a su tipo de organización, por ejemplo, el caso de la UNAM también se le pudo asignar el dominio EDU. La Internet tiene control sobre estos dominios, por ejemplo, a la UNAM le concedió el dominio unam.mx y ya dentro de este dominio la UNAM puede realizar de manera libre todas las asignaciones que desee.

3.13.6.1. Mapeo entre nombres y direcciones IP.

Además de las convenciones anteriores para definir un nombre, DNS provee un mecanismo para el mapeo con las sig. características:

- **Eficiente**, ya que la mayoría de nombres pueden ser mapeados de manera local.
- **Propósito general**, pues no se encuentra restringido a nombres de máquinas.
- **Distribuido**, ya que se basa en múltiples servidores que cooperan para resolver el problema de mapeo.

Estos sistemas cooperativos e independientes son llamados servidores de nombres, el cual es un programa dedicado a hacer dicho mapeo. El programa cliente es llamado name resolver, el cual utiliza uno o más servidores para traducir un nombre.

3.13.6.2. Servidores de nombres.

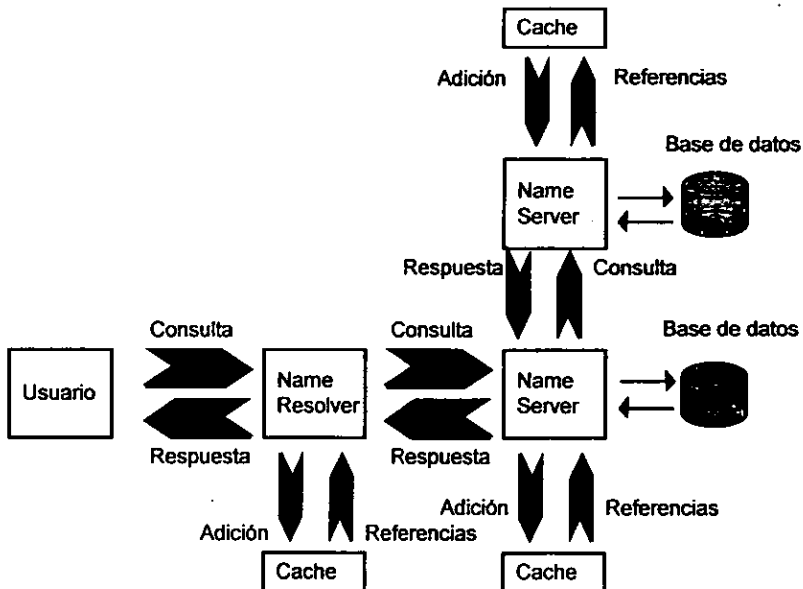
Los servidores manejan lo que se conoce como zonas. Una zona comienza en un nodo del árbol y abarca todas las ramas bajo él. El servidor puede delegar autoridad sobre una subzona o otro servidor quien controlará la información bajo su dominio. DNS consiste en zonas anidadas en las cuales los servidores de nombres operan, los servidores pueden reconocer a sus vecinos arriba de ellos y los que se encuentran abajo. Para garantizar la eficiencia cada zona tiene al menos dos servidores activos (servidor primario y secundario) que proveen la misma información, véase figura 3.4.

Un servidor puede atender una consulta con los siguientes modos de operación:

- Operación no recursiva, donde la respuesta de un servidor puede ser:
 - ◆ La respuesta esperada.
 - ◆ La identificación de un error.

- ◆ Remisión a otro servidor siendo responsabilidad del cliente volver a enviar la consulta al servidor especificado.
- Operación recursiva:
 - ◆ En este caso es el mismo servidor quien contacta a otros servidores y la respuesta obtenida es la dirección IP o una negativa.
 - ◆ La información de los objetos es manejada en registros llamados Resource Records (RR) los cuales se encuentran en una base de datos y es utilizado para definir zonas de dominio así como mapear entre nombres de dominio y objetos.

Fig. 3.4. Proceso de resolución de nombres.



3.13.7. Protocolo de Internet (IP: Internet Protocol).

El protocolo de Internet (IP) es el protocolo principal de TCP/IP. Es importante saber que aunque la palabra "Internet" aparece en el nombre del protocolo, no se limita a utilizarlo con Internet. IP define un protocolo, no una conexión.

El protocolo de Internet carece de conexión, al igual que UDP. Aquí carecer de conexión significa que IP no se preocupa de la máquina por las que pasa el mensaje. Cuando se envían datagramas en una red, IP no se preocupa ni siquiera de que máquina lo envíe o dónde debería acabar. Las direcciones IP de las máquinas que lo envían y reciben

están incluidas en la cabecera del datagrama, pero el análisis y transferencia de un datagrama no tiene nada que ver con ellos hasta que llega al destino. En su lugar, la información de ruta que le dice a IP a qué máquina tiene que enviar el datagrama en cada paso es la única información importante para la mayoría de los ruteadores.

La principal tarea del Protocolo de Internet es dirigir datagramas entre ordenadores, ya que gestiona el destino, el mejor método de ruta para llegar al destino y también asegura la recuperación en caso de problemas. IP posee su propia cabecera que se añade al principio del mensaje recibido del nivel superior (normalmente TCP o UDP).

IP también tiene otra tarea que implica dividir datagramas grandes en partes más pequeñas y luego volverlas a juntar en el destino. Los datagramas grandes se tienen que dividir por una serie de razones, incluido un límite en el tamaño de los mensajes IP (aproximadamente 65 K). Sin embargo, por lo general, una red por sí misma no puede manejar un mensaje de tal extensión, sino que necesita dividir el datagrama en partes más pequeñas de unos pocos kilobytes.

Existen una serie de términos especiales que se utilizan para describir el desglose y el volver a reunir los datagramas, estos incluyen lo siguiente:

- *Segmentación*, es el proceso de dividir un datagrama en varios datagramas más pequeños.
- *Volver a reunir*, es el proceso de combinar datagramas más pequeños en el datagrama original.
- *Concatenación*, es el proceso de combinar varios datagramas en un datagrama mayor, similar a realizar bloques excepto que los mensajes pueden proceder de aplicaciones diferentes.
- *Separación*, lo contrario de concatenación, es el proceso de separar un único datagrama en varios mensajes más pequeños procedentes de aplicaciones diferentes.

El protocolo de Internet lleva a cabo todos estos procesos sin que usted sepa lo que esta sucediendo, aunque desde luego, se tiene que realizar cierta gestión interna para asegurarse que el mensaje se vuelva unir en el orden correcto y que se reciben de forma adecuada todas las partes del mensaje más grande, lo que se consigue por la información en la cabecera IP y por un número de relojes especiales que IP utiliza para separar a todas las partes de un mensaje. Uno de los problemas que nos encontramos con la división de los mensajes, es que un mensaje fragmentado tiene una menor posibilidad de llegar que uno que no lo esté. La mayor parte de las aplicaciones de software intentan enviar la fragmentación en la medida de lo posible.

Principales Funciones del protocolo IP:

- Definir la unidad básica de transferencia utilizada a lo largo de toda la red TCP/IP.
- Realiza el ruteo de datos, al escoger el "camino" óptimo para éstos.

- Define las reglas que indican cómo los hosts y gateways deben procesar los paquetes, como y cuando deben generarse los mensajes de error y las condiciones bajo las cuales un paquete debe ser descartado.

Principales características de IP:

- *Protocolo que proporciona un servicio connectionless.*

Cada paquete es tratado de forma independiente. Si tenemos una secuencia de paquetes estos podrán viajar por distintas rutas. Podemos hablar de que no existe una "conexión" o ruta dedica para su transporte.

- *Fragmenta (divide) los paquetes si es necesario.*

Implica dividir datagramas grandes en partes más pequeñas y luego volverlas a juntar en el destino.

- *Direccionamiento a través de una dirección de 32 bits.*

La dirección Internet está formada por 32 bits agrupados en 4 grupos de 8 bits cada uno. De manera conceptual una dirección está formada por una parte que identifica la red y por otra que identifica el host.

- *Tamaño máximo del paquete de 65535 bytes.*

- *Sólo hace el proceso de checksum sobre el encabezado y no sobre los datos.*

- *Best-effort delivery.*

Significa que la red hace su mejor esfuerzo por entregar los paquetes, no es un capricho el descartarlos. Esta situación se presenta cuando todos los recursos están agotados y la red falla.

- *Tiempo de vida finito de los paquetes.*

3.13.8. Protocolo de Control de Transmisión (TCP) y Protocolo de datagramas de usuario (UDP).

La diferencia entre TCP y UDP es la forma en que se manejan las conexiones entre dos máquinas. TCP establece una conexión de tal manera que las dos máquinas están unidas, cada una de ellas esta conciente de la existencia de la otra máquina en el otro extremo. UDP no intenta establecer una conexión, sino que simplemente recoge el mensaje, añade la dirección IP de la máquina de destino y envía el paquete por la red.

Evidentemente TCP es un método de comunicación más fiable, ya que los dos extremos de la conexión pueden dejar que cada uno de ellos sepa lo que esta sucediendo e informa de cada mensaje que se envía. Con UDP, no existe ninguna garantía de que se reciba el mensaje. Como prueba de recepción, UDP hace que la máquina de destino envíe de vuelta un mensaje acusando recibo del mensaje. Si la máquina que envía no recibe dicho

mensaje dentro de un período de tiempo especificado, asume que el mensaje se ha perdido y se envíe de nuevo.

Quizá piense que a todo mundo le gusta utilizar TCP para transferir mensajes, pero de hecho la mayor parte de Internet se basa en UDP. Piense en todas las máquinas en la red e imagine cuántas conexiones se tendrían que establecer, utilizar y luego desconectar cada segundo. Los números son inmensos y poco prácticos. El hecho de utilizar UDP simplifica enormemente el tráfico en la red.

Cada servicio TCP/IP se diseña para que utilice UDP o TCP. Por ejemplo, Telnet (para acceso remoto) y FTP (para transferir archivos) utilizan TCP, ya que debe existir una conexión entre los dos extremos. Otro método de transferencia de archivos es un protocolo denominado *Trivial File Transfer Protocol* (TFTP), Protocolo Simple de Transferencia de Archivos que utiliza UDP.

Tanto TCP como UDP funcionan al añadir una cabecera al principio del mensaje que recibe el nivel de transporte desde niveles superiores. La organización sobre la cabecera TCP es diferente a la de UDP, pero ambas contienen aproximadamente la misma información básica sobre quién envió el paquete, a quien se dirige y aspectos concretos sobre el mensaje en sí.

3.14. Fundamentos del administrador.

Antes de proponer una solución para el mejoramiento de un Centro de Cómputo un Administrador debe tener en cuenta los siguientes conceptos fundamentales.

Accesibilidad: Cada nodo de la red puede hacer uso de los recursos que esta proporciona en cualquier momento. Solamente durante algunas excepciones de emergencia o tareas especiales de mantenimiento la accesibilidad a la red deberá ser restringida.

Confiabilidad: Esto se refiere a que cada vez que, el usuario desee hacer uso de los recursos en la red, esta este estable y que no presente ninguna falla, así como los datos e información contenidos sean íntegros y se puedan manejar en cualquier momento sin que tenga que tener algún contratiempo.

Costo: El costo es la mayor consideración en el diseño de redes, ya que estas son muchas veces restringidas en su diseño por limitaciones económicas.

Crecimiento: Se debe planear el impacto futuro que tendrá una red al ir incrementando más dispositivos, o si el presupuesto para mi departamento creció en un porcentaje muy amplio, cuáles serían los dispositivos que necesitaría de manera inmediata para reforzar su funcionamiento, así como si la tecnología que estoy comprando ahora podrá servir para la integración de nuevos dispositivos futuros.

Interoperabilidad: Cada vendedor de equipo y software debería trabajar en conjunto con otros vendedores. Si los componentes de una red no son compatibles, se podría tener un gasto extra y un tiempo extra en la instalación y adaptación de dispositivos que no son compatibles con el equipo que mi red cuenta, considerando que muchas de las veces estos no son compatibles en un 100% con mi equipo y son instalados en él de manera no óptima, dando como resultado un porcentaje muy bajo de confiabilidad y rendimiento en su funcionamiento.

Seguridad: En este punto se preguntaría que tanto grado de seguridad requiere mi red, en muchos diseños este punto es tocado muy ligeramente y no se da la importancia que esta debiera tener por mínima que sea. Para esta existen muchas herramientas de seguridad que son de gran ayuda y que pueden trabajar en distintos entornos de red.

Segmentación: Una red puede crecer rápidamente llegando a puntos en donde el tráfico interno tiene que ser segmentado con puentes, routers o switches, para mantener un ancho de banda aceptable que me permita trabajar adecuadamente en mi red. La elección entre usar un puente, switch o router dependerá del tráfico de información que tenga propiamente mi red.

Fácil mantenimiento: Se debe de tener en cuenta la compra de dispositivos en red, que puedan ayudar a las tareas de mantenimiento. Unidades de cintas, cartuchos de cinta, unidades de almacenamiento secundario, discos removibles, etc.

Políticas: Plantear y hacer cumplir las políticas de "uso aceptable". Se deben de realizar las políticas en común acuerdo por parte del administrador del Centro de Cómputo y con el jefe inmediato del administrador, para así evitar problemas de mal entendimiento.

Disponibilidad de monitorear la red: Eventualmente es necesario monitorear la red para identificar los problemas que esta pueda tener. Si se toma en cuenta en el diseño el monitoreo de red, este puede ayudar a resolver algunos problemas que surgen dentro de dicha red.

Muchos de los puntos mencionados anteriormente parecen estar en proporciones desiguales uno con el otro. Por ejemplo es difícil tener archivos de fácil acceso si se quiere tener una buena seguridad o tener una super seguridad solamente para guardar un archivo sacrificando para esta la accesibilidad. Sin embargo algunos puntos tienen una relación estrechamente ligada. Pero si se toman en cuenta estos puntos en el diseño será más fácil tener un buen mantenimiento tanto del hardware y software de que se componga mi red.

3.14.1. Actividades del administrador del sistema.

El administrador del sistema debe controlar los recursos de todos los equipos conectados a la red de acuerdo con las políticas de uso de su Centro de Cómputo. Es el responsable de mantener la integridad del sistema y de garantizar un funcionamiento eficiente y eficaz en las máquinas.

El administrador debe ser una persona responsable, que conozca y utilice, como usuario, la máquina que administra. Debe manejar cada detalle del equipo, características, componentes, su posible crecimiento, la configuración de la red, etcétera, a fin de utilizarlo con la máxima eficiencia posible.

Desde cierto punto de vista (el del usuario común), el administrador es la persona responsable de mantener a los usuarios contentos. A nivel técnico, esta persona necesita los conocimientos indispensables para dar mantenimiento a la máquina; a nivel personal, debe tener un carisma especial que le permita un trato cordial con los usuarios.

Puesto que el administrador es responsable de dar al equipo el mejor servicio a fin de que el usuario que lo ocupe no tenga problemas, debe tener en cuenta, entre otras, las siguientes actividades:

- Crear y borrar cuentas de usuarios.
 - Comunicación con los usuarios.
 - Respaldo y recuperación de la información.
 - Encendido y apagado de la máquina.
 - Cambio de la configuración del hardware.
 - Comunicación con otros sistemas.
 - Manejo de la Seguridad del sistema.
 - Verificación del rendimiento del sistema.
-
- **Crear y borrar cuentas de usuarios.**

El administrador del sistema es la persona responsable de crear cuentas de los usuarios autorizados, así como de borrar las cuentas de los usuarios no autorizados o que no son necesarios. Aunque es una frase técnica, también es parcialmente política; por ejemplo, si un usuario envía mensajes impropios a los demás, si utiliza el sistema sólo para jugar o si intenta dañarlo, ¿Debe conservar su cuenta? El administrador debe decidirlo, basándose en las políticas.
-
- **Comunicación con los usuarios.**

La persona encargada de la máquina es, en cierto modo, el intermediario entre el equipo y los usuarios. Si hay que dar de baja el equipo, o si es necesario que los usuarios cambien sus claves de acceso (password), el administrador debe comunicarlo a todos ellos. De manera inversa, si el usuario necesita algún dato específico del sistema el administrador debe ayudarlo.
-
- **Respaldo y configuración de información.**

Entre las tareas más importantes del administrador del sistema se encuentra la de respaldar la información. La tarea primordial será implementar la política de respaldo que asegure mantener la información respaldada accesible en cualquier momento. Para ello podrá contar con software específico que realice estas tareas y con hardware necesario para el mantenimiento de los respaldos.

- **Encendido y apagado de la máquina.**

El encendido y el apagado de las máquinas con sistema operativo UNIX es una tarea muy delicada que sólo debe ejecutar el administrador. Ya que en ocasiones necesita apagar y encender la máquina, debe poseer detallados conocimientos para hacerlo.

- **Cambio de la configuración del hardware.**

El administrador del sistema juega un papel importante en cuanto a la selección, instalación y configuración del hardware conectado al sistema, pues debe asegurar su rendimiento efectivo.

- **Comunicación con otros sistemas.**

Es muy raro encontrar una red que trabaje con un mismo tipo de sistema operativo, en especial con UNIX. Cuando se instala una red, por lo general se le conectan servidores UNIX (de diversos fabricantes) y computadoras personales. Por esa razón, el administrador debe conocer los diversos sistemas operativos que interactúan con la red. En específico, debe conocer cómo se comunica el sistema operativo con las demás máquinas.

- **Manejo de la seguridad del sistema.**

De alguna manera el administrador debe ingeniárselas para mantener la información del equipo segura. Es una tarea que nunca termina, desde el momento en que se conecta el sistema a la red, la información queda expuesta a que la obtengan usuarios que entran al sistema sin autorización e incluso, hay usuarios con acceso permitido, pero cuyos derechos no fueron asignados correctamente.

- **Verificación del rendimiento del sistema.**

Con frecuencia, el administrador tiene que revisar y perfeccionar el rendimiento del sistema, sobre todo cuando éste se vuelve lento.

3.14.2. RespalDOS.

Existe una serie de factores que hay que considerar para diseñar un plan de respaldo. Las siguientes medidas se encuentran entre las importantes:

¿Qué archivos necesitan ser respaldados?.

La respuesta más simple, es todos. Sin embargo, existen archivos y directorios temporales que no es necesario respaldar y por lo tanto se pueden dejar fuera de los respaldos.

¿Qué tan importantes son estos archivos?.

Lo que importa es determinar qué tan importantes son estos archivos para el sistema dentro de la estructura del sistema de archivos, así como determinar en dónde se encuentran localizados los datos más importantes.

¿Quiénes van a llevar acabo los respaldos?

La respuesta depende de la localización de los datos, por ejemplo, muchas organizaciones dejan esta responsabilidad al administrador, sin embargo, éste sólo se hace responsable de los archivos que los usuarios tengan almacenados en el servidor.

¿Dónde, cuándo y bajo qué circunstancia se deben de realizar los respaldos?

Esto depende de donde se encuentre situada físicamente la máquina, así como también en que servidor se encuentra almacenada la información. Lo ideal es que los respaldos se hagan con las particiones desmontadas.

¿Qué tan seguido cambia el contenido de estos archivos?

Esta información ayudará a decidir cuándo y qué tan seguido deberán realizar los respaldos.

¿Qué tan rápido se requiere un archivo importante que se haya dañado o perdido?

Esta información ayuda a determinar cuáles sistemas de archivos se respaldaran juntos y cuales serán respaldados de manera individual. También ayudará quizá a tener un respaldo de la información sensitiva físicamente en alguna región del disco, lo cual ayudaría a tener de manera casi instantánea la información.

¿Dónde será almacenada la información recuperada?

Esto nos ayudará a diseñar la forma en que se respaldará la información para determinar si ésta será utilizada únicamente en los directorios en donde fue respaldada, o si será posible ponerla en otro sistema de archivos para tomar los datos requeridos y eliminar el resto, o simplemente, para tenerla como un simple respaldo de emergencia.

3.14.2.1. Estrategias para hacer respaldos.

Los administradores del sistema deberán garantizar que la información del sistema se encuentre siempre respaldada. Para lograr este objetivo el administrador deberá definir una estrategia para respaldar día con día la información.

Es muy aconsejable que después de la instalación de un sistema de archivos se realice y personalice un sistema de respaldo.

El esquema más simple y sencillo es copiar todos los archivos del sistema a una unidad de cinta. Esta estrategia se conoce con el nombre de *respaldo completo*.

Los respaldos completos consumen mucho tiempo; extraer un sólo archivo de ellos, en los que ocasiones ocupan más de una cinta, resulta inconveniente, y cuando el contenido de los archivos no cambia rápidamente, el tiempo ocupado para realizar este respaldo no será justificable por el pequeño número de archivos que será respaldado. Desde otro punto de vista, si los archivos son modificados frecuentemente, y el perderlos ocasionaría que un buen número de usuarios no puedan trabajar, este tipo de respaldos es la estrategia adecuada.

Existe otra estrategia de respaldos conocida como *respaldos incrementales*, los cuales se realizan de manera más frecuente. En los respaldos incrementales, el sistema copia únicamente los archivos que fueron modificados desde que se realizó un respaldo previo. Son utilizados cuando se realizan respaldos completos sobre grandes sistemas de archivos y sólo ciertos archivos cambian en su contenido diariamente.

Una estrategia típica de respaldo utilizando respaldos incrementales sería la de realizar un respaldo completo al inicio de la semana, y el resto de los días realizar un respaldo incremental a nivel 1, lo cual quedaría resumido de la siguiente manera:

Lunes:	Respaldo Nivel 0. (total)	Jueves:	Respaldo Nivel 1. (incremental)
Martes:	Respaldo Nivel 1. (incremental)	Viernes:	Respaldo Nivel 1. (incremental)
Miércoles:	Respaldo Nivel 1. (incremental)		

La principal ventaja de este plan es que para recuperar el sistema de forma completa únicamente se van a emplear dos juegos de cintas. La desventaja que si la actividad del sistema aumenta, los respaldos diarios empezarán a incrementarse gradualmente hasta alcanzar casi la totalidad de los archivos. Por esta razón, las estrategias de respaldo deberán ser revisadas constantemente y actualizadas conforme los requerimientos de la información.

Al momento de decidir la estrategia de respaldo, hay que tener en cuenta que las partes más utilizadas del sistema de archivos deberán ser respaldadas con más frecuencia que aquellas que son modificadas de forma esporádica.

Siempre se debe de considerar el realizar un respaldo completo antes de hacer modificaciones al kernel, instalar nuevos paquetes de aplicaciones, instalar nuevas versiones o actualizaciones del sistema operativo para poder recuperar la funcionalidad del sistema en caso de que algún procedimiento no funcione correctamente.

Una vez definida la estrategia de respaldo, es conveniente considerar las siguientes recomendaciones:

Etiquetar las cintas. Es muy importante ponerle etiquetas a las cintas donde se especifique de manera clara y completa el contenido de los respaldos, por ejemplo, los sistemas de archivos respaldados, el día del respaldo y el nivel con que fue respaldado.

Escoger un intervalo de respaldo razonable. Entre más frecuente se realicen los respaldos, menor cantidad de información se perderá en caso de que el sistema falle. Sin embargo, no hay que olvidar que los respaldos consumen tiempo tanto del sistema como del administrador. En equipos con mucha actividad es conveniente respaldar diariamente los sistemas de archivos donde se encuentran los directorios de los usuarios.

Seleccionar los sistemas de archivos a ser respaldados adecuadamente. Los sistemas de archivos que son modificados muy poco, no deben de ser respaldados tan frecuente como los directorios de los usuarios. En caso de existir una serie de archivos que sean modificados dentro de sistemas de archivos casi estáticos, por ejemplo, /etc/passwd o

/etc/group, se recomienda copiar estos archivos a un sistema de archivos distinto y respaldarlo de forma periódica.

Realizar respaldos diarios de tal forma que puedan ser almacenados en una cinta. Con los nuevos dispositivos de respaldos en cinta (DAT, 8mm) es posible respaldar la información modificada diariamente en una sola cinta. De esta manera, se puede dejar al programa el respaldo desde el cron y a la mañana siguiente verificar que todo haya funcionado adecuadamente.

