Universidad Nacional Autónoma de Nicaragua

UNAN – León

Facultad de Ciencias

Departamento de Computación

Monografía para optar al Titulo de Licenciatura en Computación

Tema

Configuración del DNS y los Servicios Básicos de Red para la Intranet del Instituto Politécnico La Salle de León bajo la Plataforma Linux.

Presentado por:

Br. Brenda Maria Aguilar Zapata.
Br. Emerson Francisco Castillo Real.
Br. Hazzell Isabel Espinoza Moreno.

Tutor
Msc. Aldo René Martínez.

León, Nicaragua Marzo del 2007

INDICE

INDICE

INDICE

I. DEDICATORIA

Brenda Aguilar Zapata

Esta Monografía la dedico en primer lugar a Dios por haberme permitido llegar hasta este momento, a todos mis seres queridos por el apoyo y paciencia que me brindaron. Muy en especial a mi querida madre Maria Cecilia Zapata, a quien agradezco con todo mi corazón por haber hecho de mi lo que hoy en día soy, por haber alimentado mi espíritu con su amor y mi cuerpo con sus cuidados. También la dedico a mis hermanos, al señor Juan Ramón Sevilla, que ha sido como un padre para mí, a mi tía y mis abuelos. A todos ellos todo mi amor y agradecimiento.

Emerson Castillo Real

Esta Monografía la dedico a Dios todopoderoso por permitirme llegar a este momento, a mi Familia por su apoyo y paciencia incondicional. Muy en especial a mi querida madre Mayra, mi padre Francisco Castillo, mis abuelos Pilar Real, Ramón Castillo, Rafaela González, a mi tía Mercedes por estar siempre pendientes de mis estudios y aconsejándome en todo momento. También la dedico a mis hermanos, primos, tíos, que confiaron en mí.

A todos ellos más que dedicatoria, un gran agradecimiento.

Hazzell Espinoza Moreno

Este proyecto Monográfico se lo quiero dedicar en primer lugar a Dios, que es el que me ha dado el conocimiento, las fuerzas y sobre todo la vida para culminar este trabajo.

A mi madre Reyna Isabel Moreno S. La persona mas importante en mi vida, quién me ha apoyado siempre en todas mis decisiones, proyectos, y en la vida diaria, con el amor, el cariño, comprensión y sobre todo con consejos que me han sido de mucha ayuda.

II. AGRADECIMIENTO

Estamos profundamente agradecidos con Dios, que nos da fuerza y conocimiento para llegar hasta el final de nuestras metas.

Estamos agradecidos por el gran apoyo, paciencia y dedicación que nos ha dado el Ing. Marcos Cárcamo Narváez, a todo el personal de Informática del Instituto Politécnico La Salle de León, quienes con su apoyo, colaboración y amistad hicieron posible la realización de este proyecto monográfico.

Al Msc. Aldo Martínez por su apoyo y colaboración durante este proyecto monográfico.
Al Lic. Edisón Cuevas y Juan Navas de UNAN- Managua por su apoyo, colaboración y disposición a pesar de la distancia.

A Nuestros Padres por el apoyo incondicional que nos mostraron durante todo este proceso.

Y a todas aquellas personas que de una u otra forma, colaboraron o participaron en la realización de esta investigación.

III. INTRODUCCIÓN

Una Intranet es una red privada que utiliza los recursos desarrollados de Internet para Distribuir información y aplicaciones a los que solo puede obtener acceso un grupo controlado de usuarios es decir solo por los miembros de la organización, empleados o personas con autorización.

Esta implementación funciona como una alternativa al intercambio transparente de los inmensos recursos informacionales de una organización entre cada uno de los escritorios individuales con un mínimo costo, tiempo y esfuerzo.

Los servicios que pueden ofrecerse en una Intranet son muy similares a los de Internet, pero con dos ventajas fundamentales: mayor seguridad, al tratarse de un entorno cerrado y de acceso restringido, y mayor velocidad, ya que no está supeditada al funcionamiento de la red Internet.

