UNIVERSIDAD AUTONOMA DE SAN LUIS POTOSI

FACULTAD DE CIENCIAS

ADMINISTRACION DE REDES Y SERVICIOS DE INTERNET SOBRE LINUX

TESIS PROFESIONAL PARA OBTENER EL TITULO:

INGENIERO ELECTRONICO

PRESENTA:

ROSANGEL DE GUADALUPE TORRES MORENO

MARIA ELIZABETH SANTIAGO CERVANTES

OSCAR HUMBERTO CATAÑO CASTILLO

SAN LUIS POTOSI, S.L.P. SEPTIEMBRE DEL 2004.

UNIVERSIDAD AUTONOMA DE SAN LUIS POTOSI

FACULTAD DE CIENCIAS

ADMINISTRACION DE REDES Y SERVICIOS DE INTERNET SOBRE LINUX

TESIS PROFESIONAL PARA OBTENER EL TITULO:

INGENIERO ELECTRONICO

PRESENTA:

ROSANGEL DE GUADALUPE TORRES MORENO

MARIA ELIZABETH SANTIAGO CERVANTES

OSCAR HUMBERTO CATAÑO CASTILLO

SAN LUIS POTOSI, S.L.P. SEPTIEMBRE DEL 2004.

UNIVERSIDAD AUTONOMA DE SAN LUIS POTOSI

FACULTAD DE CIENCIAS

ADMINISTRACION DE REDES Y SERVICIOS DE INTERNET SOBRE LINUX

TESIS PROFESIONAL PARA OBTENER EL TITULO:

INGENIERO ELECTRONICO

PRESENTA:

ROSANGEL DE GUADALUPE TORRES MORENO
MARIA ELIZABETH SANTIAGO CERVANTES
OSCAR HUMBERTO CATAÑO CASTILLO

ASESOR DE TESIS:

FISICO JORGE ALEJANDRO OCHOA CARDIEL

SAN LUIS POTOSI, S.L.P. SEPTIEMBRE DEL 2004.

AGRADECIMIENTOS

Le doy Gracias por la vida y el entendimiento, a mi gran amor Dionicio por el apoyo incondicional, a mi madre por que sin ella no hubiera seguido adelante a pesar de las adversidades, a Analú, Cesar, Iris, Rosaura, Bety, Dr Gonzalo, Prof. José Luis, Carmelita, Oscar Velásquez, Oscar Cataño Filemón, que estuvieron conmigo durante este duro camino y nunca les falto una palabra de aliento y apoyo.
A mi querida Elizabeth por que a pesar de todo siguió a mi lado de principio a fin Y por ultimo a quien hizo esto posible, por su confianza y la enseñanza de vida que me dejo, la gran capacidad de aprender y de seguir adelante y nunca decir no puedo.

Rosangel Guadalupe Torres Moreno

Agradezco a dios por darme la oportunidad de concluir una etapa mas en el largo camino de la vida, a mi compañero de toda la vida Cesar porque si su apoyo yo no hubiera podido continuar mis estudios profesionales, a mi familia por su apoyo incondicional en todo momento. Así como también a Rosangel por nunca dejarme desfallecer en los momentos de flaqueza. Y por ultima al Físico Alejandro Ochoa Cardiel por su apoyo y por haber hecho posible que esto concluya.

Maria Elizabeth Santiago Cervantes

A todos los profesores que influyeron para que continuara este camino de enseñanzas. Y a toda mi familia mil gracias por su apoyo en el transcurso de mi carrera profesional ya que sin su apoyo no hubiera sido posible concluirla ¡Gracias!. A

Oscar Humberto Cataño Castillo

INDICE.

INTRODUCCIÓN.

Servicios de Internet.

El Internet es una red mundial que ofrece servicios como correo electrónico, boletines de noticias, transferencia de archivos por medio de protocolos FTP, conferencias informativas y charlas electrónicas, así como también ofrecer acceso remoto a millones de bases de datos. No esta a cargo de una sola entidad, a partir de un punto de acceso único; si no que comprende redes interrelacionadas y agrupa empresas e instituciones de cooperación.

Uno de los servicios más importantes que ofrece Internet es el de correo electrónico que consiste en permitir que dos interlocutores intercambien mensajes sin importar la hora del día, permite realizar una transferencia de mensajes con casi todas las plataformas existentes, la comunicación se puede realizar con gente de cualquiera de los cuatro puntos cardinales del mundo en sólo segundos, el envío se logra por medio de la interacción de la familia de protocolos de comunicación.

El Internet cumple con normas y estándares que se encuentran contenidas en documentos llamados RFC (Request For Coment) y conforman protocolos que se encargan de definir la interrelación entre dos elementos de software y hardware, con lo cual garantiza una comunicación confiable y sin errores, en otras palabras, es un lenguaje empleado por la computadora para comunicarse por la red.

Algunos protocolos se encargan de definir el tipo de interface que se requiere, la plataforma en la que se trabajará y otros los diferentes tipos de servidores, de acuerdo a las necesidades del cliente.

Los protocolos se localizan dentro de las capas de los modelos estándares OSI y TCP/IP.
El modelo OSI es un esquema de red descriptivo que con sus estándares asegura mayor interoperabilidad y compatibilidad, entre distintos tipos de tecnología de red.
Describe la forma en la que la información fluye a través de las redes, y como la información se traslada desde programas de aplicación (por ejemplo hojas de cálculo) a través de un medio de red (por ejemplo cables). Es una estructura conceptual que especifica las funciones de red que se producen en cada capa.

Este modelo consta de 7 capas o niveles:
Las 3 capas superiores (se acercan mas al usuario) se relacionan con asuntos de aplicación, y las 4 inferiores se encargan del transporte de datos.

Por otro lado el protocolo TCP/IP es la arquitectura mas adaptada para la interconexión de sistemas (mientras que OSI se ha convertido en el modelo estándar para clasificar las funciones de comunicación), se le denomina globalmente como familia de protocolos TCP/IP y consiste en una extensa colección de protocolos que se han erigido como estándares de Internet.

A diferencia de OSI no hay un modelo oficial de referencia TCP/IP, pero se basa en los protocolos estándares que se han desarrollado, todas las tareas involucradas en la comunicación se pueden organizar en cinco capas relativamente independientes:

5. -CAPA DE APLICACION: aquí los protocolos definen la manera en que las aplicaciones usan la interred.
4. -CAPA DE TRANSPORTACION: los protocolos de esta capa especifican la manera de asegurar una transferencia confiable.
3. -CAPA DE INTERRED: los protocolos de esta capa indican el formato de los paquetes enviados por la interred, así como el mecanismo para reenviar paquetes del transmisor, por medio de los routers, a su destino final.
2. -CAPA DE INTERFAZ DE RED: especifica la organización de los datos en paquetes y la transmisión de los paquetes a través de la red.
1. -CAPA FISICA: se refiere al hardware.

El protocolo TCP/IP opera en la capa de Internet y todas sus funciones necesitan una interfase entre la capa física y la capa de Internet y son definidas como el nivel de enlace
Los protocolos del nivel de enlace incluyen enlace serial WAN (PPP), éstos proporcionan servicios lógicos tales como enmarcado, control de congestión y administración de enlace; todos los protocolos de nivel de enlace deben usar un medio de comunicación en la capa física, si lo comparamos con los medios de transportes diríamos que cada vehículo debe tener un medio, por ejemplo: el carro utiliza la calle, el barco a la mar, el tren los rieles, para que funcionen.

EL TCP/IP es independiente del medio físico porque todos los protocolos de enlace proporcionan la misma interface de IP. Para la entrada y la salida de datos se utilizan los mismo datagramas IP en los protocolos de nivel de enlace.

El protocolo IP (protocolo de Internet) se ocupa del direccionamiento dentro de Internet y se asegura que los medios de transmisión guarden o envíen los mensajes mediante una dirección que consta de cuatro valores separados por un punto cada uno, que va desde el cero al 255, se divide en dos partes, los primeros tres valores indica en donde se encuentra la máquina, es decir, le indica al router en donde se encuentra situada la máquina y la parte derecha indican el número correspondiente a la máquina anfitriona en la red.

Entre los protocolos de la familia TCP/IP se encuentra el Protocolo Punto a Punto (PPP), que consiste en una transmisión por paquetes seguida de una línea de comunicación serial vía módem; el protocolo PPP proporciona un protocolo de control de enlace (LCP) que se encarga de establecer, configurar y probar la conexión del enlace de datos, así como otro protocolo de control de red (NCP) que enlaza multiprotocolos, y realiza múltiples enlaces físicos con una distribución del ancho de banda.

Otro protocolo de Internet comúnmente utilizado es el protocolo de transferencia de archivos (FTP), el cual sirve para copiar archivos de una computadora a otra, transfiere tanto archivos de texto como binarios de un sitio a la maquina del usuario.

Existe gran variedad de sitios públicos llamados FTP anónimo, los cuales permiten a varios usuarios bajar archivos al mismo tiempo, es decir, permite transmitir en dos sentidos un archivo entre una computadora local y un servidor remoto; el cual, se puede definir como un sistema distante al cual se tiene acceso con la ayuda de una aplicación como por ejemplo Telnet o SSH (que es una conexión semejante a telnet pero segura), que cosiste en hacer la conexión remota, y utiliza el código ASCII, proporcionando un acceso en modo terminal; para ello se necesita un nombre de usuario y una contraseña, una vez que se conecta ahí el sistema remoto reemplaza al sistema local.

Otra manera de realizar este tipo de conexión es especificando el acceso a este servicio en el localizador uniforme de recursos (URL), al teclear FTP

Gracias al URL es factible tener acceso a la mayoría de los servicios con la ayuda de una dirección que comprende una sintaxis, formado por una sucesión de letras y números que comprenden, de manera jerárquica a una computadora, un directorio, un archivo, en un orden que va desde lo general a lo particular.

La URL tiene el siguiente formato:

Protocolo utilizado://nombre del domino del servidor/ruta de acceso al archivo

El dominio es la identificación de los grupos de computadoras y es dividida en varias secciones que permite una identificación precisa, cada sección separada por un punto, señala una organización diferente por ejemplo:

- .mx que pertenece al país en el que se encuentra una computadora, un directorio, un archivo, que en este caso es México.
- .edu que pertenece a una organización educativa.
- .com que pertenece a una organización comercial.
- .gob que pertenece a una organización gubernamental.
- .org que pertenece a un organismo no lucrativo.

El protocolo más utilizado en el Internet es el Protocolo de Transferencia de Hipertexto (HTTP), el cual es la base para todo servidor World Wide Web, este protocolo se encuentra en los niveles mas altos del protocolo TCP/IP, es decir, es la aplicación en el modelo de referencia OSI.
Es un protocolo cliente-servidor orientado a transacciones, el uso más común es la comunicación entre un navegador Web y un servidor Web, es decir, sirve para transmitir información con la eficiencia necesaria para hacer que el hipertexto salte.

El hipertexto es una metodología de presentación de información, gracias a la cual las palabras puestas en relieve (o enlaces) remiten a otros documentos de hipertexto. Para activar un enlace, basta con posicionarse en él y hacer clic. Los documentos pueden contener texto e imágenes, datos de vídeo, sonido y PostScript.

World Wide Web es un hipermedio dinámico conocido que permite obtener información al ofrecer un acceso fácil a los recursos mundiales, por medio de servidores de hipertexto.

El poder de WWW reside en los servidores que interactúan con Internet y extraen los documentos de todo el mundo, se componen de servidores y clientes.

Detrás de todo sitio Web se encuentra una pagina de texto codificada en HTML, el cual fue creado por programadores del centro europeo de investigación nuclear, con cede en Ginebra, Suiza; lenguaje que interpreta el programa navegador y permite escoger un tipo de letra, insertar elementos gráficos, introducir imágenes y crear hiperenlaces con documentos de otros sitios.

Una manera de representar estos servicios es realizando una implementación de un servidor de correo electrónico, una pagina web (con temas de interés para los alumnos de la UASLP), la conexión remota al servidor vía SSH y Telnet, una conexión FTP, así como la implementación de servicios de red con los servidores NFS para redes homogéneas LINUX y SAMBA para redes heterogéneas LINUX-WINDOWS.

Para poder llevar a cabo estas implementaciones se utiliza el software de fuente libre o código abierto (open source) Linux, que es un sistema gratuito, flexible y multiusuario que se distribuye por Internet, en algunas de sus distribuciones mas conocidas como RED HAT, SUSE y MANDRAKE.

CAPITULO 1

Estructura de Internet.

Internet.

El Internet nació en el año de 1969 con la necesidad de comunicación entre investigadores de Estados Unidos de América (debido a que este país tenía una amenaza de ataque nuclear), esta herramienta les permitía la comunicación a lo largo de todo el país, sin preocuparse por algún ataque a una maquina y perder toda la información de la red, si no de solamente de la maquina atacada.

En 1973, la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA), de los Estados Unidos, inició un programa para la investigación de tecnologías que permitieran la transmisión de paquetes de información entre redes de diferentes tipos y características. El proyecto tenía por objetivo la interconexión de redes, por lo que se le denominó "Internetting", y a la familia de redes de computadoras que surgió de esta investigación se le denominó "Internet". Su nombre fue ARPANET (Advanced Research Projects Agency), se basaron en dos técnicas de funcionamiento:

- El desarrollo de la tecnología de la conmutación por paquetes.
- El desarrollo de TCP/IP.

La ***conmutación por paquetes*** hace posible que los datos provenientes de diferentes maquinas compartan líneas de transmisión comunes.
Sin ellas serian necesarias líneas dedicadas que enlazaran una computadora directamente con otra, la red podía construirse con líneas que enlazaran un nodo[1] con otro, con los datos direccionados a través de los nodos, en función de su origen y destino.
Su funcionamiento está basado en dividir los datos en paquetes, cada uno de ellos con un código que contiene el destino y las instrucciones para reconstruir la información.

El TCP/IP (Protocolo de Control de Transmisión / Protocolo Internet), proporciona el medio estándar mediante el cual las computadoras puedan comunicarse unas con otras, con reglas que todos aceptan, el protocolo de la computadora establece procedimientos que permiten una comunicación efectiva.

Para realizar una conexión a Internet se necesita tener relación con varias componentes para que esta se lleve a cabo, como por ejemplo:

- Backbones: líneas de comunicación de alta velocidad y ancho de banda que unen hosts o redes.

[1] Termino usado informalmente para hacer referencia a un router o a una computadora conectada a una red

- Redes: grupos de hardware y software de comunicación dedicados a la administración de la comunicación a otras redes. Todas las redes tienen conexiones de alta velocidad para dos o más redes.
- Proveedores del Servicio de Internet (ISPs): son computadoras que tienen acceso a Internet.
- Hosts: computadoras cliente/servidor. En ellos es donde los usuarios ven la interacción con Internet. Cada computadora que se conecta directamente a una red es un host. Todos los hosts tienen una dirección de red única. Esta es comúnmente conocida como la dirección IP.

El TCP / IP nació a partir del modelo de red diseñado por la Organización Internacional para la Normalización (ISO), llamado modelo OSI el cual se transformó en el modelo arquitectónico principal para la comunicación entre equipos.

Teniendo como definición de modelo, una técnica de estructuración, en esta ella, las funciones de comunicación se distribuyen en un conjunto jerárquico de capas, en donde cada capa realiza un conjunto de funciones relacionadas entre sí, necesarias para comunicarse con otros sistemas.

En la actualidad, las funciones propias de una red de computadoras pueden ser divididas en las siete capas propuestas por ISO para su modelo de sistemas abiertos (OSI). Sin embargo la implantación real de una arquitectura puede diferir de este modelo. Las arquitecturas basadas en TCP/IP proponen cuatro capas en las que las funciones de las capas de Sesión y Presentación son responsabilidad de la capa de Aplicación y las capas de Liga de Datos y Física son vistas como la capa de Interfase a la Red. Por tal motivo para TCP/IP sólo existen las capas Interfase de Red, la de Intercomunicación en Red, la de Transporte y la de Aplicación.

Los modelos están diseñados del nivel mas alto (aplicación), debido a que el usuario final solo se preocupa por utilizar programas que le permiten realizar sus actividades cotidianas sin preocuparle, como hace la maquina para realizar las tareas requeridas de conexión y el transporte de la información.

Modelos OSI.

El modelo OSI es un esquema de red descriptivo que con sus estándares asegura mayor inter operabilidad y compatibilidad, entre distintos tipos de tecnología de red.

Describe la forma en la que la información fluye a través de las redes, y como la información se traslada desde programas de aplicación (por ejemplo hojas de calculo) a través de un medio de red (por ejemplo cables). Es una estructura conceptual que especifica las funciones de red que se producen en cada capa.

Este modelo consta de 7 capas o niveles:

Capa 7: APLICACIÓN

Más cercana al usuario; brinda servicios de red a las aplicaciones del usuario.
Esta capa no brinda servicios a ninguna otra capa OSI sino a procesos de aplicación que se ejecutan fuera del alcance del modelo OSI.

Ejemplo: Hojas de calculo
Procesamiento de texto
Terminales bancarias

- Identifica y establece la disponibilidad de los elementos que deben participar en la comunicación.
- Sincroniza las aplicaciones que cooperan entre sí.
- Establece los procedimientos para la recuperación de errores y el control de la integridad de los datos.
- Determina si existen suficientes recursos para la comunicación planificada.

Capa 6: PRESENTACIÓN

- Asegura que la capa de aplicación de un sistema pueda leer la información enviada por la capa de aplicación de otro sistema.
- Si es necesario la capa de presentación realiza una traducción entre varios formatos de representación de datos utilizando un formato de representación de datos común.

Capa 5: SESIÓN

- Establece, administra y pone fin a las sesiones entre aplicaciones. Las sesiones son diálogos entre dos o más entidades de presentación.
- Brinda sus servicios a la capa de presentación.
- Sincroniza el dialogo entre las entidades de la capa de presentación.
- Administra el intercambio de datos.
- Proporciona recursos para sincronización de unidades de dialogo, para la clase de servicio e informes de excepciones relacionados con la capa de sesiona, presentación y aplicación.

Capa 4: TRANSPORTE

- Segmenta y reensambla los datos en un flujo de datos
- Intenta suministrar un servicio de transporte de datos que proteja las capas superiores de los detalles de implementación de transporte.
- Se ocupa de temas tales como la confiabilidad del transporte a través de una inter red.

Capa 3: RED

- Esta capa realiza la transferencia de información entre sistemas finales a través de un tipo de red de comunicación.
- Libera a las capas superiores de la necesidad de tener conocimiento sobre la transmisión de datos subyacentes y las tecnologías de conmutación utilizadas para conectar los sistemas.
- La computadora establecerá un dialogo con la red para especificar la dirección destino y solicitar facilidades necesarias como por ejemplo la gestión de prioridades.

Capa 2: ENLACE DE DATOS

- Intenta que el enlace físico de los datos sea seguro.
- Proporciona los medios necesarios para activar, mantener y desactivar el enlace.
- Detección y control de errores.

Capa 1: FÍSICA

- Se encarga de la interfaz física de los dispositivos, define las reglas que rigen en la transmisión de los bits.
- Tiene cuatro características importantes:
- Mecánicas: Relacionadas con las propiedades físicas de la interfaz y con el medio de transmisión. Normalmente, dentro de estas características se incluye la especificación del conector que transmite las señales a través de conductores.
- Eléctricas: Especifica como se representan los bits, y la velocidad de transmisión.
- Funcionales: Especifican las funciones que realizan cada uno de los circuitos de la interfaz física entre el sistema y el medio de transmisión.
- De procedimiento: especifican la secuencia de eventos que se llevan a cabo en el intercambio del flujo de bits a través del medio físico.

TCP/IP

Se le denomina globalmente como familia de protocolos TCP/IP y consiste en una extensa colección de protocolos que se han erigido como estándares de Internet.

Sirve como protocolo de transporte para la Internet, permitiendo que millones de equipos informáticos de todo el mundo puedan comunicarse, estos protocolos de Internet pueden utilizarse a través de cualquier conjunto de redes interconectadas, son apropiadas tanto para las redes WAN[2] como para las LAN[3].

[2] WAN red de área amplia, geográficamente ilimitada.

La manera en que Internet permite a las computadoras conectarse es similar a como trabaja una LAN. Es decir, en una red simple, se tienen dos computadoras y una conexión de datos. Las computadoras se comunican enviando un paquete a través de la conexión, en donde un paquete es una unidad de datos que viaja entre hosts de una red específica, y que está conformado por dos secciones:

- Encabezado: contiene la localización de la dirección física y otros datos de red.
- Datos: contiene un datagrama.

A diferentes niveles de la estructura de capas estas unidades se conocen normalmente con diferentes nombres. En el nivel de capa de enlace de datos se llaman **tramas**, en el nivel de red se llaman **paquetes**, en el nivel de transporte se llaman **segmentos** y en el nivel de aplicación se llaman **mensajes**.

A medida que la información pasa por la estructura de capas cada una de ellas le agrega información de cabecera e incluye la unidad de la capa superior dentro de la carga.

Los dos protocolos de Internet que trabajan en conjunto para la transmisión de datos son:

- Transmission Control Protocol (TCP).
- Internet Protocol (IP).

Para realizar una transmisión de datos del interior de una red con otra red que se encuentra en el exterior, es necesario tener en cuenta que se utilizaran algunos equipos como los siguientes:

Repetidor, si se necesita regenerar la señal entre dos segmentos de red que se interconectan.

Módem, si se va a acceder a una computadora independiente o a otro sistema que esté lejos.

Puente (bridge) para conectar dos redes.

Encaminador (router) que dirige el paquete de datos determinando la ruta hacia su destino.

Pasarela (gateway) para establecer un enlace con una computadora o un mainframe.

Los router y gateways proveen las conexiones entre diferentes LANs. Si las LANs son del mismo tipo, se usa un router.

Si las LANs utilizan diferentes protocolos de comunicación, o topologías, se utilizan los gateways(que son usados para convertir los paquetes en el formato requerido).

[3] LAN: red de área local, en un edificio, aula.

Cuando un gateway recibe un paquete, el gateway utiliza la información de la dirección y el encabezado del datagrama para determinar la localización del destinatario de los datos. El gateway reempáqueta el datagrama en el formato del paquete adecuado, hacia la siguiente conexión. Los datos pueden cruzar varias LANs antes de llegar a su destino.

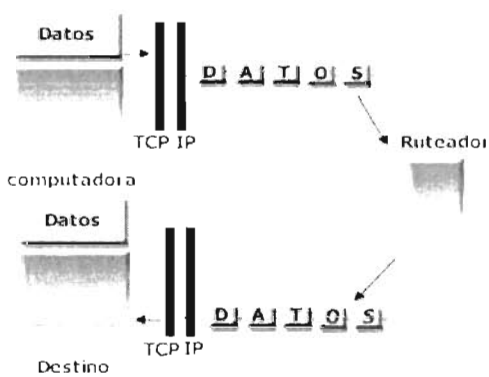
Internet es considerada una red de área amplia, independiente a la topología, ya que ve como iguales a todas las redes al conectarse, sin tomar en cuenta el tamaño de ellas, ya sean locales o de cobertura amplia. TCP/IP define que todas las redes que intercambiarán información deben estar conectadas a una misma computadora o equipo de procesamiento (dotados con dispositivos de comunicación); la independencia de las diversas topologías de LAN se debe al protocolo estándar IP. El encabezado del paquete IP contiene una dirección de cuatro octetos que identifican a cada una de los equipos. Cuando un paquete es enviado hacia un host, la computadora determina si el paquete es local o remoto (dentro o fuera de la LAN).

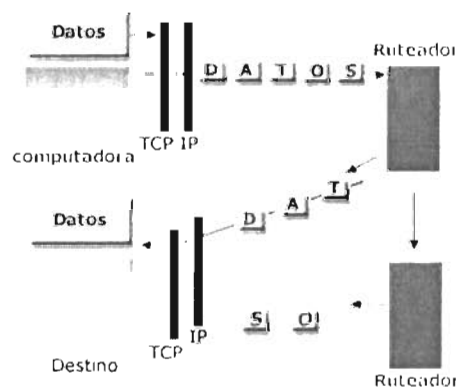
Si el paquete es local, el mismo lo transmite; si es remoto lo envía hacia un gateway el cual determina la dirección final.

La información de la dirección también determina cómo será ruoter el paquete a través de Internet. Normalmente el gateway utiliza la localización del destinatario para determinar la mejor ruta para enviar el paquete.

Si alguna red intermedia llegara a estar demasiado ocupada o no disponible, el gateway dinámicamente selecciona una ruta alterna. Una vez que el paquete es enviado, cada red que reciba el paquete, repite el proceso redirigiéndolo cuando sea necesario. Este proceso se repite hasta que el paquete llega a su destino.

Diferentes paquetes pueden tomar diferentes rutas, aún cuando contengan información del mismo archivo o mensaje. Los datos del paquete son reensamblados en el destinatario.



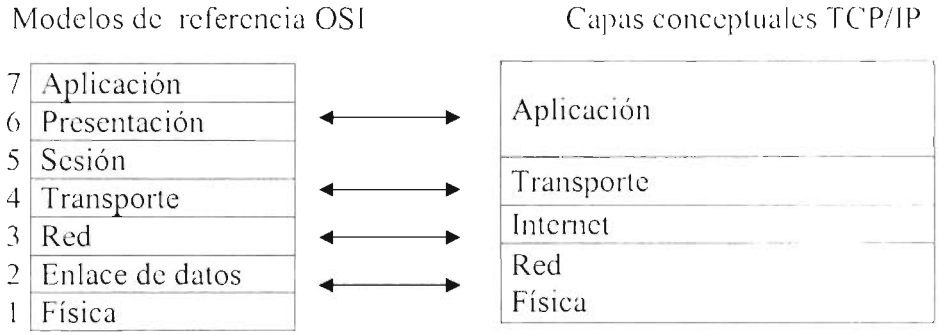


La labor principal de un router es disipar y coordinar la información perteneciente a las direcciones lógicas de red en un sistema, disipar la información para que los datos que viajan a través de una red lo hagan de la manera más eficiente posible.

Por definición ruteo es básicamente informar y decidir cual es la ruta más eficiente para enviar información. Si solo se tienen 10 o 15 computadoras, un servidor utilizando Linux es capaz de rutear toda la información en la red. Pero si se tiene una Red de computo compleja (con diversos sistemas operativos, abarcando diversas ciudades o países) es recomendable utilizar un producto especializado para esta labor.

Por ejemplo, si estamos en el nodo 152.23.14.232 y el sitio que deseamos visitar es otro que se encuentra en el nodo 232.12.10.12, para llegar de 152.23.14.232 a 232.12.10.12, el router disipa la información de ruteo, mediante algoritmos especializados (comúnmente llamados protocolos de ruteo) que agilizan y facilitan la transferencia de información de estas direcciones lógicas (nodos IP), estos algoritmos pueden ser implementados en varios Sistemas Operativos y su selección depende del tipo de conectividad que se emplee.

TCP/IP se relaciona estrechamente con las capas inferiores del modelo de referencia OSI, tal como se muestra a continuación, soporta todos los protocolos físicos y de enlace de datos estándar.



CAPA DE APLICACIÓN:

En esta capa las aplicaciones obtienen el acceso a la red.

Cuando una aplicación transmite datos a otro nodo, cada capa añade su propia información como un encabezado. Al ser recibido el paquete la capa remueve su encabezado correspondiente y trata el resto del paquete como datos.