Limitar la actividad del sistema durante el tiempo de respaldo. La actividad de los sistemas de archivos deber ser limitada durante la ejecución de los respaldos, dado que los cambios que hace en los archivos pueden ocasionar errores al momento de estar respaldando la información.

3.14.2.2. Respaldos remotos.

Es muy común que se tenga que llevar a cabo respaldos a través de la red. Las razones son muy variadas: la máquina donde se desea obtener el respaldo no cuenta con una unidad de cinta, la unidad de cinta del sistema remoto es más rápida y eficiente. Casi todos los sistemas UNIX tienen alguna utilidad que permite realizar respaldos remotos.

Los comandos más comunes para llevar a cabo estos respaldos a través de la red son `rdump` y `restore`, los cuales son soportados por la mayor parte de los sistemas operativos.

Solaris soporta los dispositivos remotos en los comandos `ufsdump` y `ufsrestore`, combinando las utilidades locales y remotas en el mismo comando. Las diferencias que tiene con respecto a `dump` y `restore` es que permiten el nombre de un dispositivo bajo la forma `host:local_device`.

El comando `rdump` debe ser ejecutado de manera ideal por el superusuario. Para poder tener acceso al sistema remoto debe existir en el directorio raíz un archivo llamado `.rhosts` el cual debe contener el nombre de la máquina que desea utilizar la unidad de cinta local; éste archivo debe tener como dueño a `root` y permisos de `400`.

3.14.3. Sistema de Archivos en Red (NFS : Network File System).

Ofrecer simplemente los protocolos para comunicaciones con otro sistema no basta. Se necesita una aplicación que pueda sacar partido de los recursos del sistema remoto. Un sistema de archivos como NFS puede ofrecer estas posibilidades. NFS es un sistema de archivos distribuido desarrollado por SUN Microsystems que está construido sobre TCP/IP.

Para el usuario, NFS significa que puede conectarse a diferentes máquinas y tener acceso en todas a los mismos archivos. No se necesitan órdenes o procedimientos adicionales para listar, ver su contenido, crear o copiar archivos al disco fijo local. NFS permite llevar una administración centralizada de los discos.

El sistema de archivos en red es un servicio que permite a los usuarios tener acceso a jerarquías de archivos como si estos fueran locales. Las jerarquías de archivos pueden ser sistemas de archivos completos o directorios individuales. Los sistemas que participan dentro de NFS pueden ser heterogéneos. Pueden pertenecer a diferentes compañías, utilizar diferentes sistemas operativos y estar conectados a redes de arquitecturas diferentes. Estas diferencias son transparentes para la aplicación del sistema de archivos de red.

Los beneficios que NFS ofrece son:

- Permite que múltiples computadoras puedan usar los mismos archivos, permitiendo que los mismos datos puedan ser accedidos por todos a través de la red.
- Reduce los costos de almacenamiento por tener computadoras compartiendo aplicaciones en vez de tener espacio de disco local para cada aplicación del usuario.
- Provee consistencia de datos y rentabilidad por que todos los usuarios pueden leer el mismo conjunto de archivos.
- Realiza el montado de sistemas de archivos transparente para los usuarios.
- Realiza el acceso remoto a sistemas de archivos transparente para los usuarios.
- Soporta ambientes heterogéneos.
- Reduce las tareas de administración.

El sistema NFS realiza la localización física de los sistemas de archivos irrelevante para el usuario. NFS puede usarse para habilitar a los usuarios para que puedan ver todos los archivos relevantes, sin considerar la localización, en vez de tener copias de los archivos mas comúnmente usados sobre distintos sistemas de archivos, el software de NFS permite tener un sola copia de este archivo en un solo lugar de disco accesado esta a través de la red. Bajo la operación de NFS, los sistemas de archivos remotos son indistinguibles sobre un sistema local.

NFS: Servidores y Clientes.

Los términos cliente y servidor son usados para describir los papeles que una computadora juega cuando comparte el sistema de archivos. Si un sistema de archivos reside en el disco de una computadora y esa computadora hace el sistema de archivos disponible para otras computadoras en la red, entonces esa computadora actúa como un *servidor*. La computadora que esta accedando a ese sistema de archivos se dice que es un *cliente*. El software de NFS habilita cualquier computadora dada para acceder a cualquier otra computadora a su sistema de archivos, al mismo tiempo, proporcionar acceso a su propio sistema de archivos. Una computadora puede estar de cliente, servidor, o ambos en cualquier momento en la red.

Un servidor puede proporcionar archivos para un cliente de Diskless (un Diskless es una computadora que no tiene disco duro). Un cliente Diskless cuenta con un servidor que le provee totalmente con un conjunto de archivos para poder interactuar con la red. Un cliente Diskless puede ser solo un cliente nunca un servidor, debido a que este no tiene un dispositivo de almacenamiento como el disco duro.

Cuando los clientes accedan a los archivos en el servidor, el sistema de archivos ha sido montado para ser compartido.

Cuando un cliente entra a un sistema de archivos remoto, este no puede hacer una copia del sistema de archivos; más bien, al entrar a un sistema de archivos remoto se crean una serie de llamadas de procedimientos remotos, esto habilita al cliente para acceder al sistema de archivos y ser transparente en los servidores de disco. Al entrar a un sistema remoto parece como si entráramos a un sistema local y los usuarios teclean órdenes como si el sistema de archivos fuera local.

Una vez que se ha compartido un sistema de archivos en un servidor por una operación NFS, este puede ser accedido por los clientes

Exportar.

Exportar es un proceso en el que un servidor de sistemas de archivos en red (NFS) permite el acceso de sus archivos a clientes remotos. Pueden ser exportados tanto en directorios individuales como sistemas de archivos, pero las entidades que se exportan se conocen como sistemas de archivos. El proceso de exportación puede realizarse de manera automática cuando la máquina se enciende, o por medio de un comando específico (share) que el administrador de la red ejecute una vez que la máquina ya esta funcionando.

Montar.

Montar es el proceso mediante el cual un cliente NFS tiene acceso a los sistemas de archivos que fueron exportados por un servidor NFS. Cuando se exportan los sistemas de archivos o los directorios NFS, se ponen a disposición de los clientes a través de la red por una serie de llamadas de procedimiento remotas que permiten al cliente tener acceso a los archivos de manera transparente, desde el disco del servidor. Los sistemas de archivos que se montan no están físicamente en la máquina del cliente, pero el procedimiento de montado permite que el usuario ejecute comandos como si el sistema de archivos fuera local.

3.14.4. Cuotas.

Antes de seleccionar cuotas, es necesario determinar cuanto espacio será asignado a cada usuario. Si se desea estar seguro de que el espacio total del sistema de archivos jamás será excedido, se puede dividir el tamaño total del sistema de archivos entre el número de usuarios. Por ejemplo, si tres usuarios comparten una partición de 100 MB y tienen las mismas necesidades de espacio en disco, se podría repartir en 33 MB para cada uno. En ambientes en donde no todos los usuarios saturan su espacio de disco se podría seleccionar cuotas individuales que sobre pasen el espacio total del sistema de archivos. Por ejemplo, si hay tres usuarios compartiendo 100 MB se puede asignar a cada uno de ellos 40 MB.

Cuando se haya seleccionado la cuota para un usuario, esta puede servir como prototipo para seleccionar a otros usuarios en el mismo sistema de archivos.

4

Propuesta de solución para el Centro de Ciencias de la Atmósfera

4.- Propuesta de solución para el Centro de Ciencias de la Atmósfera	59
4.1. Problemas que se encontraron en un inicio en el Centro de Cómputo	59
4.2. Realización de respaldos	60
4.3. Compartir recursos en red.....	61
4.4. Cuotas	62
4.5. Estandarización de los Sistemas Operativos	63
4.6. Instalación del disco optomagnético externo (Vertex).....	67
4.7. Servidores de impresión	68
4.8. Instalación de software para despliegue de imágenes postscript.....	70
4.8.1. PostScript.....	70
4.8.2. PDF (Formato de Documento Portable).....	71
4.8.3. Ghostscript.....	71
4.8.4. Ghostview	72
4.9. Instalación de software de seguridad	73
4.9.1. PASSWD+.....	74
4.9.2. COPS (Computer and Password System).....	74
4.9.3. TCP-Wrapper.....	75

Capítulo 4

Propuesta de solución para el Centro de Ciencias de la Atmósfera.

El Centro de Cómputo de Ciencias de la Atmósfera adquirió nuevos equipos de cómputo para mejorar el funcionamiento de su red y mejorar las aplicaciones que se realizan dentro de ella. Este centro deberá estar trabajando a su máxima capacidad para que los investigadores desarrollen día con día nuevas aplicaciones, con el fin de que el sistema de red sea íntegro y confiable para el usuario final, y así este no tenga nada que ver en cuanto a la administración, ni resolución de los problemas que antes tenía que resolver, como consecuencia el usuario se dedicará a desarrollar las tareas que él sabe hacer sin tener que pensar en la red de cómputo como un problema más en su trabajo.

Para ello es necesario un planteamiento de la administración de la red, configuración, estandarización, compartir los recursos y aplicaciones de las estaciones de trabajo SUN y los equipos PC's, así como la instalación de software tanto para desarrollo como para la seguridad de la red, labores de mantenimiento del equipo, con el fin de lograr una red confiable y asegurar la integridad y disponibilidad de la información para todos los usuarios del Centro de Cómputo.

4.1. Problemas que se encontraron en un inicio en el Centro de Cómputo.

Se detectaron los problemas principales en el Centro de Cómputo con el fin de tener una lista de los casos más frecuentes y comunes a los cuales nos enfocaremos a resolver, estos problemas fueron los siguientes:

1. No se tiene compartida la información utilizada.
2. Duplicidad de Información.
3. No se cuenta con respaldos de información de ningún servidor.
4. No se cuenta con un servidor de impresión para las estaciones de trabajo, sólo para los equipos PC's.
5. El proceso de impresión en las PC's es realizado con la ayuda de un multiplexor manual, el cual es un proceso muy molesto para los usuarios.
6. Cada estación trabaja en forma independiente.
7. El ambiente gráfico de comunicación de las PC's hacia las estaciones de trabajo no puede desplegar imágenes PostScript.
8. Cada estación de trabajo cuenta con un Sistema Operativo Distinto.
9. No se cuenta con los discos de los Sistemas Operativos instalados en las estaciones de trabajo.
10. No existen cuotas para los usuarios.
11. Los sistemas no son muy confiables ya que, no reciben un mantenimiento constante.

12. Necesidad de instalación de nuevo software para el desarrollo de nuevas aplicaciones.
13. Incorporación de nuevo equipo a la red.
14. Uso de distintas bases de datos de mas de 500 Megabytes

Para la resolución de los problemas antes descritos se propone el siguiente procedimiento, en base al orden de importancia de las tareas a realizar y que son de mayor prioridad en el centro de cómputo:

- I - Realización de respaldos.
- II- Compartición de recursos en red.
- III- Asignación de cuotas.
- IV- Estandarización de los sistemas operativos.
- V- Instalación del disco optomagnético (VERTEX).
- VI- Servidores de Impresión.
- VII- Instalación de Software para despliegue de imágenes PostScript.
- VIII- Instalación de Software de Seguridad.

4.2. Realización de respaldos.

Una de las más importantes funciones del administrador de sistemas es el mantener la integridad de los datos del sistema.

Todos los días, los usuarios de una red crean, modifican y borran archivos. Cuando un usuario borra un archivo, ya sea por accidente o por decisión propia, este archivo se pierde, una falla en la energía eléctrica puede dañar el hardware y propiciar la pérdida de información, por catástrofes, robo del equipo, por esas razones es conveniente hacer respaldos de la información de tal manera que ésta siempre permanezca segura. Generalmente los respaldos son realizados en unidades de cinta o en unidades de discos ópticos removibles de gran almacenamiento.

Si un administrador no da énfasis en la realización de respaldos de información sobre algún medio, algún día el disco podría fallar y la información contenida en él jamás podría ser recuperada.

Básicamente respaldar información es asegurar el funcionamiento de la organización, lo cual representa el tiempo y esfuerzo dedicados para la prevención de accidentes futuros. El tiempo establecido para los planes respaldo debe balancear el decremento en productividad, el retraso en los tiempos calendarizados, etc., en caso de que la información requerida no se encuentre disponible contra el tiempo dedicado a respaldar la información.

Uno de los principales problemas de este Centro es la falta de protección de la información, ya que nunca se han hecho respaldos de la información de los servidores, dándose accidentes de pérdida total de la información sin que ésta allá podido ser

recuperada por falta de precaución, dejando a los usuarios imposibilitados a recuperar su valiosa información.

Para evitar este problema lo primero que se planteo fue la realización de respaldos de todos los equipos.

La política propuesta para la realizar estos respaldos fue la de hacer un *respaldo total* de la información de cada servidor.

Se propuso que se realizara un respaldo total de nivel 0 el primer día de cada mes y se realizara otro cada semana de las particiones más utilizadas como lo son /home y alguna más en donde tuvieran información de mucha importancia que modificaran constantemente los usuarios.

Con la realización de estos respaldos se podrá dar seguridad a los usuarios en cuanto a la integridad de su información y se podrá empezar a trabajar con los sistemas de manera segura por parte del administrador ya que si alguna instalación al inicio de sus actividades falla este podrá recuperar los equipos sin que queden desplazados los usuarios por un largo período, o por algún imprevisto o inconveniente.

4.3. Compartir recursos en red.

El Centro de Cómputo actualmente hace uso de varias bases de datos de gran tamaño que han sido instaladas en distintas máquinas y que son utilizadas por varios usuarios.

Esto genera que la misma información sea instalada en varias máquinas y que no pueda ser utilizada por los mismos usuarios, creando gran duplicidad de información por el tamaño de las bases de datos y un mal uso de los recursos de la red.

Para resolver este problema se propone compartir la información por medio de NFS (Network File System), creando particiones que contenga la información y software de aplicación más utilizado, para exportar y compartir con los demás usuarios, reduciendo la sobre utilización de los recursos, dando pauta a liberar espacio que pueda ser utilizado para instalación de más aplicaciones que sean necesarias en un futuro.

Las ventajas que se obtienen con este tipo de configuración, es que una vez seleccionada la información que usan más los usuarios (Archivo A, Archivo B, Archivo C) se puede compartir con los demás equipos a través de NFS, véase figura 4.1, realizando esto de forma transparente para el usuario, ya que él no puede saber en cual estación esta la información que esta siendo accesada o consultada.

Con esto se reduce la información duplicada en todos los equipos, así como se reducen los costos de almacenamiento por tener aplicaciones independientes instaladas en cada servidor, proporcionando consistencia en los datos y rentabilidad por que todos los

usuarios de la red pueden leer el mismo conjunto de archivos, sin importar a que máquina estén conectados.

Red con NFS Implementada

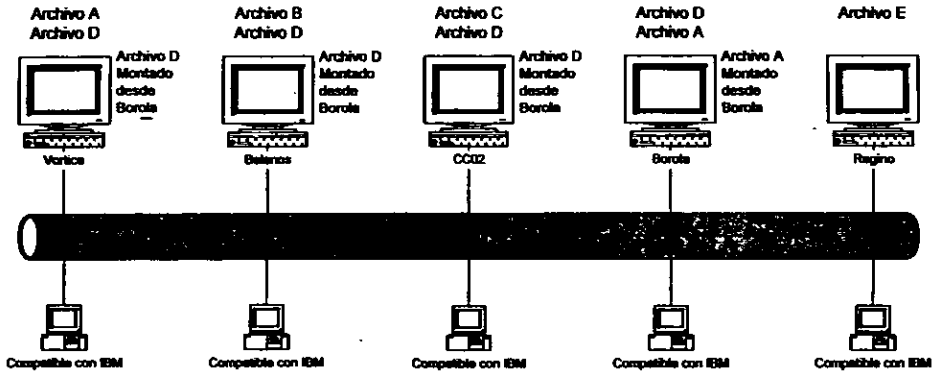


Figura 4.1. Los archivos instalados en el disco de un servidor son exportados y montados en los demás equipos a través de NFS como si fueran particiones propias de los equipos.

Otra ventaja que se tiene al utilizar este tipo de configuración es que si algún servidor llega a fallar, el otro puede seguir funcionando de manera independiente sin que esto les afecte a los demás en su funcionamiento, ya que el único problema que se tiene en momentos de falla de algún equipo es que la partición compartida, montada o exportada no estará disponible durante el tiempo en que el equipo no este proporcionando el servicio, con la ventaja de que los equipos que estén funcionando podrán seguir trabajando de manera normal.

4.4. Cuotas.

Las cuotas son un mecanismo de control sobre el uso de una partición del disco por los usuarios del sistema. Con el uso de cuotas se puede limitar la cantidad de espacio de disco disponible a los usuarios, evitando que un solo usuario monopolice el uso del disco, controlando así el uso de disco proporcionalmente. Las cuotas se activan automáticamente cada vez que el sistema de archivos es montado.

Se detecto que algunos usuarios cuentan con enormes cantidades de información distribuida en varias particiones y servidores monopolizando el uso de disco y no dando pauta a la instalación y compartición de información con los demás usuarios del sistema, en algunos casos la misma información, se tiene como respaldo en varias máquinas provocando que la mayoría de los sistemas de archivos estén a su máxima capacidad.

Además no se cuenta con un control en la cantidad de información que cada usuario puede tener en los sistemas, ocasionado que los usuarios nunca se preocupen en depurar la información que no es necesaria y llenando hasta 100% cualquier disco que este a la mano.

Otro problema es la necesidad de instalar nuevas aplicaciones para el trabajo cotidiano de los investigadores, pero esto no se puede realizar por falta de espacio en los sistemas de archivos.

Con la adquisición futura de otros servidores y discos optomagnéticos es necesario prever que estos sucesos no se repitan, por lo que se recomienda la asignación de cuotas a cada uno de los usuarios dependiendo de las necesidades de trabajo que cada uno de estos tenga y de acuerdo a la disponibilidad de disco se asignarán cuotas individuales a cada uno.

Con esto se prevé el crecimiento desbordante de información duplicada y se obliga a los usuarios a depurar sus claves ya que con la asignación de cuotas no se permitirá un crecimiento mayor al espacio asignado, con lo que se controla la saturación de los sistemas de archivos, y se tendrá más espacio disponible para la instalación de software para el trabajo de los investigadores.

4.5. Estandarización de los Sistemas Operativos.

Uno de los problemas más graves que tiene este Centro de Cómputo es la falta de estandarización de los sistemas operativos, ya que a medida que el Centro de Cómputo fue creciendo, se fueron instalando sistemas operativos y aplicaciones distintas en cada máquina, aunado a esto no se tienen los discos de los sistemas operativos instalados en cada máquina, que son de gran importancia en momentos críticos de falla de los equipos.

Otro problema más es que los nuevos equipos que llegarán, vendrán con versiones de sistemas operativos distintas a las que ya se tienen actualmente.

Para resolver este problema primero necesitamos estandarizar los sistemas operativos de los equipos en una misma versión, tomando en cuenta que las aplicaciones existentes puedan correr sin ningún problema en la versión del sistema que se elija.

Tomando como base la migración de sistema operativo 4.1.x a 2.5.x descrita en el Capítulo 2 (Estándares y requerimientos) y considerando que los nuevos equipos se compraran con el Disco de Sistema Operativo, nosotros proponemos migrar todos los equipos a Solaris 2.5.1. basándonos en las ventajas y puntos mencionados en el capítulo 2 y en el Apéndice B.

Tomando en cuenta que el equipo ULTRA 2 (Borola) había sido ya adquirido, se propuso tomar este equipo para las pruebas e instalaciones que debíamos de realizar, con esto nosotros tendremos tiempo suficiente para conocer las mejoras del sistema operativo, y verificar las propuestas realizadas en los capítulos anteriores,

durante el tiempo de pruebas no se afectará el trabajo de los usuarios ya que este equipo aun no será puesto a disposición de los usuarios.

Para hacer esto se propone hacer una planeación de la migración de los sistemas operativos de la siguiente manera.

Borola.



Ultra 2 / Creator 3D

En el equipo ULTRA 2 (BOROLA), se propone hacer los siguientes procedimientos:

- Pruebas de instalación del Sistema Operativo.
- Instalación del Software.
- Compilación de Ghostview y el Ghostscript en el servidor para el despliegue de imágenes PostScript sobre equipos PC's.
- Instalación del servicio de impresión a través del servidor multiprotocolos axis 550 NPS.
- Impresión desde PC y UNIX.
- Impresión de Imágenes PostScript.
- Instalación de bases de datos en el disco optomagnético
- Compartición del disco Optomagnético (Vertex 2.1 GB) vía NFS hacia las otras máquinas
- Bajar respaldos de /home de algunos usuarios para que realicen pruebas con las nuevas versiones de software y sistema operativo.
- Realización de respaldos totales y semanales.

En el tiempo de prueba y puesta en marcha total de este equipo, se evaluará que el equipo este respondiendo eficientemente.

Una vez hechas las pruebas e instalaciones necesarias para que el equipo pueda funcionar y los usuarios puedan trabajar de manera correcta, se harán las siguientes tareas.

- Planeación de migración de las máquinas.
- Asignación de claves y cuotas en disco para cada usuario.
- Realización de respaldos totales de cada máquina, se propone que se hagan dos respaldos totales por cada máquina y un respaldo de las particiones más importantes en cinta y en el disco optomagnético (Vertex).
- Aviso a los usuarios de la migración de los equipos y las consecuencias que esto tendrá en su trabajo.
- Suspensión del servicio de cada máquina a la que se le realizará el proceso de migración, serán notificados los usuarios de estas actividades enviándoles un correo electrónico (e-mail) y avisándoles por medio oral o por medio de mensajes de presentación en los servidores cada vez que estos entren al sistema, así como se pegarán avisos de suspensión de actividades en papel.

Una vez que se hallan probado las soluciones en el servidor Borola y verificado que el equipo este funcionando de manera óptima, será puesto en una etapa de prueba en donde

los usuarios probarán el rendimiento del equipo y se tomará nota de los comentarios de los usuarios sobre si cubre sus "expectativas".

Ya probado el servidor se acordará con los usuarios de los cambios sufridos en su forma de trabajo, los beneficios y desventajas que esto acarreará.

Basándonos en los resultados, el siguiente paso será migrar cada una de las máquinas de acuerdo a la importancia de las tareas asignadas a cada uno de ellos.

El primer equipo que tendrá el proceso de migración será Vórtice, ya que en este equipo se encuentran las cuentas de usuarios que necesitan utilizar las nuevas aplicaciones probadas y además este exportará particiones hacia los otros servidores vía NFS.

Sobre este servidor se realizarán los siguientes pasos.

Vórtice.



- Se realizarán dos respaldos totales del equipo.
- Respaldo de la partición de /home (donde reside la información del usuario) y de las particiones que serán utilizadas en la instalación del nuevo sistema operativo.
- Respaldo de los archivos más importantes del sistema (/etc/passwd, /etc/shadow, etc.).
- Cambio de Sistema Operativo SunOS 2.4 a Solaris 2.5.1.
- Recuperación de información de los usuarios en sus nuevos homes creados.
- Creación de cuentas.
- Instalación de Software.
- Compartición de Software a través de NFS desde Borola.
- Instalación de software de impresión.
- Realización de respaldos totales y semanales.

Los usuarios tendrán dos semanas para verificar la integridad de su información y verificar que el software este funcionando de manera correcta, antes de liberar totalmente el servidor.

Una vez puesto en marcha el equipo Vórtice se dará paso a migrar el servidor Belenos, el cual es uno de los dos equipos con la versión y aplicaciones más viejas del Centro. Para la migración y puesta en marcha de Belenos nosotros proponemos lo siguiente.

Belenos.