Los servicios básicos que brinda una intranet son: Servidores de nombre (DNS), Servidor HTTP o Web (Apache2), Protocolo de transferencia de mensaje simple, SMTP (Qmail), Protocolo de transferencia de ficheros (FTP).

El DNS (Domain Name System) es un conjunto de protocolos y servicios que permite a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas. Inicialmente, el DNS nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a Internet.

Con la realización de este nuevo proyecto pretendemos poner a funcionar un servidor de Intranet para el Instituto desde el punto de vista teórico-practico bajo la plataforma Linux-Suse 10.0; tomando como base de información todo lo que ya existe, tanto en infraestructura y servicios ofrecidos.

Entre las principales virtudes de esta distribución es que es una de las mas sencillas de instalar y administrar. El software, por la definición de código abierto, permite a desarrolladores y usuarios participar en la evolución de esta plataforma.

IV. ANTECEDENTES

El Instituto Politécnico La Salle es un Centro que cuenta con más de 100 años al servicio de la educación técnica y profesional en Nicaragua, con el interés de ir de la mano con los avances tecnológicos. Este centro se dedica a dar formación técnica a jóvenes y adultos de toda Nicaragua, especialmente de la zona noroccidental.

Enclavado en la ciudad de León, a 90 Kms de la capital, tiene actualmente mas de 860 alumnos en cursos regulares de los niveles básicos y Técnico Medio, y una cantidad que oscila entre 100 y 200 en los diferentes cursos de capacitación y complementación que ofrece a lo largo del año a diferentes empresas y organizaciones que los solicitan. Esta dividido en dos grandes áreas.

La primera “La Fundación Politécnico La Salle” es el área productiva que ofrece las carreras de Electricidad Industrial, Electrónica Industrial, Mecánica Industrial, Mecánica Automotriz, Mecanización Agrícola y Ebanistería. En Nicaragua solamente existen 4 Centros de esta categoría (Granada, Jinotepe, Managua y el IPLS).

La segunda área, “El IPLS”, lugar correspondiente a la parte educativa: bachillerato y técnicos medios en el área de Reparación y Mantenimiento de computadoras, Programación, Diseño grafico, Operadores en computadoras, entre otros.

Las transformaciones tecnológicas de los últimos tiempos obligan a que la comunidad de Hermanos vaya adaptando perfiles, curriculums, programas y tecnologías para que la respuesta que la Iglesia da al reto laboral sea eficaz.

Por lo que en mayo del 2007 inicia una nueva etapa en el proceso educativo, con la apertura de la universidad La Salle de León (ULSA-LEON) con el objetivo de formar profesionales capacitados ante los más exigentes retos del futuro. ULSA-León será una institución que impartirá enseñanza media superior y enseñanza superior inspirada en el evangelio, en el espíritu y carisma se San Juan Bautista de la Salle.

La misión como universidad es la formación integral, humana y cristiana de jóvenes y adultos basados en los aspectos espirituales, morales, psicológicos, cognitivo, afectivo, estético, físico y social, para el desarrollo armónico y crecimiento en valores universales. Las carreras que se ofertaran en esta universidad están orientadas a que el joven se pueda desempeñar en cualquier área o rama de la informática:
Ingeniería en Cibernética Electrónica, Ingeniería en Gestión Industrial, Ingeniería en Mecánica con Énfasis en Energías Renovables, Ingeniería en Mecatrónica con Enfasis en Control de Procesos.

En el instituto Politécnico la salle nunca se ha trabajado bajo la plataforma Linux, ni se han desarrollado proyectos sobre la implementación de Intranet bajo la misma.
Pero si se han hecho varios proyectos pilotos relacionados con el tema a cargo del Ingeniero Carlos Ramírez sin ser llevados a la práctica. Actualmente en el instituto solo existe un servidor Windows 2000 que no ha sido de uso amplio, este servidor es el encargado de proporcionar el servicio de Internet a algunos grupos de trabajos.