Los protocolos de está capa están disponibles para la transferencia de archivos , el correo electrónico, la conexión remota, la emulación de terminales y la transferencia de archivos, así como también, brinda soporte para la administración de redes.

Transferencia de archivos TFTP FTP NFS	Correo electrónico SMTP	Conexión remota Telnet SSH Putty	Administración de la red SNMP	Administración de nombre DNS

CAPA DE TRANSPORTE:

Los protocolos de esta capa especifican la manera de asegurar una transferencia confiable, es decir ejecuta dos funciones:

- Control de flujo, que se realiza mediante ventanas deslizantes
- Confiabilidad, proporcionada por números de secuencia y acuses de recibo.
- Múltiplexa las unidades de datos que envían las aplicaciones a través de los puertos,
- encapsulándolas en datagramas UDP o segmentos TCP.
- Demúltiplexa los datagramas UDP y los segmentos TCP, pasando los datos a las aplicaciones.

En la capa transporte se proporciona dos protocolos:

Las aplicaciones acceden a los puertos a través de sockets UDP o TCP.

Los puertos de identifican por un número de 16 bits. Los puertos UDP y TCP se manejan por separado: el puerto 7 UDP y el puerto 7 TCP son puertos distintos.

Las conversaciones en las que no se relaciona una aplicación con un número de puerto conocido, se le asignan números de puerto seleccionados al azar dentro de un intervalo específico.
Estos números de puerto se usan como direcciones de origen y de destino en el segmento TCP.

TCP el cual es un protocolo confiable orientado a conexión. Se encarga de dividir los mensajes en segmentos , reagruparlos en la estación de destino, reenviar todo lo que no reciba y reagrupar los mensajes a partir de los segmentos. TCP brinda un circuito virtual entre aplicaciones de usuarios finales. Establece comunicaciones confiables para aplicaciones que transfieren una gran cantidad de datos al mismo tiempo o requieran una confirmación de los datos recibidos.

El Protocolo de Datagrama de Usuario (UDP) no posee conexiones y no es confiable. Aunque UDP es responsable por la transmisión de mensajes, no se provee ninguna verificación de software para la entrega de segmentos en esta capa; de ahí su denominación de "no confiable".

El servicio ofrecido por UDP sólo aumenta el ofrecido por IP en:

- números de puerto
- un checksum optativo

Por ello el servicio ofrecido es NO fiable, presentando problemas que las aplicaciones deben resolver:

- pueden perderse datagramas.
- pueden duplicarse datagramas.
- pueden desordenarse datagramas.

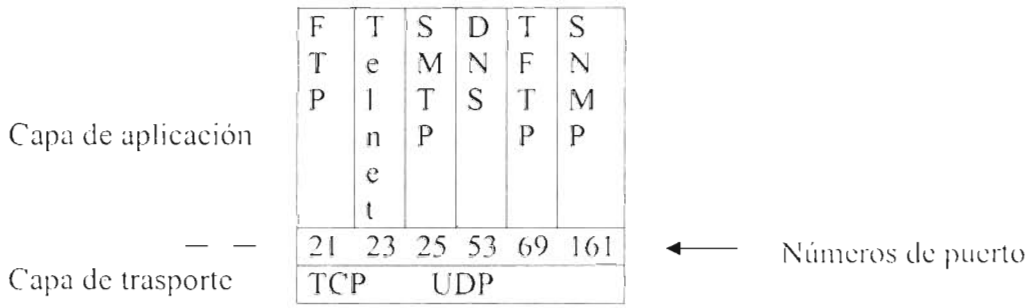
Formato de segmento TCP.

Campos de un segmento TCP:

Puerto de origen: numero de puerto que realiza la llamada.
Puerto de destino: numero del puerto que recibe la llamada.
Número de secuencia: número que garantiza la secuencia correcta de los datos entrantes.
Número de acuse de recibo: Octeto siguiente TCP esperado
HLEN: Cantidad de palabras de 32 bits en el encabezado
Reservado: se establece en cero
Bits de código: Funciones de control, tales como configuración y finalización de sesión.
Ventana: Número de octetos que el emisor desea aceptar.
Suma de comprobación: suma de comprobación calculada de los campos de encabezados y de datos.
Señal de urgencia: indica el final de los datos urgentes
Opción: La definida actualmente, tamaño máximo del segmento TCP
Datos: Datos de protocolo de la capa superior. Número de bits

Números de puerto.

Los números de puerto indican el protocolo de la capa superior que esta utilizando el transporte.



Tanto el UDP como el TCP usan (o toman) números de puerto para pasar información a las capas superiores, los números de puerto se utilizan para realiza un seguimiento a las distintas conversaciones que atraviesan la red simultáneamente. Las empresas que desarrollan software de aplicación coinciden en utilizar números de puerto conocidos que se definen en RFC 1700[4].

Ejemplos de números de puerto UDP reservados

Decimal	Clave	Descripción
0	------	Reservado
1-4	------	No Asignado
22	SSH	Conexión remota segura
23	telnet	Conexión de terminal
25	Smtp	Protocolo SMTP
42	nameserver	Servidor de nombre de host
43	nicname	Quién es
80	http	Servidor web*
21	ftp	Protocolo de transferencia de archivos
3128	Squid	Servidor proxy

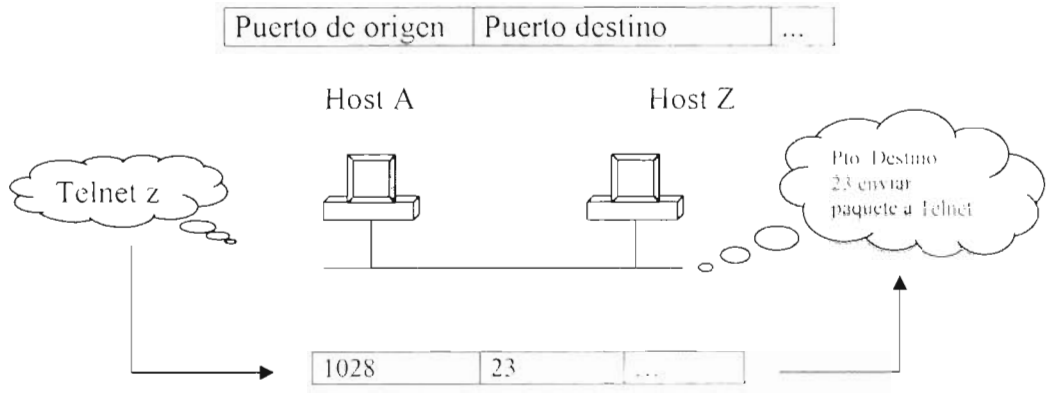
Algunos puertos están reservados tanto en TCP como en UDP, pero es posible que no se desarrollen aplicaciones que los utilice.

Los números de puerto tienen los siguientes intervalos asignados:

- Los números menores que 255 están designados para aplicaciones públicas.
- Los números del 255 al 1023 se asignan a empresas para aplicaciones comerciales.
- Los números mayores que 1023 no están regulados.

Un sistema final usa un número de puerto para seleccionar la aplicación adecuada. Un número de puerto origen.

[4] RFC (**R**equest **F**or **C**omments). En esta serie de documentos se detalla prácticamente todo lo relacionado con la tecnología de la que se sirve **Internet**: protocolos, recomendaciones, comunicaciones etc.



CAPA DE INTERNET:

Esta capa corresponde a la capa de red del modelo OSI, los protocolos de esta capa indican el formato de los paquetes enviados por la Internet, así como el mecanismo para reenviar paquetes del transmisor, por medio de los router, a su destino final.
Varios protocolos funcionan en la capa de Internet TCP/IP:

ICMP

Protocolo de mensajes de control en Internet, este protocolo se encarga de suministrar capacidades de control y de envío de mensajes, ayuda a supervisar la red.
Se utiliza para poder encontrar una ruta a través de la cual los datagramas viajan por la red y alcancen su destino.

Su objetivo principal es proporcionar la información de error o control entre nodos.
Una de las utilidades de diagnostico que utiliza este protocolo es PING (que se utiliza para comprobar si la computadora esta conectada a la red.

La implementación ICMP es obligatoria como subconjunto lógico del protocolo IP.

IP

Definido en la RFC 791, en esencia, es el sobre que contiene los mensajes generados por la mayor parte de los demás protocolos TCP/IP. Es un protocolo no orientado a conexión, no fiable, que realiza varias funciones que resultan críticas para llevar los paquetes desde el sistema origen al destino, debido a que no garantiza el control de flujo, la recuperación de errores ni que los datos lleguen a su destino.

IP proporciona un enrutamiento para la entrega de data gramas de "mejor esfuerzo" sin conexiones. No tiene en cuenta el contenido de los data gramas.

Mas bien, simplemente busca un modo para desplazar los datagramas de su destino, pudiendo llevar a cabo tareas de fragmentación y reensamblado.

Direccionamiento IP

Gracias a esta dirección otro ordenador sabe dónde tiene que enviar la información. Algunos ordenadores tienen siempre el mismo número IP (número IP fijo), mientras que a otros se les asigna un número IP nuevo cada vez que entran en Internet. En el último caso se habla de un número IP dinámico. Así pues, puede darse que un número IP determinado se asigne a distintas personas varias veces al día; y al contrario, que la misma persona entre en Internet varias veces y, por lo tanto, obtenga números IP distintos.

Los datagramas IP contiene una cabecera con información para el nivel IP y datos. Estos datagramas se encapsulan en tramas que, dependiendo de la red física utilizada, tienen una longitud determinada.

Cuando los datagramas viajan de unos equipos a otros pueden atravesar diferentes tipos de redes. El tamaño máximo de estos paquetes puede variar de una red a otra dependiendo del medio físico que se emplee para su transmisión. A este tamaño máximo se le denomina MTU (unidad máxima de transmisión) y ninguna red podrá transmitir ningún paquete cuya longitud exceda el MTU de dicha red.

Debido a este problema es necesario reconvertir los datagramas IP en el formato requerido por cada una de las redes que va atravesando. Esto es lo que se denomina fragmentación y reensamblado.

La fragmentación divide los paquetes en fragmentos de menor longitud (se realiza en el nivel más inferior posible y de forma transparente al resto de niveles) y el reensamblado realiza la operación contraria.

La dirección IP es la forma en que se localizan las computadoras. Para una computadora el manipular ***http://www.greenpeace.org*** o enviar un mail a ***usuarios@osmosislatina.com*** es sumamente ineficiente, por lo tanto utilizan direcciones IP

Cada computadora en Internet dispone de una dirección IP única de 32 bits, formados por cuatro campos de 8 bits separados por puntos, que identifican a cada uno de los equipos.

Los valores posibles están entre 0 y 255. Por lo tanto el intervalo completo de direcciones IP posibles va de 0.0.0.0 a 255.255.255.255,estos intervalos están compuestos por una dirección de red seguida de una dirección de subred y de una dirección de host (que indica el número que corresponde a la PC dentro de la red); la dirección de subred es una consecuencia del crecimiento de Internet y permite particionar la red lógica en redes menores.

Los 32 bits se representan normalmente como:

Dirección IP (binario):	11000001	10101000	00000000	00010100
Dirección IP (decimal):	192.	168.	0.	20

Todo paquete de data gramas IP transmitido por una red TCP/IP contiene la dirección de IP del sistema origen que lo ha generado y del sistema destino al que va dirigido en su cabecera IP.

Registro de Direcciones IP

Para que las direcciones IP identifiquen de forma única los sistemas de la red, resulta esencial que no se asigne la misma dirección a dos interfaces. En una red privada, los administradores deben garantizar que cada dirección es única. Pueden hacerlo controlando de forma manual las direcciones asignadas a sus redes y host o utilizando un servicio como DHCP[5] para asignarlas direcciones de forma automática.

La asignación de nodos IP en Internet es asignada por ciertas organizaciones, sin embargo cuando se requieren utilizar direcciones IP que no interfieran con estas direcciones globales se utilizan tres rangos definidos por RFC-1918. Se asume que ningún router deberá rutear información con estos nodos IP.

Los 3 rangos de nodos IP que deben de ser utilizados para configurar redes locales, son:

```
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255
```

El que no sean ruteables estos números IP garantiza que no surgirán conflictos con nodos de Internet también llamados "Routing Loops".

Además incrementa el nivel de seguridad en la Red Local (LAN), ya que estos nodos no pueden ser observados del exterior ; ahora bien, para que este tráfico pueda ser router al exterior (Internet) se requiere un mecanismo de traducción (NAT).

NAT ("Network Address Translation")

NAT es el método por el cual se traduce la dirección de un nodo en Red a otra dirección, su uso principal es cuando existen varios nodos IP en una LAN que requieren comunicarse al exterior pero solo existe un solo nodo al exterior.

[5] DHCP: un protocolo empleado para que los *hosts* (clientes) en una red puedan obtener su configuración de forma dinámica a través de un servidor del protocolo, como por ejemplo: la dirección IP, la máscara de red, la dirección de *broadcast*, las características del DNS

Varios productos "routers" ofrecen esta conversión, Cisco apoya el uso de NAT en casi todas sus plataformas mientras que una computadora Linux ofrece esta funcionalidad bajo el nombre de "IP Masquerading"

Clases de Direcciones IP

Las clases de direcciones aparecen resumidas a continuación:

	Clase A	Clase B	Clase C	Clase D	Clase E
Bits de dirección de red	8	16	24	N/D	N/D
Bits de dirección de host	24	16	8	N/D	N/D
Máscara de subred	255.0.0.0	255.255.0.0	255.255.255.0	N/D	N/D
Las direcciones comienza por: (binario)	0	10	110	1110	111
Valores del primer byte (decimal)	0-127	128-191	192-223	224-239	240.255
Número de redes	127	16.384	2.097.151	N/D	N/D
Número de hosts	16.777.214	65.534	254	N/D	N/D

CAPA DE RED.

CAPA FÍSICA.

Corresponde al Hardware. Puede ser cable, fibra óptica o línea telefónica, TCP/IP no considera oficialmente el nivel físico como componente específico de su modelo y tiende a agrupar el nivel físico con el nivel de red.

Los protocolos principales de este nivel son ARP y RARP[6].

ARP

El protocolo de resolución de direcciones, determina la dirección de la capa de enlace de datos para las direcciones IP conocidas, es decir , es utilizado para convertir las direcciones de la red física que pueden ser utilizadas por los manejadores.

Para poder realizar esta conversión, existe en cada computadora un módulo ARP que utiliza una tabla de direcciones ARP, que en la mayoría de las computadoras trata como si fuera una memoria intermedia (caché) de forma que la información que lleva mucho tiempo sin utilizarse se borra.
Si se encuentra la correspondencia entre la dirección IP y la dirección física se procede a la transmisión.
Si no la encuentra en la tabla, se genera una petición ARP que se difunde por toda la red

[6] Estos protocolos podrían ser representados por otros autores en la capa de Internet.

Si alguna de las computadoras de la red reconoce su propia dirección IP en la petición ARP, envía un mensaje de respuesta indicando su dirección física y se graba en la tabla de direcciones ARP.

RARP

El protocolo de resolución de dirección inversa determina las direcciones de red cuando se conocen las direcciones de la capa de enlace de datos, dicho en otras palabras, se utiliza cuando al producirse el arranque inicial, las computadoras no conocen su dirección IP.

Requiere que exista en la red, al menos , un servidor RARP. Cuando una computadora desea conocer su dirección IP envía un paquete que contiene su propia dirección física.

El servidor RARP, al recibir el paquete, busca en su tabla RARP la dirección IP correspondiente a la dirección física inicial indicada en el paquete y envía un paquete a la computadora origen con esta información.

Capitulo II.

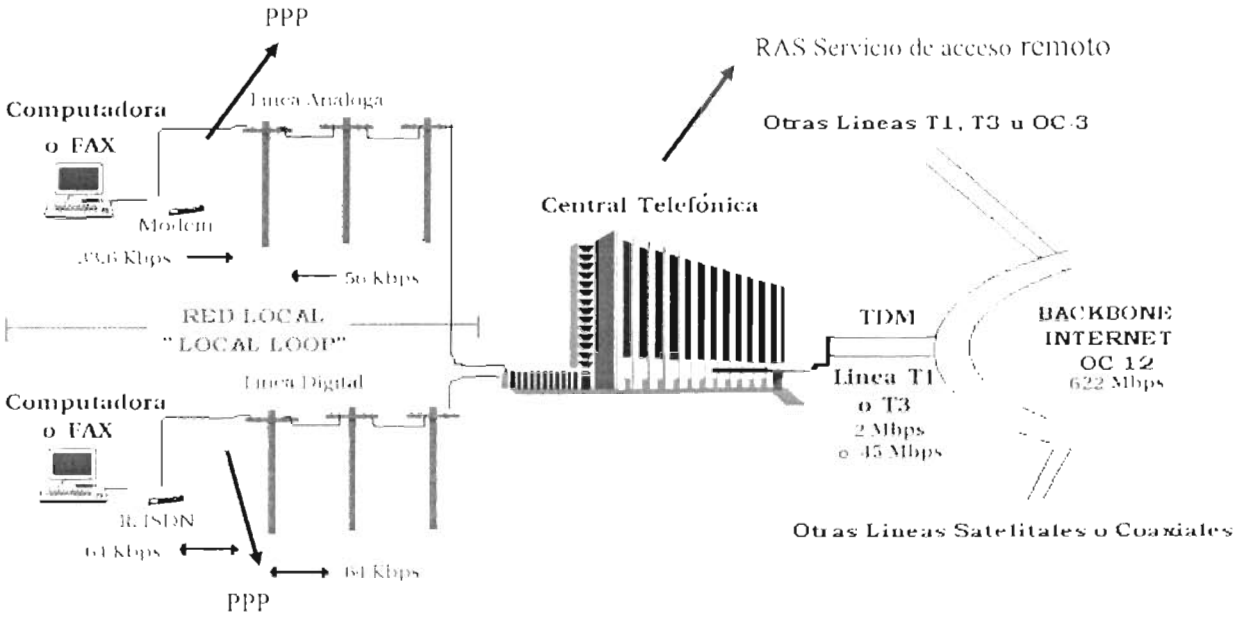
Conexión a internet.

Funcionamiento básico de Internet.

La PC llama al router del proveedor de Internet (ISP) a través de un módem conectado a la línea telefónica y así actúa como host de la red, la conexión desaparecerá cuando el usuario termine la sesión.
Una vez que el módem del router ha contestado el teléfono y se ha establecido una conexión física la PC manda una serie de paquetes de protocolo de control de enlace en el campo de datos de uno o más marcos PPP, estos paquetes y sus respuestas seleccionan los parámetros PPP por usar.
Posteriormente se envía una serie de paquetes de control de red para configurar la capa de red.
El proveedor de servicios asigna una dirección IP dinámicamente a la PC.
En este momento la PC es un host de Internet y puede enviar y recibir paquetes IP.
La PC indica al módem que cuelgue el teléfono, y así se libera la conexión de la capa física.

Tanto para la conexión por línea alquilada de router a router como para la conexión conmutada de host a router, se requiere de un protocolo punto a punto de enlace de datos en línea, para el manejo de marcos de control de errores y las demás funciones de la capa de enlace de datos.
Este protocolo pertenece al nivel de enlace de datos para adaptarse a las características de cada medio físico.

Cuando se utiliza un protocolo de enlace se requiere utilizar uno de los puertos seriales de la computadora, a la cual se conectará un módem que se encargará de convertir las señales digitales en señales que puedan viajar a través de la línea telefónica.
Estas señales serán recibidas por otro módem que se encargará de convertirlas nuevamente a señales digitales que pueden ser procesadas dentro de una red de datos.
Cabe señalar que la velocidad de transmisión de datos de la computadora, utilizando estos protocolos, estará en función de la velocidad máxima del puerto serial de la computadora, las velocidades máximas de operación de los módems locales y remotos y de la calidad de líneas telefónicas.
Una vez que se ha instalado el protocolo de enlace en la computadora, se podrán realizar actividades relacionadas con la capa de aplicación (FTP, SSH, WWW, etc.).



Tipos de acceso a Internet[7] :

Acceso indirecto: En este tipo de acceso la maquina es un terminal conectada a una computadora principal (vía módem), la cual a su vez tiene acceso a Internet. A este tipo de acceso también pertenece
el acceso terminal en el que la maquina esta dependiendo del software del servidor que tiene un acceso dedicado, es decir una terminal de otra maquina a la que esta conectada directamente.

Acceso directo: La computadora dentro de Internet se convierte en un nodo individual, capaz de hacer todo lo que sea posible de hacer en la red, la maquina tiene su propio número de IP, también se puede definir como servidor FTP, World Wide Web, Telnet, o SSH, esto dependerá de la potencia de la computadora y de la velocidad de la conexión.
Es necesario una línea dedicada de alta velocidad.
La maquina es una maquina por separado que depende de las computadoras principales, para cosas como software y archivos compartidos, pero es capaz de existir por si misma.

Otra forma de acceso directo es a través de conexiones SLIP (Serial Line Internet Protocol) o PPP (Point to Point Protocol) estos permiten permite acceso directo a Internet vía módem.

Se sigue dependiendo de una computadora anfitriona, a pesar de que se tiene acceso directo y de alta velocidad a Internet.

[7] Conocidos con otros nombres (según el autor del libro Internet en 21 días, Neil Randall), I o llama así debido a que de esta forma se distingue entre ser un nodo en la red o estar conectado a una maquina que a su vez, es un nodo en la red

PPP.

Los protocolos a nivel de enlace se ubican en los niveles bajos de la familia TCP/IP y permite que la computadora se comunique a la red utilizando líneas de comunicación seriales de baja velocidad.

El protocolo SLIP esta diseñado para el transporte de tráfico TCP/IP, es necesario conocer el número IP del usuario y del proveedor (algunas veces ocasiona problemas ya que se asignan las direcciones dinámicamente), en ocasiones es necesario configurar parámetros como por ejemplo; máxima unidad de transmisión, máxima unidad de recepción, el uso de cabeceras de compresión entre otros.

El PPP fue creado por el IETF (Internet Task Force) para mejorar algunas deficiencias, así como también es apto para líneas telefónicas conmutadas.
Fue diseñado específicamente para operar multiprotocolos sobre enlace serial, normalmente es asociado con las WAN. TCP /IP es independiente del medio físico ya que todos los protocolos de enlace proveen la misma interfase IP (es decir la salida y entrada de todos los protocolos de enlace es por el mismo IP), la interfase entre TCP /IP y una línea serial la proporciona PPP.
La línea serial es usada para conectar un router dentro de Internet y conectar usuarios a Internet.

Funcionamiento básico del Protocolo Punto a Punto.

Tiene tres elementos:

1. - Mecanismo para encapsular data gramas multiprotocolo y manejar la detección de errores.

2. - Protocolo de control de enlace para establecer, configurar y probar la conexión de datos.

3 - Protocolos de control de red, para establecer y configurar los distintos protocolos de nivel de red.

- El protocolo PPP proporciona un estándar para transportar data gramas multiprotocolo sobre enlaces simples punto a punto entre dos extremos del enlace mediante un mecanismo de enmarcado para usarse a través de módem, líneas de serie de bits, DLC[8] SONET y otras capas físicas.
- Estos enlaces proveen operación bidireccional full dúplex y se asume que los paquetes serán entregados en orden.
- Realiza detección de errores.
- Permite la negociación de direcciones de IP en el momento de la conexión.

[8] HDLC High - Level Data Link Control. Control de Enlace de Datos de Alto Nivel

- Permite la verificación de autenticidad.
- El protocolo PPP permite a una computadora establecer comunicación con una red de datos remota, convirtiéndose en un nodo de dicha red y pudiendo usar todos sus servicios tal cual lo haría si esa computadora estuviese conectada a la red directamente. Para lograr lo anterior la computadora utiliza un puerto serie, un módem y, como medio físico de enlace, una línea telefónica convencional.
- Los programas que implantan el PPP en una computadora además del protocolo mismo, implantan las capas superiores de la familia TCP/IP necesarias para una interacción total con una red de datos, que a su vez también debe estar implantada con los protocolos TCP/IP.
- Usa el relleno de caracteres en las líneas por discado con módem por lo que todos los marcos tienen un número entero de bytes.
- Proporciona un método de enmarcado que delinea el final de un marco y el inicio del siguiente, y consta de los siguientes campos:

Byte que se rellena si el protocolo acontece dentro del campo de carga útil:

Indicador estándar de HDLC	01111110

Para indicar que todas las estaciones deben aceptar el marco, para evitar tener que asignar direcciones de enlace de datos:

Dirección,	11111111

Indica un marco sin número, ya que PPP no proporciona por omisión transmisión confiable. Este campo pactará, con el campo de Dirección, una opción que los omita por completo y ahorre dos bytes por marco. Esto es posible gracias al mecanismo que proporciona otro protocolo que incluye el PPP, llamado LCP (protocolo de control de enlace).

Control	00000011

Protocolo, se encarga de indicar la clase de paquete que está en el campo de carga. Puede ser de dos bytes, y define códigos de protocolos que incluye el PPP. Los protocolos que comienzan con un bit 0 son protocolos de capa de red como IP, IPX, OSI, CLNP, y XNS. Los que empiezan por 1 se usan para negociar otros protocolos, LCP y NCP.

Protocolo	1 o 2 bytes

Carga útil, de longitud variable, negociable con LCP durante el establecimiento de la línea, si no es así se predetermina una longitud de 1500 bytes, la máxima longitud para este capo,

incluyendo el campo de protocolo, es determinada por la unidad máxima de recepción (MRU).

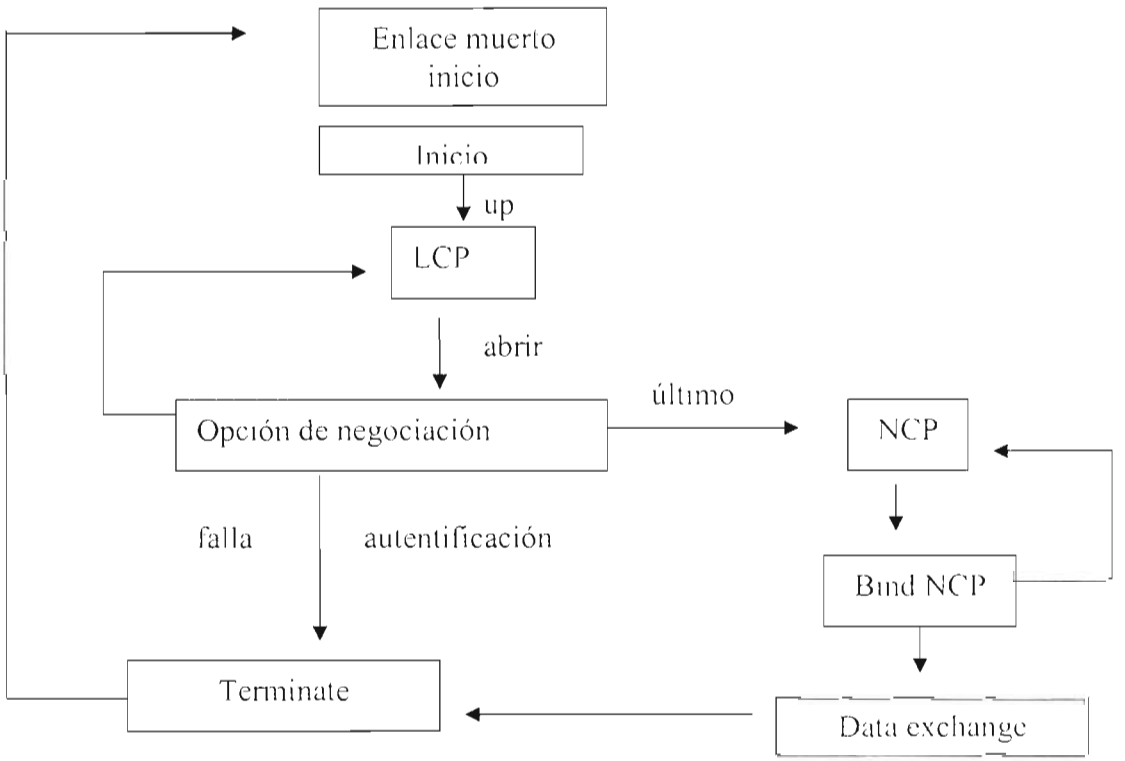
Suma de comprobación, de longitud entre 2 y 4 bytes.