- Realización de dos respaldos totales de la información del equipo.
- Respaldo de la partición de /home sobre el disco optomagnético para un mayor tiempo de respuesta en la recuperación de la información y de las aplicaciones más utilizadas.
- Cambio del S.O. SunOS 4.1.3 al S.O. Solaris 2.5.1.
- Recuperación de la información.

- Creaciones de nuevas cuentas.
- Instalación de nuevas aplicaciones.
- Importar sistemas de archivos vía NFS.
- Instalación del software de impresión.
- Realización de respaldos totales y semanales de acuerdo a lo descrito en la sección de respaldos.

Los usuarios tendrán dos semanas para verificar la integridad de su información y verificar que el software este funcionando de manera correcta, antes de liberar totalmente el servidor.

El siguiente servidor será CCA02 debido a que tiene menor carga de trabajo y las tareas a realizar propuestas:

CCA02.



- Realización de dos respaldos totales de la información del equipo.
- Respaldo de la partición de /home sobre el disco optomagnético para un menor tiempo de respuesta en la recuperación de la información y de las aplicaciones más utilizadas.
- Cambio del S.O. SunOS 4.1.3 a S.O. Solaris 2.5.1.
- Recuperación de la información.
- Creación de nuevas cuentas.
- Instalación de nuevas aplicaciones.
- Importación de sistemas de archivos vía NFS.
- Instalación de software de impresión.
- Realización de respaldo total y semanal.

Los usuarios tendrán dos semanas para verificar la integridad de su información y verificar que el software este funcionando de manera correcta.

Una vez instalados y estandarizados los sistemas operativos, el siguiente paso es verificar la integridad y seguridad de los servidores, además de esperar la entrega del último equipo que conformará dicha red. Para el último equipo que será integrado a esta red nosotros proponemos lo siguiente.

Regino.



- Instalación del Sistema Operativo Solaris 2.5.1.
- Instalación de software y aplicaciones.
- Instalación de software de impresión.
- Importar y exportar sistemas de archivos vía NFS.
- Realización de respaldos totales y semanales.

4.6. Instalación del disco optomagnético externo (Vertex).

El Disco Optico Vertex es un drive de 5.25" con una capacidad de 2.6 Gigabyte de alto performance basado sobre tecnología óptica, desarrollado por Pinnacle Micro's. El Vertex tiene una rápida velocidad de rotación de 3,755 RPM con un tiempo de búsqueda máximo de 19 mseg y una transferencia de datos de hasta 4.3 Mbytes por segundo.

El Vertex puede ser usado como una expansión de disco o un disco duro alternativo, este utiliza discos removibles de alta velocidad.

Muchas aplicaciones basadas en audio, vídeo, despliegue de gráficas, soluciones de almacenamiento masivo de datos intensos de información y grandes dispositivos de respaldos, requieren un óptimo nivel de integridad de datos, portabilidad y un rápido acceso a datos críticos.

El Vertex puede almacenar hasta 2.6 Gigabytes de información en un simple cartucho y cumple con todos los estándares de la industria en la integridad de almacenamiento de datos sobre discos ópticos. Cada disco removible tiene un tiempo de vida estimado de unos 100 años de seguridad e integridad de los datos.

El Centro de Cómputo actualmente hace uso de cantidades de bases de datos de aproximadamente 500 MB cada una, que son utilizadas por varios usuarios en distintas máquinas.

El problema que genera el uso de estas bases es que cada base ocupa gran cantidad de espacio en disco ocasionando que los sistemas de archivos en donde este instalada estén siempre al 100% de su capacidad.

Con la configuración de este equipo (véase figura 4.2) se pretende instalar las bases más usadas y compartirlas a través de NFS, ya que el Sistema Operativo ve al disco óptico como un disco propio del sistema. Además será usado como disco de respaldo de acceso rápido de la información más importante que se tenga que restaurar en el proceso de migración, ya que los tiempos de escritura y lectura son similares a los de un disco interno y superiores a los de una cinta de respaldo de 8mm.

Instalación del Disco Optomagnético Vertex

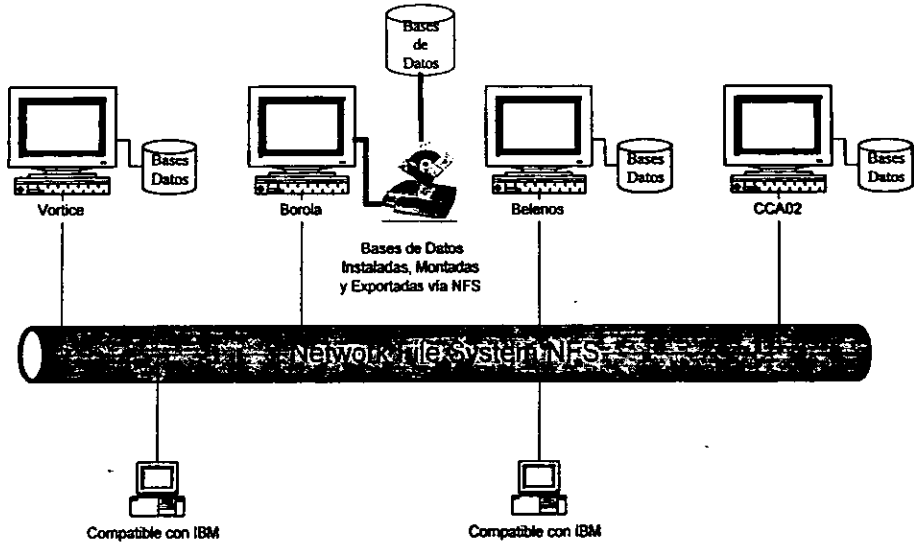


Figura 4.2. Las bases de datos instaladas en el disco optomagnético son exportadas y montadas en los demás equipos a través de NFS como si fueran particiones propias de los equipos.

4.7. Servidores de impresión.

El tema de impresión ha sido a través del tiempo y de los avances de la tecnología un tema de gran interés. Antes de que surgieran las redes era fácil imprimir un archivo ya que las impresoras estaban directamente conectadas a una computadora, en la cual solo se invocaba un comando de impresión y se imprimía mi archivo. Sin embargo, esta historia cambio cuando surgieron las redes. Si la impresora no esta directamente conectada a su computadora, el único camino que un usuario podía seguir es a través del uso de comandos de impresión remotos obteniendo para esto el nombre de algún servidor de impresión que le proporcionara el servicio de impresión.

Un servidor de impresión que tiene conectada directamente la impresora puede dar un volumen de trabajo aceptable, pero cuando se requiere un servicio de impresión más especializado existen productores en el mercado que se dedican a diseñar equipos especialmente para funcionar como servidores de impresión.

AXIS NPS 550:

El axis NPS es un servidor de impresión Standalone que trabaja sobre ambientes Ethernet. Usar el axis hace posible conectar cualquier impresora sobre la red Ethernet, dejando a todos los usuarios acceder a los recursos compartidos de la impresora. El axis se puede conectar directamente a la red y no es necesario que esta este conectada a un equipo

PC, Macintosh o un Sistema UNIX. Su soporte multiprotocolos permite imprimir bajo ambientes UNIX, NetWare, Microsoft, Apple, EtherTalk y TCP/IP en un servidor multiprotocolos. Además este cuenta con dos puertos paralelos y un puerto serie lo cual deja una combinación de hasta tres impresoras normales en un solo dispositivo.

¿Cómo Funciona?

En Ethernet los datos de las impresoras de red son transmitidos como paquetes de datos usando un protocolo de gran velocidad muy diferente a los estándares usados por las impresoras serie y paralelas. Cada paquete contiene información sobre el remitente, y el receptor, así como la forma de desempaquetar el paquete, y los datos contenidos.

El NPS 550 actúa como un nodo en las redes Ethernet, con su propia dirección única (véase fig. 4.3). Este recibe los paquetes dirigidos a él, los desempaqueta, y convierte los datos de la impresión a un formato satisfactorio para las impresoras normales.

Instalación del Servidor de Impresión AXIS NPS 550

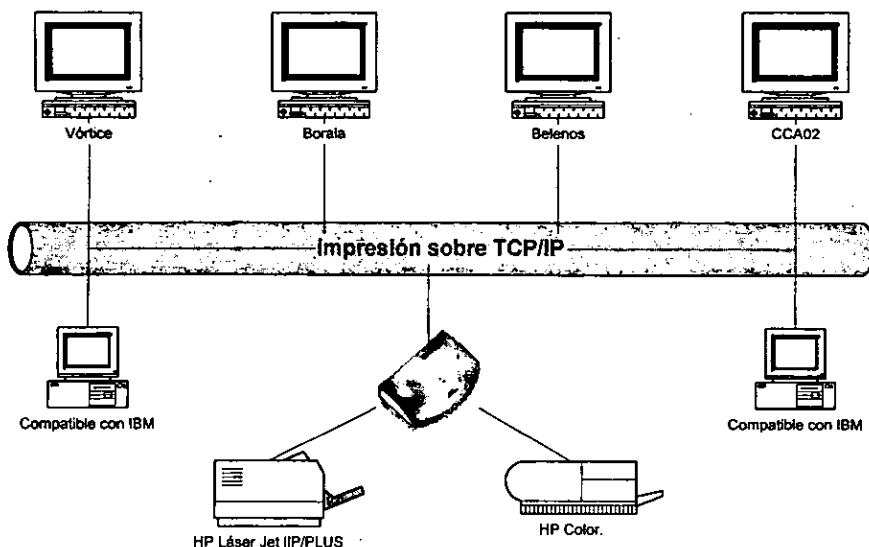


Figura 4.3. Con el servidor de impresión Axis se pueden mandar a imprimir trabajos desde cualquier equipo PC ó Servidor Unix.

Este se conecta físicamente a la red por un cable coaxial delgado (10Base2) o por un cable par trenzado (10BaseT). Se pueden dirigir los datos de la impresión a dos puertos paralelos de gran velocidad y un puerto serie, su fabricación hace posible imprimir en tres impresoras diferentes al mismo tiempo.

El Centro de Cómputo cuenta con este dispositivo que aun no se ha puesto en marcha. Actualmente no se cuenta con un servicio de impresión confiable, si se desea imprimir desde UNIX es necesario mover y conectar físicamente la impresora a la estación en donde se desea imprimir y solamente una estación tiene configurada esta opción (Belenos). Si un usuario desea imprimir desde una PC este tiene que trasladar esta misma impresora al multiplexor y seleccionar manualmente mediante un switch a la impresora donde se desea imprimir, obviamente se tiene que trasladar físicamente al lugar en donde esta dicho dispositivo para imprimir.

Se propone utilizar el axis 550 NPS para la resolución de este problema, ya que este servidor es un dispositivo multiprotocolo diseñado especialmente para funcionar como servidor de impresión, con soporte a aplicaciones con UNIX, especialmente con Solaris bajo TCP/IP y aplicaciones con Windows 3.x y Windows95 sobre el protocolo TCP/IP y * NetBEUI. Además este dispositivo cuenta con una interface de comunicación de instalación para ambos ambientes lo que hace que estos sean más amigables y transparentes en su instalación tanto para el usuario como para el administrador.

Con la instalación de este dispositivo se resolverá uno de los grandes problemas de este Centro de Cómputo: *la impresión*, ya que se podrá imprimir desde cualquier Servidor y desde cualquier PC a un solo servidor de impresión que puede estar físicamente conectado en cualquier parte de Centro, la parte más cómoda y de fácil acceso.

Además este dispositivo no genera cargas adicionales de trabajo ya que no esta conectado directamente a una máquina consumiendo tiempo de procesamiento en la espera de una petición de impresión.

4.8. Instalación de software para despliegue de imágenes postscript.

4.8.1. PostScript. Elaborado lenguaje de descripción de página (PDL) que se emplea para imprimir texto y gráficos de alta calidad en impresoras láser y otros dispositivos de impresión de alta resolución.

Aunque PostScript es un lenguaje de programación, el usuario puede aprender a escribir descripciones de página con él, PostScript es invisible y automático. El programa genera el código PostScript que va a la impresora, donde un intérprete de PostScript sigue las instrucciones para generar una imagen de la página que se apega al pie de la letra a las instrucciones.

* NetBEUI: El protocolo utilizado por redes Microsoft LanManager y redes Microsoft Windows para trabajo en grupo. NetBEUI es la abreviatura de protocolo NetBIOS de interfaz extendida de usuario, este protocolo funciona bien para pequeños grupos de trabajo o redes departamentales. Es sencillo de instalar y bastante rápido para pequeñas tareas. Pero no escala bien a redes de empresas más grandes. Está limitado a 254 sesiones (conexiones a otras computadoras) para cada proceso. Más importante es el hecho de que NetBEUI no puede rutear desde un segmento de red a otro. Esto lo hace inapropiado para grandes entornos de red en los que se utilizan los routers para conectar los diferentes segmentos de red.

Una de las ventajas más importantes de PostScript es su independencia de dispositivos; el usuario puede imprimir el código PostScript generado por un programa en cualquier impresora que cuente con un intérprete de PostScript. Asimismo, el usuario puede llevar sus archivos PostScript generados en una PC, a un taller de servicios donde imprimirán el documento con costosas máquinas de composición tipográfica, las que ofrecen resoluciones de hasta 2,400 puntos por pulgada.

4.8.2. PDF (Portable Document Format). Formato de Documento Portátil, es el standard para la distribución electrónica de documentos porque esta es la mejor manera de mantener la vista y percepción de los documentos creados. Los archivos PDF están compactados y pueden verse con un software llamado Acrobat Reader de dominio público.

Beneficios adicionales usando PDF.

- Los Archivos PDF pueden ser distribuidos globalmente vía e-mail, el Web, Intranets Corporativas o CD-ROM.
- La navegación en el Acrobat Reader habilita poder revisar los archivos PDF de texto e imágenes.
- En archivos PDF pueden fácilmente verse e imprimirse una página a la vez.

4.8.3. Ghostscript.

L. Peter Deutsch, fundador de Aladdin Enterprise, Menlo Park , California, escribió el intérprete PostScript Nivel 2 y PDF Ghostscript en el lenguaje de programación C. El programa corre en la mayoría de los sistemas operativos incluyendo MS-DOS, Windows 3.x, Windows 95, Windows NT, OS/2, Macintosh, Unix, y VAX/VMS, y ha estado libre de cargos desde su introducción en 1988. Con la ayuda de muchos usuarios y programadores Ghostscript ha llegado a tener gran versatilidad y calidad en interpretación de PostScript. Peter Deutsch contribuyó a la comercialización con perfeccionamientos y apoyo, las capacidades de Ghostscript incluyen:

Ghostscript es una herramienta que nos ayuda a desplegar datos PostScript sobre la pantalla..Esto es útil para examinar gráficas PostScript o para salvar documentos que sean solamente disponibles en formato PostScript. Ghostscript chequea los archivos antes de ser salvados, ¿Están todas las fuentes necesarias allí?, ¿ Están las gráficas bien?, ¿Los archivos contienen todas las páginas?.

Un intérprete separado llamado GSview para Windows y OS/2 o Ghostview para sistemas X Windows simplifica la manipulación de archivos PostScript con la amigabilidad de la interface GUI, con estos programas el usuario puede acceder páginas aleatorias en un documento. Sin ellos Ghostscript despliega las páginas una tras otra, de principio a fin del archivo.

Salida a la impresora. Otra importante tarea de un PostScript es enviar datos PostScript hacia una impresora con capacidades gráficas. La distribución de Ghostscript

contiene una riqueza de drivers para un amplio rango de modelos de impresoras. Desde los más populares hasta los más esotéricos. Una lista de todos los drivers soportados es encontrada en las páginas del manual distribuido con el Ghostscript, estos drivers son una parte integral de Ghostscript y no son relacionados con los drivers de los sistemas Macintosh o Windows.

PDF sobre cualquier plataforma. En la versión 3.33 Ghostscript contiene un intérprete para Formato de Documentos Portables (Portable Document Format **PDF**), de la fundación Adobe Acrobat. Grandes partes del intérprete Ghostscript PDF son escritas en PostScript. Este despliega e imprime archivos PDF y en contenidos iguales regresan a PostScript.

En la versión 4.0 el programa también es capaz de convertir archivos PostScript a PDF. Aunque este rasgo llamado dispositivo pdfwrite, todavía tiene algunas limitaciones, esto es ciertamente un punto importante desde que Ghostscript es el primero y todavía es el único programa gratuito que convierte PostScript a PDF.

Convertidores y Utilidades. Un completo intérprete PostScript junto con controladores satisfactorios y utilerías hechas hacen posible llevar a cabo las operaciones convenientes. Esto incluye despliegue de archivos gráficos en formatos GIF, JPEG, extrayendo los datos en forma textual sobre archivos PostScript o PDF, rastreando PostScript hacia formatos gráficos como TIFF y otros, convirtiendo gráficas EPS hacia formatos editables, y muchas otras mejoras útiles.

4.8.4. Ghostview.

El programa Ghostview provee una interface para el usuario X11 para interpretar Ghostscript. Ghostview y Ghostscript funcionan como dos programas de cooperación simultánea. Ghostview crea las ventanas y Ghostscript dibuja sobre ellas. No se alarme por el número de opciones que generalmente invocan a Ghostview, con los parámetros justos del nombre del archivo este es desplegado. Si el archivo es "-", Ghostview podría leer sobre "stdin". Las opciones proveen un camino para seleccionar recursos X sobre la línea de comandos por una simple invocación del Ghostview

El Centro de Cómputo actualmente hace uso de imágenes gráficas en distintos formatos, que no pueden ser desplegadas ni visualizadas en las PC's, esto provoca que estas imágenes sólo puedan ser visualizadas en los servidores causando un poco de molestia a los usuarios. Además estas no pueden ser editadas, manipuladas o cambiadas de formato de manera fácil y versátil.

Con la instalación de los programas Ghostview y Ghostscript estas imágenes podrán ser desplegadas, editadas y visualizadas sin ningún problema desde cualquier equipo en la red de Cómputo, ya sea desde las estaciones de trabajo Unix o desde forma remota en una PC ya que estos programas serán instalados en los servidores.

4.9. Instalación de software de seguridad.

El sistema operativo UNIX es altamente complejo, por lo que es imposible para los diseñadores prever todas las situaciones que se pueden llegar a presentar. Por otro lado, en muchas ocasiones los administradores y/o los usuarios no tienen plena conciencia de la importancia de la seguridad, o no tienen el conocimiento y el tiempo necesarios para preocuparse por dicho aspecto. Estos factores conducen al hecho innegable de que en general, la seguridad de los sistemas UNIX mal administrados es bastante débil.

Esto, al contrario de lo que mucha gente quiere hacer creer, no se debe tanto a debilidades o deficiencias en el sistema operativo, sino a malas prácticas de administración y uso, provocadas por ignorancia, por falta de tiempo, recursos o de interés.

Son tantos los factores que tienen que ver con la seguridad de un sistema UNIX que es prácticamente imposible para una persona estar vigilando continuamente y de manera eficiente todos los rincones del sistema para ver si no hay nada sospechoso. Por esto son de gran ayuda los programas que permiten realizar parte de esta vigilancia de manera automática, reportando a alguna persona los hallazgos realizados, sobre todo cuando hay algo poco usual en ellos que pudiera indicar un posible hueco de seguridad.

Ningún sistema puede ser completamente seguro y utilizable al mismo tiempo. Se tiene que balancear las preocupaciones contra las necesidades computacionales.

Se puede decidir que la seguridad no es una gran preocupación en nuestro lugar de trabajo, pero no podemos ignorar esto completamente. La información que el administrador protege probablemente tiene algún valor para alguien. Al menos no deseamos que esta se altere o destruya. Otra razón de asegurar los sistemas es prever que estos no sean usados para atacar a otros sistemas en la red.

Pero la seguridad es una responsabilidad compartida. Cada usuario dentro del sistema es capaz de comprometer la seguridad total de los equipos. Ellos necesitan seleccionar buenos passwords, cambiarlos periódicamente, y no compartírselos con nadie. Enseñar a los usuarios a reportar cualquier actividad sospechosa sería un buen principio, por ejemplo si hay información en sus directorios que ellos no hayan colocado ahí, etc.

Los problemas más grandes provienen de los bugs y errores del sistema operativo. Así que es necesario estar seguro de tener buenas políticas de respaldos. ¿Puedo recuperar mi sistema desde un respaldo de cinta?. Si la unidad de cinta falla, ¿se puede recuperar la información en otra unidad de cinta?.

Se puede crear una simple política genérica para los sistemas, que los usuarios puedan prontamente seguir y comprender. Se deben proteger los datos que se salvaguardan, así como se tiene que mantener la privacidad de los usuarios. Algunas preguntas que se deben de realizar antes de empezar a adoptar una política de seguridad son:

¿Qué se quiere proteger?

¿Contra qué se quiere proteger?

¿Cuánto dinero, tiempo y esfuerzo esta dispuesto a invertir para protegerlo?

A continuación sugeriremos algunas de las principales herramientas que un administrador puede utilizar en su tarea de vigilar y mejorar la seguridad general del sistema a nuestro cargo.

Descripción de las herramientas.

4.9.1. PASSWD+. El `passwd` es la primera línea de defensa de una cuenta contra los intentos de acceso no autorizado. Sin embargo en muchas ocasiones la gente tiende a elegir passwords débiles, es decir, que son fácilmente adivinables, como el mismo nombre de la cuenta, el nombre o apellido de la persona, su fecha de nacimiento, el nombre de la esposa o de algún hijo, etc. Esto hace mucho más sencillo para un atacante el acceso a alguna cuenta legítima del sistema, desde donde es mucho más fácil obtener privilegios mayores.

`Passwd+` es un programa que reemplaza al `password` estándar de Unix, cuya función es permitirle al usuario cambiar su `password`. Sin embargo, el `passwd+`, a diferencia del `passwd` (con la excepción de algunas versiones), no permite la elección de `password` débiles, basándose en una serie de reglas definidas por el usuario. Por supuesto, esto no elimina los `passwords` débiles que ya existen en el sistema, pero impide que los nuevos usuarios o los que cambien su `password` hagan una elección fácilmente adivinable. Como el archivo de reglas es modificable por el administrador del sistema, la verificación puede hacerse tan estricta u holgada como se desee.

4.9.2. COPS (Computer and Password System). es una colección de programas, cada uno de los cuales intenta cubrir un área de seguridad distinta. Los puntos principales que se cubren son los siguientes:

- Permisos de archivos, directorios y dispositivos.
- Passwords débiles (fácilmente adivinables).
- Formato, contenido y seguridad de los archivos de `passwords` y de grupos.
- Los programas y archivos utilizados en los archivos `/etc/rc*` (de inicialización del sistema) y `cron` (tareas ejecutadas periódicamente).
- Existencia de archivos con el bit SUID activado, su modificabilidad, y si son o no guiones de shell.
- Una verificación de cambios en los archivos binarios más importantes.
- Permisos de los directorios `home` de los usuarios y los archivos de arranque (`.profile`, `.cshrc`, `.login`, etc.).
- Configuración del servicio `ftp` anónimo, en caso de existir.
- Existencia de `ftpd` sin restricciones, el alias `decode` en `sendmail`, problemas con ejecución de shells en `inetd.conf` y activación de `rex(8)` en `inetd.conf`.

- Verificación de varios aspectos de la cuenta de root: directorio actual en la ruta de programas, un "+" en /etc/hosts.equiv, directorios exportados vía NFS sin restricciones, etc.

Fechas de algunos avisos del CERT (Computer Emergency Response Team) contra algunos archivos claves del sistema. Esta parte verifica la fechas en que algunos huecos de seguridad fueron reportados contra la fecha de los archivos involucrados. Si el archivo, es anterior al aviso, es señal de que puede estar presente dicho hueco, aunque no necesariamente. Sin embargo, si se recibe un aviso positivo, siempre es buena idea obtener el aviso del CERT y revisarlo para obtener más pistas. Por supuesto, si el resultado es negativo, no existe, simplemente que el archivo en cuestión ha sido modificado de alguna manera en fecha posterior al aviso.