V. JUSTIFICACIÓN

Este proyecto se realiza debido a la gran demanda que existe de los usuarios y lo que se desea es dar respuesta mediante la optimización del flujo de información y de los recursos, compartiendo información, equipos y tecnologías. Esto se logra mediante un proceso de ordenamiento en lo que es la Infraestructura de la red del Instituto.

Con Suse no solo se trabaja fácilmente, sino que es también un sistema operativo completo multitarea y multiusuario, a muy bajo costo, fue lanzado el 6 de octubre del 2005 es de código completamente abierto y tiene tanto código abierto como aplicaciones propietarias además de ser una versión completa y al por menor en centros especializados.

Además este sistema operativo es dueño de una fortaleza que ha demostrado en cuanto a soporte técnico se refiere y por la seguridad de los datos e información almacenada, prueba de esto es que hasta la fecha no se conoce de ningún ataque de virus al sistema operativo Linux, lo que nos confirma la fiabilidad y seguridad que nos proporciona en sus diferentes aplicaciones y sobre todo de su uso como plataforma.

Es importante decir que la implantación de la Intranet bajo esta plataforma mejorara la competitividad, ahorrara costes y tiempo, mejorara la productividad, las comunicaciones y promoverá la participación, además permitirá una relación directa entre sus miembros, entre otras cosas.

Es un sistema estable y potente para trabajar en red, a un coste mínimo. Es modificable y adaptable a las necesidades reales de educadores y estudiantes. Es libre para usar, modificar; la copia es legal, los alumnos y los profesores lo pueden copiar legalmente evitando la piratería.

Un dato destacable es el valor educativo del uso entre alumnos de un software completamente libre. La idea de tener un ordenador funcionando gracias a que hay personas que trabajan compartiendo sus conocimientos tiene un valor educativo en sí mismo. La elección de Suse 10.0 se basa en las múltiples ventajas de usar software libre.

En la actualidad el Instituto Politécnico La Salle invierte alrededor de los $ 35,000 (treinta y cinco mil dólares) por los derechos de software propietario, WINDOWS, por lo que al migrar a un software libre se reducirá de forma muy significativa los costos en las inversiones del mismo, lo que beneficiará al centro Politécnico la Salle León.

VI. OBJETIVOS

Objetivo General

Configurar el DNS y los servicios básicos de red para la Intranet del Instituto Politécnico La Salle bajo la plataforma de Linux e implementarla en un equipo servidor real, estableciendo su importancia y dejando documentación del trabajo realizado.

Objetivos Específicos

- Conocer que es un DNS, los servicios básicos de red para la Intranet y su funcionamiento.
- Configurar el DNS Interno como un subdominio net.ipsalle.edu.ni.
- Elaborar una documentación completa para posteriores trabajos sobre el DNS y el ofrecimiento de los servicios básicos de Intranet bajo la plataforma de Linux.
- Demostrar el correcto funcionamiento de un servidor de Intranet bajo la plataforma Linux, proporcionando servicios básicos (Web, DNS, Correo Electrónico y Otros).

VII. Marco Teórico

1. INTRANET

1.1 Generalidades

El fenómeno Intranet surge a partir de la experiencia exitosa de World Wide Web en el mundo Internet. De hecho, es una proyección al interior de lo que las organizaciones han colocado a disposición de la comunidad virtual que usa Internet y que han visto las ventajas de contar con una interfaz única para realizar sus procesos administrativos cotidianos.

Una Intranet es una red privada que la tecnología Internet usó como arquitectura elemental. Una red interna se construye usando los protocolos TCP/IP para comunicación de Internet, que pueden ejecutarse en muchas de las plataformas de hardware y en proyectos por cable. El hardware fundamental no es lo que construye una Intranet, lo que importa son los protocolos del software.