Indicador, un byte cargado con (01111110).

Fases de operación

Las diferentes fases por las que pasa una línea cuando es activada, usada y desactivada, son validas tanto para las conexiones por módem como para las conexiones router - router.

Cuando se establece una conexión sobre el enlace punto a punto cada extremo debe enviar primero los paquetes LCP[9] para configurar y probar el enlace de datos, posteriormente debe ser validado, en este momento se envían paquetes NCP[10] para configurar uno o más protocolos de red. Después de la configuración de cada protocolo de red elegido sus datagramas pueden ser enviados a través del enlace.
El enlace permanecerá configurado para la comunicación hasta que una serie de paquetes NCP o LCP cierren la conexión, o hasta que ocurra un evento externo.



[9] LCP (Link Control Protocol) protocolo de enlace de datos.
[10] NCP (Network Control Protocols) protocolo de control de red

Fase de enlace muerto

El enlace comienza y termina en esta fase, cuando un evento externo, indica que la capa física está lista para ser usada, PPP continuara con la fase de establecimiento de enlace.

Fase de establecimiento de enlace

LCP es usado para establecer la conexión de enlace a través de un intercambio de paquetes de configuración, una vez que se ha enviado y recibido por ambos extremos un paquete de reconocimiento de configuración se habrá completado el intercambio y se llegará a estado abierto.

Fase de validación

La validación o autenticación no es obligatoria, si se desea que se autentifique con algún protocolo de validación específico, entonces se debe solicitar el uso del protocolo de autenticación durante la fase de establecimiento del enlace.
Esta fase debe tener lugar lo mas pronto posible después de la fase de enlace, y solo al completar la autenticación la fase de red podrá comenzar.

En esta fase sólo son permitidos paquetes del protocolo de control de enlace, el protocolo de autenticación y el monitoreo de calidad de enlace, cualquier otro paquete debe ser descartado.

La autenticación debe tener alguna manera de retransmitir y así proceder a la fase de terminación del enlace.

Fase de red

Cada protocolo de capa de red (IP, IPX, etc.) debe ser configurado por separado por el NCP apropiado, y debe ser abierto o cerrado de a uno por vez.

Fase abierta

Al alcanzar el estado abierto, PPP transportará los paquetes correspondientes del protocolo de capa de red.
El trafico del enlace consiste en cualquier combinación de paquetes LCP, NCP y protocolos de capa
de red.

Fase de terminación de enlace

LCP intercambia paquetes de terminación de enlace, y posteriormente PPP informa a los protocolos de capa de red que tomen la acción apropiada, la implementación debe avisar a la capa física que desconecte la línea para forzar la terminación del enlace, especialmente en la falla de una autenticación.
Al enviar un mensaje de terminación debe desconectarse al instante de recibir un reconocimiento de terminación.
Esta fase puede suceder a causa de un evento externo, como por ejemplo, la perdida de la señal portadora, una falla de autenticación una falla de la calidad del enlace, la expiración de un timer, o un cierre administrativo del enlace.

CAPITULO III

SEGURIDAD EN INTERNET

Seguridad en Internet.
Para obtener una red segura se tienen que realizar proceso de enmascaramiento (masquerading) y cortafuegos (firewall) ya que éstos se encargan de controlar la transmisión de datos.

Masquerading
El enmascaramiento permite a una computadora linux que ejerza de router para unir una red interna a una única dirección IP visible desde afuera, también se puede llevar a cabo con ayuda de normas de filtrado de paquetes.
El principio en el que se sustenta el enmascaramiento básicamente es de la siguiente manera: el router tiene más de una interfaz de red, que por regla general suelen ser una tarjeta de red y un módem; la conexión hacia el exterior se realiza por medio de una de estas interfaces, otra u otras conectan la computadora con otras computadoras en la misma red, la computadora destino solo conoce el router, y no la computadora en si de la red interna desde la que se envío el paquete, puesto que esta queda escondida detrás del router. Debido a la traducción de direcciones la dirección de destino del paquete de respuesta es de nuevo el router. Este debe reconocer el paquete y modificar la dirección de destino para que aterrice en la computadora correcta de la red local, éste reconocimiento de paquetes, de conexiones originadas por el masquerading del router, ocurre con ayuda de una tabla que se mantiene directamente en el kernel del router, mientras las conexiones correspondientes estén activas.

FIREWALL o Cortafuegos.

Es una entidad software o hardware que protege a una red de los intrusos exteriores regulando el tráfico que pasa por un router que la conecta con otra red. El término se usa con más frecuencia en relación con la protección frente a usuarios no autorizados de Internet. Cuando no se tiene ningún tipo de cortafuegos, los usuarios del exterior pueden acceder a los archivos de la red, introducir virus, usar los servidores para sus fines particulares e incluso borrar por completo las unidades de disco.
El cortafuegos permite que ciertos tipos de tráfico pasen a través del router de una red a otra, mientras que se niega el acceso a el resto del tráfico. Usan varios métodos diferentes para proporcionar varios grados de protección.

Existen distintos tipos de cortafuegos que de hecho se diferencian en el nivel lógico y abstracto en el que se examina y controla el tráfico de datos, realiza la función que realizaría un filtro, es decir, un filtro de paquetes regula el pasaje siguiendo criterios como el protocolo, el puerto y la dirección IP. De esta forma, también puede intereceptar paquetes que, debido a las señas que incluyen, no deberían entrar en la red.

Un ejemplo sería si se quiere permitir el acceso al servidor Web, entonces debe dejarse libre el puerto correspondiente, de esta manera no se examinará el contenido de estos paquetes si la dirección es la correcta. Pero el paquete podría contener un ataque a un programa CGI del servidor Web y el filtro de paquetes le permitiría el paso; para evitar esto, se puede realizar una combinación entre un filtro de paquetes y aplicaciones gateway / proxy. El filtro rechazaría paquetes que se dirigen a puertos que no están liberados, y dejaría pasar los paquetes para la aplicación gateway, así mismo, el proxy actuaría como si fuera el equivalente comunicativo real del servidor que establece una conexión con otros.

Servidor Proxy

Podemos auxiliarnos con un servidor proxy, como agente de seguridad debido al funcionamiento de este. Para las plataformas linux/Unix el caché proxy es Squid, éste se comporta como un agente que recibe peticiones de clientes y pasa estas peticiones al proveedor de servicios apropiado. Cuando los datos llegan de nuevo al agente, éste almacena una copia de los datos en un caché de disco. La ventaja de este sistema aparece cuando varios clientes intentan acceder a los mismo datos: ya no hará falta ir a buscarlo otra vez en Internet, si no que se servirán directamente desde el caché de disco, beneficiándose los usuarios de un ahorro importante en el ancho de banda y en el tiempo de descarga. También es posible emplear squid con un cortafuegos para proteger una red interna del exterior mediante un caché proxy. El cortafuegos cierra todo los servicios externos a excepción de squid, forzando a que sea el proxy quien establezca todas las comunicaciones con la WWW.

CAPITULO IV

SERVIDOR DE NOMBRES

DNS (Servidor de nombres de dominios).

Los equipos están diseñados para funcionar con números, mientras que las personas se sienten más a gusto trabajando con palabras. Está dicotomía fundamental es la razón de la creación del sistema de nombres de dominio (DNS).
DNS consiste en tres elementos básicos:

- Un espacio de nombres jerárquico que divide la base de datos de sistemas host en elementos diferenciados llamas dominios.
- Servidores de nombres de dominio que contienen información acerca de los host y de los subdominios del dominio.
- Resolvedores que hacen peticiones de información a los servidores de nombres de dominio.

Para asignar direcciones IP únicas a los equipos en toda la red Internet, se diseño un sistemas con dos partes en el que los administradores reciben los identificadores de red que forman la primera parte de las direcciones IP y después ellos asignan identificadores de host a los equipos individuales para formar la segunda parte de las direcciones.
Es importante establecer la identificación de una estación de trabajo de una forma que evite su duplicidad dentro de todas las computadoras que puedan conectarse, para ello, se utiliza el nombre del usuario y el del dominio de la red.

Para identificar al usuario es necesario nombrarlo de manera que evite que pueda haber dos con el mismo nombre y produzca confusiones al servidor de red.

Para identificar a la red se utiliza el concepto de dominio [es equivalente a un directorio, en cuanto a que puede contener subdominios (subdirectorios), o bien host (archivos)], esta formado por varios apartados separados por puntos.
El subdominio situado mas a la derecha es el de carácter mas general y recibe el nombre de dominio de nivel alto.

DNS asigna a los administradores nombres de dominio y, entonces, ellos son los responsables de especificar los nombres de host de los sistemas dentro de dichos dominios. Cada uno de los nombres entre los puntos puede tener hasta 63 caracteres con una longitud total del nombre DNS completo de 255 caracteres incluidos el host y todos sus dominios.

Esta denominación debe estructurarse de la siguiente manera:

nombre de la estación de trabajo (Host).nombre de la red(DOMINIO)

Si esta red formara parte de otra red superior, se volvería a poner otro punto y el nombre de dicha red. También se puede identificar la organización a la que pertenece así como el país al que pertenece la institución.

Dominio de Alto nivel de organización	
com	Organización comercial
edu	Organización educativa
gov	Organización gubernamental
mil	Organización militar
org	Organización si ánimo de lucro

Cuando alguien se conecta a Internet, usa DNS cada vez que pone un nombre o una URL en el explorador Web o en otra aplicación para convertir el nombre del sistema que se especifique a una dirección IP. En una red TCP/IP los administradores o los usuarios configuran clientes con las direcciones de los servidores DNS que van a usar. Este puede ser un proceso manual, realizado por cada estación, o automático, realizado por medio de un servicio como DHCP (protocolo de configuración dinámica de host).

DNS usa servidores distribuidos a lo largo de la red para resolver un nombre de la computadora (con la estructura de nombre de usuario, nombre de servidor, nombre de subdominio y nombre de dominio) en una dirección IP.

La resolución de nombres *(www.osmosislatina.com)* a nodos IP *(213.123.123.1)* ,es realizada por DNS y para llevar a cabo esta tarea se apoya en el software llamado **BIND** ("Berkeley Internet Name Domain") la localización de un sitio en Internet y el envió de correo electrónico dependen de esta resolución.

BIND funciona como un base de datos distribuida que mantiene información sobre las direcciones textuales de una Red.

Existe una autoridad que delega los Nodos IP únicos en Internet llamada IANA ("Internet Assigned Numbers Authority") , su registro en el Continente Americano esta delegado a ARIN, y en Europa y Medio Oriente a RIPE , generalmente su registro es llevado acabo únicamente por los proveedores de Internet más grandes (aquellos que mantienen parte del backbone de Internet).

Además de la asignación de los Nodos IP, lógicamente existe un depósito central de nodos IP a nombres (De *213.61.48.245* a *www.greenpeace.org*), aparentemente parece que fuera Network Solutions quien mantiene este depósito, pero este depósito central de nombres de nodos IP se mantiene actualmente en 13 DNS servidores raíz ("root servers") en el Mundo

(5 en U.S.A., 2 en Sudamérica, 3 en Europa y 3 en Asia). Estos servidores raíz contienen información relativa a los dominios .com, .edu, .org ,y claro esta, también existen otros servidores raíz de cada país .mx, .ar , .cl., y las raíces más recientes como .tv,.aero, y demás. La cuota que se paga al registrar un dominio es precisamente para la manutención de este servicio.

En el momento que se busca www.ibm.com la computadora no busca en los servidores raíz sino que, la resolución de estos nombres debe tratarse de realizar lo más cercano a la PC solicitante, es por eso que el proveedor de Servicios de Internet (ISP) mantiene un servidor DNS, ya que si para todas las paginas y envíos de correo electrónico se realizará una búsqueda en los servidores raíz, además de la carga que se llevarían estos servidores raíz, la resolución en lo que a tiempo se refiere sería muy tardada.

Por el contrario si se busca la página www.japanesesteel.com en México o un Italiano busca www.mexicansteel.mx es muy probable que los Servidores DNS de ambas ISP no contengan el nodo IP correspondiente, por lo tanto buscaran en otros servidores DNS para encontrar una resolución, y finalmente buscaran en uno de los servidores raíz del dominio (.com o .mx) que obligatoriamente debe de contener esta resolución.

CAPITULO V

SERVIDOR WEB

Los pilares básicos de la web son los siguientes:

- Servidores web: equipos que ejecutan un software que procesa peticiones de recursos
- de los clientes.
- Exploradores: Software de cliente que genera peticiones de recursos y las envía a los servidores web.
- Protocolo de transferencia de hipertexto (HTTP) El prototocolo de nivel de aplicación de TCP/IP que usan los servidores y exploradores para comunicarse.
- Lenguaje de marcado hipertextual (HTML) lenguaje de marcas usado para crear las páginas Web.

Un servidor web es un es un programa software que procesa peticiones de archivos específicos, que hacen los exploradores, y devuelve estos archivos al explorador. El servidor no lee el contenido de los archivos ni participa en el proceso que controla cómo se visualiza una página web en el explorador.

Plataformas de servidor web.

La plataforma de los equipos en los que se ejecuta el servidor no afecta generalmente a su conectividad con los clientes. Cualquier explorador puede conectarse a cualquier servidor

El servidor web de Unix más conocido es, Apache, un producto de dominio público basado en el servidor original httpd, su nombre se deriva del hecho de que el servidor usa el código httpd más una colección parches, por lo que se convierte en un servidor por parches.

Hay muchos módulos que se pueden añadir al núcleo del servidor que proporcionan características más avanzadas, tales como soporte de varios tipos de secuencias de comandos (scripts) y opciones de autentificación.

Suse Linux emplea el servidor de paginas web Apache. Sus archivos de configuración se encuentran en el directorio **/etc/httpd.conf** en el se realiza la configuración pertinente de acuerdo a las necesidades que requiera ofrecer a los usuarios entre ellos se encuentran los siguientes parámetros:

- Cantidad de usuarios que accesarán al servidor.
- Nombre de dominio que tendrá el servidor.
- Correo electrónico del administrador del servidor.

Tiempo que tardará en realizar la presentación de la página al usuario final.

Apache ofrece la posibilidad de poner varias paginas web de manera independiente, por medio de sus hosts virtuales.

SERVIDOR APACHE.

WWW es un hipermedio dinámico conocido que permite obtener información al ofrecer un acceso fácil a los recursos mundiales por medio de servidores de hipertexto.
Estos servidores de hipertexto utilizan la metodología de presentación de información gracias a la cual las palabras puestas en relieve (también llamados enlaces) remiten a otros documentos hipertexto y para ello basta con posicionarse en él y presionar entrar.

El poder de WWW reside en los servidores que interactúan con Internet y extraen los documentos de todo el mundo, se compone de servidores y clientes, los servidores son necesarios si se desea establecer una referencia de documentos hipertexto a los cuales otros usuarios pueden tener acceso y si solamente se quiere explorar la web, un visualizador y una conexión TCP/IP serán suficientes.

Funcionamiento de un servidor web.

El programa se ejecuta en segundo plano en un equipo y escucha en un puerto TCP/IP particular para detectar peticiones entrantes. Un programa de este tipo tiene diferentes nombres en los diversos sistemas operativos. En Windows es un servicio; en un sistema Unix es un demonio. El puerto TCP estándar para el servidor HTTP es el 80, a pesar de que la mayoría de los servidores permiten especificar un número de puerto diferente para un sitio y pueden utilizar un segundo número de puerto para la interfaz administrativa del servidor. Para acceder a un servidor Web usando un puerto diferente, se tiene que especificar ese número de puerto como parte de la dirección URL (localizador uniforme de recursos).

URL: localizador uniforme de recursos, gracias a el es factible tener acceso a la mayoría de los servicios con la ayuda de una dirección que comprende una sintaxis ,detrás de cada enlace se encuentra un URL y estos están ocultos a la vista.

La URL se compone de cuatro elementos que identifican los recursos a los que se quiere acceder:

- Protocolo, se especifica el protocolo de nivel de aplicación que el explorador usa para conectarse al servidor.
- Nombre de servidor, especifica el nombre DNS o la dirección IP del servidor.
- Número del puerto, especifica el numero del puerto en el que el servidor escucha en espera de trafico en espera de trafico entrante.
- Directorio y archivo, identifica la ubicación del archivo que el servidor debería enviar al explorador.

Protocolo://nombre del dominio del sitio web: puerto/directorio/archivo.html

Cuando se escribe simplemente un nombre DNS, el explorador asume que se está usando el protocolo HTTP, puerto 80 y el directorio principal del servidor web.

El único elemento que puede variar en los diferentes servidores es el nombre de la página web predeterminada, en los servidores Unix es index.html. El nombre de archivo predeterminado se configura en cada servidor y especifica el archivo que el servidor enviará al cliente cuando no se especifique ningún nombre de fichero en la dirección URL. El nombre de archivo predeterminado para los servidores web de Microsoft es default.htm

CGI.

La mayoría del tráfico generado en la web viaja del servidor al explorador. El trafico de subida del explorador al servidor consiste principalmente en peticiones http de archivos específicos. Sin embargo, hay mecanismos mediante los cuales los exploradores pueden enviar otro tipo de información a una aplicación para su proceso. Common Gatwey Interface (CGI) es el mecanismo de este tipo mas ampliamente admitido.

En la mayoría de los casos, los usuarios suministran información en un formulario diseñado en una pagina web por medio de etiquetas HTML estándar y después envía el formulario a un servidor. El servidor, cuando recibe los datos del explorador, ejecuta una secuencia de comandos CGI que define cómo se debe usar la información. El servidor podría enviar la información como una consulta a un servidor de base de datos, utilizarla para realizar una transacción financiera en línea o usarla para cualquier otro propósito.

HTML.

Formato estándar de documentos hipertexto llamado (lenguaje de señalización de hipertexto).
Detrás de todo sitio web, se encuentra una página codificada en HTML, el lenguaje que interpreta el navegador, y permite escoger un tipo de letra, insertar elementos gráficos, introducir imágenes y crear hiperenlaces con documentos de otros sitios.
El hecho de que la mayoría de estos archivos contengan código HTML es indiferente, porque el servidor no los lee. Sólo afectan a las funciones del servidor cuando el cliente analiza el código HTML y pide archivos adicionales al servidor si son necesarios para que el explorador muestre la página Web como archivos de imágenes.

Para programar HTML debe utilizar de forma simultanea un editor de texto para redactar los scripts y el programa de Internet para probar localmente las programaciones.

Una vez que termine de hacer los ajustes a la página, debe indicar la manera de bajarlas al servidor apache, a fin de realizar las ultimas pruebas.

Las formas de llevar a cabo esta operación varia conforme a los lineamientos de los proveedores de servicios de acceso a Internet.

HTTP (protocolo de transferencia de hipertexto).

Es el protocolo base del World Wide web (WWW) y se puede aplicar en cualquier aplicación cliente servidor que suponga la utilización de hipertextos.
Es un protocolo para transmitir información con la eficiencia necesaria para hacer que el hipertexto salte. Los datos transferidos por el protocolo pueden ser texto propiamente dicho, hipertexto, audio, imágenes o cualquier información accesible a través de Internet.

El protocolo de transferencia de Hipertexto (Hypertext Transfer Protocolo) es un protocolo cliente-servidor que articula los intercambios de información entre los clientes Web y los servidores http.

Desde el punto de vista de las comunicaciones, está soportado sobre los servicios de conexión TCP/IP y funciona de la misma forma que el resto de los servicios comunes de los entornos UNIX: un proceso servidor escucha en un puerto de comunicaciones TCP y espera las solicitudes de conexión de los clientes Web.

Una vez que se establece la conexión, el protocolo TCP se encarga de mantener la comunicación y garantizar un intercambio de datos libre de errores.
HTTP se basa en sencillas operaciones de solicitud-respuesta. Un cliente establece una conexión con el servidor y envía un mensaje con los datos de la solicitud. El servidor responde con un mensaje similar, que contiene el estado de la operación y su posible resultado. Todas las operaciones pueden adjuntar un objeto o recurso sobre el que actúan; cada objeto Web (documento HTML, fichero multimedia o aplicación CGI) es conocido por su URL.

En HTTP una sesión de usuario con el cliente Web supone obtener una secuencia de páginas y documentos Web así como la localización de las distintas páginas y documentos Web, puede ser una serie de servidores distribuidos mundialmente. Otra característica importante de HTTP es que es flexible en cuanto a los formatos que puede tratar. Cuando un cliente emite una solicitud a un servidor, puede incluir una lista de prioridades de formatos con los que puede operar, y el servidor responde con el formato adecuado. Por ejemplo, un navegador lynx no puede operar con imágenes, por lo tanto el servidor no necesita transmitir ninguna imagen de las páginas Web.
En cuanto a su funcionamiento el caso más sencillo es cuando se abre una conexión TCP. Por ejemplo, aquel en el que un agente usuario (cliente que inicia una petición). Entre estos se incluyen los navegadores, editores, etc.) establece una conexión directa con el servidor origen (servidor donde reside el recurso de interés)
Un ejemplo lo constituye un servidor Web en el que reside la página central deseada. Para este caso, el cliente abre una conexión TCP que es extremo-a-extremo entre el cliente y el servidor. El cliente emite una solicitud HTTP, la solicitud consta de la orden específica, referida a un método, un URL y un mensaje tipo MIME que contienen los parámetros de la solicitud, información sobre el cliente y tal vez alguna información de contenido adicional. Cuando el servidor recibe la solicitud, intenta llevar a cabo la acción solicitada y después devuelve una respuesta HTTP. La respuesta incluye información de estado, un código de éxito /error y un mensaje tipo MIME que contiene información del servidor con la respuesta misma y posiblemente el contenido del cuerpo. A continuación se cierra la conexión TCP.
Otro de los casos en cuanto al funcionamiento de HTTP es cuando no existe conexión TCP extremo-a-extremo entre el agente usuario y el servidor origen, en éste existen uno o más sistemas intermedios con conexiones lógicas entre sistemas adyacentes. Cada sistema adyacente actúa como un retransmisor, para que una solicitud iniciada por el cliente se retransmita a través de los sistemas intermedios hasta el servidor y la respuesta del servidor se retransmita de nuevo al cliente.

Se definen tres tipos de sistemas intermedios:

* Representante (proxy)
*Pasarela (gateway)
*Túnel (tunnel)

El representante funciona como un programa intermedio que actúa tanto como un servidor, como un cliente con objeto de hacer las peticiones de otros clientes. Las peticiones son servidas internamente o pasándolas, con la posible traducción a otros servidores. Un representante debe interpretar y si es necesario reescribir un mensaje de petición antes de reenviarlo. Los representantes son utilizados a menudo como pasarela del lado del cliente a través de cortafuegos de red y como aplicaciones de ayuda para tratar las peticiones a través de protocolos implementados por el agente usuario.

En la pasarela un servidor actúa como intermediario para otros servidores. A diferencia del representante, una pasarela recibe peticiones como si ella fuera el servidor original del recurso solicitado; el cliente solicitante podría no estar seguro si está comunicado con una pasarela. Las pasarelas se utilizan a menudo como puertas del lado del servidor a través de cortafuegos de red y como traductores de protocolos para acceder a recursos en sistemas que no siguen HTTP.

Finalmente el túnel es un programa intermedio que está actuando como un retransmisor ciego entre dos conexiones. Una vez que está activo, no se considera como una parte de la comunicación HTTP. Un túnel finaliza cuando ambos extremos de la conexión retransmitida se cierran. Los túneles se utilizan como portal si es necesario y el intermediario no puede o no debería interpretar la comunicación retransmitida.

Configuración del Servidor Apache

Durante el proceso de instalación pregunta el nombre del dominio y del servidor que se puede ser llenado con " localhost ".
En esta implementación el nombre del servidor es:

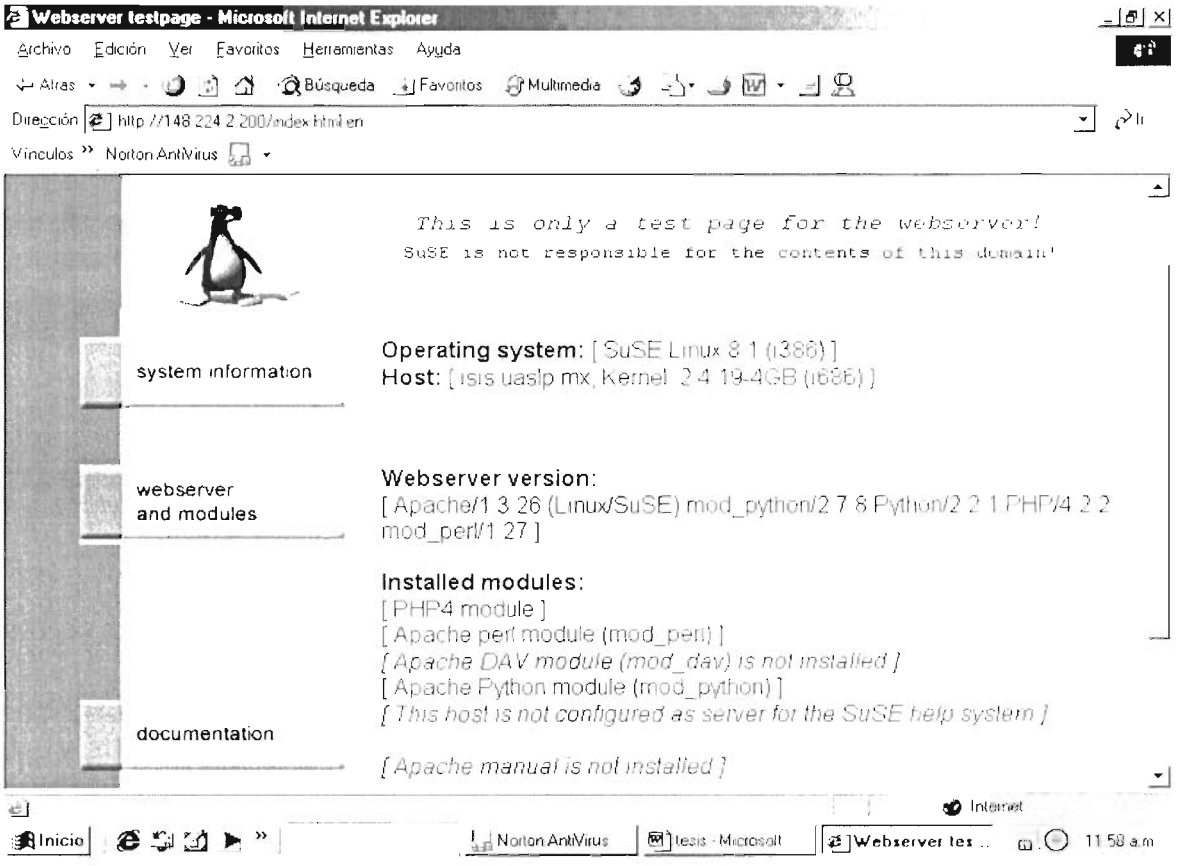
http://*Isis.fc.uaslp.mx* que es sustituido para fines prácticos por la dirección IP http://*148.224.2.200* por falta de nombre de dominio; aun que si se llama al servidor como localhost es posible hacerlo con este nombre.