Todos los programas solamente avisan a los usuario de los problemas potenciales. COPS no intenta explotar ninguno de los problemas potenciales que encuentra. Solamente envía un mensaje de correo electrónico o crea un archivo conteniendo el reporte de los problemas encontrados.

Como COPS no hace ningún intento de corregir los problemas, no es necesario ejecutarlo con ninguna clase de privilegios especiales. El único programa que es necesario ejecutar con privilegios de root para obtener los mejores resultados es la búsqueda de archivos SUID (para poder revisar todos los subdirectorios existentes) y a veces la verificación de cambios en los ejecutables.

COPS proporciona un método de encontrar errores y malas configuraciones comunes. De ninguna manera puede remplazar a un administrador con sentido común y que esté alerta a lo que sucede en el sistema. Más que otra cosa, COPS puede ayudar al administrador a protegerse contra la ignorancia, la falta de cuidado y ocasionalmente una acción mal intencionada, tanto por parte de los usuarios como de los mismos administradores.

4.9.3. TCP-Wrapper.

Esta herramienta, desarrollada por Wietse Venema, de la Universidad de Eindhoven, en Holanda, permite monitorear y controlar el acceso a los servicios de red ofrecidos en un sistema Unix. Como telnet, ftp, finger, talk, rlogin, y rsh. Una vez instalado el tcpd, toda petición de servicio es registrada con fecha, hora, servicio solicitado y máquina desde la cual se hizo la solicitud. Posteriormente al registro se consultan unas tablas de control de acceso que determinan, en base al tipo de servicio y dirección electrónica de la máquina solicitante, si dicho servicio se debe proporcionar. Finalmente, tanto si el servicio se proporciona como si no, es posible ejecutar algún comando en respuesta a dicho intento de acceso.

En Unix, casi todos los servicios de red son proporcionados por un programa llamado `inetd`, que se arranca al iniciar el sistema y esta corriendo de forma continua.

Cuando inetd detecta alguna petición de servicio, ejecuta el demonio adecuado, tal como el telnetd, ftpd, etc. El funcionamiento del tcpd se basa en modificar el archivo de configuración del inetd (/etc/inetd.conf) de manera que cuando reciba alguna petición, en vez de ejecutar directamente el servidor correspondiente, se ejecute el tcpd, pasándole como argumento el nombre del servicio solicitado. El tcpd hará el registro de la petición de servicio, consultará las tablas de acceso y, si se debe proporcionar el servicio, arrancará el servicio apropiado. Por ejemplo:

```
ftp stream tcp nowait root /usr/etc/ftpd ftpd
```

se convierte en:

```
ftp stream tcp nowait root /usr/etc/tcpd ftpd
```

Aparte de eso, hay que modificar el archivo /etc/syslog.conf para que los mensajes generados por tcpd sean enviados a un archivo apropiado (por ejemplo, /usr/local/adm/tcpd.log). La categoría en que serán generados los mensajes está definido en el archivo Makefile de la distribución de TCP-Wrappers, y viene configurado para generar los mensajes en la categoría mail.info. Sin embargo, conviene modificarla a alguna otra (posiblemente auth.info o local0.info) para poder separar los mensajes del tcpd de los generados por sendmail.

Posteriormente es necesario configurar los archivos de control de acceso, normalmente ubicados en /etc/hosts.allow y /etc/hosts.deny. Con estos archivos se puede especificar a qué servicios y máquinas (y bajo ciertas circunstancias, usuarios) se les otorgarán ciertos servicios, y a cuáles no. Incluso se pueden especificar acciones a tomar cuando alguna de las reglas se cumple. Estas acciones pueden incluir la ejecución de comandos en un shell, imprimir un mensaje al puerto del servicio en cuestión, sustituir el servidor por defecto para ese servicio por otro, etc. Es importante notar que, para obtener toda la flexibilidad de las reglas de control de acceso, es necesario activar la variable STYLE en el archivo Makefile antes de compilar el programa.

La distribución de TCP-Wrappers incluye otros programas que permiten probar las reglas de control de acceso, así como una versión del comando finger que es inmune a respuestas "poco amigables" por parte del servidor (como, por ejemplo, enviar una salida infinita).

Definitivamente, TCP-Wrappers es una herramienta indispensable en todo sistema Unix. Aunque no se impida el acceso a nadie, el sólo hecho de contar con un registro detallado de los servicios solicitados es invaluable, y puede ayudar a rastrear problemas de todo tipo, tales como errores de configuración en el servidor de nombres, errores en la tabla de hosts de la máquina, etc. Para información detallada acerca de la instalación de esta herramienta, consulte la documentación (bastante buena) que viene en la distribución del paquete.

Hasta la fecha no se han dado casos de violación de los equipos pero, es una tarea fundamental de todo administrador prever cualquier tipo de ataque que ponga en riesgo la integridad de los mismos.

Para proteger a los equipos de posibles ataques de seguridad nosotros proponemos dar a conocer a los usuarios los problemas que podemos tener, si no se sigue una política de seguridad interna para la integridad y seguridad de los equipos, ya que esta no solo depende del administrador si no de todos los usuarios que hagan uso de los equipo.

Para esto es necesario aplicar e implantar políticas y software de seguridad que nos ayuden a prever posibles violaciones o ataques que pongan en riesgo la consistencia de la información y de los equipos.

Nosotros recomendamos la utilización de herramientas de seguridad que nos puedan prever de futuros accesos indeseados y que pongan en riesgo la integridad de los equipos y la información contenida en ellos. El objetivo de este planteamiento no es el de describir el funcionamiento de las herramientas de seguridad, sino sólo hacer uso de las más comunes y dejar esta actividad a personas que sean especialistas en el tema.

ESTA TESIS NO DEBE
SALIR DE LA BIBLIOTECA

5

Implementación

5.- Implementación	81
5.1. Realización de respaldos	81
5.2. Compartir archivos a través de NFS	83
5.3. Cuotas	84
5.4. Estandarización de los Sistemas Operativos	86
5.5. Instalación del disco optomagnético externo (Vertex)	90
5.6. Servidores de impresión	90
5.7. Instalación de software para despliegue de imágenes PostScript	91
5.8. Seguridad	91
5.8.1. Buenos passwords	92
5.8.2. Malos passwords	93
5.8.3. Restringiendo el comando su	94
5.8.4. Sistemas de archivos en UNIX	95
5.8.5. Umask	96
5.8.6. Permisos en directorios	96
5.8.7. Herramientas de seguridad	97
5.8.7.1. PASSWD+	97
5.8.7.2. COPS	98
5.8.7.3. TCP-Wrapper	98

Capítulo 5

Implementación

Este capítulo presenta los resultados obtenidos en la resolución de los problemas que se plantearon en el inicio de la presente tesis.

5.1. Realización de respaldos.

Una de las tareas principales que el administrador debe realizar antes de empezar a administrar un Centro de Cómputo es el de mantener y proteger la información de los usuarios.

Todos los días, los usuarios de una red crean, modifican y borran archivos. Cuando un usuario borra un archivo, ya sea por accidente o por decisión propia, este archivo se pierde. Una falla en la energía eléctrica puede dañar el hardware y propiciar la pérdida de información total, *caso que se había suscitado en el Centro de Cómputo*, antes de la realización de dicha tesis.

El primer paso fue la de establecer una política de respaldos de la información de todos los equipos, esto se hizo solamente con una unidad de cinta y varios cartuchos de 8 mm.

Lo primero que realizamos fue un respaldo de nivel 0 o respaldo total de cada una de las estaciones de trabajo. Compartiendo la unidad de cinta para todas las estaciones de trabajo a través de la red (véase la figura 5.1.), dejando conectada la unidad de cinta al servidor Vórtice, realizando en esta estación respaldos locales y utilizando la unidad de cinta conectada a esta estación para la realización de respaldos remotos desde las demás estaciones que están en la red. Estos respaldos se realizan en las noches cuando no hay ninguna carga de trabajo ni usuarios, con la utilidad de *cron* con el fin de que no exista ninguna perturbación ni errores en la integridad de la información al momento de ser respaldados.

Debido a la cantidad de unidades, cintas y al manejo que se tenía en la información por parte de los usuarios, el *respaldo total* se realizaba cada mes, y se realizaba un *respaldo semanal* de las particiones de /home (es la partición en donde reside toda la información de los usuarios y por lo tanto es la que mas importa), por cada máquina.

La decisión que nos llevo a tomar esta política de realización de respaldos semanales fue tomada basándose en pláticas con los usuarios de qué tan importante era para ellos la protección de su información. Los usuarios explicaron que la información que ellos manejaban no variaba mucho de una semana a otra ya que hacían uso de programas en donde solo cambiaban algunas líneas y por lo tanto la información que ellos manejaban no necesitaba una política de respaldo de un alto nivel, como lo puede tener un banco en donde

cada minuto la información esta cambiando, por lo tanto la política de respaldos semanal estaba correcta, sin olvidar la integridad de los datos.

RESPALDOS

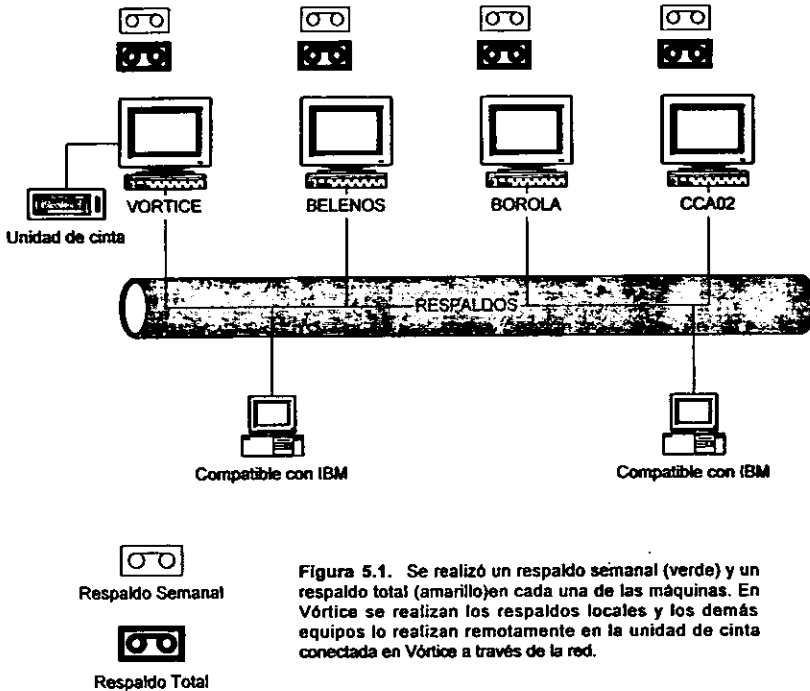


Figura 5.1. Se realizó un respaldo semanal (verde) y un respaldo total (amarillo) en cada una de las máquinas. En Vórtice se realizan los respaldos locales y los demás equipos lo realizan remotamente en la unidad de cinta conectada en Vórtice a través de la red.

Otra consideración que siempre se tomo en cuenta fue la de realizar un respaldo completo antes de hacer modificaciones al kernel, instalar nuevos paquetes de aplicaciones, instalar nuevas versiones o actualizaciones del sistema operativo para poder recuperar la funcionalidad del sistema, ya que en caso de que algún procedimiento no funcione correctamente, la información puede ser recuperada de manera eficiente y en el menor tiempo posible.

Una vez tomada la política de realización de respaldos, cada unidad de cinta de 8mm fue etiquetada y marcada con un código de colores que nosotros decidimos, en donde los *respaldos semanales* fueron etiquetados con colores *verdes* y se coloca el nombre de la máquina así como se colocaba la fecha de realización de cada respaldo, y etiquetas de color *amarillo* para *respaldos de nivel cero o totales* en donde también se le colocaba el nombre de la máquina y la fecha de realización de respaldo (véase figura 5.1.), tomando en cuenta que el sistema también guardaba una bitácora de la última fecha de realización de respaldo.

Resultados:

Con esta política se dio el primer paso para empezar a trabajar íntegramente con los sistemas de manera segura dando confianza a los usuarios y al administrador, en la prevención de cualquier imprevisto en la consistencia de la información.

5.2. Compartir archivos a través de NFS.

El sistema de archivos en red es un servicio que permite a los usuarios tener acceso a jerarquías de archivos en el servidor como si estos fueran locales. Las jerarquías de archivos pueden ser sistemas de archivos completos o directorios individuales. Los sistemas que participan dentro de NFS pueden ser heterogéneos. Con NFS se permite que múltiples computadoras puedan usar los mismos archivos, permitiendo que los mismos datos puedan ser accedidos por todos a través de la red.

Se hizo uso de NFS para compartir, exportar y montar sistemas de archivos a través de la red.

Lo primero que se realizó fue compartir las particiones en donde estaba la información de mas común acceso vía NFS, las particiones fueron exportadas y montadas en los equipos que necesitaban el uso de esta información.

Con la incorporación de la unidad de disco optomagnético (Vertex) que se describirá más adelante, la información de mayor tamaño como bases de datos serán instaladas, exportadas y montadas a través de NFS, ya que Unix ve a la unidad de disco optomagnético como una unidad de disco duro propia, lo cual nos permite montar y exportar esta unidad sin ningún problema.

Los resultados obtenidos con la utilización de NFS fueron los siguientes:

- Se logró que las estaciones de trabajo Sun pudieran usar los mismos archivos, permitiendo que los mismos datos puedan ser accedidos por todos a través de la red.
- Reducción de los costos de almacenamiento por tener computadoras compartiendo aplicaciones en vez de tener espacio de disco local para cada aplicación del usuario.
- Se logró la rentabilidad de los equipos, ya que todos los usuarios pueden leer el mismo conjunto de archivos.
- El montaje de sistemas de archivos es transparente para los usuarios.
- Los accesos remotos de los sistemas de archivos son transparentes para los usuarios.

El sistema NFS hace que la localización física de los sistemas de archivos sea irrelevante para el usuario. NFS puede usarse para habilitar a los usuarios para que puedan ver todos los archivos relevantes, sin considerar la localización, en vez de tener copias de los archivos mas comúnmente usados sobre distintos sistemas de archivos, NFS permite

tener una sola copia de este archivo en un solo lugar de disco accedendo esta a través de la red. Bajo la operación de NFS, los sistemas de archivos remotos son indistinguibles sobre un sistema local.

5.3. Cuotas.

En los sistemas en donde no se tienen compartidas las aplicaciones de red es muy común tener gran cantidad de duplicidad de información. Duplicidad que en muchas casos se reciente en la productividad de los equipos ya que estos generalmente siempre llegan a estar a su máxima capacidad en su uso de disco en tiempos extremadamente cortos.

Históricamente cualquier unidad de almacenamiento que se le proporcione a un usuario es usada a su máxima capacidad en intervalos de tiempo relativamente cortos sin que la productividad presente un crecimiento notable con dicha adquisición.

La mayoría de los usuarios hacen uso de todos los recursos disponibles a su alcance sin escatimar ni depurar la información contenida en ellos, llegando en algunas ocasiones a monopolizar los sistemas de archivos. Estos recursos son de gran valor para cualquier Centro de Cómputo ya que cada Byte de información contenido en cada dispositivo tiene un costo no solo cuantitativo sino productivo, y en muchas ocasiones cuando se intenta instalar nuevas aplicaciones, no es relativamente fácil ya que no hay espacio disponible.

Diariamente los usuarios hacen uso del sistema generando grandes cantidades de información. Información que sufre día con día cambios y que en muchas ocasiones el usuario opta por generar otros directorios para guardar dicha información, para después revisarla cuando este tenga tiempo libre (esto rara vez llega a suceder).

Para que se logre mantener un control en el crecimiento y almacenamiento de información es necesario el uso de cuotas en el uso de disco. Este tipo de cuotas son útiles para que el administrador pueda mantener un control con los usuarios en el crecimiento de información, para prever y proteger los sistemas en futuros crecimientos.

Un problema que se presentó al empezar a administrar estos equipos fue que casi todos los sistemas estaban a su máxima capacidad en uso de disco en la mayoría de las particiones. Problema que daba como resultado que los sistemas de archivos llegaran a estar al 100% de su capacidad y que por lo tanto el sistema se diera de baja por razones de diseño de Unix, además de que por todas las particiones existieran archivos y directorios personales de diferentes usuarios. Si no había espacio en home creaban directorios en otras particiones.

En muchas ocasiones se logró detectar que cada usuario tenía los mismos archivos en cada una de las máquinas en donde tenía algún tipo de cuenta, en algunos casos se detectó que inclusive algunos servidores eran utilizados como máquinas de respaldos de sus propios directorios.

Este tipo de actitudes fueron tomadas por los usuarios a raíz de la pérdida total de su información, ya que como habíamos descrito anteriormente había existido dicho accidente.

En otros casos este tipo de actitud era por falta de una cultura informática en cuestión de uso compartido de disco y conceptos fundamentales de redes.

El objetivo de las cuotas es:

- Asignar a cada usuario una cuota en el uso del disco y forzarlos a depurar su información, ya que con el uso de cuotas, el usuario no puede usar más del espacio que se le asigne en su cuenta.
- Evitar la duplicidad de información, ya que las políticas de respaldos y la compartición de recursos a través de la red vía NFS ya están funcionando y no es necesario almacenar o respaldar su información en otras máquinas.
- Forzar a los usuarios a que cambien su información a sus directorios y no la dejen por todo el sistema.

Para resolver este problema se realizó lo siguiente:

1. - Aviso de la realización de respaldos totales de todos los equipos.
2. - Asignación de cuotas basándose en la carga de trabajo de cada usuario, y a la cantidad de disco disponible en cada sistema, esta fue impuesta por el responsable del proyecto del Centro de Cómputo.
3. - Aviso de la cantidad de espacio asignada a cada usuario.
4. - Aviso de depurar sus cuentas y sobre todo su correo, con una semana de anticipación para que depuren su información, ya que de lo contrario no se podrá escribir ni modificar ningún tipo de información si su home sobrepasa dicha cuota.
5. - Aviso de guardar en su home toda la información distribuida en los sistemas, ya que de lo contrario toda información que estuviera en particiones del sistema como /var, /usr / o cualquier otra partición sería borrada.
6. - Envío por correo electrónico de herramientas y procedimientos del sistema para la compactación de información.
7. - Depuración de cada una de las particiones, borrando archivos que no fueran propios del sistema

Resultados.

Se logró que cada uno de los usuarios depurara su información liberando un poco los sistemas de archivos. También se les transmitió una política de depuración y compactación de la información con la cual se logró que cada uno de los usuarios comprendiera el valor que tiene el uso de disco y sobre todo en estas estaciones de trabajo.

Otro punto es que se detectaron varios directorios duplicados, olvidados y con versiones pasadas, los cuales fueron eliminados de los equipos, no sin antes haber hecho una notificación al dueño del directorio.

5.4. Estandarización de los Sistemas Operativos.

Uno de los grandes problemas que tiene este Centro de Cómputo es la falta de estandarización tanto de los sistemas operativos como de las aplicaciones instaladas, sin tomar en cuenta que no se tienen los discos del sistema operativo original, que son de gran importancia en momentos críticos de falla de los equipos.

El objetivo del presente subcapítulo es estandarizar los sistemas operativos a la versión de Solaris 2.5.1. fundamentada en las investigaciones realizadas en los capítulos anteriores y describiendo los cambios de las versiones en el apéndice B al final de la presente tesis.

Lo primero que realizamos en el proceso de estandarización de los equipos, fue lo siguiente:

Borola. S.O. Solaris 2.5.1.



Ultra 2 / Creator 3D

- Pruebas de instalación del Sistema Operativo.

En este punto se realizaron pruebas en la instalación del sistema operativo, tomando en cuenta los procedimientos que se describen en el apéndice A de la presente tesis, y los cambios significativos de algunos comandos descritos en el apéndice B.

- Se verificaron las mejoras que se habían investigado en los capítulos anteriores, así como también nos familiarizamos con el sistema operativo en su uso y manejo.
- Pruebas en la instalación de nuevas versiones de software.
Se realizaron pruebas de instalación de las nuevas versiones de software y se verificó qué diferencia había entre las versiones antiguas y las nuevas. En este punto se pidió a los usuarios que probaran algunas de sus aplicaciones y que realizaran pruebas con las nuevas versiones ya que ellos son los conocedores de estas aplicaciones y son los usuarios finales, mencionado alguna inconsistencia que esta pudiera tener.
- Compilación de Ghostview y el Ghostscript para el despliegue de imágenes PostScript sobre equipos PC's. Con la compilación de este software fue posible el despliegue de imágenes PostScript desde los equipos PC's.
- Instalación del servicio de impresión a través del servidor multiprotocolos Axis 550 NPS. Con la instalación del servidor multiprotocolos Axis NPS 550 se logró que se pudiera imprimir desde cualquier punto de la red a un par de impresoras que están físicamente conectadas al servidor de impresión Axis y no a una estación de trabajo, liberando a estas de mayor carga de trabajo. La impresión se realizó desde estaciones Unix, así como de equipos PC's sin que hubiera ningún problema.

- Instalación del disco optomagnético (Vertex). Se instaló el equipo optomagnético, en la estación de trabajo Borola, en el cual se realizaron pruebas de respaldo y recuperación de información de sistemas de archivos completos.

También se logró comprobar que los tiempos de lectura y escritura en los respaldos eran superiores a los de una cinta de 8mm y mayores a los de un disco propio del sistema.

Uno de los usos principales que se le dio a este disco fue el de instalación de bases de datos de gran tamaño, las cuales fueron compartidas, montadas y exportadas a través de NFS a todos los demás equipos sin que hubiera ningún problema en la diferencia de versiones de sistemas operativos.

- Recuperación de respaldos de particiones de home. Se realizaron pruebas de recuperación de homes de todos los equipos y usuarios, sobre todo en las versiones más antiguas del sistema operativo, con el fin de verificar qué cambios y problemas podríamos tener con la migración del nuevo sistema operativo.
- Realización de respaldos totales y semanales de acuerdo a lo descrito en la sección de respaldos.
- Realización de pruebas por parte de los usuarios, en donde estos realizaron pruebas de las nuevas versiones tanto de sistema operativo como de software instalado, y uso de su información que fue recuperada por los respaldos, en donde los usuarios reportaron cualquier inconsistencia en el comportamiento del equipo.

En el mes de pruebas que se tuvo en este equipo no se reportaron cambios drásticos en el manejo de la información, tanto en el uso de software como en la recuperación de información, y no se reportó ninguna inconsistencia en la integridad de la información ni pérdidas totales, ó parciales.

El proceso de migración fue transparente para los usuarios, los cuales no resintieron un cambio notable en la utilización de las nuevas versiones de software instaladas en el equipo Borola.

Una vez que fue probado el equipo se puso a punto y se tomó como modelo para la migración total de todos los demás sistemas a la nueva versión del sistema operativo no se reportó ninguna inconsistencia en la integridad de la información ni pérdidas totales, ó parciales.

La nueva versión del sistema operativo resultó ser más amigable para los usuarios ya que esta proporciona un ambiente gráfico y contiene más herramientas que ayudan al trabajo y mejor desempeño de cada usuario.

Una vez hechas las pruebas e instalaciones necesarias para que el equipo pudiera funcionar y los usuarios pudieran trabajar de manera correcta, se realizaron las siguientes tareas:

- Planeación de migración de las máquinas
- Asignación de claves y espacio en disco para cada usuario.
- Realización de respaldos totales de cada máquina, se realizaron dos respaldos totales por cada máquina y un respaldo de las particiones más importantes en cinta y en el disco optomagnético (Vertex).
- Aviso a los usuarios de la migración de los equipos y las consecuencias que esto tendrá en su trabajo.
- Aviso de la suspensión de servicio de cada máquina a la que se fue realizado el proceso de migración, en base a un calendario previamente enviado a los usuarios vía correo electrónico y contestación de enterados

En base de importancia en la tareas realizadas dentro del Centro, el siguiente equipo que tuvo un proceso de migración fue Vórtice en el cual realizamos las siguientes actividades:

Vórtice. 2.4 a 2.5.1



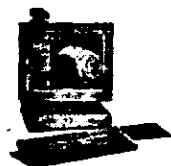
El tiempo de instalación y puesta en marcha total del equipo fue de dos días completos de trabajo, ya que tuvimos un mes de pruebas de instalación de software y aplicaciones

Después de la instalación y liberación de los equipos los usuarios tuvieron dos semanas de pruebas con los equipos y verificación de la integridad de los sistemas y de sus cuentas.