Con el enorme crecimiento de Internet, un gran número de personas en las empresas usan Internet para comunicarse con el mundo exterior, para reunir información, y para hacer negocios. A la gente no le lleva mucho tiempo reconocer que los componentes que funcionan tan bien en Internet serían del mismo modo valioso en el interior de sus empresas y esa es la razón por la que las Intranets se están haciendo tan populares. Algunas corporaciones no tienen redes TCP/IP: el protocolo requerido para acceder a los recursos de Internet. Crear una Intranet en la que todas las informaciones y recursos se puedan usar sin interrupciones tiene muchos beneficios. Las redes basadas en TCP/IP facilitan a las personas el acceso a la red remotamente, desde casa o mientras viajan. Contactar con una Intranet de este modo es muy parecido a conectar con Internet, La operabilidad interna entre redes es otro suplemento sustancial. Los sistemas de seguridad separan una Intranet de Internet. La red interna de una compañía está protegida por firewall. La tecnología firewall usa una combinación de enrutadores, servidores y otro hardware y software para permitir a los usuarios de una Intranet utilizar los recursos de Internet, pero evitar que los intrusos se introduzcan en ella.

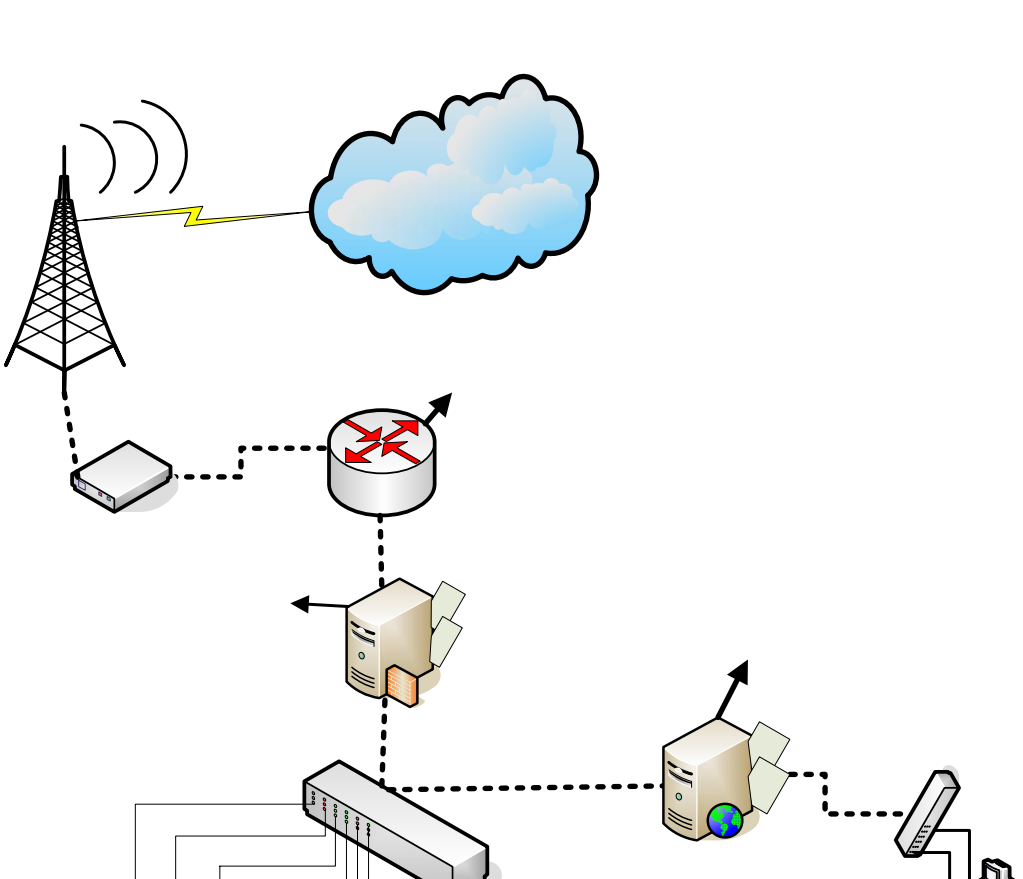
Mucha intranets tienen que conectarse a "sistemas patrimoniales": el hardware y las bases de datos que fueron creadas antes de construir la Intranet. A menudo los sistemas patrimoniales usan tecnologías más antigua no basada en los protocolos TCP/IP de las intranets. Hay varios modos mediante los que las intranets se pueden unir a sistemas patrimoniales. Un método común es usar los guiones CGI para acceder a la información de las bases de datos y poner esos datos en texto HTML formateado. Haciéndolos asequibles a un navegador para Web.