Solicita una dirección de correo la cual fue asignada como administrador del servidor: *webmaster@isis.uaslp.mx* de igual manera la parte del dominio se sustituye como *webmaster@148.224.2.200.*

Pregunta si deseamos que el servidor responda por el puerto 80 para todos los usuarios ó si deseamos que solo se active para el usuario actual en el puerto 8080[11], cuando se inicie manualmente. Lo normal es activarlo para todos los usuarios. Con esto quedará configurado el servidor inicialmente. En cualquier momento se puede editar según las necesidades, para ello se debe editar el archivo httpd.conf que se encuentra en /etc/httpd/httpd.conf.

[11] Es importante verificar que no se tenga otro servidor trabajando en el puerto 80 (por ejemplo IIS que viene en las versiones profesionales o servidores de windows.

Para verificar si esta funcionando el servidor correctamente es necesario abrir un explorador y probar acceder a la URL http://localhost, si todo está bien se observara un mensaje de bienvenida del servidor como el siguiente:



CAPITULO VI

SERVIDOR DE CORREO ELECTRONICO

CORREO ELECTRÓNICO.

Es un medio de comunicación único que combina la inmediatez del teléfono con la precisión de la palabra escrita, el auge de Internet revolucionó el concepto de correo electrónico porque hoy día, las direcciones de correo son tan populares como los números telefónicos.
El correo electrónico de Internet, lo mismo que http y ftp , es una aplicación cliente / servidor. Sin embargo, en este caso, hay varios tipos de servidores involucrados en el proceso de comunicación del correo electrónico. Los servidores SMTP son responsables de recibir el correo saliente de los clientes y de transmitir los mensajes de correo a los servidores de destino. Otro tipo de servidor es el que mantiene los buzones y el que los clientes de correo electrónico usan para recuperar su correo entrante. Los dos tipos de protocolo predominantes para este tipo de servidor son el protocolo de oficina postal versión 3 (POP3) y el protocolo de accesos a mensajes de Internet (IMAP). En éste caso es importante entender que el término <<servidor>> se refiere a una aplicación y no necesariamente a un equipo separado. En muchos casos los servidores SMTP, POP3 o el IMAP se ejecutan al mismo tiempo.

Una dirección de correo electrónico consiste en el nombre del usuario y un nombre de dominio, separados por un símbolo @.
El nombre del dominio de una dirección de correo electrónico, que es todo lo que sigue al símbolo @, identifica a la organización que aloja los servicios de correo electrónico de un usuario en particular. La parte de usuario de la dirección , representa el nombre de un buzón que se ha creado en el servidor de correo que da servicio al dominio.
Como el correo electrónico se basa en nombres de dominio estándar para identificar a los servidores de correo, el sistema de nombres de dominio (DNS), es una parte esencial de la arquitectura del correo, los servidores DNS almacenan información en unidades de varios tipos llamadas registros de recursos. El registro MX es el que utiliza para distinguir a un servidor de correo de un dominio en particular. Cuando un servidor de correo recibe un mensaje saliente de un cliente de correo, lee la dirección del destinatario y realiza una búsqueda DNS del nombre dominio de la dirección. El servidor genera un mensaje DNS pidiendo el registro de recursos MX del dominio especificado, y el servidor DNS, después de realizar el proceso iterativo estándar que puede suponer reenviar la petición a otros servidores de dominio, responde con la dirección IP del servidor de correo electrónico del dominio de destino. El servidor que tiene el mensaje saliente abre entonces una conexión con el servidor de correo electrónico del dominio destino usando el protocolo sencillo de transferencia de correo (SMTP). Es el servidor de correo de destino el que procesa la parte de dirección de correo electrónico que lleva el nombre del usuario, poniendo el mensaje en el buzón adecuado, donde espera a que el cliente lo recoja.

Clientes y servidores de correo electrónico.

El correo electrónico, es una aplicación cliente servidor. Sin embargo, en este caso , hay varios tipos de servidores involucrados en el proceso de comunicación del correo electrónico. Los servidores SMTP son responsables de recibir el correo saliente de los clientes y de transmitir los mensajes de correo a los servidores destino. Otro tipo de servidor es el que mantiene los buzones y el que los clientes de correo usan para recuperar su correo entrante. Los dos protocolos predominantes para este tipo de servidor son Protocolo de oficina postal versión 3 (POP3) y el protocolo de acceso a mensajes de Internet (IMAP).
En muchos de los casos los servidores SMTP y el POP3 o el IMAP se ejecutan en el mismo equipo.
Uno de los servidores de SMTP más comunes usado en Internet es un programa gratuito llamado sendmail de Unix.
Después de instalar las aplicaciones de servidor de correo, el administrador crea un buzón para cada usuario y registra la dirección IP del servidor en un registro de recursos DNS MX del dominio. Esto permite a otros servidores SMTP de internet enviar correos a nuestros buzones. Los clientes acceden al servidor POP3 o IMAP para recoger el correo de sus buzones y envían mensajes salientes usando el servidor SMTP.

Protocolo SMTP.

SMTP especifica el formato exacto de los mensajes que un cliente debe enviar desde una computadora al servidor de otro pero no especifica cómo debe almacenarse el correo ni con que frecuencia se debe intentar el envío de los mensajes.
Los mensajes se pueden transportar mediante el protocolo TCP y usa en el puerto 25. Los mensajes se basan en comandos de texto ASCII, mas que en las cabeceras y campos usados en los protocolos de los niveles mas bajos de la pila de protocolos. El modelo de comunicación es siempre el mismo. Un equipo, llamado emisor SMTP, inicia la comunicación con el otro, llamado receptor SMTP, estableciendo una conexión TCP mediante la negociación estándar en tres fases.

Protocolo de oficina postal (POP3).

Es un servicio diseñado para proporcionar servicios de buzón a los equipos clientes que no son capaces por sí mismos de realizar transacciones con servidores SMTP.
En la mayoría de los casos la razón de que los clientes necesiten un servicio de buzón es que ellos no pueden estar conectados a internet continuamente y por consiguiente no son capaces de recibir mensajes en cualquier momento que un servidor SMTP quiera mandárselos. Un servidor POP3 está conectado continuamente y siempre puede recibir mensajes para los usuarios que están fuera de línea. El servidor mantiene los mensajes en un buzón hasta que el usuario se conecta al servidor y los pide.
POP3 es similar a SMTP en que se basa en el protocolo TCP para los servicios de transporte, usando el puerto 110, y se comunica con los clientes usando comandos basados en texto y respuestas.

POP3 tiene una desventaja debido a que si se quiere descargar el correo desde otro equipo de trabajo se eliminan automáticamente del equipo en el que originalmente se encontraban almacenados.

Protocolo de acceso a mensajes de Internet.

POP3 es un protocolo relativamente simple que proporciona a los clientes sólo las características más básicas de un servicio de buzón. En casi todos los casos, el servidor POP3 es un medio de almacenamiento temporal; los clientes de correo electrónico descargan sus mensajes del servidor POP3 y los borran del servidor inmediatamente después.
Es posible configurar un cliente para no borrar los mensajes después de descargarlos, pero el cliente debe entonces descargarlos de nuevo durante la sesión siguiente.

El protocolo de acceso a mensajes de Internet (IMAP) proporciona un número mayor de funciones que POP3, ya que esta diseñado para almacenar mensajes de correo electrónico en el servidor permanentemente y proporciona más comandos para que los clientes puedan acceder y manipular sus mensajes. El almacenamiento de correo en el servidor permite a los usuarios acceder fácilmente a su correo desde cualquier equipo o desde equipos diferentes (incluso los mensajes ya leídos desde otro lugar de trabajo).

IMAP incluye un número de características organizativas y de rendimiento:

Creación de carpetas en los buzones, así como, poder mover los mensajes de correo entre las carpetas para una organización jerárquica de los mismos.

El usuario puede ver las listas de los mensajes de su buzón con solo la información de la cabecera y después seleccionar los mensajes que quieren descargar completamente.

El usuario puede buscar mensajes basándose en el contenido de los campos de cabecera o en el cuerpo del mensaje.

Es importante notar que este servicio exige mas recursos de red que POP3, además del espacio de disco requerido para almacenar el correo en el servidor indefinidamente, así como consume mas ancho de banda de red por que los usuarios permanecen conectados al servidor durante periodos más largos de tiempo.

Configuración del correo electrónico.

En linux los mensajes se almacenan en el directorio **/var/spool/mail**, dentro de ese directorio hay varios archivos con los mails de todos los usuarios del sistema. Cada archivo lleva como titulo el nombre de usuario de su propietario.
El archivo de sendmail se encuentra en **/etc/sendmail.conf**.

Para realizar la configuración es necesario seguir los siguientes pasos:

- Crear un usuario en el sistema con el mismo nombre de su cuenta de Internet y que tenga acceso a los servicios de Internet.
- Indicar el servidor de correo para el envío de mensajes. De no saberlo es necesario consultarlo con el ISP. Una vez obtenida la dirección, se busca la siguiente cadena dentro del archivo de configuración.

#"Smart"relay host (maybe null)
DS

Y se le agrega la dirección del servidor pegada a la segunda línea. El resultado será el siguiente:

#"Smart"relay host (maybe null)
DSmail.isis.com

Si la segunda línea esta comentada es necesario quitar el comentario.

- Agragar una definición para que en todos los mensajes que se envíen se incluya la dirección del ISP en la celda FROM, para ello es necesario buscar la línea:

#Who Imasquerade as (null for no masquerading) (see also $=M)
DM

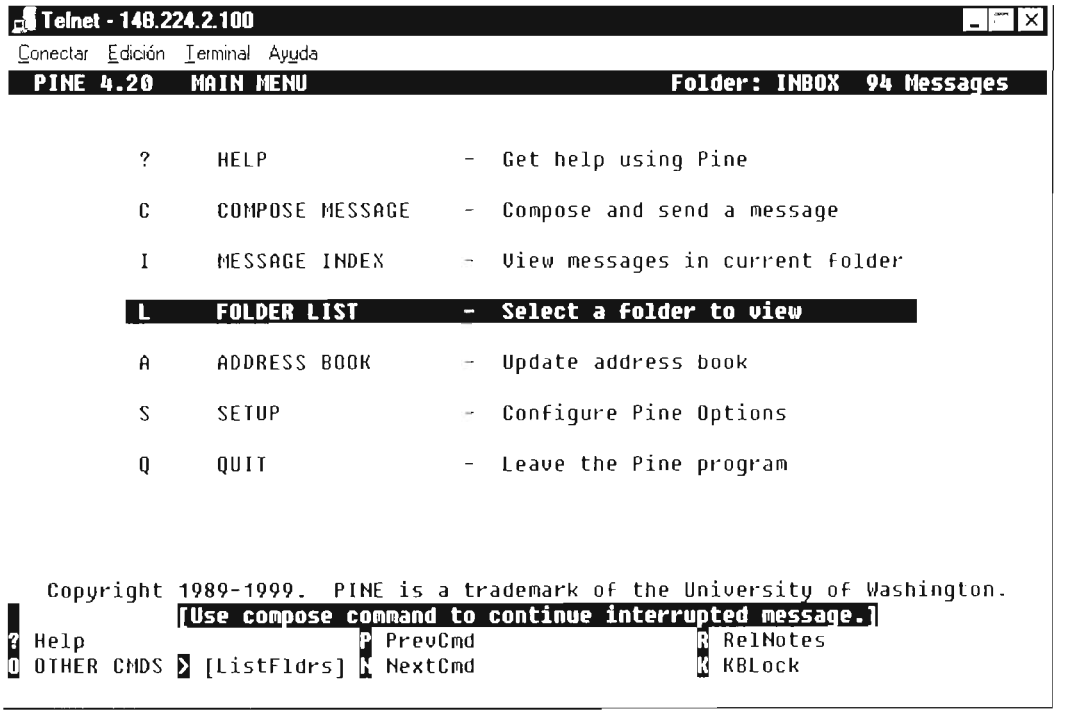
Y se debe modificar por la siguiente:

#Who Imasquerade as (null for no masquerading) (see also $=M)
DMisis.com

Siendo isis.com la dirección del servidor que figura luego de la "*@*" en la dirección de e-mail.

- Ahora se pueden enviar mails utilizando el comando ***mail*** seguida de la dirección de correo electrónico.
- Cuando se desean enviar todos los mails que se encuentran en la cola de envío, tecleamos "***sendmail -q*** ". Si se requiere consultar la cola de envío se utiliza el comando ***mailq***.

Para realizar la lectura del correo electrónico desde una maquina remota podemos utilizar SSH o putty; en la terminal es necesario únicamente escribir el comando PINE el cual nos introduce una pantalla mostrada en la parte inferior, en donde podemos realizar las tareas que requiramos, como enviar, configurar nuestro correo según nuestras necesidades, almacenar y ver los mensajes recibidos.



Mensajes instantáneos.

Si los usuarios están operando en el sistema al mismo tiempo (en diferentes terminales), pueden enviarse mensajes utilizando el comando:

write usuario
MENSAJE (...)
[ctrl.-D]

Si el sistema te envía un mensaje de error:

write: you have write permission turned off.

Esto se debe a que no esta habilitado el permiso para escribir mensajes, para habilitarlo, se utiliza el comando:

Mesg [y/n) topear
Mesgy

Chat.

Para establecer una comunicación con un usuario que esta conectado en el sistema, uno de los usuarios debe comenzar tipeando:

Talk usuario@localhost

Para permitir la sesión se utiliza ***ctrl.+c.***

El comando ***wall*** sirve para enviar mensajes colectivos (write all):

Wall mensaje

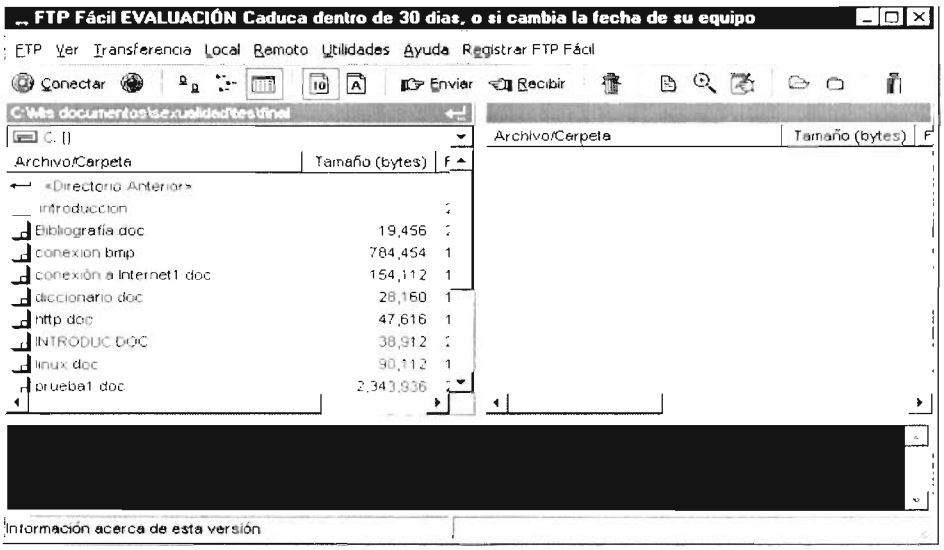
Capitulo VII

Servidor de transferencia de archivos

FTP.

Transfiere archivos entre una estación de trabajo y un servidor FTP y viceversa (pueden ejecutar sistemas operativos distintos).

Permite al cliente acceder al sistema de archivos de cualquier equipo que ejecute un servidor FTP. Por ejemplo: no se puede editar una archivo de un sistema remoto, pero se puede descargar al sistema local, editarlo aquí y volver a enviar la nueva versión a la ubicación original.
Al igual que telnet los usuarios deben autenticarse ante el servidor FTP antes de conseguir acceso al sistema de archivos. Muchos sistemas que ejecutan FTP, como los de Internet , soportan acceso anónimo , pero aun estos requieren un cierto proceso de autenticación en el que el usuario da el nombre <<anonymous>> y el servidor se configura para no aceptar contraseña.



Todas las estaciones de trabajo de trabajo Unix ejecutan un demonio de FTP y tienen un cliente de FTP, y muchos usuarios dependen del protocolo, para transferencias básicas de archivos LAN. FTP también es una utilidad normal en Internet, con miles de servidores públicos disponibles de los que los usuarios pueden descargar archivos.

FTP usa, como HTTP, el protocolo TCP para los servicios de transporte y se apoya en comandos de texto ASCII para su interfaz de usuario.

La gran diferencia entre FTP y HTTP, lo mismo que con muchos otros protocolos, es que FTP usa dos números de puerto en el curso de sus operaciones. Cuando un cliente FTP se conecta a un servidor, usa el puerto 21 para establecer una conexión de control. Esta conexión permanece abierta durante toda la sesión; el cliente y el servidor la usan para intercambiar comandos y respuestas. Cuando un cliente pide una transferencia de archivo, el servidor establece una segunda conexión en el puerto 20, que usa para transferir el archivo y la termina inmediatamente después.

Un cliente FTP consiste en una interfaz de usuario, que puede ser gráfica o basada en texto, y un interprete de protocolo de usuario. El intérprete de protocolo de usuario se comunica con el interprete de protocolo de servidor mediante comandos de texto que pasan por la comunicación de control. Cuando los comandos piden una transferencia de datos, uno de los interpretes de protocolo dispara un proceso de transferencia de datos, que se comunica con un proceso similar en la otra maquina usando una conexión de datos. Los comandos enviados por el interprete de protocolo de usuario no se corresponden necesariamente con los comandos tradicionales basados en texto de la interfaz de usuario.

Cuando se ejecuta en forma de sesión interactiva, es necesario utilizar las ordenes FTP.
Entre las más utilizadas se encuentran:

OPCION	SIGNIFICADO
! < comando>	Ejecuta el comando indicado en el equipo local (si no se especifica ningún comando, mostrará el símbolo del sistema. Escriba exit para volver a FTP.
? < orden>	Presenta una descripción de la orden indicada (si no se escribe ninguna, mostrará la lista de ordenes que reconoce).
APPEND < arch1> <arch2>	Añade el archivo de la estación de trabajo indicado en primer lugar al archivo del servidor FTP especificado en segunda posición.
QUIT	Termina la sesión FTP y sale de FTP.

Servidor_FTP indica el nombre del equipo remoto con el que se establece la conexión.

Opciones:
Este comando tiene las siguientes opciones:

a	Hace que se utilice cualquier interfaz local al realizar una conexión FTP.
d	Hace que la orden introducida haga eco en la pantalla.

Mensajes de FTP.

Una sesión FTP comienza cuando un cliente establece una conexión con un servidor usando una interfaz GUI o la línea de comandos para especificar el nombre DNS o la dirección IP del servidor. Lo primero es establecer una conexión TCP usando un protocolo estándar de negociación en tres fases. El servidor FTP escucha en el puerto 21 para ver si llegan mensajes, y esta conexión TCP nueva se convierte en una conexión de control que va a permanecer abierta durante toda la sesión. El primer mensaje FTP lo transmite el servidor, anunciándose e identificándose.

Durante la sesión ambos sistemas responden a los mensajes intercambiados con paquetes ACK de TCP/IP, según sea necesario. Después de enviar el asentimiento inicial, el cliente pide al usuario un nombre de cuenta y una contraseña y realiza la secuencia de conexión. Posteriormente el cliente informa al servidor de su dirección IP y del puerto que va a usar para la conexión de datos en el sistema cliente.

En este momento el cliente puede enviar comandos al servidor pidiendo transferencias de archivos o procedimientos del sistema de archivos, como creación o eliminación de directorios.

Capitulo VIII

Login Remoto

El momento de login (o logueo) es cuando el sistema pide un nombre de usuario y una contraseña al operador, para poder usarlo. Cada usuario del sistema posee un perfil diferente, que esta compuesto por:

- Su propia configuración del entorno de trabajo.
- Sus propias herramientas.
- Sus propios limites de acceso a datos.

Telnet.

Funciona abriendo el puerto 23 del sistema y esperando peticiones de registro su parte. Para que el sistema acepte este tipo de conexiones, deberá estar ejecutando el sistema el demonio de telnet (telnetd), si se cuenta con *inetd* se puede habilitar en el archivo */etc/inetd.conf*, otra forma de configurarlo es con el gestor de servicios de la distribución.

Para realizar una conexión telnet solo es necesario escribir en la línea de comandos lo siguiente:

telnet [host/ip]

esto hará que el sistema muestre el mensaje de bienvenida (este es definido por el administrador en el archivo */etc/issue.net*) y preguntará por un nombre de usuario y una contraseña.

SSH (Secure Shell) Conexión segura remota

Anteriormente era muy utilizado el protocolo TELNET que establece una conexión con otro sistema a través de la red y proporciona acceso a su shell. Una vez establecida la conexión, cualquier comando que se introduzca se ejecuta en el otro equipo usando su procesador. En telnet es necesaria la autentificación para que el sistema establezca la conexión, de esta manera exige el uso de un nombre de usuario y una contraseña para autentificarse, y así permite que un usuario, desde una terminal, acceda a los recursos y aplicaciones de otras computadoras. Una vez hecha la conexión queda establecida, actúa de intermediario entre ambos. Pero en la actualidad y en base a la necesidad de seguridad en las actividades que se realice con esta aplicación se implementa otra aplicación similar basada en la seguridad llamada ssh (secure shell).

Tradicionalmente en sistemas Unix en el momento de entrar en el sistema, tanto el login como el password, así como el resto de la sesión, se transmiten a través de nuestra LAN o incluso a través de router y nodos ajenos al nuestro en texto claro. Esto quiere decir que cualquiera que tenga activado un sniffer puede capturar nuestras sesiones con el potencial

peligro que ello conlleva. La manera de evitar que alguien pueda espiar las claves y sesiones, se utiliza una herramienta muy potente, fácil de instalar y muy cómoda para el usuario que no va a notar la diferencia entre el uso de ésta y la utilización de una sesión rlogin/telnet convencional.

En estos tiempos en los que las redes ya son omnipresentes, el acceso a un sistema es algo evidente. Antes de acceder siempre deberemos autentificarnos.

Por norma general los usuarios hoy en día deberían ser conscientes de que el nombre de usuario y la contraseña son sólo y exclusivamente para ellos. Por lo contrario sigue siendo temeraria la práctica que aun existe de enviar datos y autentificaciones en texto legible. Esto atañe principalmente a servicios tan usados como el Post Office Protocol (POP), usado para recoger correo. Estas condiciones de trabajo hacen que datos e informaciones del usuario, consideradas privadas (como por ejemplo el contenido de cartas o conversaciones realizadas a través del comando talk), circulen sin protección alguna a través de la red. Esto compromete por una parte la privacidad del usuario y por la otra deja abierta la puerta para posibles ataques. Este tipo de accesos se usan generalmente para poder desde ellos atacar a otros sistemas o para conseguir los derechos de administrador de ese sistema.

SSH (Secure SHell) es el nombre de un protocolo y del conjunto de herramientas que lo implementan. Este protocolo sirve para acceder a máquinas a través de una red, de forma similar a como se hacía con telnet o FTP.

La diferencia principal es que SSH usa técnicas de cifrado para que ningún atacante pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión. Al igual que telnet, sólo permite conexiones tipo terminal de texto, aunque puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un servidor X arrancado.

El software SSH ofrece una buena alternativa a nuestros problemas. Una autentificación completa, el nombre general se compone por nombre de usuario y contraseña, y además las comunicaciones se realizan de forma codificada. Y sí es cierto que aún así es posible el robo de datos transmitidos, estos no podrán ser leídos porque están encriptados. De esta manera es posible comunicarse de forma segura a través de redes inseguras como la Internet.

Además de la conexión a otras máquinas, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA] para no escribir claves al conectar a las máquinas y pasar los datos de cualquier otra aplicación por un canal seguro de SSH (esto sólo si tenemos acceso como administrador a ambas máquinas).

Como ya estamos acostumbrados en las aplicaciones de red y en especial dentro de Internet, ssh/sshd actúan basándose en la arquitectura cliente/servidor , en este caso concreto sshd se ejecuta en el servidor en un puerto (el defecto es el 22) a la espera de que

alguien utilizando un cliente ssh se conecte para ofrecerle una sesión segura encriptándola de extremo a extremo. Como veremos más adelante, también nos sirve para ofrecer mayor seguridad sustituyendo a programas ya clásicos y algo anticuados como rlogin, rsh, rcp, y rdist.

Sí bien vamos a resumir cómo trabaja y que otras opciones ofrece.

Previene ataques hechos mediante ip-spoofing.

Utiliza varios algoritmos (RSA para la llave de intercambio e IDEA, DES o triple DES para la encriptación de la sesión).

Permite sesiones X Window.

Permite redirección arbitraria de puertos en ambas direcciones. (Ideal para transferencias monetarias a través de la red, ejemplo e-cash).

Programa que viene con la distribución

sshd Es el servidor propiamente dicho, escucha a la espera de conexiones

ssh Es el cliente, con él nos podemos conectar a un servidor sshd así como ejecutar comandos.

scp Copia archivos con seguridad entre hosts. (Sustituto ideal de rcp)

ssh-keygen Usado para crear RSA keys (host keys y user authentication keys).

ssh-agent Agente de autentificación. (Usado para manejar RSA keys en la autentificación.)

ssh-add Se usa para añadir nuevas llaves con el agente.

make-ssh-known-hosts Usado para crear el archivo /etc/ssh_known_hosts .

4 Instalación y configuración.

En la mayoría de sistemas Unix, una vez descomprimido el paquete y dentro del directorio ssh-1.2.X se deberá teclear:

./configure

make

make install

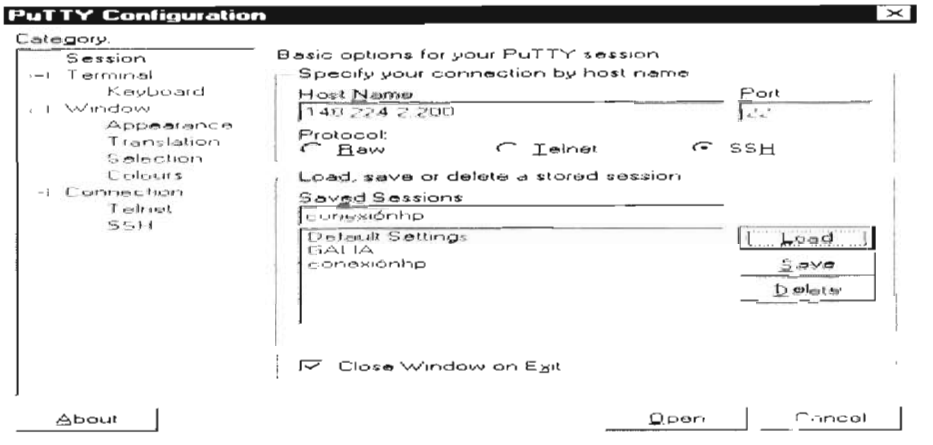
Después podemos revisar editar los archivos

/etc/sshd_config (Configuración del servidor sshd)

/etc/ssh_config (Configuración del cliente ssh)

Es muy importante preparar el sistema para que cada vez que lo reiniciemos, nos active el sshd, para ello basta con editar el /etc/rc.local o similar donde acostumbremos a poner nuestros ficheros de arranque y añadir la entrada /ruta/sshd . Una vez hecho esto y reiniciado el equipo, estará preparado y dispuesto para ofrecer sesiones seguras a aquellos que utilicen ssh y por supuesto estén dados de alta en el sistema.