En este proceso no se reportó ninguna inconsistencia en la información ni ninguna anomalía por parte del equipo. Se llevaron al cabo todos los puntos propuestos en el capítulo 4.5. en lo concerniente a Vórtice.

Una vez puesto en marcha el equipo Vórtice se dio paso a migrar uno de los dos equipos con la versión y aplicaciones más antiguas del Centro.

Belenos. 4.1.3 a 2.5.1



El procedimiento que se siguió en el proceso de migración fue basado en las investigaciones realizadas en los capítulos anteriores y en las tablas comparativas que se describen el apéndice B.

El tiempo de instalación y puesta en marcha total del equipo fue de dos días, para echar a andar totalmente los equipos. Una vez liberado

el equipo, se dio dos semanas a los usuarios para verificar la integridad y consistencia de su información.

En este proceso no se reportó ninguna inconsistencia en la información ni ninguna anomalía por parte del equipo, se lograron cubrir todos los puntos descritos en el capítulo 4.5. concerniente a Belenos..

Con la puesta en marcha de estos tres equipos se dio un gran paso en el proceso de migración y estandarización de los mismos.

Una vez puesto en marcha el equipo Belenos el siguiente equipo que será tendría el proceso de migración era CCA02.

CCA02. 4.1.3



En este equipo el proceso de migración no se llevó al cabo, ya que existen algunos programas propios de los investigadores que no funcionan en las nuevas versiones del Sistema Operativo. La decisión fue hecha por los mismos investigadores ya que aún no habían probado programas los programas escritos para Solaris 4.1.3. en la nueva versión del Sistema Operativo. Estas viejas aplicaciones no han podido ser rescritas para la nueva versión, ya que en su mayoría son programas que fueron escritos en Estados Unidos, por lo que no se conoce muy bien el código en que fueron hechos.

Además, los programas no son de mucha trascendencia para el funcionamiento del Centro de Cómputo, pero son muy importantes para la recuperación de algunas bases de datos que son utilizadas por los investigadores. La tarea de reestructuración de código se dejó en manos de los investigadores, ya que ellos son los que conocen más afondo como funcionan dichos programas y, además, tienen más experiencia en la programación de Fortran 77, lenguaje en que fueron escritos los programas.

El propósito de la presente tesis es administrar los equipos de Cómputo y no la de programar en Lenguaje Fortran 77, es por eso que esta función se deja en manos de los programadores del Centro de Cómputo, ya que ellos tienen mayor experiencia en el uso del lenguaje de programación.

Para ayudar a los investigadores se realizó la tabla de equivalencias de comandos entre Solaris 2.5.1 y Solaris 4.1.3 descrita en el apéndice B de la presente tesis.

Lo único que se hizo con este equipo fue la realización de respaldos remotos de acuerdo a la política establecida y la compartición de bases de datos a través de NFS del disco optomagnético, así como las tareas normales de administración.

Regino. S.O. Solaris 2.5.1.



Este es el último equipo que será incorporado a la red de Cómputo, con este equipo daremos por terminado el proceso de migración en la red de Cómputo. Los procedimientos que realizamos en este equipo fueron los planteados en el capítulo 4.5. concerniente a Regino

Con la instalación de este último equipo se dio por terminado la fase de estandarización de sistemas operativos y aplicaciones.

La puesta en marcha de dicho equipo fue la más fácil y rápida que se tuvo en el proceso de migración, gracias a la experiencia obtenida en el proceso de instalación de los equipos anteriores.

5.5. Instalación del disco optomagnético externo (Vertex).

Para solucionar el problema descrito en el capítulo 4.6. se hizo uso del disco optomagnético el cual fue instalado, configurado, montado, compartido y exportado en el equipo Borola como una expansión más de disco duro sin que se tuviera ningún problema en el proceso de instalación.

El uso principal que se le dio a este dispositivo fue el de instalación de grandes bases de datos que eran cambiadas de acuerdo al uso que estas tuvieran por parte de los investigadores, así como de compartir esta información con los demás sistemas vía NFS, sin importar la versión de sistema operativo de forma transparente, sin que se presentara ningún problema gracias a las características propias de NFS y del dispositivo.

Otro uso que se le dio a este dispositivo fue el de realización de respaldos de información y sobre todo en el proceso de migración este dispositivo fue ampliamente utilizado gracias a los tiempos de escritura y lectura que eran superiores a los tiempos de recuperación a través de cinta de 8mm y a la flexibilidad que este dispositivo permite en este tipo de acciones.

Los resultados obtenidos fueron los previstos en las investigaciones, logrando instalar dicho dispositivo como una extensión de disco duro y poder montar, compartir y exportar el disco óptico a través de NFS sin que se presentara ningún problema.

5.6. Servidores de impresión.

De acuerdo con las investigaciones realizadas en el capítulo 4, el servicio de impresión fue habilitado por medio del servidor de impresión Axis NPS 550, ya que debido a las características de diseño y flexibilidad de impresión multiprotocolos que el equipo presentaba se pudo activar el servicio de manera eficaz y transparente tanto para los sistemas como para los usuarios, ya que es posible realizar impresiones desde cualquier estación de trabajo Sun o equipo PC's sin que el proceso presente alguna falla o anomalía.

El problema que se resolvió, fue la simplificación del proceso de impresión ya que el servidor puede ser conectado en cualquier parte en donde exista algún punto de red, sin que este tenga que estar conectado físicamente a una estación de trabajo o equipo PC para que se puede imprimir algún documento. Además el proceso de impresión es transparente para el usuario, ya que no se tiene que especificar que el archivo a imprimir proviene de un equipo Sun con TCP/IP o desde un equipo PC's con protocolo NetBeui de Microsoft, este protocolo NetBeui lo usan las computadoras con Windows 3.11 o Windows 95 siempre y cuando lo tengan configurado.

5.7. Instalación de software para despliegue de imágenes postscript.

El Centro de Cómputo hace gran uso de imágenes hechas en distintos formatos gráficos y sobre todo en formatos PostScript que necesitan ser desplegadas desde equipos PC's por accesos remotos a las estaciones, ya que las estaciones no son suficientes para que todos los usuarios puedan trabajar en ellas

Solución:

Para resolver estos problemas nosotros instalamos los programas Ghostview y Ghostscript, los cuales nos ayudaron a desplegar, editar y visualizar imágenes PostScript sin ningún problema desde cualquier equipo en la red de Cómputo, ya sea desde las estaciones de trabajo Unix o desde forma remota en una PC, ya que estos programas fueron instalados en los estaciones de trabajo Sun.

Este software no se instaló en cada una de las estaciones de trabajo, solamente se instaló en el equipo Borola y se compartió con los demás equipos vía NFS.

5.8. Seguridad.

Una vez que se puso en marcha los equipos con las políticas descritas anteriormente el punto final en la administración de este Centro de Cómputo fue la de instalar utilerías de seguridad que nos ayudarán a prever posibles ataques, accesos indeseados e inclusive alteración de información por mínima que esta fuera.

Sabemos que el sistema operativo UNIX es altamente complejo, por lo que es imposible para los diseñadores prever todas las situaciones que se pueden llegar a presentar.

Por otro lado, en muchas ocasiones los administradores y/o los usuarios no tienen plena conciencia de la importancia de la seguridad, o no tienen el conocimiento y el tiempo necesarios para preocuparse por dicho aspecto. Estos factores conducen al hecho innegable de que en general, la seguridad de los sistemas UNIX mal administrados es bastante débil.

Sabemos que la seguridad es una responsabilidad compartida. Cada usuario dentro del sistema es capaz de comprometer la seguridad total de los equipos. Ellos necesitan seleccionar buenos passwords, cambiarlos periódicamente, y no compartirlos con nadie.

Las preguntas que hicimos para adoptar una política de seguridad fueron las siguientes.

¿Qué se quiere proteger? Lo que deseamos proteger es la integridad y protección de los datos dentro del Centro de Cómputo.

¿Contra que se quiere proteger? Contra accesos indebidos por parte de los mismos usuarios y contra posibles ataques de personas ajenas al Centro de Cómputo.

¿Cuánto dinero, tiempo y esfuerzo esta dispuesto a invertir para protegerlo?

Ningún tipo de recurso económico será destinado a la implementación de la seguridad, por lo que el tiempo y esfuerzo será el necesario para instalación de una seguridad básica que nos ayude a prever cualquier tipo de alteración o violación de la integridad de los equipos.

Passwords

La primer línea de seguridad que nosotros implementamos fue una política de uso de buenos passwords por parte de los usuarios, ya que es el primer paso para evitar accesos indebidos dentro del sistema. Esto significó enseñar a los usuarios a seleccionar buenos passwords y asegurarse de que ellos adopten esta política.

5.8.1. Buenos passwords.

Los buenos passwords son aquellos que son fáciles de recordar. En general un buen password es:

- Que no tenga palabras o frases lógicas.
- Difícil de adivinar.
- Fácilmente recordable.
- Incluye metacaracteres.
- Combina palabras cortas.
- Incluye números, mayúsculas, minúsculas.
- Incluye signos de puntuación.
- Es compuesto por algún acrónimo.
- Si se usa el mismo password en varias máquinas variarlo ligeramente en cada una de ellas.
- NUNCA mandarlo por correo electrónico.
- No escribir el password en papeles pegados en la computadora o en algún otro lugar que este a la mano de cualquier persona.

Si alguna persona tratara de adivinar un password con estas características realizándolo en una máquina que pueda realizar una comparación de 1 millón de passwords por segundo (la mayoría de las máquinas pueden hacer esto en cantidades de mil millones de passwords por segundo), podría requerir de cerca de cien años para completarlo.

A todos los usuarios de los equipos también se les sugirió que si debían escribir su password que este no fuera fácilmente recordable, realizar lo siguiente:

- No identificarlos como tal
- No escribir a qué máquina o cuenta pertenece.
- No pegar un papelito en la máquina.
- Mezclar caracteres aleatorios.
- Nunca enviarlo por correo electrónico ni con PGP (Pretty Good Privacy - Privacidad Muy Buena) o talk , hacer esto vía telefónica.

5.8.2. Malos passwords.

Un mal password es cualquiera que sea fácilmente adivinable, la guía que se les proporcionó a los usuarios sobre la selección de malos passwords fue la siguiente.

- Su nombre.
- El nombre de su esposa.
- El nombre de sus parientes.
- Nombre de su mascota.
- El nombre de sus hijos.
- El nombre de viejos amigos o compañeros de trabajo.
- El nombre de su fantasía favorita.
- El nombre de su jefe.
- El uso de cualquier nombre.
- El nombre del sistema operativo que se esta usando.
- El nombre de la computadora que se esta usando.
- Su número telefónico.
- El número de su licencia para conducir.
- Cualquier parte del número de seguro social.
- Fechas de nacimiento.
- Otra información que sea fácilmente obtenida de la persona.
- Palabras como güru, wizard, dios o cosas por el estilo.
- Cualquier palabra del diccionario.
- Palabras de diccionarios extranjeros.
- Nombre propio.
- Simples cadenas del teclado, como qwerty.

Todas estas recomendaciones fueron hechas ya que un significativo porcentaje de todas las computadoras contienen por lo menos una cuenta en donde el nombre del usuario y el password es el mismo.

La mayoría de los ^{*} crackers pueden encontrar un punto de entrada dentro de cualquier sistema simplemente con verificar cada cuenta, y darle el nombre del usuario.

El siguiente programa en C puede buscar dentro de la computadora, cuentas con el nombre de usuario y password similar, así como de detectar cuentas sin passwords.

/ busca.c : Programa que busca cuentas con el mismo nombre de usuario y password. */*

```
#include <stdio.h>
#include <pwd.h>
int main(argc,argv)
char **argv;
{
    struct passwd*pw;

    while(pw=getpwent()){
        char *crypt();
        char *result;

        if(pw->pw_passwd[0]==0){
            printf("%s Cuenta sin password\n", pw->_name);
            continue;
        }
        result = crypt(pw->pw_name,pw->pw_passwd);
        if(!strcmp(result,pw->pw_passwd)){
            printf("%s Cuenta con el mismo password\n",pw->pw_name);
        }
    }
}
```

5.8.3. Restringiendo el comando su.

En cuanto al password de root este se restringió a que solo fuera usado por nosotros y por el encargado del Centro de Cómputo de manera que si alguien intentaba tomar la

-
- **cracker:** Entusiasta aficionado a las computadoras cuya diversión estriba en aprender todo acerca de un sistema de computación y, mediante una programación hábil se dedican a violar sistemas de seguridad causándoles daños.
 - **Hacker:** Entusiasta aficionado a las computadoras cuya diversión estriba en aprender todo acerca de un sistema de computación y, mediante una programación hábil, llevar el sistema al nivel máximo de rendimiento.
 - **Phreaker:** Persona que usa comunicaciones sin pagarlas o pagando menos de lo que corresponde.
 - **Joker:** Persona que se dedica a bromer en la red, como por ejemplo mandando correos que inundan la red con mensajes sin sentido alguno.

personalidad de root este no lo podría realizar. Esto se realizó con la restricción de uso del comando **su** por parte de los usuarios, ya que este solo podía ser ejecutado por nosotros y el encargado del Centro de Cómputo.

```
# chmod 4554 /usr/bin/su
```

Si alguna persona intentaba hacer uso de este comando se podía detectar con la ayuda de las bitácoras del sistema, en las cuales aparecen los malos intentos por parte de los usuarios que trataron de entrar a la cuenta de **su** sin autorización.

Las bitácoras que se registraban periódicamente eran:
/usr/adm/messages
/usr/adm/sulog

5.8.4. Sistemas de archivos en UNIX.

Para ayudar a los usuarios a proteger sus archivos se les indicó que los permisos de lectura, escritura y ejecución tienen significados específicos para los archivos, como se muestra en la siguiente tabla:

Símbolo	Permiso	Significado
r	Lectura	Se puede abrir el archivo con open y leer su contenido con read.
w	Escritura	Se puede sobre escribir el archivo o modificar su contenido. Se puede usar write, truncate y ftruncate para modificar su longitud.
x	Ejecución	Solo puede ser utilizado por programas. El archivo se puede ejecutar tecleando su ruta, o mediante algunas de las funciones de exec. Como se ejecuta, depende de los dos primeros bytes del archivo.

Si un archivo tiene accesos de **escritura**, se puede escribir información en el archivo o hacia otro objeto, si se tiene permisos de **lectura**, su puede leer sobre este, y si no se tiene ningún permiso no se puede hacer nada sobre este archivo.

Notas: Se pueden tener accesos de ejecución sin tener accesos de escritura, en este caso, se puede correr un programa sin leer este. Esto es útil en caso de que se desee esconder la función de un programa. Otra razón para hacer esto es permitir a las personas ejecutar un programa sin permitir que ellos hagan la copia de un programa.

Si se tiene permisos de lectura pero no de ejecución, se puede hacer una copia del archivo y correrlo por si mismo. La copia sin embargo podría ser diferente por dos path importantes, esta podría tener un pathname diferente y podría no ser poseído por otra persona, sino solamente por el programador original.

5.8.5. Umask.

El umask (user file creation mask) es un número octal de tres dígitos que Unix usa para determinar los permisos que tendrá un archivo recién creado. Cada proceso contiene su propio umask. El umask especifica los permisos que no se quiere dar por default a los archivos o directorios que sean creados. El modo especificado por el programa que crea el archivo es modificado de acuerdo al umask del proceso.

Para esto nosotros como administradores tomamos la decisión de poner el valor umask a **022** de acuerdo a la siguiente tabla.

Umask	Usuario	Grupo	Otros
0000	rwX	rwX	rwX
0002	rw-	rw-	r--
0007	rw-	rw-	---
0022	rw-	r--	r--
0037	rw-	r--	---
0077	rw-	---	---

5.8.6. Permisos en directorios.

Los directorios son interpretados como caminos especiales por el sistema de archivos, los cuales tienen significados especiales.

Símbolo	Permiso	Significado
r	Lectura	Se puede usar <code>opendir</code> y <code>readdir</code> o el comando <code>ls</code> para ver qué archivos existen en el directorio.
w	Escritura	Se pueden añadir y borrar archivos del directorio.
x	Ejecución	Se puede usar <code>stat</code> para determinar los dueños y los archivos que existen en el directorio actual, y se pueden abrir archivos dentro de este directorio.

Para esto se les dio la siguiente guía.

Si se desea prevenir que otros usuarios lean el contenido de sus archivos, se tiene que realizar lo siguiente:

1.- Se puede seleccionar los permisos para cada archivo con 0600, así que solamente el dueño tiene permisos de lectura y escritura.

2.- Se pueden poner archivos en un directorio si se selecciona los permisos del directorio a 700, así otro usuario puede acceder a los archivos.

5.8.7. Herramientas de seguridad.

Unix no fue diseñado desde el principio para ser seguro. Fue diseñado con las características necesarias para poder darle mantenimiento a la seguridad.

Dennis Ritchie.

Debido a las muchas “historias de terror” existentes sobre problemas de seguridad de Unix, gran parte de la comunidad computacional tiene la convicción de que la frase “Seguridad en Unix” no existe.

Sin embargo todos los huecos de seguridad que han sido encontrados en Unix han resultado de fallas en programas individuales, o en las interacciones entre ellos, y de fallas en los sistemas operativos. La reputación de Unix como sistema inseguro no viene de sus diseño sino de la práctica. Durante sus primeros 15 años, Unix fue usado principalmente en ambientes académicos, en los que la seguridad no era una preocupación.

Desafortunadamente, debido a su diseño, una falla en un solo programa Unix puede comprometer la seguridad de todo el sistema.

Es por eso que es necesaria una vigilancia y atención constantes para mantener un sistema funcionando en forma segura.

Para resolver este problema, nosotros realizamos la instalación de herramientas de seguridad que nos ayudaran a prever ataques no deseados y verificar los bugs del sistema.

5.8.7.1. PASSWD+.

La primer herramienta que se instaló en el Centro de Cómputo fue el **passwd+** el cual, es la primera línea de defensa de una cuenta contra los intentos de acceso no autorizados. Para esto nos apoyamos en la elección de buenos passwords descrita en el tema anterior, pero sin embargo sabemos que en algunas ocasiones los usuarios tienden a elegir passwords débiles, es decir, que son fácilmente adivinables, como el mismo nombre de la cuenta, el nombre o apellido de la persona, su fecha de nacimiento, el nombre de la esposa o de algún hijo, etc. Con la instalación de esta herramienta es mucho más difícil, para un

atacante el acceso a alguna cuenta legítima del sistema, desde donde es mucho más fácil obtener privilegios mayores.

Con la ayuda de **passwd+** se logró que los usuarios no utilizaran passwords débiles, por supuesto, esto no elimina los passwords débiles que ya existen en el sistema, pero impide que los nuevos usuarios o los que cambien su passwd hagan una elección fácilmente adivinable. Como el archivo de reglas es modificable por el administrador del sistema, la verificación puede hacerse tan estricta u holgada como se desee. Es este caso nosotros implementamos una política estricta en el uso de passwords.

5.8.7.2. COPS.

La segunda herramienta que se instaló dentro del sistema fue COPS con la cual cubrimos los siguientes puntos principales:

- Permisos de archivos, directorios y dispositivos.
- Passwords débiles (fácilmente adivinables).
- Formato, contenido y seguridad de los archivos de passwords y de grupos.
- Los programas y archivos utilizados en los archivos `/etc/rc*` (de inicialización del sistema) y `cron` (tareas ejecutadas periódicamente).
- Existencia de archivos con el bit SUID activado, su modificabilidad, y si son o no guiones de shell.
- La verificación de cambios en los archivos binarios más importantes.
- Permisos de los directorios `home` de los usuarios y los archivos de arranque (`.profile`, `.cshrc`, `.login`, etc.).
- Verificación de varios aspectos de la cuenta de `root`: directorio actual en la ruta de búsqueda de programas, un "+" en `/etc/hosts.equiv`, directorios exportados via NFS sin restricciones, etc.

Con la instalación y ejecución de COPS, se pudieron detectar y prever algunas fallas de seguridad del sistema, aunque sabemos que este software ya no es mantenido por sus creadores, es una buena herramienta en la ayuda de prevención de fallas de seguridad, ya que el archivo generado a su ejecución genera un reporte de su actividad en el cual se avisa sobre algunas inconsistencias del sistema, las cuales pueden ser reparadas por el administrador y ser notificado cada vez que este corre el programa.

5.8.7.3. TCP-Wrapper.

La última herramienta que fue instalada dentro de los sistemas fue TCP-Wrapper. Con la instalación de este software se pudo controlar y monitorear el acceso a varios de los servicios de red por Unix. Como `telnet`, `ftp`, `finger`, `talk`, `rlogin`, y `rsh`. Una vez que se instaló el `tcpd`, toda petición de servicio se registró con fecha, hora, servicio solicitado y máquina desde la cual se hizo la solicitud.

Las ventajas que se tuvieron en la instalación de este software fueron:

- Controlar los accesos al sistema (Como telnet, ftp, talk, rlogin, rsh).
- Obtención de una bitácora de las máquinas que están entrando y saliendo del sistema.
- Realización de tablas de los equipos que pueden y no pueden entrar al sistema.

Este es el punto final en la instalación de la seguridad básica que se propuso en el capítulo 4, y que cumple con las normas de seguridad elementales que cualquier Centro de Cómputo con equipo Unix debe de implementar.

Con este punto nosotros cumplimos en solucionar la problemática que pudiera tener el Centro de Cómputo en cuestiones de Seguridad e integridad de los equipos.

Resultados y Conclusiones

Resultados.

Con la implantación de una política de respaldos se logro empezar a trabajar íntegramente con los sistemas de manera segura ya que es posible recuperar la información, perdida accidental o intencionalmente, dando confianza a los usuarios y al administrador, en la prevención de cualquier imprevisto en la consistencia de la información.

La instalación de la unidad de disco optomagnético (Vertex), nos permitió instalar las bases de datos de gran tamaño que fueron compartidas a través de NFS, sin que se presentara ningún problema para los usuarios, ya que este es un procedimiento transparente para ellos así como también fue de utilidad en el proceso de migración debido a que en este dispositivo se realizaron respaldos de información..

El disco optomagnético y otras aplicaciones fueron montados, compartidos y exportados a través de NFS, los resultados obtenidos con la utilización de NFS fueron los siguientes:

- Se logró que las estaciones de trabajo **Sun** pudieran usar los mismos archivos, permitiendo que los mismos datos puedan ser accedados por todos a través de la red.
- Reducción de los costos de almacenamiento de datos en disco por tener computadoras compartiendo aplicaciones en vez de tener espacio de disco local para cada aplicación del usuario.
- Se logro la rentabilidad de los equipos, ya que todos los usuarios pueden leer el mismo conjunto de archivos.
- El montado de sistemas de archivos es transparente para los usuarios.
- Los accesos remotos de los sistemas de archivos son transparentes para los usuarios.

Con respecto a la asignación de cuotas se logro que cada uno de los usuarios depurara su información liberando un poco los sistemas de archivos. Uno de los objetivos principales que se logro fue el de transmitir una política de depuración y compactación de la información con la cual se logro que cada uno de los usuarios comprendiera el valor que tiene el uso de disco y sobre todo en estas estaciones de trabajo.

Como punto adicional se detectó varios directorios duplicados, olvidados y con versiones pasadas, los cuales fueron eliminados de los equipos, no sin antes haber hecho una notificación al dueño del directorio.

En el objetivo de la estandarización de los sistemas operativos fue como se había planeado tener en todos ellos la misma versión de Sistema Operativo reduciendo así las tareas de administración que antes se tenían que realizar. El único equipo que no se logro estandarizar fue CCA02 por decisión propia de algunos de los investigadores, ya que aun no habían realizado las modificaciones de algunos programas de investigación que eran de utilidad para ellos y que no corrían en las nuevas versiones de Sistema Operativo.

La incorporación del servidor de impresión AXIS NPS 550 se logro imprimir desde cualquier estación de trabajo SUN o PC's sin que existiera un servidor de impresión dedicado para realizar esta tarea. El problema que se resolvió, fue la simplificación del proceso de impresión ya que el servidor puede ser conectado en cualquier parte en donde exista algún punto de red, sin que este tenga que estar conectado físicamente a una estación de trabajo o equipo PC, para que pueda imprimir algún documento. Además, el proceso de impresión es transparente para el usuario, ya que no se tiene que especificar que el archivo a imprimir proviene de un equipo Sun con TCP/IP o desde un equipo PC's con TCP/IP o NetBeui, solo el usuario debe de especificar a que cola de impresión desea imprimir.

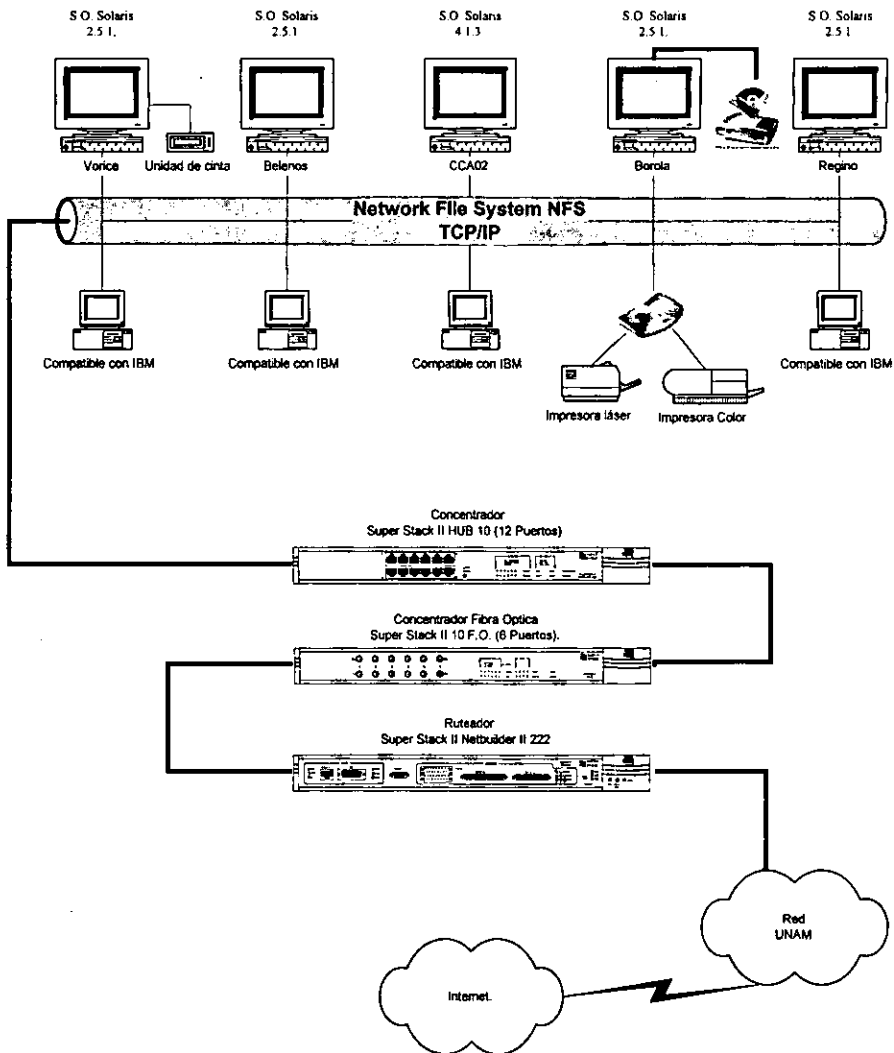
La instalación de Ghostscript y Ghostview nos permitió desplegar imágenes PostScript en los equipos PC's, con lo que se simplifico una vez más el trabajo de los investigadores, ya que estos no podían desplegar ningún tipo de gráfica lo cual es de vital importancia para ellos.

En la implementación de las políticas de seguridad, se tuvieron algunos problemas en la puesta en marcha de estas, ya que algunos usuarios se rehusaban a implementar las políticas propuestas, estos no tenían plena conciencia de la importancia que esto implicaba para ellos. Una vez que se les explico la importancia que tiene la implementación de estas políticas poco a poco se fueron adaptando a la utilización de ellas.

Con la culminación de la presente se logra alcanzar la mayoría de los objetivos, planteados documentando como administrar un Centro de Cómputo, prácticamente de una manera sencilla y profesional

La gráfica que se muestra a continuación se puede apreciar en resumen como la red del Centro de Ciencias de la Atmósfera quedo finalmente.

SITUACIÓN FINAL DEL CENTRO DE CÓMPUTO



Conclusiones.

La UNAM como centro de enseñanza, e impulso al desarrollo científico y tecnológico busca que todas sus entidades se hallen a la vanguardia.

Uno de los puntos más relevantes en la administración de una red de cómputo es la documentación, esta tesis de licenciatura se ha convertido en la piedra angular de la Administración de la Red de Cómputo del Centro Ciencias de la Atmósfera, que dará pie al crecimiento y fortalecimiento de la misma.

El Centro de Ciencias de la Atmósfera como Centro de Investigación Científico busca la eficiencia de las herramientas de trabajo que le permita ejercer a sus investigadores día con día sus labores, sin que la red de cómputo que ellos utilizan sean un problema más en su trabajo si no una herramienta útil que les faciliten sus tareas.

Como hemos visto, para poder realizar la implantación o optimización de una red de computadoras, es necesario analizar diversos factores, tomar diferentes alternativas de cada uno de ellos y conjuntar todos estos, de manera que se elija la alternativa más adecuada, por lo regular la menos costosa pero sin descuidar la calidad y eficiencia de ella, es decir, obtener el máximo de beneficios.

Con esta instalación se obtuvieron varios beneficios como fueron los respaldos, Compartición de recursos en red vía NFS, asignación de cuotas, estandarización de los sistemas operativos, instalación del disco optomagnético (VERTEX), instalación de un servidor de Impresión en un punto de red, instalación de software para despliegue de imágenes PostScript, instalación de software de seguridad, etc.

Por último, haciendo un balance de la inversión efectuada en la compra del nuevo equipo como fue servidores equipo Sun ... y en la instalación (la cual no contempla el costo adicional de horas/hombre tanto en la instalación y administración, debido a que fue realizado por becarios de la Dirección de Cómputo para la Administración Académica - Dirección General de Servicios de Computo Académico (DCAA - DGSCA) , únicamente se invirtió en material propio), y los beneficios que se obtendrán a corto, mediano y largo plazo, teniendo en cuenta el ahorro en el costo de almacenamiento de información, en disquetes y el tiempo del personal que se aprovecharía en realizar otras actividades ya que no se preocuparían por la red de cómputo que ellos utilizan sino en sus labores que realmente deben de hacer, lo cual repercute en beneficio para el Centro; por lo tanto la inversión realizada es reembolsable a corto o mediano plazo, teniendo un beneficio mayor que el costo de la instalación y administración.

Como nota adicional cabe mencionar que la falta de un departamento que se dedique a la administración de la Red de Cómputo del Centro de Ciencias de la Atmósfera, este dependerá de los servicios de gente externa como fue nuestro caso. Sin embargo, se espera que en un lapso de tiempo corto pueda contar con su propio departamento.

Apéndices

Apéndices	107
A Instalación del Sistema Operativo Solaris 5.x	109
Preinstalación.....	109
Requerimientos de hardware.....	110
Instalación.....	111
Notas y tips de instalación	115
Posinstalación	116
B Diferencias de SunOS 4.1.X y Solaris 5.X	119
Diferencias en los comandos de administración.....	119
Diferencias en los archivos de administración SunOS 4.1.X y Solaris 5.X.....	122

Apéndice A

Instalación del Sistema Operativo Solaris 5.X

Preinstalación.

Para instalar satisfactoriamente Solaris hay pocas decisiones que se deben de tomar antes de empezar con la instalación.

Server

Un servidor cuenta con los siguientes sistemas de archivos:

- Sistemas de archivos de root (/) y /usr, mas espacio de swap.
- Sistemas de archivos de /export, /export/swap, y /export/home, para dar soporte y proveer directorios de home para los usuarios.
- El sistema de archivo de /opt para almacenar las aplicaciones de software.
- Los servidores también pueden contener software para dar soporte a otros sistemas.
- Imágenes de CD (Solaris) y software para inicializar o realizar instalaciones remotas a través de la red.

Standalone

Un sistema Standalone en red puede compartir información con otros sistemas dentro de la misma, sin que este se vea afectado por un aislamiento de la red en caso de que esta falle, ya que tiene la capacidad de seguir trabajando por si solo.

El sistema Standalone puede trabajar por si solo, por que es dueño de su propio disco duro que contiene los sistemas de archivos root (/), /usr, /home y espacio de swap. Así el sistema Standalone tiene acceso local al software, espacio de memoria virtual y crear archivos para los usuarios.

El sistema Standalone debe de tener suficiente espacio de disco duro para poder soportar los cuatro sistemas de archivos necesarios.

Un Servidor y un Standalone proveen servicios de ftp, telnet, etc. pero el Server además tiene la capacidad de proporcionar S.O. a clientes Diskless y Dataless.

Requerimientos de hardware.

Memoria Mínimo 16MB (recomendado 32).

Espacio en Disco Hay 4 diferentes grupos de software para seleccionar en la instalación de Solaris.

Grupo de Software	Espacio de Disco Aproximado.
Core System Support	70 MB
End User System Support	180 MB
Develover System Support	270 MB
Entire Distribution	360 MB

Obviamente esto no incluye los directorios del los usuarios, mail, spool de impresión o área de swap.

1. Seleccionando el método de instalación.

Jumpstart.- Esta opción es usada automáticamente para instalar el sistema vía red e instalándola en el servidor SUN.

Interactive.- Este es el método a mano sobre un drive de CD-ROM local.

Custom Jumpstart.- Para usuarios avanzados, para la creación de perfiles y reglas de archivos, se pueden seleccionar reglas para instalar automáticamente software de Solaris vía red o sobre un servidor.

2. Información específica necesaria para la instalación de un sistema.

- Nombre de la máquina del sistema.
- Interface de red usada por el sistema. La más comúnmente usada es la le0.
- Dirección IP del servidor.
- Servicio utilizado. Desde que NIS y NIS+ pueden ser activados después de la instalación y no son usualmente necesarios, la opción **None** podría ser seleccionada.
- Nombre del Dominio del sistema.
- Número de la Subred y la máscara usados en el sistema.
- Tiempo de la Zona Geográfica. (México General).

3. Respaldo el sistema antes de la instalación.

Es muy importante hacer un respaldo completo de la información antes de proceder a la instalación de cualquier sistema.

Instalación.

Instalación de Solaris sobre CD-ROM.

Para dar un boot desde un CD-ROM local, es necesario prender el sistema (o dar de baja el sistema usando el comando shutdown si esta actualmente en uso). Si el sistema arrancó, después de un periodo de pruebas presiona **STOP-A** para obtener el PROMT **ok**. Si se va a dar de baja el sistema, cambiarse a la cuenta de root, con el comando **su root** y teclear **halt**. En algunos sistemas podría ser que el prompt **ok** aparezca en otra forma como un signo **>**. Si tu sistema es una SPARCstation, después del prompt **>** teclee: **n** para obtener el prompt. **ok**. Para dar el proceso de boot sobre el CD-ROM nos podríamos referir a la siguiente tabla.

Tipo de Sistema	Comando de Boot
Sun-4/1*	b sd(0,30,1)
Sun-4/2*	
Sun-4/3*	
Sun-4/4*	
SPARCstation 1 (4/60).	Boot sd(0,6,2)
SPARCstation 1 (4/65).	
SPARCstation SLC (4/20).	
SPARCengine 1E	boot sd(0,6,5).
SPARCstation 4	boot cdrom
SPARCstation 5	
SPARCstation 10	
SPARCstation 20	
(todos los nuevos modelos)	

Usar el comando de boot de acuerdo al tipo de sistema que se este utilizando. Por ejemplo una SPARCstation 5 podría requerir el siguiente comando.

boot cdrom

El proceso de boot podría tomar algunos minutos, mientras los componentes de hardware y software son checados. Una vez que los componentes del sistema son checados, OpenWindows se iniciará y la ventana de instalación aparece.

Instalación de Solaris: Interactivo.

Esta es manejada basándose en menús, los programas interactivos podrían ser una guía en el proceso de instalación. Una serie de paneles de OpenWindows podrían ser los pasos en la instalación. El primer panel es el programa de la instalación de Solaris y describe este proceso brevemente. Tendrá unos números de diferentes opciones sobre cada panel y podrá usar la ayuda de los paneles en cualquier momento para su asistencia en sus

elecciones. Siguiendo lo pasos de abajo y llenando cuidadosamente las hojas de trabajo después de la instalación no tendrás ningún problema.

Hostname:

Supply your Unix machine's Hostname.

Inserte el Hostname de su maquina Unix. Este debe ser un nombre único dentro de su red. Por ejemplo xcaret.dcaa.unam.mx.

Network Connectivity.

Will this be connected to the network? Yes or No.

La estación podría estar conectada sobre la red así que seleccione. **Yes.**

IP Address.

Enter the IP address that was assigned.

Insertar la dirección IP que le fue asignada al equipo. Recordar que la Dirección IP y el Hostname del servidor Unix deben ser agregados en el servidor de nombres (nameserver) para que la máquina funcione correctamente.

Por ejemplo: 132.248.27.15

Donde 132.248 es el número de la red, 27 es el número de la subred y 15 es el número del host.

Confirm Information: If the information correct? Continue, Change, Help. Si la información es correcta, seleccione **Continue.**

Name Service.

Podría el sistema ser usado por cualquier servicio de nombre para obtener información como passwords, Hostname, etc. La opciones aquí están: NIS+, NIS, OTHER, NONE. Si deseas seleccionar NIS+ para administrar passwords, etc. entonces selecciona NIS+. En Solaris 2.x no puede ser servidor de NIS, solamente cliente. Si tu estas usando NIS sobre la red, puedes agregar tu máquina Solaris al servidor de nombres sobre la red seleccionando NIS. Si estas usando algún otro tipo de servicio de nombres puedes utilizar DNS, seleccionando other. No significa que no tengas servicios de nombres.

Seleccione **other.**

Subnets.

Is your network subnets?. Yes or no. Si es si debe estar seguro de que la máscara este correcta.

Seleccione **yes.**

Netmask.

Enter the netmask for your subnet. La máscara es usada para especificar la cantidad de direcciones IP a ser reservadas para la red. La porción de la red podría ser los 1's y la porción de los hosts la de los 0's.

Por ejemplo 255.255.255.0

Confirm the information: If the information correct? Continue, Change, Help. Si la información es correcta seleccione **Continue**.

Time Zone.

Especificar el tiempo de Zona por, Geographic Region, Offset from GMT, Time Zone. Seleccione **Geographic Region**.

Date and Time.

Introduzca la fecha y el tiempo en campos de año, mes, día, hora y minutos. Esto podría seleccionar el reloj. Si la información es correcta seleccione **Continue**.

Install Software Solaris.

Initial. Un panel aparecerá preguntando si desea empezar la instalación. Seleccione:

Continue.

- Upgrade System? Un panel podría preguntar si estas actualizando el sistema. Para actualizarlo deberías estar corriendo Solaris 2.1, Solaris 2.2 o Solaris 2.3. No se puede realizar la actualización desde Solaris 4.1.X. (Solaris 1.1.x).

Se puede realizar la instalación completa sin actualizar. Seleccione **Initial**.

- System Type: Seleccione el tipo de sistema. Standalone, Server, o Dataless Client. Seleccione **Standalone**.
- Software: Hay 4 grupos de software para seleccionar, Entire Distribution, End User System Support, Developer System Support, Core System Support. Selecciona el tipo de sistema basado en tus aplicaciones y a espacio de disco. **Selecciona Developer System Support**. Si se desea se puede personalizar el Developer System con la selección de **Customize**. Seleccione **Continue** cuando la selección de software sea completada.
- Disks: Se puede seleccionar los discos que instalaras dentro de Solaris. Un panel podría desplegar los discos conectados al sistema y preguntar si deseas agregar estos a la instalación. Una ventana aparecerá en donde se despliega el espacio recomendado para cada partición. Recordar que esto no incluye espacio de swap, ni spool (mail, impresoras, etc.).

Se puede configurar el sistema con discos internos. Seleccionar `e0t3d0` y agregar este a la lista:

- **Preserve Data?:** Su puede conservar los datos sobre particiones individuales que la instalación podría no actualizar durante la instalación. Por ejemplo se puede conservar `/home` para que la instalación no ponga archivos dentro de dicha partición. Si esta es una nueva instalación seleccione **Continúe**.
- **Automatically Layout File Systems?:** Se puede seleccionar en el programa de instalación los sistemas de archivos. El programa de instalación clasificará según tamaño los sistemas del archivo basándose en su configuración de sistema y grupo de software seleccionado. O se puede seleccionar manualmente el tamaño de los sistemas de archivos.

Seleccionar Automatically Layout.

- **File System and Disk Layout:** Un panel podría aparecer mostrando el esquema de los sistemas de archivos automontables. Seleccione `/`, `/usr`, `swap`, `/opt` y `/var` que serán particiones de discos separadas.
- **Customize Disks?:** Los sistemas de archivos y sus tamaños en MB podrían ser desplegados. Se podrá observar algo similar a lo siguiente:

Slice	Mount Point	Size (MBs)
0	<code>/</code>	20
1	<code>Swap</code>	64
2	<code>Overlap</code>	1002
3	<code>/var</code>	90
4		0
5	<code>/opt</code>	90
6	<code>/usr</code>	103
7		0

Se puede seleccionar **Customize** para ajustar esta auto partición. Seleccione **Continue**. Como fue indicado anteriormente estos valores cambiarán dependiendo del espacio total disponible en el disco y el software seleccionado. Los valores listados son de una SPARCstation con 32 MB en RAM y 1G de disco duro y usando por default la configuración de **Developer System Support**.

Como regla la partición de "swap" debería de ser el doble de la cantidad de RAM instalada en el sistema para un óptimo performance sobre sistemas con poca cantidad de memoria. En sistemas con cantidades más grandes de RAM, la cantidad swap y de RAM debe ser cantidad de RAM + 32 MB. Si el sistema tiene 424Mb de espacio de disco o más, por lo menos se debe reservar para `/var` 32Mb de espacio por si el sistema cambia en un futuro, el software de las aplicaciones adicionales no llene rápidamente la partición `/var`. Sin embargo se recomienda ampliamente que `/var` sea más grande de 32MB de tamaño.

Acerca de la partición de home ...ninguna de las tablas anteriores lista la partición de home. A menos que sus directorios de home sean montados desde otro servidor vía NFS, se debería tener la partición de home seleccionada sobre el sistema. Tradicionalmente en Unix estas particiones son montadas en /home.

Sin embargo, Solaris 2 sugiere que el usuario podría montar home sobre el punto de montura "/export/home" por razones que serán discutidas más adelante. Con tal de que el espacio de disco sea suficiente para las particiones presentes y futuras los requerimientos de disco están bien. Sin embargo si no se esta seguro de otros tamaños de particiones en un futuro, y si no se tiene espacio de disco reservado disponible es altamente recomendado que se use el punto de montura "/export" para el espacio restante de su disco. Esto proporciona a los administradores una máxima flexibilidad mientras se preservan directorios y convenciones de nombres. Así si el espacio llega a ser limitado sobre "/opt" o cualquier otra partición, entonces tu puedes crear un directorio de expansión en /export como /export/opt y crear ligas simbólicas a las necesidades del sistema.

- Mount Remote File Systems?: Se puede montar cualquier sistema de archivos remoto montándolo vía NFS. Esto se puede realizar editando el /etc/vfstab. Esto no trabaja correctamente con el programa de instalación.

No agregar ningún punto de montura. Seleccione la opción **Continue**.

En general la opción Remote Mount no es necesaria. Sin embargo podría tenerse la necesidad de montar permanentemente sistemas de archivos sobre otras estaciones de trabajo, sobre la red, estos puntos de montura pueden ser definidos aquí.

- Profile: Un panel podría aparecer con la descripción de la instalación que se ha seleccionado. Se tiene la opción de empezar la instalación, cambiar, salir o ayuda.

Si se esta conforme con el profile, seleccione **Continue**.

- Ok to Reboot after Installing Solaris. Reboot or No. Hay parches que deberían ser instalados después del reboot. Select **No**.

El proceso de instalación puede tomar entre ½ Hora y dos horas dependiendo de su configuración y el sistema.

Notas y tips de instalación.

Una vez que la instalación esta completa, se pedirá introducir el password de root o super usuario. Es importante que los administradores de sistemas no vuelvan a dar las pautas para posibles intrusiones en los sistemas que acaban de ser instalados, ya que la información esta íntegra y segura por el momento.

Seleccionar passwords que sean **únicos**. Compartir passwords en múltiples sistemas significa muchos problemas. La probabilidad de que el password sea adivinable es alta. Si una máquina llega a ser vulnerable a la intrusión TODAS las máquinas que comparten el mismo password también llegan a ser vulnerables.

Compartir los passwords solamente con las personas que necesiten tener el acceso como root. Accesar con la cuenta de root sobre cualquier sistema Unix podría ser limitado a personas que conozcan las bases del equipo. Cuando más de una persona tiene acceso como root, los procedimientos estrictos que se deben de seguir, es de estar seguros que los cambios hechos a la información sean registrados en algún tipo de bitácora y que la otra persona que vea esta bitácora este informada de lo hecho por el otro super usuario para que no se llegue a perder el status del sistema, algo que suele pasar muy comúnmente.

Posinstalación.

- **El archivo /etc/defaultrouter**

Como se refirió durante el proceso de instalación, las redes tienen subredes. El efecto de esto es que el tráfico de la red es restringido por cada subred individual, en lugar de viajar sobre todo el campus cuando las comunicaciones pueden ser restringidas a solo algunos puntos de los aparatos de comunicación. Cada subred tiene un aparato especial llamado "router" que regresa el tráfico de la red si no está una máquina sobre su subred, a otra máquina sobre otra red. Usualmente, el default router tiene una dirección IP de la forma 132.248.xxx.254 donde xxx se refiere al número de la subred.

Una vez que se conoce esta información, es necesario crear un campo necesario llamado /etc/defaultrouter y colocar esta dirección en el archivo.

```
echo 132.248.xxx.254 > /etc/defaultrouter
donde xxx es el número de la dirección IP de la subred.
```

- **El archivo "/etc/resolv.conf"**

El próximo archivo para tener un completo soporte DNS sobre el equipo, es la creación del archivo /etc/resolv.conf. Hay 4 caminos para correr DNS sobre una máquina: Primary Nameserver, Secondary Nameserver, Cache-Mode NameServer y Resolver-Mode. Hay 3 Primary Nameservers y pocos Secondary Nameservers. Para la mayoría de las máquinas, el método resolver-mode, es el mejor. Este solamente es seleccionado y mantenido. Para seleccionar el método resolver-mode, solo se necesita un archivo llamado /etc/resolv.conf.

```
{hostname}# cd /etc <enter>
{hostname}# vi resolv.conf <enter>
```

e insertar las siguientes líneas.

```
domain dcaa.unam.mx
search dcaa.unam.mx unam.mx
nameserver 132.248.10.2
nameserver 132.248.204.1
```

donde cada dirección IP corresponde a uno de los servidores de nombres y el domain usado es el dominio local para esta máquina, como dcaa.unam.mx.