La conexión que se realiza no dependerá de la plataforma a la que deseemos conectarnos ya que para ello existe el protocolo para las computadoras Microsoft, el cual es llamado PUTTY, de igual manera se configuran las preferencias de conexión.



5 Uso básico

ssh host (Iniciamos una sesión segura)

ssh host command (Ejecutamos un comando remoto en una sesión segura)

xterm -e ssh host & (en el caso de querer iniciar una sesión X-Window.

VNC.

El sistema VNC (Virtual Network) permite, utilizar el escritorio de un sistema de forma remota. Esto significa que podemos controlar un sistema desde otra terminal de una red, o desde cualquier computadora de Internet.

Se ejecutan dos aplicaciones que permiten llevar a cabo el proceso de control remoto.
Por un aldo tenemos el servidor VNC el cual se ejecutado en el sistema operativo que queremos controlar remotamente. Desde otra terminal, ejecutaremos un cliente VNC, que se encargara de establecer la conexión y mostrarnos en pantalla lo que supuestamente debería verse en el servidor.

Características.

Multiplataforma.- existen servidores y clientes para casi todos los sistemas operativos que poseen un entorno grafico. No hay necesidad que el cliente y el servidor estén ejecutándose en el mismo sistema operativo, sino que podemos tener por ejemplo, un servidor VNC en un sistema Windows, y el cliente puede estar ejecutándose desde un sistema GNU/Linux bajo Xwindow. Lo mas interesante es que hay clientes de VNC para Java, lo que quiere decir que podemos estar en la china viendo la pantalla del monitor de una computadora que esta en Nueva York por medio del navegador.

No se almacena información en el cliente.- El cliente actúa solo como visor del servidor. Ningún tipo de información del servidor se almacena en el cliente, además podemos estar trabajando en el escritorio, cerrar el cliente y al regresar el escritorio quedara en el mismo estado con las mismas aplicaciones abiertas tal cual como se dejo la ultima vez que se acceso al servidor VNC.

Permite compartir conexiones.- Una sesión VNC puede ser usada por muchos clientes simultáneamente

Es compacto.- Tanto servidor como cliente ocupan muy pocos KBs y se ejecutan hasta en sistemas carentes de recursos.

Funcionamiento.

El sistema VNC es un protocolo, que funciona transfiriendo imágenes de servidor a cliente. El servidor se encarga de realizar todas las tareas importantes de la conexión; los clientes son programas muy pequeños que solo se limitan a recibir el mensaje correspondiente que generalmente es del tipo "poner un píxel de n color en la posición x,y"


arpeta de inicio
de oscarhcc
mpezar aqui
Servicios
Papelera
VNC: WINXP
Inicio
Linux
VNC : WINXP

CAPITULO IX

Instalación De Servicios.

UNIX.

Unix no es un sistema operativo amigable, ni se puede encontrar en el escritorio del usuario medio de equipos personales. Para los partidarios de Unix, es el sistema operativo existente más potente, flexible y estable.

Como sistema operativo de servidor, Unix tiene fama de ser suficientemente estable para soportar aplicaciones con misiones críticas , bastante adaptable para ejecutarse en muchas plataformas hardware y suficiente capacidad ampliación para trabajar con una base de usuarios de casi cualquier tamaño.

A pesar de todo lo que se dice de su potencia y complejidad, no es imposible proporcionar a un usuario un sistema Unix con interfaz GUI (Interfaz grafica de ventanas para usuario) que ejecute aplicaciones como procesadores de texto y exploradores web, que funcionan de modo muy parecido a sus oponentes de Windows. Muchas de las características más potentes de Unix requieren la utilización de comandos en la interfaz de comandos del sistema, y en muchos casos, la GUI es simplemente otro programa que se ejecuta en el equipo, que se ejecuta en el equipo, que proporciona un método más simple para ejecutar estos comandos, más que una parte integral del sistema operativo.

Todos los sistemas Unix usan TCP/IP como protocolo nativo, de modo que resultan adecuados por naturaleza para su uso en internet y en redes con otros sistemas operativos.
De echo los sistema Unix fueron de gran ayuda en el desarrollo de Internet desde el experimento inicial como red de paquetes descentralizada hasta el fenómeno mundial que es hoy día.

Arquitectura de Unix

Los requisitos hardware de las diversas plataformas Unix varían sustancialmente, dependiendo de las funciones que se piden al equipo.
Independiente del hardware que use un sistema Unix, los componentes básicos son los siguientes:

Programas
Interfaz de comandos Shell
Núcleo (Kernel)
Hardware

El kernel es un modulo central que aísla a los programas del hardware, usa controladores de dispositivos que interaccionan con los dispositivos hardware instalados en el equipos para realizar funciones básicas como administración de memoria, entrada / salida, manejo de interrupciones y control de acceso.

Por encima del kernel está la interfaz de comandos que proporciona la interfaz para introducir comandos y ejecutar programas, esta interfaz es un interprete de comandos, muestra un símbolo del sistema basado en carácter utilizado para interaccionar con el sistema. Funciona como lenguaje de programación que se puede utilizar para archivos de comandos (scripts).

Los comandos básicos utilizados para la gestión de archivos y otras tareas estándar del sistema son iguales en todos. Las diferencias se hacen más evidentes cuando se ejecutan comandos más complejos y se crean secuencias de comandos.

La shell original de unix es un programa *sh*, mejor conocida como *Bourne shell* Algunas otras shell comunes son las siguientes:

Csh conocida como C shell; utiliza una sintaxis similar a la del lenguaje C e introduce características como un listado histórico de comandos y alias.

Ksh conocido Korn shell

Bash Es el shell predeterminada de Linux; muy relacionada con la Korn shell, con elementos de la C shell.

Linux.

Es el kernel ó núcleo de un sistema operativo parecido a UNIX, escrito por Linus Torvalds; al instalar y utilizar linux, se esta utilizando una distribución o colección de programas asociados y empaquetados con el kernel de linux.

Entre las distribuciones mas conocidas están:

- Red Hat
- Debian
- Caldera
- Mandrake
- Turbo Linux
- SuSE.

Es un sistema gratuito, flexible y potente que se distribuye bajo términos de la GPL o licencia Publica General de la Fundación de Software Gratuito, es distribuido por Internet y es fácil de descargar, actualizar y compartir.

Este sistema operativo pertenece a un género de software de fuente libre o abierta (open source); funciona de la siguiente manera:

El software debe acompañarse con el código fuente que lo haga funcionar, esto permite que los usuarios puedan realizar cambios, ejecuten reparaciones de errores, instalen parches y realicen mejoras para hacer que el software funcione mejor.

El software utiliza los conocimientos de los desarrolladores del mundo entero, en vez de unos pocos que trabajan para una sola empresa.

Los parches y reparaciones aparecen de la noche a la mañana, en vez de años después.

La Shell.

Después de haber instalado linux e iniciar una sesión linux se inicia un programa llamado Shell que proporciona una interfaz de línea de comandos entre el usuario y el kernel de linux. Los comandos escrito los interpreta la shell y se envía al kernel, que su vez abre, cierra, lee y escribe archivos; entre las funciones internas de la shell también se pueden usar para escribir programas.

Administración de usuarios y grupos.

Un usuario es alguien que tiene un identificador único en el sistema, un nombre y un número.
Esto permite que el Sistema operativo controle la forma en que se asegura el acceso al sistema y lo que puede hacer la persona una vez que ha sido aceptada.
Las actividades que cada usuario realice pueden ser monitoreadas o controladas por el sistema a través de su número de identificación de usuario.

Un grupo es un conjunto de usuarios. Cada grupo consta de un numero de identificación único, y un nombre único con los cuales se hace referencia a el. El administrador del Sistema controla el acceso por grupos.

Todo usuario y todo grupo poseen cierta información adjunta.

Información de usuario.

Campos de un usuario	Descripción
Login	Es el nombre con que se identifica un usuario en el sistema, este nombre debe ser único para evitar confusiones.

Password	La contraseña con la cual el usuario accede al Sistema.
UID	Abreviatura de Identificación de usuario. Este número se adjunta con el login. Y esta combinación debe ser única en el Sistema.
GID	Abreviatura de Identificación de Grupo. Este número se adjunta con el grupo al que pertenece el usuario. Cada usuario debe pertenecer al menos a un grupo.
Comentario	Aquí generalmente se pone el nombre completo del usuario para poder identificarlo, pero este campo esta libre para poder poner cualquier cosa que se desee.
Ruta de directorio de inicio	En este campo se va a almacenar la ruta del directorio donde se van a almacenar todos los archivos del usuario, como las configuraciones personales y de configuración.
Shell	Almacena el programa que se ejecutara automáticamente cuando el usuario inicia una sesión. Un programa shell es por ejemplo /bin/bash, lo que proporciona al usuario una orden UNIX.

Información de Grupo

Campos de un Grupo	Descripción
Name	Nombre de Grupo.
Password	Aquí se almacena la contraseña si se desea proteger al grupo para acceder a el. Generalmente este campo esta vació.
GID	Abreviatura de identificación de Grupo. Este se adjunta al nombre de grupo y todas las combinaciones Name/GID deben de ser únicas
Lista de usuarios	Aquí se almacena una lista de todos los usuarios que pertenecen a este grupo, separados por una coma.

Esta información se encuentran almacenadas en los archivos /etc/passwd y etc/group. Las aplicaciones y/o comandos que administran los usuarios y grupos modifican directamente estos archivos.

Agregar, modificar y eliminar usuarios desde la línea de comandos.

La instrucción ***useradd*** sirve para agregar un usuario desde la línea de comandos.

useradd *-c comentario -d directorio_de_inicio -e fecha_de_expiracion -f días_inactivos -g grupo_inicial -G grupos adicionales(,....) -m –k skeleton_dir -M -n -o -p password -r login*

en donde *login* es el nuevo nombre de inicio de sesión del usuario que se va a agregar. Cuando llamamos esta instrucción, crea una nueva cuenta de usuario con los valores especificados en la línea de comandos y los valores por defecto de el sistema. Las opciones que se pueden aplicar con useradd son:

Parámetros	Descripción
-c comentario	Se especifica los comentarios del nuevo usuario.
-d directorio_de_inicio	El nuevo usuario debe tener una carpeta para almacenar sus archivos y configuraciones, en este campo se le indica al sistema que directorio es. Por defecto RedHat le asigna un directorio dentro /home/ llamado igual que el nombre de inicio de sesión.
-e expire_date	Se asigna la fecha de que se deshabilitara la cuenta. La fecha debe ser especificada en el formato AAAA-MM-DD.
-f dias_inactivo	Aquí se especifican los días que la cuenta se desactivara después que la contraseña ha caducado. (Si se especifica 0 la cuenta se desactivara inmediatamente después de que la contraseña expire, Si se especifica -1 la cuenta no se desactivara después de que la contraseña caduque.)
-g grupo_inicial	El nuevo usuario tiene que pertenecer a un grupo, a través de este parámetro se especifica cual es. En caso de no especificar el sistema crea un nuevo grupo llamado igual que el nombre de inicio de sesión y lo asigna. El grupo debe existir
-G grupos_adicionales(,.....)	Se especifica una lista de grupos adicionales a los cuales el usuario también es miembro. Los grupos se encuentran separados por una coma.
-m	Con este parámetro se crea un directorio principal si no existe.
-M	Con este parámetro no se crea un directorio principal.
-n	No crea un grupo de usuario privado para el usuario.
-p pasword	Especifica la contraseña con la cual el usuario debe iniciar la sesión.
-r	Este parámetro es usado para crear una cuenta de sistema, esto es una cuenta con UID por debajo de 500 y esto significa que la cuenta nunca expira
-s shell	En este parámetro se asigna la shell (línea de comandos de conexión por defecto), generalmente se asigna /binb/bash.
-u UID	Valor numérico de la identificación del usuario, este valor debe ser único y no negativo. Generalmente redhat los empieza a asignar a partir del numero 500 ya que los restantes están reservados para cuentas del sistema.

El comando ***usermod*** permite modificar las configuraciones de un usuario existente.
Sintaxis:

usermod -c *comentario* -d *directorio_de_inicio* -m -e *fecha_de_expiracion* -f dias_*inactivos* -g *grupo_inicial* -G *grupos adicionales(,....)* -l *login* -p *password* -s *shell* -u *uid* -o -L -U *login*

en donde *login* es el nombre de inicio de sesión del usuario que se desea modificar. Cuando invocamos esta instrucción el sistema modifica la cuenta de usuario con los parámetros dados en la línea de comando. Las opciones que se aplican con esta instrucción son las mismas utilizadas con la instrucción useradd.

userdel

El comando userdel, elimina un usuario del sistema y sus archivos, siempre y cuando este no tenga iniciada su sesión.
userdel *–r login*

en donde *login* es el nombre de inicio de sesión del usuario que se desea eliminar. La opción que se aplica para esta instrucción es:

Parámetros	***Descripción***
-r	Si empleamos este parámetro la instrucción borrara todos los archivos, como su directorio principal y su correo electrónico. Los archivos que se encuentren fuera de estos directorios tendrán que ser buscado y ser borrados manualmente.

Agregar, modificar y eliminar grupos desde la linea de comandos.

Los comandos para la manipulación de grupos en Linux son sencillos de manejar, ya que no emplean tantos parámetros.

groupadd
Esta instrucción agrega usuarios desde la línea de comandos, usando la siguiente sintaxis.

groupadd -g *gid* -o -r -f *grupo*

donde grupo es el nuevo nombre de grupo que se va a agregar. Esta opción se puede aplicar con las siguientes opciones:

Parámetros	***Descripción***
-g gid	En este parámetro se asigna la identificación numérica de grupo, en caso de no hacerlo el sistema asigna por defecto un número mayor de 499.

Parámetros	***Descripción***
-o	Esta opción se aplica conjuntamente con la opción -g y obliga al usuario no asignar una identificación de grupo negativa.
-r	Esta opción le dice al sistema que se va a agregar un grupo de sistema. Y la primera identificación de grupo libre debajo de 499 se le es asignada.
-f	Esta opción causa que la instrucción pare con un error, cuando el grupo que esta siendo añadido ya existe en el sistema. En este caso grupo no se altera.

groupmod

Esta instrucción modifica los datos de grupo con los especificados en la línea de comandos.

Sintaxis:
groupmod -g *gid* -o -n *nuevo_nombre_grupo grupo*

donde grupo es el nombre de grupo del cual se van a modificar sus datos. Esta opción se puede aplicar con las siguientes opciones:

Parámetros	***Descripcion***
-g gid	Para cambiar el número de identificación de grupo (GID), se asigna este parámetro junto con su valor.
-o	Cuando esta opción es aplicada fuerza a no aceptar un numero de identificación negativo.
-n *nuevo_nombre_grupo*	Para cambiar el nombre del grupo, se asigna con esta opción seguida de su nuevo nombre de grupo.

groupdel

Elimina un grupo existente en el sistema, y todas las entradas que hacen referencias a ese grupo.

Sintaxis:
groupdel *nombredegrupo*

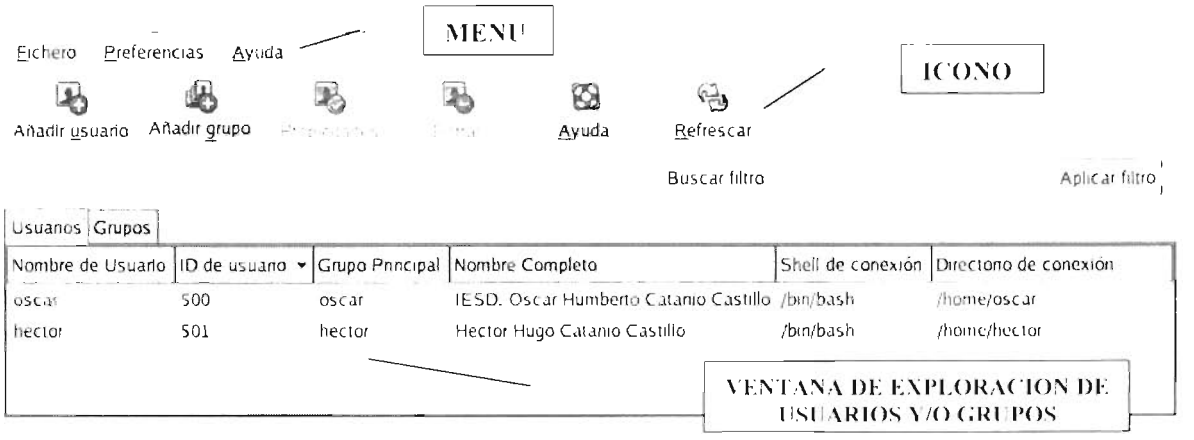
Donde nombre de grupo es el nombre de grupo que deseamos eliminar. Es importante decir que el grupo debe existir y que este no debe de tener usuarios perteneciendo a este grupo.

Uso de herramientas grafica user manager

La herramienta user manager para la distribución de redhat 9 sirve para la manipulación de todos los aspectos relacionados a la creación, modificación o eliminación de usuarios y grupos. Y debido a su interfaz grafica es muy ameno trabajar con esta herramienta.

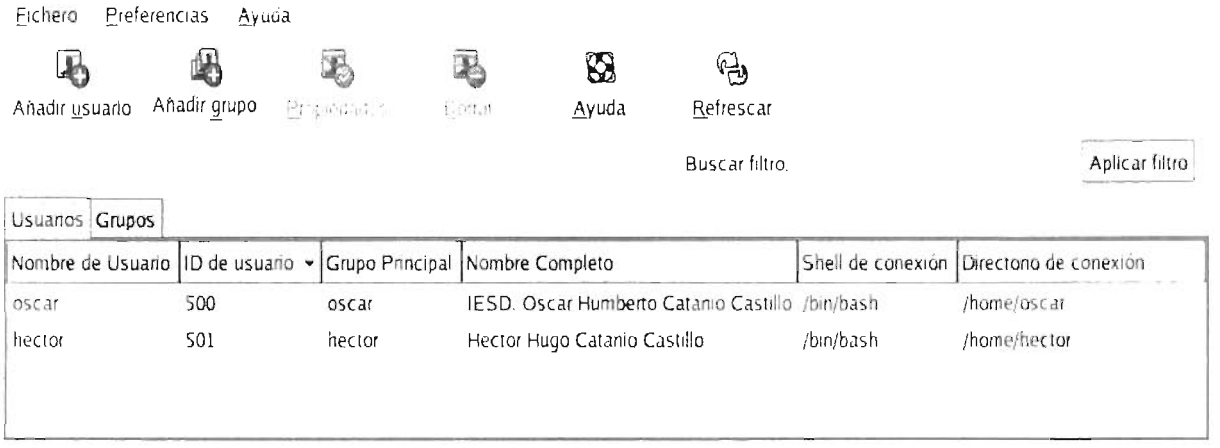
Para iniciar esta herramienta hay que ejecutar el lanzador que se encuentra en el Menú Principal de redhat 9 y en el submenú configuración del sistema, o bien teclear en una terminal siguiente: redhat-config-users.

Esto nos abrirá una nueva ventana como la que se muestra en la figura siguiente



Inicialmente esta ventana muestra en la parte de arriba una serie de menús para la manipulación los usuarios y grupos, también como iconos para tareas específicas. como añadir usuario, añadir grupo, propiedades, borrar, ayuda y refrescar, debajo de esto tendremos una ventana con dos pestañas; Usuarios y Grupos.
Cada pestaña muestra la información de los usuarios o grupos que se encuentran en nuestro sistema Linux.

La ventana de usuarios se compone de seis columnas, como se muestra en la figura siguiente, que corresponden a la información contenida en cada cuenta de usuario:



- Nombre de Usuario.- Muestra el nombre de inicio de sesión de los usuarios.
- ID de Usuario.- Muestra la identificación numérica del usuario para el sistema.
- Grupo Principal.- Muestra el grupo principal a la que pertenece el usuario.

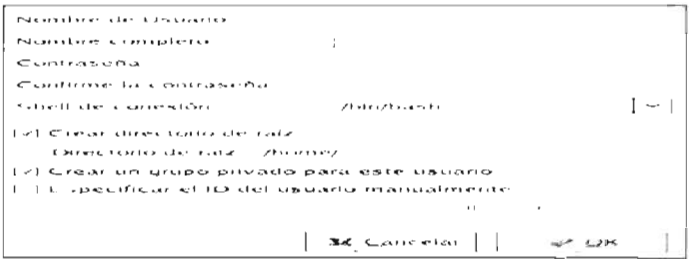
- Nombre Completo.- Muestra el Nombre completo del usuario propietario de esta cuenta.
- Shell de conexión.- El Shell principal del usuario.
- Directorio de conexión.- Directorio principal del usuario donde guarda todos sus documentos personales y de configuración.

La ventana de grupos se compone de tres columnas como se observa y contienen información acerca de los grupos:

- Nombre de Grupo.- Como lo indica esta columna muestra el nombre del grupo.
- ID de grupo.- Identificación numérica interna del grupo
- Usuarios.- en esta columna aparecen todos los usuarios que pertenecen a este grupo separados por una coma para su apreciación.

Añadir usuarios.

Existen dos formas para añadir usuarios en esta herramienta grafica. La primera de ellas y mas directa es hacer un clic sobre el icono "Añadir usuario" situado en la parte superior de la ventana, la segunda forma es acceder al menú fichero y dar clic sobre el submenú "Añadir usuario" las dos formas nos dan acceso a un nuevo cuadro de dialogo, en el cual debemos introducir la información del nuevo usuario.



Para poder dar de alta un usuario se tiene que escribir la información requerida en cada campo.

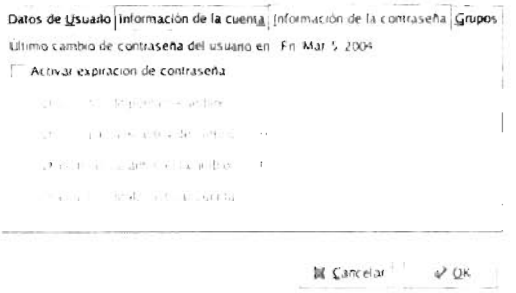
Por defecto linux proporciona la shell de conexión establecida /bin/bash pero se puede cambiar desplegando la lista de shell's admitidos, también crea una carpeta para el usuario dentro de /home/ . automáticamente especifica el UID .

Datos de Usuario.

En esta ventana se encuentran aspectos básicos de la información del usuario si se quiere hacer algún cambio basta con modificar el campo correspondiente.

Información de la cuenta.

En esta ventana su puede activar la expiración de la cuenta activando la casilla de verificación y especificando la fecha cuando queramos que la cuenta expire.

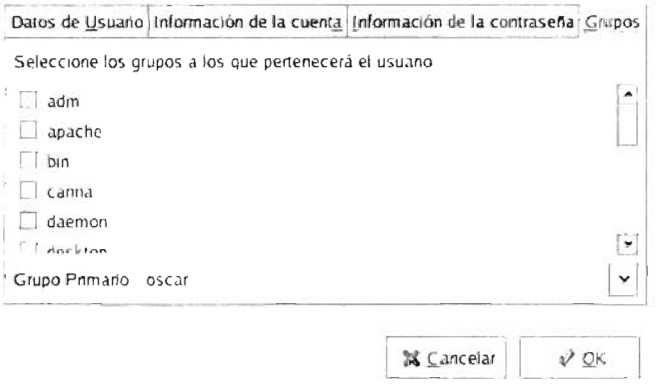


Información de la contraseña.

En esta ventana se activa la expiración de la contraseña activando la casilla de verificación y poniendo los valores que corresponden.

Grupos.

En esta ventana podemos especificar los grupos a los que el usuario pertenece para hacerlo miembro de un grupo tenemos que activar su casilla de verificación correspondiente.



Eliminación de Usuarios.

Para eliminar un usuario desde la herramienta grafica tenemos que seleccionar el usuario que queramos eliminar y hacer un clic sobre el icono que se encuentra en la parte superior Borrar.

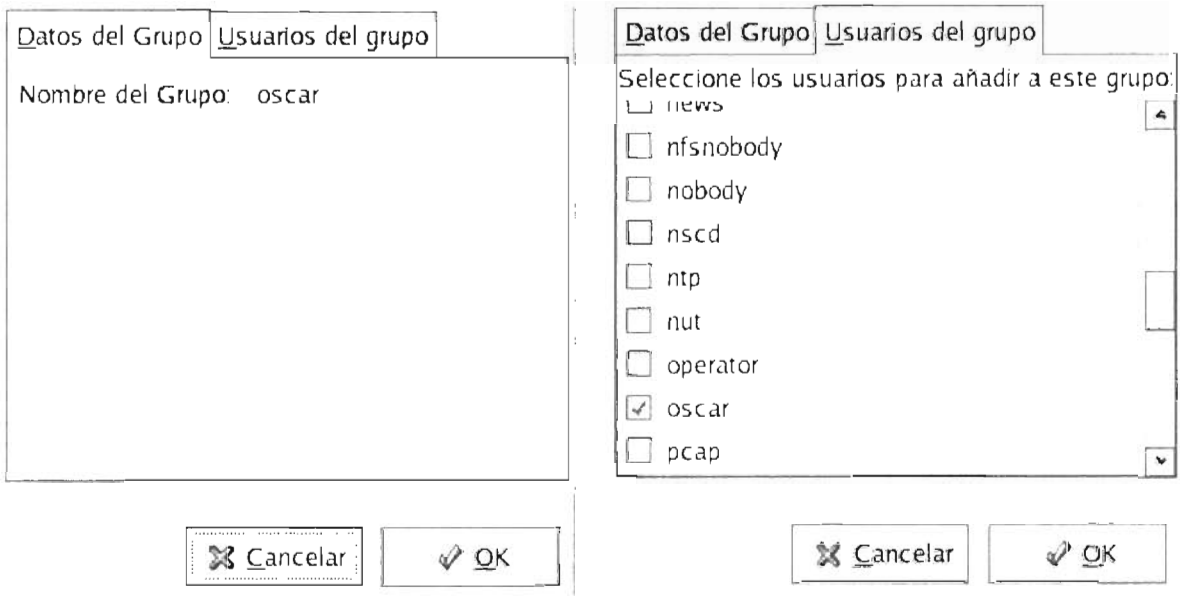
Después de esto preguntara si se desea borrar el directorio principal del usuario en caso de contestar afirmativamente borrara todo el directorio que se encuentra dentro de la carpeta /home/ y que corresponde al usuario.

Añadir grupos.

Para añadir un grupo tenemos que hacer clic sobre el menú fichero y sobre el submenú Añadir grupo o dar un clic sobre el icono Agregar grupo de esta forma de abrirá una nueva ventana simple donde tenemos que introducir el nombre de el grupo que deseemos agregar a nuestro sistema, así como el GID solo si queremos asignar un GID diferente al propuesto debemos activar la casilla y poner el valor numérico. Solo faltaría aceptar esto para tener un nuevo grupo en nuestro sistema.

Modificación de Grupos.