- **El archivo /etc/nsswitch.conf**

Este archivo es usado por Solaris para ayudar al sistema a conocer donde aparecerá la información pertinente de su propio sistema.

Los servidores de nombres tienen distintas operaciones, que son conocidas en la Internet como Servidores de nombres, estos funcionan para proveer información de los equipos cuando esta es solicitada. Esto es ayudado por el servicio llamado DNS (Domain Name Service).

En estaciones recién instaladas para usar automáticamente DNS, es necesario alterar el archivo nsswitch cambiando la línea de abajo.

hosts: files

por la siguiente línea

hosts: files dns

Apéndice B

Diferencias de SunOS 4.1.X y Solaris 5.X

Diferencias en los Comandos de Administración.

SunOS 4.X	SunOS 5.X	Comentarios
add_services	pkgadd	Agrega paquetes de software
arch	uname-m	Determina la arquitectura del sistema.
at	at	Es más segura y restringido sobre SunOS 5.X.
automount	automount	El nuevo de nombre del sistema maestro es auto_master y auto_home. El directorio de home por default es /export/home/<username>.
bar	ninguna	usar tar o cpio -H para reemplazar bar.
biff -y	chmod o+x /dev/tty	Seleccione los permisos de tty, como los de diff si no esta disponible
biff -n	chmod o-x /dev/tty	Seleccione los permisos de tty, como los de biff si no esta disponible.
biod	Ninguna	Bloque de I/O deamon.
cc	/opt/sunwsprow/bin/cc	Producto por separado.
chown	chown	El comando ahora sigue a la liga y cambias los permisos sobre el archivo. Para cambiar el dueño de la liga use chown -n.
dcheck	Ninguna	El sistema de archivos checa la consistencia del directorio.
dd	dd	Ahora usa dos bytes, en lugar de palabras de 4 bytes
devinfo	devinfo sysdef -d	Reporta la información que se ha cambiado
df	df-k	El formato de salida y las opciones han cambiado.
dkinfo	prtvtoc	Información de reportes similares; comandos privilegiados en Solaris 5.4
dorts	rfstart/rfstop	RFS commands.
du	du -k	Ahora realiza reportes de 512 bytes, en lugar de bloques de 1024 bytes.
dump	ufsdump	Algunas nuevas opciones. Ahora reconoce nuevos medios.
etherfind	snoop	Funciones similares.
exportfs	share	Ambos funcionan para NFS y RFS

Diferencias en los Comandos de Administración, Continuación.

SunOS 4.X	SunOS 5.X	Comentarios
extrac_files	ninguna	Extrae archivos sobre medios de instalación.
extract_patch	ninguna	Extrae parches sobre medios de instalación.
extract_unbundled	pkgadd swmtool	Agrega paquetes de software.
fastboot	init 6	Corre el nivel 6.
fasthalt	init 0	Corre el nivel 0.
file	file	No tiene la opción -L.
find	find	No tiene la opción cpio -n.
fsck	fsck	Cambio
hostid	sysdef -h	Sysdef es usado para reportar las definiciones del sistema de archivos actual, incluyendo periféricos conectados y drivers leídos.
hostname	uname -n	Uname imprime las definiciones actuales del sistema
init	init	Muchos cambios incluyendo los niveles que se corren.
iostat	iostat	Algunas opciones han cambiado
ldconfig	ninguna	Configura el cache para correr en tiempo las ligas del editor, ld.so.
lpc	lpsched	Trabajos de impresión
lpd	lpadmin	Comando de configuración de las impresoras.
lpq	lpstat	Estatus de los trabajos de impresión.
lpr	lp	Algunas diferentes opciones.
lprm	cancel	Cancela trabajos de impresión
lptest	ninguna	Genera un test del modelo de la impresora en línea
ls	ls	Algunas opciones han cambiado
mach	uname -p	Reporta el tipo de máquina
make	make	Ahora localizado en /usr/ccs/bin
makekey	ninguna	Genera una llave de encriptación
mkfs	mkfs	Cambia en el soporte adicional de los sistemas de archivos.
mknod	mknod	Ya no tiene que ser root para crear bloques y caracteres de archivos especiales.
modstat	modinfo	Despliega información acerca de los módulos leídos del kernel.
mount	mount	Incluye cambio adicionales en los tipos de sistemas de archivos.
ncheck	ncheck	Incluye cambio adicionales en los tipos de sistemas de archivos.
portmap	rpcbind	Mapas de direcciones universales para números de programas RPC.

Diferencias en los Comandos de Administración, Continuación.

SunOS 4.X	SunOS 5.X	Comentarios
printenv	env	Impresión de variables de ambiente para el usuario.
ps	ps	Las opciones cambiaron.
pstat	sar	Reportes sobre la actividad de el sistema.
pstat -s	swap -s	Reporta el espacio disponible de swap.
rdump	ufsdump	Unidades de cintas remotas pueden ser especificadas.
restore	ufsrestore	Programas que restauran los sistemas de archivos.
rpc.etherd	ninguna	Servidor de estadísticas de Ethernet
rcp.lockd	lockd	Archivo que bloquea los demonios.
rcp.mountd	mountd	Demonio de montura
rcp.rquota	rquota	Servicio de cuotas remotas.
rcp.statd	statd	Monitorea el status de la red.
rcp.yppasswdd	rpc.yppasswdd	Demonio de passwords en NIS.
restore	ufsrestore	Unidades remotas pueden ser especificadas.
rusage	ninguna	Recursos usados sobre comandos específicos.
shutdown	shutdown	Cambios significativos.
stty	stty	Algunas opciones han sido cambiadas
suninstall	suninstall	Cambios significativos.
swapon	swap-a	Agrega espacio de swap.
ttysoftcar	ninguna	Control de la portadora de Módem.
tzsetup	ninguna	Selección del tiempo.
umount	umount	Cambios significativos en la adición de tipos de sistemas de archivos.
unload	pkgrm	remueve paquetes de software.
update	fsflush	Actualiza los buffers de memoria.
vipw	/usr/ucb/vipw	Edita el /etc/passwd, también permite editar el /etc/shadow.
vmstat	vmstat	Algunas opciones han cambiado.
who	who	Se disponen de opciones adicionales.
whoami	id	Imprime el nombre del usuario.
yppasswd	passwd yppasswd nispasswd	El comando yppasswd esta todavía disponible para cambiar la información del password sobre el servidor de NIS. Usar nispasswd para acceder servidores NIS+.
ypserv	/usr/lib/netsvc/yp/ypserv rcp.nisd	Demonio de NIS(paquete instalado en SUNWnsktu). NIS+ usa este demonio para responder a las peticiones de información.

Diferencias en los archivos de administración SunOS 4.1.X y Solaris 5.X.

SUNOS	SOLARIS	Diferencias
/boot	/ufsboot	Programa de booteo.
/etc/auto.master	/etc/auto_master	Configuración del archivo Automounter
/etc/auto.home	/etc/auto_home	Configuración del archivo Automounter
/etc/exports	/etc/dfs/dfstab	Comparte archivos para NFS Y RFS.
/etc/fstab	/etc/vstab	Monta la tabla del sistema de archivos.
/etc/gettytab	/etc/ttydefs	Definiciones de terminales.
/etc/passwd	/etc/passwd /etc/shadow	El archivo de password shadow es ahora utilizado.
/etc/printcap	/etc/share/lib/terminfo /etc/lp	Base de datos de las características de la terminal y la impresora. Directorio de la información de las impresoras.
/etc/rc	/sbin/rc# /etc/rc#.d/	Los scripts del subdirectorio /etc/rc# ahora son usados con cada script rc# y directorio rc#.d controlados por el nivel que se corre #.
/etc/rc.boot	"	"
/etc/rc.local	"	"
/etc/rc.single	"	"
/etc/tremcap	/usr/share/lib/terminfo	Base de datos de las características de la terminal y las impresoras.
/etc/ttytab	/etc/inittab	Tabla de los servicios que son compartidos por el init.
NINGUNA	/etc/saf	Directorio de los servicios SAF.
NINGUNA	/etc/default/login	Defaults para login. Login de root es limitado para la consola.
/var/share/man	/var/share/man	La organización de las páginas de manual han sido cambiadas. Las páginas de administración son de 1M. Se puede especificar una variable de ambiente para especificar el orden de búsqueda de los directorios.
/usr/share/spool/mail	/var/mail	Directorio de spool de mail
/vminix	/kernel/unix	El hardware es independiente del kernel de Unix. Parte del hardware depende de el kernel.

Glosario

GLOSARIO DE TERMINOS USADOS

A

Address Resolution Protocol (ARP) Protocolo de Resolución de Direcciones Un estándar de Internet que proporciona direcciones IP a las estaciones de trabajo en una red de área local (LAN).

address resolution resolución de direcciones En una red de área local (LAN) conectada a Internet, el proceso automatizado mediante el cual la dirección de la LAN de cada estación de trabajo se convierte en una dirección IP. La traducción es necesaria debido a que Internet y las LANs controlan las direcciones de las estaciones de trabajo de manera distinta. Los programas basados en el Protocolo de Resolución de Direcciones (ARP) controlan la traducción.

Administrador: Persona que se encarga de todas las tareas de mantenimiento de un sistema informático.

Adobe Acrobat: Un programa de aplicación que crea documentos transportables con un formato enriquecido, a los que se puede tener acceso desde una amplia gama de computadoras. Para leer un documento Acrobat se necesita una copia del lector Adobe Acrobat, diseñado para ejecutarse en su computadora. El lector está disponible para bajarse gratuitamente de Internet. Una vez instalado el lector, usted puede desplegar cualquier documento de Adobe Acrobat, y verá las fuentes, gráficos y demás elementos de diseño del documento elegidos por el autor. Cada vez más populares en World Wide Web, los documentos Acrobat permiten a los editores superar las limitaciones de formato del Lenguaje de Marcación de Hipertexto (HTML). Adobe Acrobat 2.0 presenta características similares al hipertexto que permiten a los autores crear rutas de desplazamiento a través de las diversas secciones de sus documentos.

Adobe Photosop: Un programa editor de imágenes muy poderoso que permite modificar una fotografía de manera más amplia que en un cuarto oscuro. Los filtros elaborados (y adaptables), los efectos de luz y las herramientas de edición permiten preparar imágenes para su publicación. A algunos críticos no les agrada el hecho de que Adobe Photoshop requiera un microprocesador rápido y grandes cantidades de memoria de acceso aleatorio (RAM), pero otros dicen que la capacidad del programa bien vale la inversión en hardware.

Adobe PostScript: Véase PostScript.

Advanced Research Projects Agency (ARPA): Agencia para Proyectos Avanzados de Investigación Una dependencia del Departamento de Defensa (DoD) de Estados Unidos, ahora llamada Agencia para Proyectos Avanzados de Investigación de la Defensa (DARPA) y una de las principales fuentes de apoyo para importantes innovaciones de computación. A finales de la década de 1960 y principios de la de 1970, ARPA apoyó el desarrollo de ARPAnet, el predecesor de Internet, y los protocolos TCP/IP, que desde

entonces proporcionaron las bases para el surgimiento de una red de área amplia (WAN) de grandes proporciones.

Anchura de Banda: Medida de frecuencia, expresada en ciclos por segundo (hertz) o bits por segundo (bps), de la cantidad de información que fluye a través de un canal. A mayor frecuencia, mayor ancho de banda.

Anchura de Banda de Fibra: Simplemente, la frecuencia más baja a la cual la pérdida de la fibra no aumenta sobre 3dB comparada con la salida de frecuencia cero. Específicamente, la frecuencia más baja en la cual la magnitud de la función de transferencia de la fibra disminuye a una fracción especificada del valor de la frecuencia cero. La anchura de la banda de fibra es expresada como una función de la distancia, típicamente en Mhz - km. Es una medida de la capacidad de la fibra de cargar información.

Anillo (Ring): La topología de red de área local en donde los datos son enviados desde la estación de trabajo a través de un círculo o anillo.

Aplicación: Un programa de computadora diseñado para ayudar al usuario a realizar un determinado tipo de trabajo. Una aplicación trabaja con datos que pueden ser texto, números, gráficos o una combinación de todos ellos.

ARPAnet: Una red de área amplia (WAN), creada en 1969 con fondos de la Agencia para Proyectos Avanzados de Investigación (ARPA). ARPAnet tuvo un proceso de constante investigación y desarrollo a principios y mediados de 1970 y sirvió como prueba para el desarrollo de TCP/IP (los protocolos que hacen posible a Internet). Uno de los principales objetivos de ARPAnet era incrementar el comando militar y la capacidad de control, permitiendo la comunicación a través de varios medios físicamente diferentes, incluyendo los satélites. Un objetivo era crear una red robusta capaz de soportar los sabotajes, como aquellos que podrían resultar de un bombardeo nuclear.

ARPAnet cumplió estos objetivos, pero también sorprendió a sus creadores. Pronto se vio que la mayoría de los usuarios de ARPAnet preferían utilizar la red para comunicación, como el correo electrónico y los grupos de discusión. En un principio, sólo estaba disponible para los institutos de investigación del gobierno y las universidades que tenían contratos de investigación con el Departamento de Defensa. En 1983, ARPAnet fue dividida en una red militar de alta seguridad (Milnet) y una ARPAnet que fue clasificada como una red para investigación y desarrollo.

Arquitectura cliente/servidor: Modelo de diseño para aplicaciones que corren en redes, en el que la mayor parte del procesamiento de segundo plano, como realizar una búsqueda física en una base de datos, se lleva a cabo en el servidor. El procesamiento de primer plano, que incluye la comunicación con el usuario, lo manejan varios programas pequeños distribuidos en las estaciones de trabajo clientes. Véase local area network (LAN) y wide area network (WAN).

Atenuación: La pérdida de la fuerza de la señal como función de la distancia. En fibras ópticas, es la pérdida de la intensidad de la luz según viaja a través de la fibra expresada en decibeles por pie unitario (usualmente 1000 pies ó 305 metros).

ATM: Modo de transferencia asincrona (Asynchronous Transfer Mode). ATM es una tecnología de conmutación y transporte de relé de celdas de lata velocidad (155 Mbps y mayor) para ambientes locales o de área amplia.

AUI: Attachment Unit Interface (Interface de Unidad de Acoplamiento). Término más comúnmente usado en referencia al conector tipo D de 15 espigas y los cables usados para conectar equipos de canal único y canales múltiples a un transceptor Ethernet.

AWG: American Wire Gauge. Un estándar para designar el tamaño de alambres. El número de la calibración (gauge) varía inversamente proporcional con el diámetro del alambre.

B

Backbone: El Backbone (cableado troncal o vertical) es la parte de la red que lleva el tráfico más pesado. Es el cableado troncal principal del cual todas las conexiones a la red se hacen.

Background (Segundo plano): En computadoras capaces de realizar varias tareas al mismo tiempo, ambiente en el que las tareas (como la impresión de un documento o la carga de un archivo) se llevan a cabo mientras el usuario trabaja con una aplicación en primer plano.

En un sistema de computación sin capacidad multitarea, las tareas de segundo plano se realizan durante las pequeñas pausas en la ejecución de las tareas principales del sistema (las de primer plano).

Backup (Respaldo o copia de seguridad): Copia del software de aplicación instalado o de los archivos de datos creados por el usuario. También es la acción de copiar archivos a otro disco. Se requieren procedimientos de respaldo periódicos para el buen funcionamiento de un sistema de disco duro. Véase archival backup, full backup e incremental backup. Banda Ancha

Banda Base: En redes de área local (LANs), método de comunicación mediante el cual la señal de transferencia de información se coloca directamente en el cable de forma digital y sin modulación.

Las señales de computadora puede transmitirse en cables mediante dos tipos de señales: analógicas y digitales. La red de comunicación analógica se conoce como red de banda ancha.

Como muchas redes de banda base pueden usar cables de par trenzado (cables de teléfono ordinarios), su instalación es más económica que la que requieren las redes de banda ancha, las cuales necesitan cable coaxial. No obstante, un sistema de banda base está limitado en su extensión geográfica y proporciona un solo canal de comunicación a la vez. La mayoría de las redes de área local de computadoras personales son de banda base.

Base de datos: Conjunto de información relacionada sobre un tema, organizada de una forma práctica tal que suministra una base o fundamento para procedimientos, como la recuperación de información, la elaboración de conclusiones y la toma de decisiones. A cualquier conjunto de información que sirva a estos propósitos se le califica como base de datos, aun cuando la información no esté almacenada en una computadora. De hecho, los importantes predecesores de los actuales y complejos sistemas de bases de datos empresariales eran archivos registrados en tarjetas de índice y guardados en archiveros. La información se divide por lo general en distintos registros de datos, cada uno con uno o más campos de datos.

Berkeley Software Distribution (BSD): Versión del sistema operativo UNIX que fue desarrollada y mantenida por la Universidad de California en Berkeley. BSD ayudó a establecer Internet en las universidades, debido a que el software distribuido incluía TCP/IP.

Berkeley UNIX: Versión del sistema operativo UNIX, desarrollada por la Universidad de California en Berkeley, que aprovecha al máximo las capacidades de memoria virtual de las minicomputadoras DEC (Digital Equipment Corporation).

Bit: Unidad básica de información en un sistema de numeración binario; proviene del término BInary digiT. La circuitería electrónica de las computadoras detecta la diferencia entre dos estados (corriente alta o baja) y representa estos estados como uno de los dos números de un sistema binario: el 1 o el 0. Estas unidades básicas de información alto/bajo, esto/o, sí/no se conocen como bits. Como la construcción de un circuito confiable que indique la diferencia entre un 1 y un 0 es fácil y barata, las computadoras son precisas en sus capacidades de procesamiento interno. En general, las computadoras cometen menos de un error interno en cada 100,000 millones de operaciones de procesamiento. Ocho bits conforman un octeto, también llamado byte.

Boot (arrancar, iniciar): Arrancar una rutina automática que limpia la memoria, carga el sistema operativo y prepara la computadora para su uso.

broadband (banda ancha): En redes de área local (LANs), método de comunicación analógico caracterizado por un ancho de banda amplio. En general, se divide o multiplexa la señal para proporcionar canales múltiples de comunicación.

Bps: Siglas para "bits por segundo". Muchas veces precedido por K (kilo/mil) o por M (Mega/millón).

Bug: (error). Error de programación que ocasiona que un programa o sistema de computación trabaje erráticamente, genere resultados incorrectos o se detenga por completo. El término bug (error) se acuñó cuando se descubrió que un verdadero insecto (bug, en inglés) hizo fallar uno de los circuitos de la primera computadora digital electrónica, la ENIAC. Un problema de hardware se denomina glitch.

Un error en un programa o en un equipo. Se habla de bug si es un error de diseño, no cuando la falla es provocada por otra cosa.

Bus: La topología de una red local en donde todas las estaciones de trabajo están conectadas a un mismo cable. En una red de bus, todas las estaciones de trabajo escuchan todas las transmisiones en el cable. Cada estación de trabajo selecciona aquellas transmisiones dirigidas a la estación basada en la información de dirección contenida en la transmisión.

Byte: Ocho bits contiguos, que es la unidad de información fundamental de las computadoras personales. Como guarda el equivalente de un carácter, el byte también es una unidad de medida básica para el almacenamiento en computadoras. Ya que la arquitectura de las computadoras está basada (en su mayor parte) en números binarios, los bytes se cuentan en potencias de dos. Muchos miembros de la comunidad Internet prefieren llamar octetos a los grupos de ocho bits.

Aunque los términos kilo (en kilobyte, K) y mega (en megabyte, M) se usan para contar bytes, son engañosos, pues provienen del sistema decimal (base 10). Un kilobyte en realidad son 1,024 bytes, y un megabyte, 1,048,576 bytes. Muchos científicos en computación critican estos términos, los que, sin embargo, proporcionan a quienes emplean el sistema decimal un medio fácil para hacer la medición de la memoria.

C

Cache (caché): Area de almacenamiento que guarda datos solicitados con frecuencia o instrucciones de programa fácilmente disponibles para que el usuario no tenga que estarlas recuperando una y otra vez.

Los cachés mejoran el rendimiento mediante el almacenamiento de datos o instrucciones en secciones más rápidas de la memoria y mediante el uso de un diseño eficaz a fin de aumentar la probabilidad de que los datos que se necesiten enseguida estén en el caché.

CDDI: Siglas para "Copper Distributed Data Interface" (Interface de datos distribuidos por cobre). Es el estándar que trasmite a 100 Mbps sobre UTP propuesto por el comité X3T9.5 de ANSI. CDDI es la marca de fábrica de crescendo Communications/CISCO.

CD-ROM: Un acrónimo de compact disk-read only memory (disco compacto de memoria de sólo lectura), que es una tecnología de almacenamiento óptico de sólo lectura mediante discos compactos.

Los CD-ROMs pueden almacenar hasta 650 M de información. Originalmente, la tecnología CD-ROM se usó para guardar enciclopedias, diccionarios y bibliotecas de software, pero ahora se usan con frecuencia en aplicaciones multimedia

Client: (cliente). En una red, estación de trabajo con capacidades de procesamiento, como una computadora personal, que puede requerir información o aplicaciones del servidor de la red. En la vinculación e incrustación de objetos (OLE), aplicación que incluye datos en otra aplicación, llamada aplicación servidor. Véase client application.

Cracker: Entusiasta aficionado a las computadoras cuya diversión estriba en aprender todo acerca de un sistema de computación y, mediante una programación hábil se dedican a violar sistemas de seguridad causándoles daños.

Controlador: Se emplea también el término inglés driver. Se trata de un programa que controla un determinado dispositivo o realiza una función específica en el sistema.

Correo electrónico: Uso de una red para enviar y recibir mensajes. Se le conoce también como e-mail. Unidos mediante conexiones de datos de alta velocidad que cruzan las fronteras de los países, el correo electrónico permite redactar mensajes y transmitirlos en segundos a uno o más receptores en su oficina, a las oficinas generales en otro estado o a un amigo en otro país.

Corta fuegos (Firewall): Computadora que registra todos los paquetes de información que entran en una compañía para que una vez verificados, derivarlos a otra que tiene conexión interna y no recibe archivos que no provengan de aquella. Es como un embudo que mira si la información que desea entrar a un servidor, tiene permiso para ello o no. Los hackers o crackers tienen que interceptar los paquetes de información, para entrar ya sea buscando un bug (error de diseño) o mediante algún programa que le permita encontrar alguna clave válida.

Cyberpunk: Corriente literaria dentro de la ciencia-ficción que, entre otras cosas, se destaca por incorporar a sus argumentos el uso de la tecnología de las redes de computadoras.

D

Daemon (demonio): Un programa, que se utiliza generalmente en una computadora que ejecuta UNIX y sirve para alguna función oculta (como establecer la ruta en el correo electrónico a sus receptores) y por lo general tiene una interfaz muy limitada con el usuario. Existe algo de debate acerca de los orígenes de la palabra, pero muchos dicen que se deriva de los espíritus malignos de la mitología griega.

Diafonía: La introducción no deseada de las señales de un canal a otro.

Disco magnético: En almacenamiento de datos, medio de almacenamiento de acceso aleatorio que es el método más popular para guardar y recuperar programas de computación y archivos de datos. En computación personal, los discos magnéticos comunes son los flexibles de 5¼ y 3½ pulgadas y los duros de distintos tamaños.

Disco Optomagnético: El dispositivo de almacenamiento removible utilizado en una unidad magneto - óptica (MO). Los cartuchos MO son de 5¼ pulgadas (con capacidades superiores a los 1,300 M) o de 3½ pulgadas (con capacidades superiores a los 230 M). Los datos de un cartucho magneto - óptico son muy estables, a diferencia de los datos de un disco flexible o de un disco duro, que tienden a borrarse si no se reescriben en forma regular.

Domain Name Service (DNS) (Servicio de Nombres de Dominio): Un programa que se ejecuta en un sistema de cómputo conectado a Internet (llamado servidor DNS) y proporciona una traducción automática entre los nombres de dominio (como watt.seas.virginia.edu) y las direcciones IP (128.143.7.186). La finalidad de este proceso de traducción, llamado resolución, es permitir a los usuarios de Internet continuar utilizando un nombre familiar (como www.yahoo.com) aunque la dirección IP del servicio se modifique.

Driver: Programa de control de un dispositivo. Elemento software que proporciona al sistema o al entorno operativo el control sobre un determinado periférico (por ejemplo los drivers de la impresora)

E

EIA 568: 1. Electronic Industries Association (Asociación de la Industria Electrónica) 2. Un estándar de alambrado para edificios comerciales desarrollado en 1989 por la EIA para la comunicación de voz y datos.

EMI: Siglas para Electromagnetic Interference (Interferencia Electromagnética). Energía generada por fuentes externas tales como sistemas de alumbrado y motores eléctricos que es recibida por el cable de cobre para voz datos e interfiere con la transmisión.

Empalme: Una unión permanente de dos fibras ópticas.

Encapsulated PostScript (EPS): Archivo en PostScript encapsulado.

Imagen gráfica de alta resolución almacenada en lenguaje de descripción de páginas PostScript. El estándar EPS permite transferir gráficos de alta resolución entre aplicaciones. Las imágenes EPS se pueden ampliar sin menoscabo en la calidad de la imagen.

Una de las principales desventajas de los gráficos EPS es que se requiere una impresora láser compatible con PostScript para imprimirlas. Una segunda desventaja es que

con la mayoría de los programas de aplicación, la imagen no es visible en pantalla a menos que se agregue un formato de imagen de pantalla. Como alternativa a las costosas impresoras PostScript, se han creado programas, como GoScript de LaserGo, Inc., que interpretan e imprimen archivos EPS en las impresoras estándar de matriz de puntos o en impresoras láser no compatibles con PostScript.

Estación de trabajo: Cada una de las computadoras conectadas a la red capaces de manejar un programa almacena en algún servidor de archivos.

Estándar: Normalizado. Que cumple determinadas especificaciones, genéricas en su especialidad.

EtherNet: Estándar para hardware, comunicaciones y cableado de redes de área local (LANs) desarrollado originalmente por Xerox Corporation, capaz de enlazar hasta 1,024 nodos en una red de bus.

Como estándar de alta velocidad que usa una técnica de comunicación de banda base (un solo canal), EtherNet proporciona una transferencia simple de datos de 10 megabits por segundo (Mbps), con un rendimiento real en el rango de 2 a 3 megabits por segundo. EtherNet usa técnicas de acceso múltiple de percepción de portadora con detección de colisiones (CSMA/CD) para prevenir fallas en la red cuando dos dispositivos intentan acceder la red al mismo tiempo.

Ética del hacker, hacker ethic: Conjunto de principios morales que fueron comunes a la primera generación de la comunidad de hackers (alrededor de 1965-1982), descrita por Steven Levy en *Hackers* (1984). De acuerdo con la ética del hacker, toda la información técnica debería, en principio, estar disponible en forma gratuita para todos. Por lo tanto, no es inmoral obtener la entrada a un sistema para explorarlo y obtener más conocimiento. Sin embargo, siempre es inmoral destruir, alterar o mover datos de tal forma que cause daño o gastos a otros. Cada vez son más los lugares de Estados Unidos donde es ilegal irrumpir en los sistemas de bases de datos. Véase cracker, cyberspace, cyberspace, hack y phreaking.

Estrella (star): Una topología de red de área local en donde todas las estaciones de trabajo están directamente alambradas a una estación central de trabajo o centro que establece, mantiene y ramifica las conexiones a las estaciones de trabajo.

F

FDDI: Siglas para Fiber Distributed Data Interface (Interface de datos distribuidos por Fibra). El estándar para las redes locales de velocidad de 100 Mb/s.

FRD: Retardador de fuego. Una calibración usada para cables con aislamiento de teflón o una aislación de la camiseta equivalente. Este cable se debe usar cuando los códigos de fuego locales requieren un bajo nivel de llama y de humo o cuando el cable es corrido por el ducto de ventilación.

G

GUI (graphical user interface - interfaz gráfica para usuario): Diseño para la parte de un programa que interactúa con el usuario y que usa iconos para representar las características del programa. Los ambientes operativos de Apple Macintosh y Microsoft Windows son GUIs populares.

Luego de descubrir que la gente reconoce con más rapidez las representaciones gráficas que las palabras o frases que lee, un equipo de investigadores de XEROX diseñó una interfaz para usuario con imágenes gráficas llamadas iconos. Las GUIs funcionan comúnmente como interfaces operadas mediante ratón con menús descendentes, cuadros de diálogo, casillas de verificación, botones de radio, cuadros de listas descendentes, barras de desplazamiento, cuadros de desplazamiento y elementos semejantes. Los programas con una GUI requieren de una computadora con suficiente velocidad, potencia y memoria para desplegar una pantalla en mapa de bits de alta resolución.

H

Hacker: Entusiasta aficionado a las computadoras cuya diversión estriba en aprender todo acerca de un sistema de computación y, mediante una programación hábil, llevar el sistema al nivel máximo de rendimiento.

Durante la década de los ochenta, la prensa redefinió el término para incluir a aquellos aficionados que se dedicaban a violar sistemas de seguridad llamados crackers. La prensa sensacionalista daba cuenta de las peligrosas actividades de los hackers, lo que creó una histeria hacia éstos.

Hardware: Componentes electrónicos, tarjetas, periféricos y equipo que conforman un sistema de computación; se distinguen de los programas (software) porque éstos le indican a los componentes mencionados lo que deben hacer.

I

IEEE: Siglas de Institute of Electrical and Electronic Engineers. Una sociedad profesional intencional que establece sus propios estándares y es miembro de ANSI e ISO.

IEEE 802.3

Es un estándar de la capa física para 10BASE-T, 100BASE-T, Ethernet y starlan.

IEEE 802.5

Es un estándar de la capa física para token Ring.

IEEE 802.12

Es un estándar de la capa física para 100 VG.

Índice de refracción (IR): La densidad relativa de un material de transmisión en comparación con la velocidad de la luz en el material en cuestión y la velocidad de la luz en el vacío.

Interconexión: La conexión física entre los paneles de conexión o los bloques de inserción que facilita la conexión de la estación de trabajo al anfitrión de la red.

Interface: Se dice de cualquier procedimiento, tanto hardware como software que sirva de enlace y coordinador entre dos sistemas o dispositivos que emplean distinto tipo de señal.

Interface de red: El punto físico donde el alambrado del edificio o del equipo se interconecta con las compañías de teléfono locales.

ISO: Siglas de International Standards Organization (organización Internacional de estándares).

Internet: Sistema de redes de computación ligadas entre sí, con alcance mundial, que facilita servicios de comunicación de datos como registro remoto, transferencia de archivos, correo electrónico y grupos de noticias. Internet es una forma de conectar las redes de computación existentes que amplía en gran medida el alcance de cada sistema participante.

Internet, que en un principio se denominó ARPAnet, estaba diseñada para servir a instituciones militares, aunque su tecnología permite que virtualmente cualquier sistema se le conecte por medio de una compuerta electrónica. De esta forma, miles de sistemas de computación corporativos, así como sistemas de correo electrónico con fines de lucro, como MCI y CompuServe, se han vuelto parte de Internet. Con más de 2 millones de computadoras que sirven en promedio a 20 millones de usuarios, Internet crece a razón de un millón de nuevos usuarios por mes.

IP (Internet Protocol - Protocolo Internet): En TCP/IP, el estándar que describe la forma en que una computadora conectada a Internet debe descomponer los datos en paquetes para su transmisión a través de la red, y la forma en que deben dirigirse estos paquetes para que lleguen a su destino. IP es la parte sin conexión de los protocolos TCP/IP; el Protocolo de Control de Transmisión (TCP) especifica la forma en que dos computadoras Internet pueden establecer un vínculo de datos confiable por medio de un protocolo de diálogo.

IP dirección: Un número binario de 32 bits que identifica de manera única y precisa la posición de una computadora particular en Internet. Toda computadora que esté conectada de manera directa a Internet debe tener una dirección IP. Debido a que los números binarios son difíciles de leer, las direcciones IP están dadas en números decimales de cuatro partes, donde cada parte representa 8 bits de la dirección de 32 bits (por ejemplo, 128.143.7.226). En las redes y conexiones SLIP/PPP que asignan en forma dinámica los

números al registrarse en ellas, este número puede cambiar de una sesión a otra. Véase domain name.

J

Joker: Persona que se dedica a bromer en la red, como por ejemplo mandando correos que inundan la red con mensajes sin sentido alguno.

K

kernel (núcleo): En un sistema operativo, componentes principales del programa que residen en memoria y llevan a cabo las tareas más importantes del sistema operativo, como el manejo de operaciones de entrada y salida del disco y la administración de la memoria interna.

kill (eliminar): Detener un proceso en funcionamiento. En los mejores lectores de noticias de UseNet, eliminar un artículo que contiene cierta palabra, nombre, o sitio de origen de modo que los artículos que contienen esta información no aparezcan más adelante en el selector de artículos. Véase article selector, global kill file y kill file.

kilobit: 1,024 bits de información.

kilobyte (K): Unidad básica de medida para la memoria de las computadoras y la capacidad de los discos; equivale a 1,024 bytes. El prefijo kilo- indica 1,000, pero el mundo de las computadoras trabaja con doses, no con dieces: 210=1,024. Ya que un byte es lo mismo que un carácter en computación personal, 1 K de datos puede contener 1,024 caracteres (letras, números o signos de puntuación).

L

LAN: Siglas para Local Area Network (red de área local). Una red de comunicación de datos que cubre un área limitada.

LED: Siglas para Light Emitting Diode. Diodo emisor de luz.

login name: nombre de registro de entrada

En una red de computación, nombre único asignado por el administrador del sistema al usuario, que se usa como medio de identificación inicial. El usuario debe usar ese nombre, así como su contraseña, para tener acceso al sistema.

M

MAU: Siglas para Multi Station Access Unit (Unidad de acceso de estaciones múltiples). Un concentrador de alambrado usado para formar una configuración de cableado estrella.

Mb: Abreviatura alternativa de megabyte (1,048,576 bytes).

Megabyte (MB): Medida de capacidad de almacenamiento equivalente a aproximadamente un millón de bytes (1,048,576 bytes).

Megaflop: Una evaluación comparativa empleada para probar estaciones de trabajo, macrocomputadoras y minicomputadoras profesionales; un megaflop equivale a un millón de operaciones de punto flotante por segundo.

Megahertz (MHz) megahertzio: Unidad de medida que equivale a un millón de vibraciones o ciclos eléctricos por segundo; se usa por lo general para comparar las velocidades de reloj de las computadoras.

Aunque un millón de ciclos por segundo parece algo impresionante, según las normas actuales, la velocidad de reloj de 4.77 MHz de la primera computadora personal de IBM es considerada primitiva. En computación personal, cada vez son más comunes las velocidades de reloj de 66, 100 e incluso 133 MHz. Véase hertz (Hz).

Migración: Cambio de una antigua plataforma de hardware, un sistema operativo o una versión de software por uno más reciente.

Multimodo: Un dispositivo que emite o una fibra que carga modos de luz múltiples.

Multitareas. La palabra multitareas describe cómo un sistema operativo puede correr un número de aplicaciones al mismo tiempo. Esta es una de las características clave que distingue a UNIX como un sistema operativo poderoso.

Multiprocesamiento. El multiprocesamiento es la habilidad de usar múltiples microprocesadores sobre una misma computadora. Cuando se empieza a construir un sistema operativo, se diseña específicamente para aprovechar múltiples microprocesadores y por consiguiente este es capaz de ejecutar más instrucciones por segundo que un sistema operativo sin multiprocesamiento. El resultado final desde el punto de vista del usuario es que estos sistemas operativos son capaces de correr mucho más rápido que sus predecesores.

Multiusuario. El concepto de que muchos usuarios accederán aplicaciones o poder de procesamiento sobre un servidor era un sueño hace unos pocos años. UNIX ayudó a que este sueño se hiciera realidad en pocos años.

N

Name server (Servidor de Nombres): En una red de área local (LAN) conectada a Internet, una computadora que proporciona el Servicio de Nombres de Dominio, es decir, la traducción entre los nombres de dominio alfabético y las direcciones IP numéricas. Para

establecer una conexión con el proveedor del servicio Internet, usted necesita conocer la dirección IP del servidor de nombres.

NetBEUI: El protocolo utilizado por redes Microsoft LanManager y redes Microsoft Windows para trabajo en grupo. NetBEUI es la abreviatura de protocolo NetBIOS de interfaz extendida de usuario, este protocolo funciona bien para pequeños grupos de trabajo o redes departamentales. Es sencillo de instalar y bastante rápido para pequeñas tareas. Pero no escala bien a redes de empresas más grandes. Está limitado a 254 sesiones (conexiones a otras computadoras) para cada proceso. Más importante es el hecho de que NetBEUI no puede rutear desde un segmento de red a otro. Esto lo hace inapropiado para grandes entornos de red en los que se utilizan los routers para conectar los diferentes segmentos de red.

Network File System (NFS) Sistema de archivos de red: Una utilidad para acceso de archivos en una red, creado por Sun Microsystems y ofrecido posteriormente al público como estándar abierto, que permite a los usuarios de las estaciones de trabajo UNIX y Microsoft Windows NT tener acceso a archivos y directorios de otras computadoras como si estuvieran almacenados en la estación de trabajo del usuario.

O

Operador: Persona que usa una computadora. A menudo se le llama 'Operador' al administrador del sistema.

P

Parche: Reparación rápida en forma de uno o más enunciados de programa agregados a un programa para corregir errores o para mejorar las capacidades del mismo.

Password: Clave. Palabra que sirve para verificar que un usuario es realmente quien dice ser. Por eso mismo, el único que debe conocerla es ese mismo usuario.

Path (Ruta de acceso): Ruta que debe seguir el sistema operativo para encontrar un programa ejecutable guardado en un subdirectorio.

PGP: Siglas del programa Pretty Good Privacy (Privacidad muy buena). Está considerado el mejor programa de encriptación de correo electrónico para Internet y utiliza una combinación de claves públicas y privadas de hasta 2048 bits en su modalidad avanzada. El programa trata de aplicar algoritmos de encriptado a cada byte del fichero que vamos a enviar, con una clave de 128 bits o más, de forma que el resultado es un conjunto de caracteres incomprensibles. Una vez codificado, el archivo solo se puede decodificar con la clave opuesta a la que se ha utilizado. Si queremos mandar un mensaje codificado para que solo pueda abrirlo su destinatario legítimo, debemos encriptarlo con su clave pública y así solo se podrá abrir con la clave privada. Al revés, si queremos mandar un mensaje de forma que sólo lo hayamos podido mandar nosotros, debemos codificarlo con nuestra clave

privada y el destinatario usara nuestra clave privada para abrirlo. A diferencia de la firma, este sistema esconde el contenido del mensaje y lo hace inalterable.

Plug and Play: Un estándar emergente de hardware para accesorios, el cual requiere que el hardware sea capaz de identificarse a sí mismo, según la demanda, de manera estándar. Microsoft Windows 95 soporta Plug and Play y debe ayudar a crear un mercado para los periféricos de este tipo, que se espera sustituyan a los periféricos antiguos en breve.

Plug and Play BIOS (PnP BIOS): Un sistema básico de entrada-salida (BIOS) compatible con el estándar Plug and Play, que, al ser utilizado junto con un sistema operativo compatible con Plug and Play (como Microsoft Windows 95) y adaptadores compatibles con Plug and Play, le permite instalar adaptadores en el bus de expansión sin crear conflictos de solicitud de interrupción (IRQ) o conflictos de puertos. Observe que un BIOS "plug and play" no necesariamente es lo mismo que un BIOS Plug and Play (con mayúsculas), el cual se ajusta de manera precisa al estándar Plug and Play.

PostScript: Elaborado lenguaje de descripción de página (PDL) que se emplea para imprimir texto y gráficos de alta calidad en impresoras láser y otros dispositivos de impresión de alta resolución.

Aunque PostScript es un lenguaje de programación y el usuario puede aprender a escribir descripciones de página con él, PostScript es invisible y automático. El programa genera el código PostScript que va a la impresora, donde un intérprete de PostScript sigue las instrucciones para generar una imagen de la página que se pega al pie de la letra a las instrucciones.

Una de las ventajas más importantes de PostScript es su independencia de dispositivos; el usuario puede imprimir el código PostScript generado por un programa en cualquier impresora que cuente con un intérprete de PostScript. Asimismo, el usuario puede llevar sus archivos PostScript generados en una PC, a un taller de servicios donde imprimirán el documento con costosas máquinas de composición tipográfica, las que ofrecen resoluciones de hasta 2,400 puntos por pulgada. Véase PostScript font y PostScript printer.

PostScript font (fuente PostScript): Fuente perfilada escalable que se ajusta a las especificaciones de Adobe Software para las fuentes Type 1, las que requieren de una impresora PostScript.

A diferencia de una fuente en mapa de bits, la que a menudo se imprime con orillas y curvas burdas, la tecnología de fuente perfilada de PostScript produce caracteres uniformes que su impresora genera a su máxima resolución posible. Una fuente PostScript viene acompañada con una fuente para pantalla, la que emula la apariencia del tipo en pantalla, así como una fuente para impresora, que puede venir integrada en la impresora o debe copiarse a ésta antes de la impresión.

Advierta que el tipo puede tener una apariencia dentada en pantalla a menos que adquiera Adobe Type Manager, el que se encarga de llevar la tecnología de fuentes escalables PostScript a las pantallas de los monitores.

PostScript Nivel 2: Una versión mejorada de PostScript que es más rápida y soporta la impresión a color y la compresión de archivos.

PostScript Impresora: Por lo general láser, que incluye la circuitería de procesamiento necesaria para decodificar e interpretar instrucciones de impresión escritas en PostScript, lenguaje de descripción de página (PDL) muy usado en edición por computadora.

Como las impresoras PostScript requieren de su propia circuitería de microprocesador y por lo menos 1 M de RAM para crear la imagen de cada página, son más costosas que las impresoras que no son PostScript. Sin embargo, imprimen texto o gráficos en tonos sutiles de gris. También pueden usar gráficos y fuentes perfiladas PostScript Encapsulado (EPS), cuyo tamaño y escala puede modificar sin producir distorsiones.

Phreaker: Persona que usa comunicaciones sin pagarlas o pagando menos de lo que corresponde.

Protocolo: conjunto de reglas que se aplican para definir el método de intercambio de información entre dos dispositivos o computadoras.

R

RJ: Siglas para registered jack (jack o receptáculo registrado).

S

SC: Un tipo de conector de fibras ópticas. El SC utiliza el mismo casquillo de 2.5mm que el conector ST, contenido en una cubierta que permite la inserción y remoción del conector del adaptador por medio de empujar o halar. Se convirtió rápidamente en el conector de preferencia para redes de datos.

Servidor de Impresión: En una red de área local (LAN), computadora personal dedicada a recibir y guardar temporalmente archivos listos para impresión, los que se distribuyen uno a uno a una impresora. El servidor de impresión, accesible para todas las estaciones de trabajo de la red, corre un software integrador de impresión para manejar una cola de impresión.

Sistema Operativo: Programa que sirve de base para el funcionamiento de otros programas, supervisa la entrada y salida de datos y establece el conjunto de instrucciones que una computadora pueda ejecutar.

STP: Siglas para Shielded Twisted-pair par de conductores retorcidos con pantalla.

T

Topología: La arquitectura de una red o la forma en que los circuitos están conectados para enlazar los nodos de la red.

Transceptor: Un dispositivo usado en las redes de contención para enviar datos sobre la red y recibir datos de la red.

U

Unidad Optomagnética: Dispositivo para almacenamiento de datos que emplea tecnología láser para calentar un punto extremadamente pequeño en un cartucho magneto-óptico (MO) para que el medio magnético usado en el disco MO adquiera la capacidad de cambiar su orientación magnética cuando pasa la cabeza de lectura-escritura, son muy adecuadas para el almacenamiento de respaldo de grandes programas o datos que no se accesan con frecuencia.

UTP: Siglas para Unshield Twisted Pair par de conductores retorcidos sin pantalla. Cable de par retorcido sin protección o pantalla individual o conjunta.

VWXYZ

Vertical: La parte de una red de cableado que conecta el computador anfitrión o el cuadro de distribución principal al equipo localizado en otros pisos.

10BASE-T: Especificación de 10 Mb/s 802.3/Ethernet sobre cables de pares de conductores retorcidos sin pantalla. La 10BASE-T soporta configuraciones de red usando el método de acceso CSMA/CD en un sistema de transmisión sobre pares retorcidos hasta 100 metros de largo sin el uso de un repetidor.

Bibliografía

Bibliografía:

- System Administration Guide, Volume I. SunSoft, Sun Microsystems, Inc. Busines. 823 p.p.
- System Administration Guide, Volume II. SunSoft, Sun Microsystems, Inc. Busines. 624 p.p.
- NFS Administration Guide. SunSoft, Sun Microsystems, Inc. Busines. 120 p.p.
- Solaris 1.x to 2.x Transition Guide. SunSoft, Sun Microsystems, Inc. Busines.
- BRUCEH. Hunter Karen Bradford. Unix Networks An Overview For System administrators. USA, Hunterpretice Hall, 1996. 374 p.p.
- SIMSON Garfinkel & Gene Spafford. Practical UNIX & Internet Security, 2nd Edition, O'Reilly, 1004 p.p.
- LARRY Schumer, Chris Negus. Using Unix. 2^{da} ed. USA, QUE, 1995. 948 p.p.
- HERNANDEZ Jiménez Ricardo. Administración de centros de cómputo. 3^{ra} ed. México, Trillas, 1991. 267 p.p.
- KEVIN Stoltz. Todo acerca de redes de computación. México, Prentice Hall, 1995. 518 p.p.
- STAN Schatt, A fondo redes de área local. España, Anaya Multimedia, 1996. 294 p.p.

Páginas del WEB:

Manuales de Administración.

<http://www.ugu.com/sui/ugu/show?I=help.articles.admin&F=1111111111&G=Y>
<http://www.uwsg.indiana.edu/usail/installation/so/preinstall.html>

Unix Guru Universe

<http://www.ugu.com>

Página de Sun Micro Systems

<http://www.sun.com>

Página del servidor de Impresión Axis Print Server.

<http://www.axis.com>

Ghostview y Ghostscript

<http://www.adobe.com/prodindex/acrobat/adobepdf.html>

<http://www.adobe.com/prodindex/acrobat/prodinfo.html>

Glosario Hacker

<http://www.redestb.es/personal/hugo/byron/glosario.html>

Lista de productos utilizados

Sun, el logo de Sun, Sun Microsystems, SunSoft, el SunSoft logo, Solaris, SunOS, Open Windows, NFS, Solstice. Son marcas registradas de Sun Microsystems.

UNIX es marca registrada en los Estados Unidos y otros países, exclusivamente licenciada a través de X/Open Company, Ltd.

OPEN LOOK es una marca registrada por Novell, Inc.

PostScript y Display PostScript son marcas registradas por Adobe Systems, Inc.

Todas las SPARC marcas registradas, incluyendo SCD logo, son marcas registradas por SPARC International, Inc. SPARCstation, SPARCserver, UltraSPARC, y SPARCcompiler solamente tienen licencia para Sun Microsystems.

X Windows System es marca registrada de Xconsorcio.

UNIX y Berkeley 4.3 BSD Systems bajo licencia de UNIX systems laboratories, Inc, un dueño de totalmente subsidiario de Novell, Inc; y la Universidad de California respectivamente.

Los distribuidores de Software de terceros de este producto son protegidos por los derechos de proveedores de Sun.

Axis NPS 500
Axis Corporation.

Disco Optomagnético Vertex.
Pinnacle Micro Systems.

Office 95
Microsoft.

Visio
Visio Corporation.