Para modificar grupos al igual que al modificar un usuario tenemos que hacer doble clic sobre el grupo a modificar o seleccionar el grupo y dar clic sobre el boton modificar cualquiera de las dos formas de ingresar nos mostrara una ventana con dos pestañas en la parte superior como se ve en la figura siguiente:

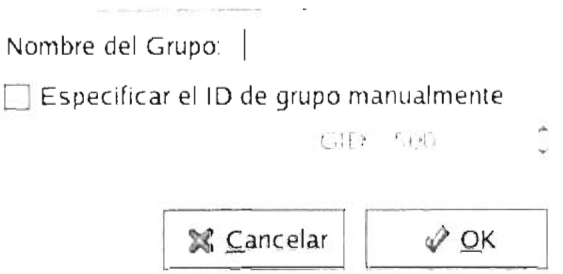


Datos de Grupo.

Aquí se puede cambiar el nombre de grupo solo hay que modificarlo y presionar OK para aceptar el cambio realizado.

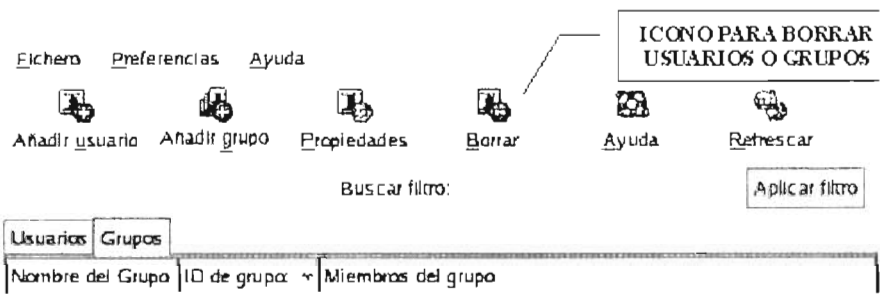
Usuarios del Grupo.

En esta pestaña se encuentra los usuarios que son miembros de este grupo en particular para agregar algún usuario al grupo tendremos que seleccionar la casilla correspondiente, y si queremos que algún usuario no pertenezca a este grupo solo tendremos que desmarcar la casilla correspondiente. Solo nos queda presionar OK para aceptar estos cambios.



Eliminación de un grupo.

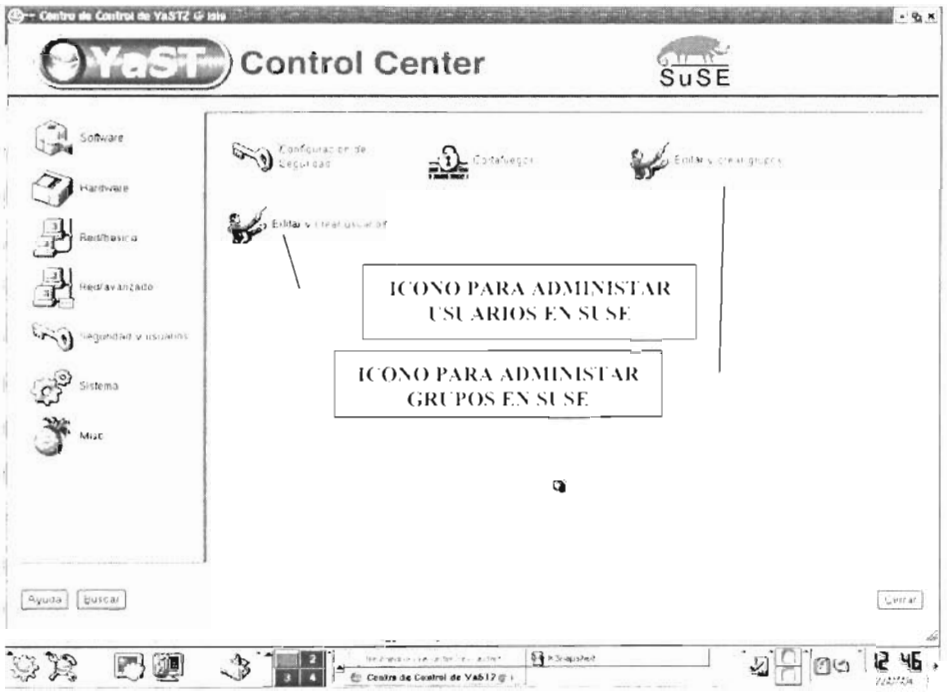
Para eliminar un grupo solo tenemos que seleccionar el grupo a eliminar y hacer un clic sobre el botón borrar que se encuentra en la parte superior de esta herramienta esto borrara el grupo sin pedir ninguna confirmación.



Herramientas graficas en otras distribuciones.

Al igual que en redhat existe el redhat-configure-user dentro de SuSe existe una herramienta similar a esta dentro de Yast el configurados de SuSe.

Trabajar con los usuarios en esta herramienta es casi intuitivo, tenemos botones para añadir, modificar y borrar usuarios y grupos tal como lo vimos en red hat.



Cabe recalcar que cualquier herramienta grafica que usemos en cualquiera de las diferentes distribuciones de Linux modifica directamente los archivos de /etc/passwd y /etc/group.

La seguridad de la computadora es primordial para linux y por ello es que a cada usuario se le proporciona su propia cuenta y los privilegios de acceso que al administrador le convenga.

Existe un operador llamado root este es utilizado para actualizar, agregar o particionar un nuevo disco duro, llevar a cabo tareas de mantenimiento o recuperación del sistema o ejecutar herramientas para solo root.

Como operador root (raíz), se puede crear o destruir cualquier archivo en cualquier directorio.

Es recomendable trabajar en un usuario y desde allí trabajar como operador root mediante el comando **su** o súper usuario para ser temporalmente usuario root, para ello se pide la contraseña.

Instalación y Configuración con la utilidad YAST2

SuSE Linux cuenta con un asistente de instalación y configuración automático llamado YAST 2 (se encarga del trabajo) y es muy flexible, fácil de entender y accesible, con el se crea una partición del disco duro, se instalan los programas y se realizan las configuraciones del hardware detectado.

La primera actividad a realizar es la selección del idioma, la cual quedará automáticamente incorporada al teclado. Posteriormente procede a comprobar todo el sistema y preguntará si se requiere de una instalación nueva, si se quiere arrancar con el sistema que se encuentra en el disco duro, o en el caso de tener una instalación previa a esta, pregunta si se quiere únicamente actualizar el sistema.

Después de la detección del sistema aparecen las siguientes propuestas:

- Modo de instalación → nueva por defecto
- Distribución del teclado → según idioma
- Ratón → tipo de mouse detectado
- Partición → Se debe saber para que se usará la maquina(servidor, estación de trabajo, servidor de aplicaciones), cuantas personas trabajarán en la computadora, cuantos discos duros tiene la computadora, que tamaño tienen y que tipo de interfaz (EIDE, SCSI o una controladora RAID).
- Software → dependerá de las necesidades del administrador, el sistema estándar predeterminado incluye KDE y un paquete ofimática
- Gestor de arranque → revela el lugar en el que SuSE instalará el gestor de arranque: "Master Boot Record"
- Zona horaria → Se modifica manualmente la configuración requerida una vez determinada, de acuerdo al país en donde se encuentre.

Una vez configurados estos parámetros se inicia la instalación de los paquetes de software que se pidió fueran instalados.
Al terminar esta instalación es necesario configurar tres parámetros muy importantes para poder empezar a trabajar con SuSE:
Definir una contraseña para el usuario root ,que utilizara también el súper usuario cuando quiera tener los privilegios de usuario root.
Crear un usuario normal (generalmente el administrador).
La computadora indica la tarjeta gráfica , el monitor , este será el momento en el que se puede realizar la configuración manual de hardware adicional del sistema como por ejemplo:

- Impresora
- Tarjeta de red
- Modem
- Tarjeta de sonido, etc.

Acceso a la Red.

TCP/IP se ha impuesto como el protocolo de red estándar y todos los sistemas operativos modernos son capaces de comunicarse con este protocolo. Sin embargo Linux sigue soportando otros protocolos de red como IPX usado (anteriormente) por Novell.
La tarjeta de red debe estar instalada en la computadora. Normalmente esta se reconoce durante la instalación y el drive adecuado se activa.
Configuración de una interfaz de red:

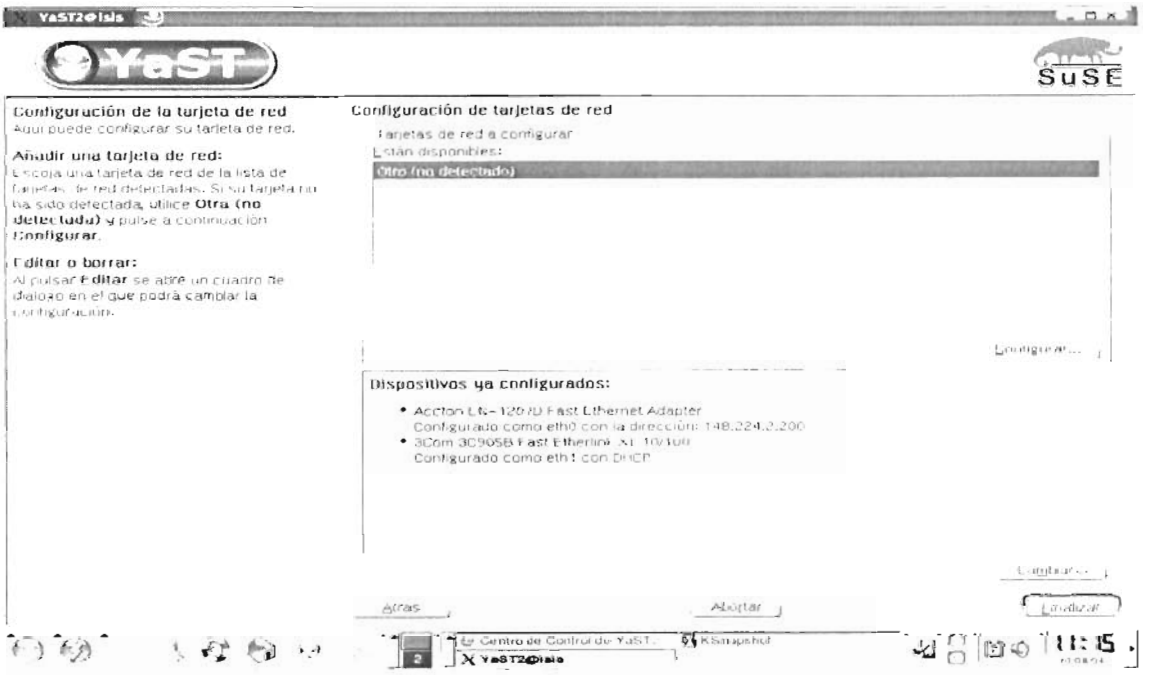
Para poder comunicarse en la red es necesario configurar una tarjeta de red también llamada interfaz de red, linux ofrece sus propias herramientas para configurar de manera que almacena con frecuencia información (comandos) en distintos lugares. Una de las maneras mas sencillas es la integración de comandos en la línea de comandos (también llamada shell[12]) que consiste en añadirlos al final de los archivos de configuración del sistema pero la desventaja es que al configurar manualmente puede crear problemas si decide usar la herramienta de configuración del sistema.

Pensando en este problema, suse linux creó una utilidad de configuración grafica llamada yast que le permite al administrador configurar parámetros de redes.

Las dos maneras que ofrece linux de configurar conexiones de red se realizan dentro del ambiente grafico de suse linux, suse se instalo mediante el ambiente grafico integrando parámetros de configuración que se añadían automáticamente a los archivos de configuración como por ejemplo:

[12] manipula las entradas del usuario que invoca a otros programas para ejecutar comandos. Incluye un lenguaje de programación

- Configuración de una interfaz de red.
- Asignación de la dirección IP.
- Asignación de la pasarela.
- Asignación de el nombre de dominio del servidor.



La otra forma de configuración mediante Shell nos ayudará a integrar el parámetro de configuración de una interfaz local llamada loopback, es decir que la computadora o nuestro servidor podrá realizar conexiones consigo misma, esto se realiza mediante el comando ifconfig y route en la consola de la siguiente manera:

 # ifconfig lo 127.0.0.1
 # route add -host 127.0.0.1 lo

El comando ifconfig le indica la computadora que active la interfaz **lo** (abreviatura de loopback) con una dirección IP de **127.0.0.1**. El comando route le indica a la computadora que añada una ruta del host 127.0.0.1 a través de la interfaz lo.
Una vez ejecutado estos comandos, probamos si la dirección loopback funciona, escribiendo lo siguiente:

 # ping -c 1 localhost

Configurada la interfaz loopback, se le asigna un nombre siguiendo los siguientes pasos:

1. Abrir el archivo **/etc/hosts** con cualquier editor.
2. Incluir la siguiente linea 127.0.0.1 localhost localhost
3. Salir y guardar el archivo modificado.

Para realizar una configuración y verificación de los parámetros de la interfaz de red en la línea de comandos es mediante el comando **ifconfig**.
Con éste comando escrito directamente como usuario root obtendremos la información configurada de los dispositivos ya configurados, es decir, nos mostrará el número IP, netmask (mascara de red) y broadcast.

Configurar una tarjeta Ethernet

Una vez configurada la interfaz loopback, el proceso de configuración de una tarjeta Ethernet. Se tiene una tarjeta eth0 reconocida por el sistema se configuran las propiedades necesarias para ejecutarse en una red TCP/IP.

Nuevamente empleamos el comando ifconfig para acceder a la tarjeta de red, para ello utilizamos la sintaxis **ifconfig device ipaddressnetmask networkmask broadcast address.**
Por ejemplo, para configurará una red (eth0)con la dirección 148.224.2.200, una máscara de subred de 255.255.255.0 y una dirección de emisión dew 148.224.225.255, tendríamos que usar la siguiente sintaxis:

[root@isis network-scripts]# ifconfig eth0 148.224.2.200 netmask 255.255.0.0 broaadcast 148.224.255.255

Puede verificar cuando quiera que la interfaz de red está ejecutándose con el propio comando ***ifconfig***.

[isis@fc.uaslp.mx isis]$ ifconfig

```
eth0    Link encap:Ethernet Hwaddr 00:A0:C9:B3:5B:A2
        inet addr:148.224.2.200 Bcast:148.224..255.255 Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:214 errors:0 dropped:0 overruns:0 frame:0
        TX packets:195 errors:0 dropped:0 overruns:0 carrier:0
        Collisisons:0
Lo      Link encap:Local Loopback
        Inet addr:127.0.0.1 Mask:225.0.0.0
        UP LOOPBACK RUNNING MTU:3924 Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        Collisions:0
```

Una vez aquí, se anota el comando que se utilizó y se debe añadir a un archivo que se ejecute en el inicio, como rc.local.

Establecer una ruta predeterminada.

Se añadirá la pasarela predeterminada de la red, este es el dispositivo que se usa para conectar a la red con el resto del mundo o con otras redes. Si no se configura la ruta predeterminada, sólo será capaz de comunicarse con las computadoras de la red local. Si está en una LAN, probablemente no tenga que configurar la pasarela.

La sintaxis para añadir la pasarela predeterminada es **route add default gw gateway address**. Para agregar una pasarela predeterminada se escribe lo siguiente:

Route add default gw 148.224.2.1

Para probar la conectividad, se hace ping a un host que esté fuera de la red , con uno de los servidores con nombre.

Configurar información relativa al nombre de host y DNS.

Ahora que la computadora puede hablar por la red, se tendrá que dotar de los medios necesarios para que pueda identificar a otras computadoras (y a sí misma) por el nombre. Esto se consigue principalmente enumerando hosts conocidos del archivo **/etc/hosts** y añadiendo servidores con nombre a **etc/resolv.conf**.

Para configurar un servidor de nombres, tendrá que modificar el archivo /etc/resolv.conf. Puede incluir hasta tres servidores con nombres distintos; como mínimo, se recomiendan dos.

El archivo /etc/resolv.conf de ejemplo (estos números no le funcionarán):
Search brevardmpo.com poisontooth.com

Nameserver 148.224.19.3
Nameserver 148.224.2.80
Nameserver 148.224.17.2

REDES HOMOGENEAS.

NFS (Network File System) permite a máquinas remotas montar particiones en un sistema en concreto y usarlas como si estuvieran en el sistema de archivos local. Esto permite centralizar archivos en una localización, mientras se permite su acceso continuo a los usuarios autorizados.

Metodología

Linux usa una combinación de soporte a nivel de kernel y demonios en continua ejecución para proporcionar compartición de archivos NFS, y el soporte NFS debe estar activo en el kernel de Linux para que funcione. NFS usa *Remote Procedure Calls (RPC)* para enrutar peticiones entre clientes y servidores, implicando que el servicio portmap debe estar disponible y activo en los niveles de ejecución adecuados para que la comunicación NFS funcione. Trabajando con portmap, varios otros procesos se aseguran que una conexión particular NFS esté permitida y pueda proceder sin error:

- **rpc.mountd.-** El proceso que recibe la petición de montaje desde un cliente NFS y chequea para mirar si coincide con un sistema de archivos actualmente exportado.
- **rpc.nfsd.-** El proceso que implementa la parte de usuario del servicio NFS. Trabaja son el kernel Linux para conocer las demandas dinámicas de clientes NFS, tales como proporcionar procesos adicionales del servidor para que los clientes NFS lo utilicen.
- **rpc.lockd.-** Un demonio innecesario en los kernels modernos. El bloqueo de de archivos NFS ahora lo hace el kernel. Está incluido en el paquete nfs-utils para usuarios que usan versiones antiguas del kernel que no incluyen esta capacidad por defecto.
- **rpc.statd.-** Implementa el protocolo RPC *Network Status Monitor (NSM)*. Esto proporciona notificación de reinicio cuando un servidor NFS es reiniciado abruptamente.
- **rpc.rquotad.-** Un servidor RPC que proporciona información de cuotas de usuarios a usuarios remotos.

No todos estos programas son requeridos para el servicio NFS. Los únicos servicios que deben estar activos son rpc.mountd, rpc.nfsd, y portmap. Los otros demonios proporcionan funcionalidades adicionales, basadas en los requerimientos concretos del entorno de su servidor.

NFS puede usar UDP o TCP corriendo sobre una IP. La conexión UDP sin estado minimiza el tráfico de red, como el servidor NFS manda al cliente una cookie, después el cliente es autorizado a acceder al volumen compartido. Esta cookie, o valor aleatorio que es guardado en la parte del servidor, es pasado por cualquier petición RPC del cliente al servidor. El servidor NFS puede ser reiniciado sin afectar a los clientes y las cookies permanecen intactas.

Con NFS, la autentificación sólo se produce cuando el cliente intenta montar un sistema de archivos remoto.

El servidor NFS utiliza los archivos /etc/hosts.allow y /etc/hosts.deny para determinar si a una máquina particular le debe ser explícitamente permitido o denegado su acceso vía NFS. Entonces, el servidor NFS se refiere al archivo /etc/exports para descubrir estos privilegios de máquinas para los distintos puntos de montajes disponibles. Después de garantizar el proceso, cualquier operación de archivos y directorios es enviada al servidor usando llamadas a procedimientos remotos[13].

NFS y portmap

NFS se apoya en las llamadas de procedimientos remotos (RPC) para funcionar. Se requiere portmap para trazar las peticiones RPC a los servicios correctos. Los procesos RPC notifican a portmap cuando comienzan, revelando el número de puerto que ellos están monitorizando y el número de programas RPC que esperan servir. El sistema cliente entonces contacta con el portmap del servidor con un número de programa RPC particular. Entonces portmap redirecciona al cliente al número del puerto apropiado para que se comunique con el servicio apropiado.
Como los servicios basados en RPC confían en portmap para hacer todas las conexiones con las peticiones de clientes entrantes, portmap debe estar disponible antes que cualquiera de esos servicios comience. Si, por alguna razón, el servicio portmap inesperadamente se quita, reinicie portmap y cualquier servicio que estuviera ejecutándose entonces.
El servicio portmap puede ser usado con los archivos de accesos de máquinas (/etc/hosts.allow y /etc/hosts.deny) para controlar a qué sistemas remotos les son permitidos usar servicios basados en RPC en su máquina. Las reglas de control de acceso para portmap afectarán a todos los servicios basados en RPC. Alternativamente, puede especificar a cada uno de los demonios RPC NFS para que sean afectados por una regla de control específica. Las páginas man de rpc.mountd y rpc.statd contienen información relativa a la sintaxis precisa de estas reglas.

Estado de portmap

Como portmap proporciona la coordinación entre servicios RPC y los números de puertos utilizados para comunicarlos, es útil plasmar una imagen de los servicios RPC actuales que están usando portmap cuando estamos resolviendo algún problema.
El comando rpcinfo muestra cada servicio basado en RPC con su número de puerto, número de programa RPC, versión y tipo de protocolo (TCP o UDP)
Para asegurarse que los servicios NFS basados en RPC están activos para portmap, rpcinfo puede ser útil:

```
[root@localhost /]# rpcinfo -p
```

[13] Los privilegios de montajes NFS son permitidos específicamente a máquinas, no a usuarios. Si permite a un sistema acceder a una parte en concreto de su disco duro, los usuarios de esa máquina podrán acceder a esos datos compartidos.

La opción -p prueba el portmap de la máquina especificada, o en la maquina local por defecto si no se especifica ninguna máquina. Otras opciones están disponibles en la página manual de rpcinfo.

En la salida obtenida de ejecutar la instrucción, varios servicios NFS se pueden ver ejecutándose. Si uno de los servicios NFS no comienza correctamente, portmap puede ser incapaz de corresponder las peticiones RPC con sus respectivos puertos. En muchos casos, reiniciando NFS como root (service nfs restart) provocará que estos servicios funcionen correctamente con portmap y empiecen a funcionar.

Archivos de configuración del servidor NFS.

Es sencillo configurar un sistema para compartir archivos y directorios usando NFS. Cada Sistema de archivos que se exporta a usuarios remotos vía NFS, así como los derechos de acceso relativos a ellos, es localizado en el archivo /etc/exports. Este archivo es leído por el comando exportfs que da a rpc.mountd y rpc.nfsd la información necesaria para permitir el montaje remoto de un sistema de archivos por una máquina autorizada.
El comando exportfs permite exportar o no directorios concretos sin reiniciar los servicios NFS. Cuando se le pasan las opciones apropiadas a exportfs, el sistema de archivos a exportar es incluido en /var/lib/nfs/xtab. Como rpc.mountd se refiere al archivo xtab para decidir privilegios de acceso a un sistema de archivos, los cambios en la lista de sistemas de archivos exportados toman efecto inmediatamente.

Hay varias opciones disponibles cuando usamos **exportfs**:

- **-r** Provoca que todos los directorios listados en /etc/exports sean exportados construyendo una nueva lista de exportación en /etc/lib/nfs/xtab. Esta opción refresca la lista de exportación con cualquier cambio que hubiéramos realizado en /etc/exports.
- **-a** Provoca que todos los directorios sean exportados o no, dependiendo de qué otras opciones hemos pasado a **exportfs**.
- **-o *opciones*** Permite al usuario especificar directorios a exportar que no estén listados en /etc/exports. Estos sistemas de archivos adicionales compartidos deben ser escritos de la misma forma que son especificados en /etc/exports. Esta opción es usada para probar un sistema de archivos antes de añadirlo permanentemente a la lista de sistemas a exportar.
- **-i** Le dice a **exportfs** que ignore /etc/exports; sólo las opciones dadas en la línea de comandos serán usadas para definir los sistemas de archivos exportados.
- **-u** Termina de exportar directorios que puedan ser montados por usuarios remotos. El comando **exportfs -ua** suspende la compartición de archivos NFS mientras que mantiene los demonios activos. Para continuar con la compartición NFS, teclee **exportfs -r**.
- **-v** Operación descriptiva, donde los sistemas de archivos exportados o dejados de exportar son mostrados en gran detalle al ejecutarse el comando **exportfs**.

Si no se pasan opciones al comando **exportfs**, mostrará una lista de los sistemas de archivos actualmente exportados.

Los cambios efectuados a /etc/exports pueden ser leídos al recargar el servicio NFS con el comando **service nfs reload**. Esto deja a los demonios NFS ejecutándose mientras reexporta el archivo /etc/exports.

/etc/exports

El archivo /etc/exports es el estándar para controlar que sistemas de archivos son exportados a que máquinas, así como para especificar opciones particulares que controlen todo. Las líneas en blanco son ignoradas, se pueden comentar líneas con #, y las líneas largas pueden ser divididas con una barra invertida (\). Cada sistema de archivos exportado debe tener su propia línea. La lista de máquinas autorizadas colocada después de un sistema de archivos exportado, debe estar separada por un espacio. Las opciones para cada uno de las máquinas deben ser colocadas entre paréntesis directamente detrás del identificador de la máquina, sin ningún espacio de separación entre la máquina y el primer paréntesis.

De esta sencilla manera, /etc/exports sólo necesita saber el directorio a exportar y las máquinas que pueden utilizarlo, por ejemplo:

/home/compartida nameserver.fc.uaslp.mx
/otro/directorio/exportado 148.224.2.204

Después de reexportar /etc/exports con el comando **/sbin/service nfs reload**, la máquina *nameserver.fc.uaslp.mx* será capaz de montar /home/*compartida*, y 148.224.2.204 podrá montar /otro/directorio/exportado. Como no hay opciones especificadas en este ejemplo, varias preferencias por defecto toman efecto:

- **ro.-** Sólo lectura (read-only). Las máquinas que monten este sistema de archivos no podrán cambiarlo. Para permitirlas que puedan hacer cambios en el sistema de archivos, debe especificar la opción rw (lectura-escritura - read-write).
- **async**.- Permite al servidor escribir los datos en el disco cuando lo crea conveniente. Mientras que esto no tiene importancia en un sistema de sólo lectura, si una máquina hace cambios en un sistema de archivos de lectura-escritura y el servidor se cae o se apaga, se pueden perder datos. Especificando la opción sync, todas las escrituras en el disco deben hacerse antes de devolver el control al cliente. Esto bajará el rendimiento.
- **wdelay**.- Provoca que el servidor NFS retrase el escribir a disco si sospecha que otra petición de escritura es inminente. Esto puede mejorar el rendimiento reduciendo las veces que se debe acceder al disco por comandos de escritura separados. Use no_wdelay para desactivar esta opción, la cual sólo funciona si está usando la opción sync.
- **root_squash**.- Hace que cualquier cliente que acceda al sistema de archivos exportado (como root en la máquina cliente), se convierta en el ID del usuario nobody.

Esto reconvierte el poder del usuario root remoto al de usuario local más bajo, previniendo que los usuarios root remotos puedan convertirse en usuarios root en el sistema local. Alternativamente, la opción no_root_squash lo desactiva. Para reconvertir a todos los usuarios, incluyendo a root, use la opción all_squash. Para especificar los ID de usuario y grupo para usar con usuarios remotos desde una máquina particular, use las opciones anonuid y anongid respectivamente. De esta manera, puede crear una cuenta de usuario especial para usuarios NFS remotos para compartir y especificar (anonuid-*<uid-value>*,anongid=*<gid-value>*), donde *<uid-value>* es el número ID de usuario y *<gid-value>* es el número ID de grupo.

Para saltarse estas opciones predeterminadas, debe especificar la opción que desea cambiar. Por ejemplo, si no especifica la opción rw, entonces se exportará en sólo lectura. Cada opción predeterminada debe ser explícitamente sobrescrita con su opción correspondiente Adicionalmente, hay otras opciones que están disponibles que no afectan a las predeterminadas. Estas incluyen desactivar el navegar por subdirectorios, permitir el acceso a puertos inseguros, y permitir bloquear archivos inseguros.

Para especificar máquinas a las que permitir usar un sistema de archivos en concreto, podemos usar varios métodos, entre los que se incluyen:

- ***una sola máquina***.- Cuando una máquina en particular es especificada con nombre completo de dominio, nombre de máquina o dirección IP.
- ***comodines***.- Cuando usamos un carácter * o ? para referirnos a un grupo de nombres completos de dominio o direcciones IP o que coincidan con una cadena particular de letras. Sin embargo, hay que ser cauteloso cuando use comodines con nombres de dominios completos, y hay que intentar ser lo más exacto que se pueda.
- ***redes IP***.- Permite el acceso a máquinas basadas en sus direcciones IP dentro de una red más grande. Por ejemplo, 148.224.2.200/04 permite al acceso a las primeras 5 direcciones IP, desde la 148.224.2.200 a la 148.224.2.204, acceden al sistema de archivos, pero no a la 148.224.2.205 y superiores.
- ***grupos de redes***.- Permite que un nombre de grupo de red NIS, escrita como *@<group-name>*, sea usada. Esto pone al servidor NIS controlando el acceso de este sistema de archivos, donde los usuarios pueden ser añadidos o borrados de un grupo NIS sin que afecte a /etc/exports.

  /home/compartida nameserver.fc.uaslp.mx(rw)
  /home/compartida nameserver.fc.uaslp.mx (rw)[14]

La primera línea permite sólo a los usuarios acceder en modo de lectura-escritura al directorio /home/compartida.

[14] Hay que recordar separar siempre los sistemas de archivos exportados de máquina a máquina y de uno a otro con un espacio. Sin embargo, no debería haber otros espacios en el archivo a menos que se usen en líneas comentadas

La segunda línea permite a los usuarios de montar el directorio de sólo lectura (el predeterminado), pero el resto del mundo puede instalarlo como lectura-escritura.

Archivos de configuración de clientes NFS

Cualquier compartición NFS puesta a disposición por un servidor puede ser montada usando varios métodos. Desde luego que puede ser montada manualmente usando el comando mount, para adquirir el sistema de archivos exportado como un punto de montaje concreto. Sin embargo, esto requiere que el usuario root teclee el comando mount cada vez que el sistema reinicie. Además, el usuario root debe recordar desmontar el sistema de archivos cuando apague la máquina. Otros métodos de configurar los montajes NFS incluyen el modificar /etc/fstab o utilizar el servicio autofs.

/etc/fstab

Colocando una línea adecuadamente formada en el archivo /etc/fstab tiene el mismo efecto que el montaje manual del sistema de archivos exportado. El archivo /etc/fstab es leído por el script /etc/rc.d/init.d/netfs cuando arranca el sistema. Los sistemas de archivos montados, incluyendo NFS, son puestos en su sitio.
Un ejemplo de línea /etc/fstab para montar un NFS exportado será parecida a:

<server-host>:</path/to/shared/directory> </local/mount/point> nfs *<options>* 0 0

La opción *<server-host>* tiene que ver con el nombre de la máquina, dirección IP o nombre del dominio totalmente cualificado del servidor que exporta el sistema de archivos. *</path/to/shared/directory>* le dice al servidor que exporta para montar. *</local/mount/point>* especifica dónde, en el sistema de archivos local, monta el directorio exportado. Este punto de montaje debe existir antes en /etc/fstab de donde es leído o el montaje fallará. La opción nfs especifica el tipo de sistema de archivos montado.
El área *<options>* especifica como el sistema de archivos es montado. Por ejemplo, si las opciones rw,suid en un montaje en concreto, el sistema de archivos exportado será montado en modo de lectura-escritura y los ID de usuario y grupo puestos por el servidor serán usados. Aquí no se usan paréntesis.

Asegurar NFS

NFS trabaja muy bien compartiendo sistemas de archivos enteros con un gran número de máquinas conocidas de una manera muy transparente. Muchos usuarios que acceden a archivos sobre un punto de montaje NFS pueden no estar atentos a que el sistema de archivos que están usando no está en su sistema local. Sin embargo, esta facilidad de uso trae una variedad de potenciales problemas de seguridad.
Los puntos siguientes deberían ser considerados cuando se exporte sistemas de archivos NFS en un servidor o cuando se monten en un cliente. Haciendo esto reducirá los riesgos de seguridad NFS y protegerá mejor los datos en el servidor.

Acceso al sistema.

NFS controla quien puede montar y exportar sistemas de archivos basados en la máquina que lo pide, no el usuario que utilizará el sistema de archivos. Las máquinas tienen que tener los derechos para montar los sistemas de archivos exportados explícitamente.
El control de acceso no es posible para usuarios, aparte de los permisos de archivos y directorios. En otras palabras, cuando exporta un sistema de archivos vía NFS, cualquier usuario en cualquier máquina remota conectada al servidor NFS puede acceder a los datos compartidos. Para limitar estos riesgos potenciales, los administradores sólo pueden permitir acceso de sólo-lectura o reducir a los usuarios a un usuario común y groupid. Pero estas soluciones pueden impedir que la compartición NFS sea usada de la forma en que originalmente se pensó.

Adicionalmente, si un atacante gana el control del servidor DSN usado por el sistema que exporta el sistema de archivos NFS, el sistema asociado con un nombre de máquina concreto o nombre de dominio totalmente cualificado, puede ser dirigido a una máquina sin autorización. En este punto, la máquina desautorizada *es* el sistema que tiene permitido montar la compartición NFS, ya que no hay intercambio de información de nombre de usuario o contraseña para proporcional seguridad adicional al montaje NFS. Los mismos riesgos corre el servidor NIS, si los nombres de red NIS son usados para permitir a ciertas máquinas montar una compartición NFS. Usando direcciones IP en /etc/exports, esta clase de ataques son más difíciles.

Los comodines o metacaracteres deben ser usados lo menos posible cuando garantizamos el acceso a una compartición NFS. El uso de los comodines puede permitir el acceso a sistemas que puede no saber que existen y que no deberían montar el sistema de archivos.

Permisos de archivos

Una vez que el sistema de archivos es montado como lectura-escritura por una máquina remota, la única protección que tiene cada archivo son sus permisos. Si dos usuarios que comparten el mismo valor de userid montan el mismo NFS, ellos podrán modificar sus archivos mutuamente. Adicionalmente, cualquiera con acceso root en el sistema cliente puede usar el comando su - para volverse un usuario que tenga acceso a determinados archivos a través de la compartición NFS.

El comportamiento por defecto cuando se está exportando un sistema de archivos a través NFS es usar *root squashing*. Esto coloca el userid de cualquiera que esté accesando la compartición NFS como el usuario root en su máquina local al valor de la cuenta de 'nobody'. Nunca desactive el aplastamiento (squashing) de root.
Si se está exportando una compartición NFS como de sólo lectura, considere usar la opción all_squash, la cual hace que todos los usuarios accesando el sistema de archivos exportado tomen el userid del usuario nobody.

Redes Heterogéneas.

SAMBA es una suite de aplicaciones de red que hablan el protocolo SMB. SAMBA permite a una máquina LINUX enmascararse como un servidor más en una red *Microsoft* TCP/IP. SAMBA puede ayudar a las maquinas Windows y Linux coexistir en la misma red de área local (LAN)

Un servidor SAMBA es capaz de ofrecer los siguientes servicios de red:

- Compartir uno o más sistemas de ficheros.
- Compartir impresoras instaladas en el servidor o en sus clientes.
- Ayudar a los clientes a examinar el entorno de red.
- Autentificación de conexiones de clientes en un dominio *Windows*.
- Suministrar el servicio de resolución de nombres *WINS*

SAMBA está implementada mediante un par de *daemons* de LINUX que ofrecen recursos compartidos a los clientes SMB de la red. Estos *daemons* son:

- *smbd:* Demonio que permite compartir directorios e impresoras en una red SMB y proporciona autentificación y autorización para clientes SMB.
- *nmbd:* Demonio que mantiene el servicio de resolución de nombres WINS, y Ayuda a la exploración (*browsing*).

Configuración del servidor Samba

Samba usa por defecto un archivo de configuración localizado en /etc/samba/smb.conf que permite a los usuarios visualizar sus directorios principales en Linux como una partición Samba (Samba share). También comparte impresoras configuradas en Linux como impresoras compartidas de Samba. En otras palabras, puede conectar, por ejemplo una impresora al sistema linux e imprimir desde un ordenador de la red que tenga instalado el sistema Windows.

Configuración de línea de comandos

Samba como ya se menciono antes usa el archivo /etc/samba/smb.conf Si cambia el archivo de configuración, los cambios no tienen efecto hasta que no reinicie el demonio Samba con el comando service smb restart. O utilizando una herramienta grafica para este fin.

Para especificar el grupo de trabajo Windows y una breve descripción del servidor Samba, tenemos que modificar las líneas siguientes en el archivo smb.conf:

```
workgroup = labdinfo
server string = Servidor Samba
```

workgroup se refiere al nombre del grupo de trabajo Windows al cual debería pertenecer la máquina, en nuestro caso labdinfo. El server string es opcional y es usado como el comentario de Windows sobre el sistema Samba.

Para crear un directorio compartido Samba en el sistema Linux, tenemos que modificar la siguiente sección a el archivo smb.conf:

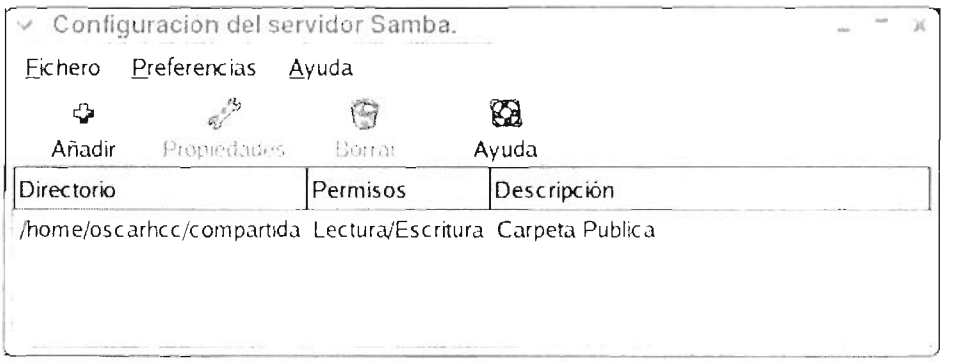
```
[sharename]
comment = Servidor Samba
path = /home/compartida
valid users = usuario1 usuario2 usuario3
public = no
writable = yes
printable = no
create mask = 0765
```

El ejemplo de arriba permite a los usuarios leer y escribir el directorio /home/compartida, en el servidor Samba, desde un cliente Samba.

Configuración gráfica.

La Herramienta grafica de configuración del servidor Samba es una interfaz gráfica para el manejo de comparticiones Samba, usuarios y configuraciones básicas. Modifica los archivos de configuración en el directorio /etc/samba/. Cualquier cambio que no se haya realizado usando esta aplicación a estos archivos, se mantienen.
Para usar esta aplicación, debe estar ejecutando el sistema X Window, y tener privilegios de root.

Para arrancar la Herramienta de configuración del servidor Samba desde el escritorio, escriba el comando redhat-config-samba en el intérprete de comandos o vaya al Botón de menú principal, Configuración del sistema, Configuración de servidores, Servidor Samba. Esto nos abre una ventana como la que se muestra a continuación[15]:



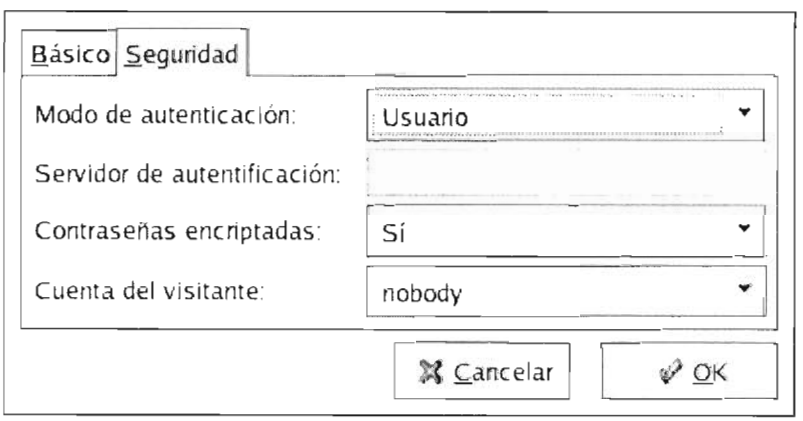
[15] La Herramienta de configuración del servidor Samba no muestra las impresoras compartidas o la estancia por defecto que permite a los usuarios ver sus propios directorios principales en el Servidor Samba.

Configuración de las propiedades del servidor

El primer paso para configurar un servidor Samba es configurar las propiedades básicas y algunas opciones de seguridad. Para realizar esto después de arrancar la herramienta seleccionamos Preferencias y luego configuración de servidores esto nos mostrara una ventana con dos pestañas Básica y Seguridad.

En la pestaña Básica, tenemos que especificar en cual grupo debería estar la computadora así como también una breve descripción del Servidor Samba. Esto corresponde a las opciones workgroup y server string en el archivo smb.conf.

La pestaña de Seguridad contiene las opciones siguientes:



Modo de autenticación.- Esto corresponde a la opción seguridad. Seleccione uno de los siguientes tipos de autenticación.

- Dominio.- El servidor Samba confía en un Controlador de Dominio Windows NT Primario o de Backup para verificar un usuario. El servidor pasa el nombre del usuario y la contraseña al Controlador y espera para que éste la devuelva. Especifique el nombre del NetBIOS del Controlador de dominio primario o de backup en el campo Servidor de autentificación.

- Servidor.- El servidor Samba intenta verificar la combinación del nombre de usuario y la contraseña pasándolos a otro servidor Samba.
- Si no puede, el servidor intenta verificar usando el modo de autentificación del usuario. Especifique el nombre del NetBIOS del otro servidor Samba en el campo Servidor de autentificación.
- Partición.- Los usuarios Samba no tienen que ingresar un nombre de usuario y contraseña para cada servidor. No se les pide un nombre de usuario y contraseña hasta que ellos traten de conectarse a un directorio compartido específico desde el servidor Samba.
- Usuario.- Es la opción por defecto y los usuarios Samba deben proporcionar un nombre de usuario y contraseña válidos por servidor Samba.

Contraseñas encriptadas.- Esta opción debe estar activada cuando se conecta desde un cliente Microsoft Windows (9X, Me, NT, XP). Las contraseñas se transfieren entre el servidor y el cliente en un formato encriptado en vez de texto plano el cual puede ser fácilmente interceptado.

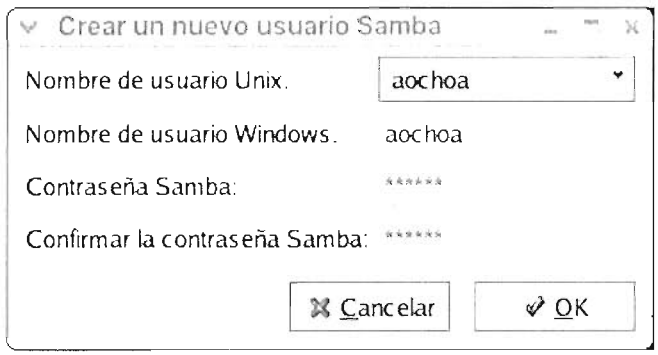
Cuenta del visitante.- Cuando los usuarios o invitados se conectan a un servidor Samba, ellos deben ser comparados con un usuario válido en el Sistema Linux. Tendremos que seleccionar uno de los nombres de usuarios válidos en el sistema para que sea la cuenta de invitados de Samba. Cuando los invitados se conectan a un servidor Samba, ellos tienen los mismos privilegios que este usuario. Esto corresponde a la opción cuenta del visitante.

Administración de usuarios Samba

La herramienta de configuración del servidor Samba requiere que haya una cuenta activa de usuarios en el sistema Linux actuando como el servidor Samba antes de que se pueda agregar un usuario Samba.
El usuario Samba está asociado con la cuenta de usuario existente en el sistema Linux.

Para añadir un usuario Samba, seleccione preferencias y luego Usuarios Samba esto nos desplegara una ventana como la que se muestra a continuación:

Hacemos clic sobre el botón Añadir usuario. En la ventana que aparece a continuación tenemos que seleccionar el Nombre de usuario que se encuentra en el sistema Linux desde la lista de usuarios existentes.



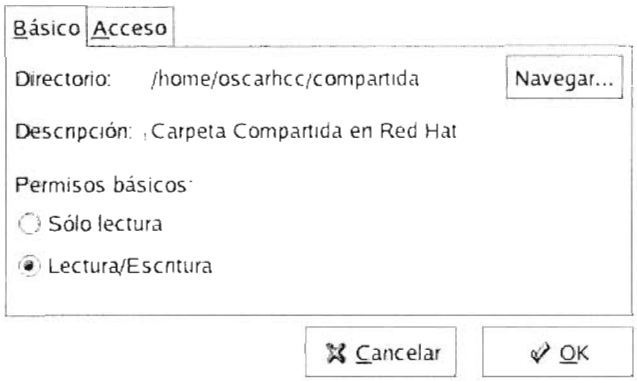
Si el usuario tiene un nombre diferente en una máquina Windows y será conectado en un servidor Samba desde una máquina Windows, especifique ese nombre de usuario Windows en el campo Nombre de usuario Windows.
También configure una Contraseña Samba para el usuario Samba y confírmela escribiéndola nuevamente. Aún si selecciona usar contraseñas encriptadas para Samba, se recomienda que las contraseñas Samba para todos los usuarios sean diferentes a las de su inicio de sesión en Linux.
Para modificar un usuario existente, seleccione el usuario desde la lista y haga clic en Modificar usuario.
Para eliminar un usuario Samba existente, seleccione el usuario, y haga clic en el botón Borrar usuario.

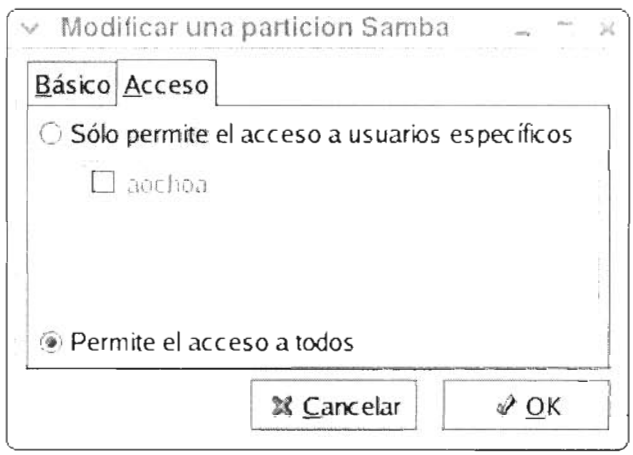
Añadir una partición Samba

Para añadir una partición Samba, haga clic en el botón Añadir. La pestaña Básica configura las opciones siguientes:

- Directorio— El directorio a compartir vía Samba. El directorio debe existir.
- Descripción — Una breve descripción de la recurso compartido.
- Permisos básicos — Especifica si los usuarios sólo podrán leer los archivos en el directorio compartido o si pueden leer y escribir.

En la pestaña de Acceso, seleccionamos si deseamos que sólo usuarios específicos accedan a el recurso compartido o si quiere que todos los usuarios Samba tengan acceso a la partición.





Arrancar y detener el servidor

En el servidor que esta compartiendo directorios a través de Samba, el servicio smb debe estar ejecutándose. Para manipular este servicio existen estas instrucciones básicas:

- Visualizar el estado de el servicio /sbin/service smb status
- Arrancar el servicio /sbin/service smb start
- Detener el servicio /sbin/service smb stop

Conexión a una compartición Samba.

Para conectarse a una compartición Linux Samba desde un sistema Microsoft Windows, basta con usar normalmente el Entorno de red o el administrador de archivos.

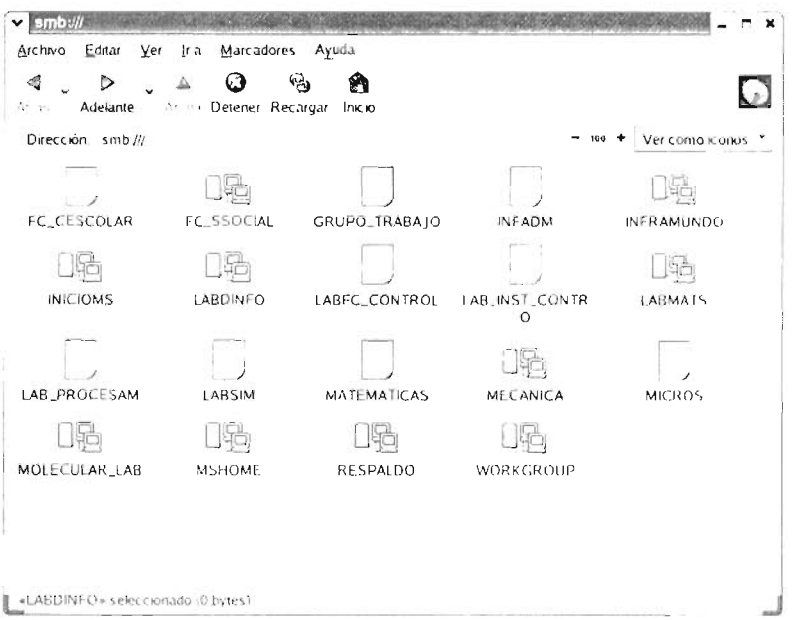
Para conectarse a una compartición Samba desde un sistema Linux, escriba en la línea de comandos de la shell el comando:

smbclient
***//148.224.2.201*/home/compartida -U**
username

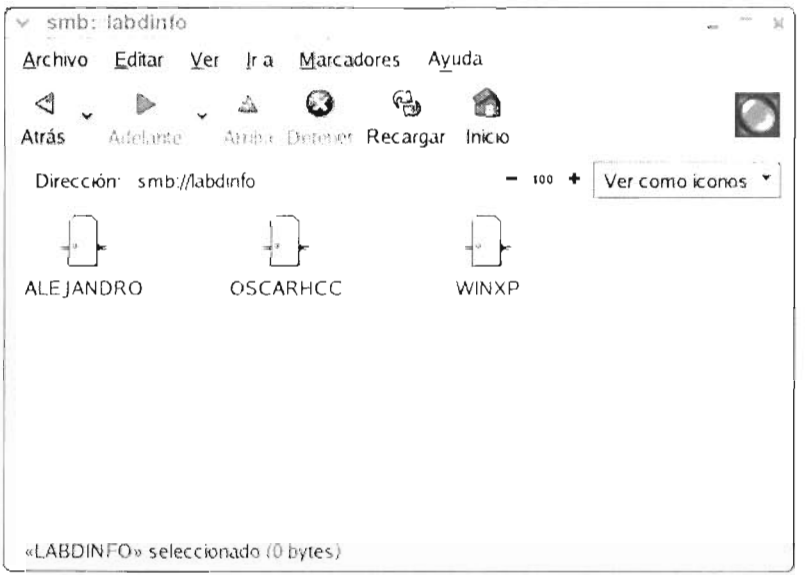
Donde 148.224.2.201 es el nombre de la máquina o la dirección IP del servidor Samba al que desee conectarse, /home/compartida el nombre del directorio compartido al que quiera acceder y *username* es el nombre del usuario para el sistema Samba.

Si observamos que en la pantalla aparece smb:\> la conexión se habrá realizado sin ningún problema. Si omitimos la opción -U, el nombre del usuario actual es pasado al servidor Samba. Si queremos salir del servidor Samba tenemos que ejecutar la instrucción exit en la línea de comandos smb:\>

También podemos ejecutar un administrador de archivos en esta caso Nautilius para poder ver la red



Y para acceder a los hosts de un grupo de trabajo en especial solo tenemos que abrirlo.



Como se puede ver en la ilustración, hay un icono para cada máquina dentro del grupo de trabajo.
Si queremos ver las comparticiones Samba en la máquina solo hay que hacer doble clic sobre el icono de la computadora. Si se requiere una combinación de nombre de usuario y contraseña, se le pedirá.

Conclusiones.

Unix es un sistema operativo que nació entre los años 50's y 60's con el fin de ofrecer seguridad, compatibilidad y que además fuera multiusuario, este proyecto fue solicitado por las Universidades para enseñar a los alumnos como funcionaba un sistema operativo y así poder desarrollar software, pero este se tornó muy difícil de entender y el desarrollo de un sistema operativo se restringió a un reducido grupo de personas y compañías. El profesor Andrew Tenembaum se preocupó por esto y creo un nuevo sistema inspirado en Unix pero muy reducido, llamado MINIX con el cual actualmente se enseña en todas las universidades del mundo, las bases del diseño de los sistemas operativos. En base a este sistema MINIX un estudiante de 23 años llamado Linus Torvalds comenzó a desarrollar un sistema operativo muy amigable llamado Linux.

En octubre de 1991, anuncio la primera versión "oficial" de LINUX, la 0.02, que ya era capaz de ejecutar el SHELL bash y el compilador gcc de GNU.

En comp.os.minix, un foro de discusión en Internet acerca del sistema operativo de Tenembaum, Linus Torvals escribió un llamamiento que comenzaba con una famosa frase:

¿Añoras los maravillosos días del MINIX-1.1, cuando los hombres eran hombres y escribían sus propios drivers? ¿Careces de proyectos interesantes y te mueres por desafiar a un sistema operativo que puedas modificar a tu antojo? ¿Te resulta frustrante que todo funciones con MINIX? ¿Estás harto de trasnochar para poder conseguir que funcione un programa?

Entonces, esta carta puede ser justamente para ti.

Como comenté hace un mes, estoy trabajando en una versión libre de un sistema tipo MINIX para computadoras AT-386. Finalmente ha sido mejorado el entorno, que incluso se puede utilizar, y estoy deseoso de sacar las fuentes de una distribución más potente

A partir de ahí, el sistema de Linux empezó a crecer. De todas partes le llegaban cartas interesándose por la idea, y comenzaron a desarrollarse proyectos destinados a incrementar la potencia de la plataforma.

Sin duda, el factor esencial y determinante en el éxito y la rápida difusión del sistema operativo ha sido la red de redes, Internet. A través de foros de discusión y noticias, miles de personas de todo el mundo se han propuesto demostrar que, sin mediar tiranía y los intereses económicos de las empresas, se pueden conseguir productos que incluso superen en calidad a los desarrollados por los gigantes del software.

Con el pasar del tiempo Linux ha ido creciendo, mejorando y personas de todo el mundo tienen acceso al código fuente, permitiéndoles así crear sus propias distribuciones con los nombres que se han mencionado durante todo este trabajo de investigación.

Ofrece todos los servicios necesarios para trabajar en red e Internet es amigable, cuenta con una interfase gráfica que ayuda al usuario promedio a trabajar sin ningún problema, ofrece al administrador configurar los servicios ajustándose a sus necesidades, y además por medio de foros de discusión los desarrolladores de software pueden realizar mejoras y solucionar problemas y errores con los que cuenta una distribución.

En al amplio mundo de las PC un sistema operativo domina, Windows y muy pocos saben que existen otras alternativas como Linux que fácilmente pueden satisfacer las necesidades del usuario común como las de un administrador.

Linux como servidor de Internet es una opción muy recomendable ya que incorpora en casi todas sus distribuciones un Servidor Web llamado Apache, mas del 60% de los servidores Web que existen, utilizan este servidor, esto nos da una idea de que es un servidor altamente confiable.

Como servidor de una red de Área Local tenemos muchas opciones para compartir sistema de archivos lo que no sucede con Windows, ya sea NFS para redes Homogéneas o Samba para redes Heterogéneas, también podemos compartir archivos vía FTP a cualquier parte del mundo. Además podemos acceder remotamente a nuestro sistema ya sea en modo texto (TELNET, SSH) o gráficamente (VNC), y todo esto con una gran seguridad ya que podemos establecer permisos para archivos para que algún intruso no puede leerlas o ejecutarlas.

Por todo esto creemos que Linux es un sistema operativo confiable y potente que fácilmente se puede utilizar para Administrar Redes y Servicios de Internet, y sigue en constante desarrollo por usuarios de todo el mundo además de que su valor monetario es casi cero de ahí que ya se este utilizando en muchas empresas y gobiernos en el mundo.

APENDICE A

Para realizar las configuraciones adecuadas en linux existen archivos de configuración los cuales están estructurados de acuerdo a los procesos que sean necesarios llevar a cabo para así poder dar un servicio.

A continuación se ofrece una recopilación de los directorios de configuración. Y de algunos comandos.

Archivos y Funciones (divididos por directorio).

`Directorio de configuración /etc/:`

aliases : Contiene los "alias" (sinónimos) de varios usuarios del sistema a donde deben ser dirigidos sus correos electrónicos.

crontab : Contiene información sobre los eventos que se realizaran en el sistema cada cierto tiempo (hora, día ,semana ,mes). A diferencia del directorio /var/spool/cron donde cada usuario tiene su archivo y especifica sus horarios, este archivo mantiene un **crontab** que ejecuta los archivos que se encuentren en los directorios **cron.hourly, cron.daily, cron.weekly, cron.monthly**.

cronhourly : En este directorio se encuentra los "scripts" que serán ejecutados cada hora por el sistema.

crondaily : En este directorio se encuentra los "scripts" que serán ejecutados cada día por el sistema.

cronweekly : En este directorio se encuentra los "scripts" que serán ejecutados cada semana por el sistema.

cronmothly : En este directorio se encuentra los "scripts" que serán ejecutados cada mes por el sistema.

cron.deny : Si existe, contiene la lista de usuarios que NO pueden acceder el comando crontab

cron.allow : Si existe, contiene la lista de usuarios que pueden accesar el comando crontab

fstab : Mantiene las particiones y las esepcificaciones con que deben de ser montadas (auto,ro,"file system",etc) al iniciarse el servidor. Vea su formato en "cuotas de Disco Unix".

group: Los grupos que están definidos en el sistema.

hosts : Contiene la resolución **local** de "Hostnames" a direcciones IP, generalmente este archivo se usa para realizar la resolución de instalaciones muy pequeñas.

lilo.conf : Contiene parámetros que serán leídos por LILO.

lmhosts : Contiene la resolución de nombres en **NetBEUI** a direcciones IP, este archivo es de importancia cuando se utiliza Samba y su formato es muy similar a **hosts** .

host.conf : Especifica el orden de donde serán resueltos los nombres de los "Hostnames" , generalmente contiene `order hosts,bind` , esto indica que primero intentará realizar la resolución del archivo `hosts` y posteriormente de un servidor DNS.

hosts.deny : Especifica que "Host's" no pueden accesar los servicios de este sistema.

hosts.allow : Especifica que "Host's" pueden accesar los servicios de este sistema.

inetd.conf : Los servicios que serán accesibles por el super server, el daemon inetd o "Internet Súper Server" es el encargado de correr los puertos de servicio que se especifican en /etc/services

login.defs : Si se están utilizando "shadow passwords", este archivo también es utilizado al generar un usuario nuevo.

inittab : Es el primer archivo que es leído al arranque del sistema, contiene especificaciones sobre que otros archivos deben de ser ejecutados, el nivel de arranque del sistema (2,3 o 5), inicializa el daemon *inetd* (conocido como "Súper Server")

named.conf : Archivo que contiene los parametros que serán utilizados para ejecutar DNS

nologin : Este archivo NO debe de existir si se requiere acceso al servidor vía Telnet o ssh. Ya que el programa "login" no permitirá el acceso a ninguna cuenta de usuario normal "nonroot" accesar si existe este archivo.

profile : Programas de Arranque y ambiente global del Sistema ("System Wide Enviroment")

passwd : Nombre de usuario, contraseñas, numero de usuario(UID), grupo de usuario(GID),nombre completo, directorio de arranque (Home Directory), Shell.

printcap : Contiene las impresoras que pueden ser accesadas del sistema Unix. (Vea : Imprimir en Unix)

resolv.conf : Contiene la dirección(es) IP donde se encuentra(n) el(los) servidor(es) DNS que resolverán todos los nombres, que se le presenten a este "Host".

securetty : Contiene las terminales utilizadas por el PAM de login, de donde puede realizar un login un súper usuario (UID = 0, GID = 0). Para realizar un login vía telnet se puede especificar los seudo-TTY (ttyp1 a ttyp12), pero esto incurre en falta de seguridad, lo mas recomendable es que los usuarios utilicen el comando `su` una vez que accesen el sistema vía un usuario común.

services : Despliega que puertos están disponibles para los diferentes daemons.

shells : Contiene todos los "shells" que puede accesar el sistema

syslog.conf : Indica donde deben de ser enviados mensajes del sistema, sus líneas son de la forma: `servicio, prioridad destino`

Donde `servicio` puede ser: *auth, Authpriv, cron, daemon, kern, lpr, mail, news, syslog user, uucp y local0 - local7*

Donde `prioridad` puede ser: *debug, info, notice, warning, err, crit, aler , emerg, none.*

Donde `destino` es la secuencia de un directorio o archivo (default: /var/log) o `/dev/console` la consola

smb.conf : Archivo de configuración para SAMBA .

sudoers : Archivo que permite a usuarios comunes ejecutar "ciertos" comandos en los que se requiere acceso de "súper usuario" UID = 0, GID = 0.

`/etc/skel/`

Contiene todos los archivos **.** (ejemplo:.bashrc, .kde, etc) u otros que serán colocados en el directorio de un usuario ("Home Directory") al generar al usuario.

`/etc/logrotate.d`

Este directorio contiene archivos de configuración que permiten a los archivos de registro ("logs") rotarse, ya que en sistemas muy activos puede darse el caso que los "logs" se sobrescriban uno sobre el otro, perdiendo todo rastro de la actividad del sistema.

`/etc/pamd/`

login: Archivo que contiene especificaciones del PAM (Pluggable Authentication Module) de *login*. Si se encuentra especificado el modulo `/lib/security/pam_securetty.so` , este modulo indica que: Para realizarse un login de un "superuser" (UID=0, GID=0), este login debe de ser de una terminal que se encuentre en /etc/securetty.

`/etc/default`

useradd : Contiene los valores default para cuando sea agregado un usuario.

GROUP =100 { grupo de usuario cuando se utlize useradd -n }

HOME = /home { lugar donde se guardaran los directorios de todos los usuarios}

INACTIVE = -1 { Numero de día a los cuales se volverá inactiva la cuenta del usuario, contadas a partir del día de la desactivación}

EXPIRE = { Día en el que será desactivada la cuenta }

SEPL = /bin/bash { El Shell default para el usuario }

SKEL = /etc/skel { Lugar de donde se deben copiar archivos al nuevo directorio del usuario }

`/etc/rc.d`

rc.local : Este archivo se ejecuta cuando se inicia el sistema ("Host"), es ejecutado después de los niveles 2, 3 y 5. Contiene el desplegado que se observa en todas las terminales al realizar el "login".

init.d : En este directorio se encuentran todos los "scripts" que facilitan el inicio y cierre de deameons /programas, estos "scripts" comúnmente toman los argumentos "stop" , "start" , "restart", estos argumentos generalmente provienen de lo que se especifica en los directorios /etc/rc.d/rc[0-6].d

rc0.d | rc1.d | rc2.d | rc3.d | rc4.d | rc5.d | rc6.d : Estos subdirectorios contienen "soft links" hacia los "scripts" ubicados en el directorio **/etc/rc.d/init.d** , dependiendo del nombre del "softlink"(empezando en S o K) el argumento que envían a estos "scripts" es "stop" o "start", la modificación de estos argumentos es mediante los comandos: chkconfig o ntsysv.

`/etc/sysconfig`

network : Este archivo contiene la información más relevante de un Servidor Linux en entrono de Red.

Su forma es:

NETWORKING = yes

FORWARD_IPV4 = yes

HOSTNAME = server1.osmosislatina.com

DOMAINAME = osmosislatina.com

GATEWAY = 192.168.32.1

GATEWAYDEV=eth0

Los primeros dos parámetros habilitan al servidor para que funcione como tal, notese que el parámetro HOSTNAME debe de contener el DOMAINAME donde se encuentra el servidor.

El parámetro GATEWAY, generalmente es la dirección IP de la interfase de un router , mientras que GATEWAYDEV es la interfase del servidor (Host) por donde se enviará la información hacia el GATEWAY.

network-scripts : Este directorio contiene los scripts *"ifup" y "ifdown"* para habilitar y deshabilitar las interfaces del "Host" (eth0,eth1..), además de esto "scripts" cada interfase mantiene un archivo en este subdirectorio que lleva por nombre: **ifcfg-<interfase>** (ejemplo: ifcfg-eth0,ifcfg-eth1).

network-scripts/**ifcfg-<interfase>** : Cada interfase que existe en un servidor tiene un archivo de este tipo que proporciona datos acerca de la interfase, suponiendo que existe una Interfase Ethernet en el servidor, habrá un archivo llamado **ifcfg-eth0** que contiene:

DEVICE=eth0

IPADDR=192.168.32.131

NETMASK=255.255.255.240

NETWORK=192.168.32.128

BROADCAST=192.168.32.159

ONBOOT=YES

El parámetro DEVICE indica la interfase de la cual se trata, IPADDR, NETMASK, NETWORK Y BROADCAST son los parámetros de red, mientras que ONBOOT significa que la interfase debe de ser habilitada cuando el Servidor "Host" se inicie

El comando ifconfig se utiliza para observar la actividad de esta interfase.

`./etc/src`

Contiene el código fuente de los paquetes del sistema

linux . Este directorio contiene todo código fuente del kernel

`/var/log`

Este directorio contiene todos los archivos de registro "logs"

messages :Todos los registros "logs" con prioridad *info* son enviados a este archivo, con la excepción de prioridad *info* de los servicios *mail* y *authpriv* .

`/var/spool`

at : Este directorio contiene todos los eventos que se hayan programado con el comando at

cron : Este directorio contiene los archivos de cada usuario, donde especifican los detalles de sus trabajos crontab

`/var/lock`

Contiene los "lock files" del sistema

subsys : Este directorio contiene todos "lock files" que protegen a un programa para que éste no sea abierto por dos o más usuarios

Comandos Generales

dmesg : Imprime los mensajes desplegados por el "kernel" al inicio.

depmod -a : Genera un archivo que contiene las dependencias de los modulos que son cargados para el "Kernel",esto es, es capaz de reconocer cuales modulos deben de ser cargados para que un tercero sea utilizado en el sistema.

free : Estadisticas de uso de Memoria.

init q : Comando que vuelve a leer los parametros que se encuentran en inittab.

insmod : Habilita ("loads") el modulo que se especifica en la línea, para que el "kernel" sea capaz de utilizarlo.(ejemplo: `insmod ip_alias.o`)

ldconfig : Actualiza las librerías utilizadas por el sistema, recomendable ejecutarlo cada vez que se instale un programa.

lsmod : Despliega la información referente a los módulos que están habilitados por el "kernel".

mount: Permite que particiones del sistemas, CD-ROMs, floppys puedan ser leídas en el sistema. Su formato: `mount -t <file system(ext2,vfat)> <partición (/dev/hda1,/dev/cdrom)> <punto de lecutra"` *mount point* `" (/mnt/home/ /mnt/cdrom)>.`

smbmount: Similar al comando **mount** , excepto que este comando es utilizado para montar particiones en samba.

smbumount: Utilizado para desactivar las particiones activadas con **smbmount**

setup: Presenta un menú para configurar varios parámetros del sistema (Sonido, Xwindow, Mouse..).

slocate : Actualiza la base de información que es utilizada para encontrar archivos con el comando **locate** .

source : Recarga el archivo de configuración indicado al ambiente de Shell .

stat : Despliega información detallada sobre el archivo especificado como: fechas de modificación y cambio, dueño del archivo..etc.

umount : Desactiva la partición que se indicada, los parámetros que toma este comando son similares a los de **mount** .

uname -a : Información completa sobre el "Host".

uptime : Hora actual, tiempo que lleva el sistema corriendo desde el ultimo "reboot", usuarios conectados al servidor, carga del sistema en los últimos 1, 5 y 15 minutos.

hostname : El nombre del "Host".

chkconfig : Este comando despliega la información sobre los niveles de ejecución de los "scripts" ubicados en el directorio /etc/rc.d/init.d

chkconfig --list httpd, Este comando despliega:

httpd 0:off 1:off 2:off 3:on 4:on 5:on 6:off

Lo anterior indica que cuando se utilice el nivel de arranque 3, el "script" httpd en el directorio /etc/rc.d/init.d recibirá el argumento "start", cuando se corra el nivel de arranque 6, httpd recibirá el argumento "stop",etc..

Para modificar hacia argumento "start" :

chkconfig --add <nombre del script en directorio init.d> --level <nivel de arranque[0 a 6] >

Para modificar hacia el argumento "stop" :

chkconfig --del <nombre del script en directorio init.d> --level <nivel de arranque[0 a 6] >

Es precisamente de los directorios `/etc/rc.d/rc[0-6]` de donde proviene la información que despliega **chkconfig**

ntsysv : Es una herramienta gráfica que tiene la misma funcionalidad que **chkconfig** , la diferencia es que esta herramienta despliega todos los "scripts" por nivel, esto es, si se utiliza el comando `ntsysv --level 3` , la gráfica mostrará el status "stop" o "start" de todos los "scripts" para el nivel de arranque `3` . De la misma forma se utilizan: `ntsysv --level 5` , `ntsysv --level 0` ,etc.

Al igual que **chkconfig** , **ntsysv** modifica y toma la información que se encuentra en los directorios `/etc/rc.d/rc[0-6]`

En entorno de Red

host : Determina la dirección IP de un "Host" , `host -a` despliega toda la información de DNS.

ifconfig : Permite configurar una interfase de Red y ver el "status" de ésta. Es de la siguiente forma:

ifconfig <interfase> , ejemplo: ifconfig eth0

ifup : Habilita la interfase especificada, ejemplo : `ifup eth0` .

ifdown : Deshabilita la interfase especificada, ejemplo : `ifdown eth0`

netstat -a : Todas la conexiones de Red originadas y recibidas por el "Host"

netstat -r : Muestra la tabla de ruteo "routing table" del sistema

netstat -i : Estadisticas de red de cada interfase

nslookup : Busca información en los servidores DNS, ejemplo: `nslookup -query=mx osomosis.com` , si no se especifican parámetros se entra en modo interactivo

ping -s 1016 : Manda paquetes de ping de 1024 bytes (header 8 bytes), mientras que el "default" es 512.

route add : Permite agregar tablas de ruteo de y hacia el "Host". Ejemplo: Para guiar toda la información de la red 206.171.55.16 netmask 255.255.255.240 vía la interfase eth0 :

route add -net 206.171.55.16 255.255.255.240 eth0

Para rutear todo el trafico por cierta interfase ("Default Gateway"):

route add default gw 206.171.55.51 eth0

Esto enviará toda la información por la dirección 206.171.55.51

route -n : Despliega la tabla de ruteo del "Host". NOTA: Debe de estar "IP Forwarding" ON en /etc/sysconfig/network , además el "kernel" debe de estar configurado para "IP Forwarding" .

smbclient : Funciona como un cliente FTP, que simula conexiones que serán realizadas a través de Samba.

tcpdump : Permite el "debugging" de una interfase en el host.

testparm : Verifica la validez del archivo **smb.conf** utilizado por Samba

Control de Procesos

ps -aux : Despliega todos los procesos del sistema, con nombre y tiempo de inicio

kill : Es utilizado para mandar señales a los procesos en Unix.

kill -HUP <pid> : Señala al proceso con numero `<pid>`, que vuelva a leer sus archivos de configuración

kill -INT <pid> : Señala al proceso con numero `<pid>`, que será interrumpido

kill -TERM <pid> : Señala al proceso con numero `<pid>`,que debe de terminar, a diferencia de -KILL , esta opción da la oportunidad al proceso de terminar.

kill -STOP <pid> : Señala al proceso con numero `<pid>`, que pare momentáneamente

kill -CONT <pid> : Señala al proceso con numero `<pid>`, que continúa, este comando se utiliza para reanudar un proceso que le fue aplicado -STOP

kill -KILL <pid> : Señala al proceso con numero `<pid>`,que termine de inmediato, el proceso es terminado abruptamente.

killall : A diferencia de **kill** , **killall** permite mandar un señal al proceso **por nombre**.

killall <nombre del proceso > : Envía la señal -TERM al proceso con el nombre especificado. NOTA: Por "default" la señal que toma **kill** y **killall** es **-TERM** .

ps -l : Este comando despliega dos parametros PRI y NI. El parametro PRI indica la prioridad actual del proceso, que es calculada por el sistema operativo, el valor de NI es tomado encuenta cuando se determina el PRI.

NI : NI es llamado el numero gentil o "nice number" , este numero es especificado por el "súper usuario"("root") o dueño del proceso y afecta el orden final del PRI, le da prioridad a los menos gentiles. Sus valores oscilan desde -20 (menos gentil = mas prioridad) y 20 (mas gentil = menos prioridad)

nice : Este comando especifica el numero NI de cada proceso.

`nice -10 named` : Esto bajaría la prioridad de `named` en 10 unidades.(Si estaba en -10, pasará a -20).

`nice +10 named` : Esto incrementaría la prioridad de `named` en 10 unidades.(Si estaba en 0, pasaría a +10).

snice y **renice** : El mismo funcionamiento que **nice** , excepto que utiliza el numero de proceso :

```
snice -10 <pid>
```

<comando> & : El **&** es utilizado para indicar que el proceso debe de ejecutarse en el fondo.

top : Esta herramienta monitorea varios recursos del sistema y tiene un caracter dinámico, muestra uso de CPU por proceso, cantidad de memoria, tiempo desde su inicio, etc .

vmstat : Es muy similar a **top** ya que es un condensado de los procesos del sistema, para que esta herramienta se vuelva dinámica se deben especificar los argumentos: vmstat -n <numero de segundos por actualización >

at : Este comando permite programar ciertas actividades a una cierta hora, ejemplo : at 22:00 , el comando anterior abre un "prompt" de la forma at> , sobre este "prompt" se especifican todos los comandos que se deseen ejecutar, en este caso a las 22:00, una vez especificados, se utiliza Ctlrl-d para salir.

Ya finalizado, los comandos estarán programados para ejecutarse a la hora indicada, el directorio /var/spool/at contiene el trabajo.

El comando atq despliega los trabajos at que están pendientes, y el comando atrm <numero de at> elimina un trabajo programado con at .

crontab : : Al igual que **at** especifica el tiempo al cual se ejecutará un programa "script", **crontab** tiene la siguiente forma:

minutos horas días meses fin_de_semana nombre_de_usuario instrucción argumentos

El siguiente ejemplo ejecutará el programa oracle.pl cada media hora todos los días:

30 * * * * root /usr/oracle.pl

Si se desea realizarlo mensualmente:

01 3 1 * * root /usr/oracle.pl

Lo anterior ejecutará oracle.pl el día primero de cada mes, a las 3:01 AM.

Para especificar trabajos cron cada usuario mantiene un archivo en el directorio /var/spool/cron/ , este directorio lo accesa cada usuario con el comando crontab -e

La ejecución de **crontab** se facilita debido al archivo /etc/crontab que especifica trabajos **crontab** por hora, día ,semana y mes, de esta forma solo se requiere que el usuario coloque un archivo en los directorios correspondientes: /etc/cron.hourly | /etc/cron.daily | /etc/cron.weekly | /etc/cron.monthly

Control de Registros "Logs"

tail : Permite ver el final de un archivo, este comando es util ya que los archivos de registros "logs" crecen constantemente tail --f /var/log/messages

También se puede especificar el numero de renglones que se deben observar:

tail --f --line 15 /var/log/messages

Este comando anterior despliega las ultimas 15 lineas del archivo ("default" = 10). La --f mantiene el archivo abierto para poder observarlo conforme se agregen eventos.

Configuración de Sistema

/usr/sbin/sndconfig : Ejecutable utilizado para configurar el sonido del sistema.

/bin/netconf : Ejecutable utilizado para configuración de Interfases de Red.

GLOSARIO.

Broadcast.
Difundir, diseminar información a varios receptores simultáneamente.

Browser.
Hojear o visualizar y posiblemente, editar un archivo en la pantalla, tal como si fuera texto de un documento de procesamiento de texto. Los comandos <brouse> permiten al usuario navegar a través de los datos, horizontalmente por campos y verticalmente por filas o pantalla completa.
Visualizar y editar la jerarquia de clases de los objetos en un lenguaje de programación orientado a objetos.

FTP
Protocolos de transferencia de archivos; sirve para copiar archivos de una computadora a otra en Internet. Transfiere tanto archivos de texto como binarios de un sitio a la maquina del usuario.

DNS
El servicio DNS (ingl. Domain Name Service) se necesita para convertir nombres de dominio y nombres de computadoras en direcciones IP; generalmente se habla de "resolver nombres". Por ejemplo al nombre de computadora tierra se le asigna la dirección IP 192.168.0.20.

DHCP
Denominado "Dynamic Host Configuration Protocol" tiene como función proveer configuraciones desde un servidor en la central de la red, para no tener que hacerlo de forma de descentralizada, desde cada estación de trabajo. Un cliente que no ha sido configurado con DHCP no posee direcciones estáticas si no que se configura totalmente a si mismo según las especificaciones del servidor DHCP.

Gestor de ventanas.
Agente de configuración. En linux todas las ventanas son configurables y cada una posee su propio Kernel.

Hipertexto.
Metodología de presentación de información gracias a la cual las palabras puestas de relieve (o enlaces) remiten a otros documentos hipertexto. Para activar un enlace. Basta con posicionarse en él y hacer clic. Los documentos pueden contener texto e imágenes, datos de video sonido y postscript.

Internet.
Red mundial que ofrece servicios como correo electrónico, boletines de noticias, noticias, transferencia de archivos por medio de protocolos FTP, conferencias informativas y charlas electrónicas acceso remoto a millones de bases de datos y recopilación de datos, además no esta a cargo de una sola entidad, a partir de un punto de acceso único; comprende redes interrelacionadas y agrupa empresas y instituciones de cooperación.

ISP.
Proveedor de servicios de Internet.

Kernel.
También conocido como el corazón de la maquina. Maneja todas las operaciones internas del sistema operativo. Se instala al directorio /boot durante la instalación.

Linux.
Es un clónico de Unix escrito desde el inicio por Linus Torvalds con la ayuda de un grupo de hackers dispersó por toda la Red. Su objetivo es la conformidad con el estándar POSIX.

Login.
Es el proceso de registro de un usuario en el sistema.

Parches.
Un parche para el núcleo es un fichero que solamente contiene información, sobre las líneas de código que han cambiado desde la versión precedente del núcleo. De esta manera, solamente te tienes que bajar un fichero con los cambios, en vez del núcleo completo. El ahorro en cantidad de Mb bajados es bastante considerable, sobre todo para aquellos que dependen del módem y no tienen una conexión buena a Internet

Protocolo.
Define la interrelación entre dos elementos de software y hardware, con lo cual garantiza una comunicación confiable y sin errores. Es un lenguaje empleado por la computadora para comunicarse con la red.

Root.
Es una barra / conforma a partir de ella una estructura de directorios; se puede llegar desde el directorio raíz a cualquier subdirectorio. También es un usuario, el más poderoso del sistema linux y el que más responsabilidades tiene.

Servidor.
Computadora de gran tamaño enlazada a la red de área local que ofrece uno o varios servicios a los usuarios, como almacenamiento de archivos, impresión de documentos, etc Las otras computadoras cliente en la red se comunican con el programa servidor por medio del software cliente adecuado.

Shell.
Proporciona un a interfaz de línea de comandos entre el usuario y el kernel de linux.
Los comandos escritos los interpreta el shell y se envía al kernel, que a su vez abre, cierra, lee y escribe archivos; las funciones internas de la shell también se pueden usar para escribir programas

Sistema operativo.
Debe proporcionar un entorno cómodo para la relación hombre-ordenador Esto incluye, por ejemplo, gestionar los recursos de la máquina de manera que no se produzcan conflictos entre quienes quieran usarlos al mismo tiempo, proporcionar un nivel extra de abstracción al programador por encima de las características específicas de cada recurso y hacerlo todo de la manera más "humana" posible.

Sistema operativo multitarea y multiusuario.
Permite que varias personas puedan estar ejecutando distintos programas al mismo tiempo en un mismo ordenador.

Sistema remoto.
Sistema durante el cual el usuario tiene acceso con la ayuda de una aplicación como telnet. Una vez que se conecta ahí, el sistema remoto reemplaza al sistema local.

URL.
(Localizador uniforme de recursos) gracias a el es factible tener acceso a la mayoría de los servicios con la ayuda de una dirección que comprende una sintaxis, detrás de cada enlace se encuentra una URL y estás están ocultas a la vista.
Esta formada por una sucesión de letras y números que corresponden a nivel jerárquico a una computadora, a un directorio, un archivo, en orden que va de lo general a lo particular.
La estructura de una URL es la siguiente:
Protocolo utilizado con el sitio web:// nombre del dominio del sitio web/ ruta de acceso al archivo del sitio web : *http:// www.yahoo.com.mx/search*

WWW.
Es un hipermedio dinámico conocido que permite conocer información al ofrecer un acceso fácil a los recursos mundiales por medio de servidores de hipertextos.

XFREE.
Agente de configuración, conocido en su versión XFREE86 y esta se divide en dos clases: XFREE86 CONFIG que maneja el modo texto y XFREE86 SETUP que maneja el ambiente gráfico.

YaST.
Componente básico de la distribución SuSE LINUX, ayuda a instalar el sistema y administra el Software.
YaST 1 maneja el modo texto Disquete y YaST 2 maneja el modo grafico CD ROM.

BIBLIOGRAFIA.

José Luis Raya - Cristina Raya.
TCP/IP en Windows NT Server.
Madrid España.
Editorial RA-MA.
Pág. 34, 35, 41- 47, 364-365.

Wilder, Floyd
A Guide to the TCP / IP protocol suite
Second Edition 1998
Boston – London
Artech House Telecommunications.
Capítulo 2.

Alan Freedman
Diccionario de computación
Mc Graw – Hill
Traducción 1995.

Vito Amato
Guía del primer año Academia de Networkin de Cisco Systems.
Mcmillan publishing y Cisco Systems, Inc.
Capítulo 5, 10

Daniel Leduc
Armand St-Pierre
Internet
Guía practica de Navegación
Editorial Trillas

Héctor Facundo arena
La Biblia de Linux
Manual de uso, instalación y configuración
Colección manuales USERS.
Editorial MP Ediciones

http://linux.org.mx
http://hispalinux.es
http://suselinux.com
http://www.redhat.com