En la actualidad, la creación de productos para Intranet ocupa un alto porcentaje de los recursos de investigación y de desarrollo de las empresas de software. Las empresas ligadas al hardware, también han potenciado sus productos para trabajar o soportar aplicaciones de Internet e Intranet. Es más,

se supone que la mitad de lo que hoy se desarrolla en ambiente Web está orientado a Intranet.

La tendencia actual sobre este tema es el desarrollo de intranets valiéndose de lenguajes de programación que permitan extender el uso de HTML. Nos referimos a los lenguajes Java y ActiveX y C++, los cuales están obteniendo un grado de aceptación progresivo en la industria del software y especialmente con bases de datos y compatibilidad de distintos sistemas operativos. Todo esto implica ser cuidadosos al momento de definir qué es una Intranet.

Diagrama Actual de la Intranet



ISP=> Alfanun
Antena Alfanu
512 Subida, 512

Ro
1 F
Sa

1.2 Definición de Intranet

1.2.1 Visión Técnica

Una definición con enfoque técnico, sostiene que "Intranet es un conjunto de Sitios Web que están instalados en la red interna de una institución o empresa y que permiten mostrar datos o documentos a cualquiera de los computadores conectados a ella" (Ryan Bernard, 1996).

Esto es, un computador con categoría de servidor de sitios Web dentro de la empresa, y que alberga información que sólo puede utilizar quien esté definido como usuario válido de la Intranet. Esta definición, siendo válida, es muy similar a lo que entendemos por LAN o WAN, tan sólo sustituyendo el concepto "Sitio Web" por el de "Servidor".

La diferencia radica en el uso de una interfaz común, que es independiente del computador desde el cual el usuario se conecta al servidor, utilizando para ello, ya sea un PC-compatible, una Workstation o un Macintosh. La interfaz será la misma y el usuario podrá obtener o ingresar información del mismo modo. De hecho, esta interfaz es un software de interpretación desarrollado para cada sistema operativo y que trae al usuario la información organizada utilizando un lenguaje estandarizado como HTML, Java o ActiveX, sin ser excluyentes entre sí.

La comunicación entre los equipos, independiente de la plataforma utilizada, se realiza sobre un protocolo de comunicaciones estándar como TCP/IP u otro diferente, siempre que todos los equipos que se comuniquen a la Intranet utilicen el mismo protocolo.

1.2.2 Visión funcional

Una definición desde el punto de vista funcional, sostiene que Intranet es un sistema para la gestión de información, desarrollado principalmente sobre las potencialidades del mundo World Wide Web, y que es de acceso limitado a la institución o empresa que lo crea o a quien ella autorice.

Bajo esta concepción, la Intranet no sólo se desarrolla para quienes trabajan dentro de la empresa, sino también para aquellos que usan servicios de información que esta empresa produce y pone a disposición del usuario externo. La información se mantiene dentro de la institución; los que trabajan en ella, generan u obtienen datos para su trabajo cotidiano, pero también los clientes pueden acceder a ciertos servicios autorizados.

Para establecer una Intranet, las consideraciones funcionales son tan importantes como las técnicas y en definitiva, las técnicas están condicionadas a los requerimientos funcionales definidos por la organización.

Esto, porque la concepción de una Intranet no sólo considera el uso de cierta tecnología disponible en el mercado, sino también el re-pensar los procesos de generación y administración de los recursos de información.

1.2.3 Visión general

Intranet es simplemente aplicar una tecnología de Internet (la Web) a un grupo cerrado de usuarios. Basta con controlar la entrada a una Web mediante claves y contraseñas, para que se convierta en una Intranet. De este modo, sólo los usuarios autorizados tendrán acceso a recursos e información privada, esté donde esté la ubicación de sus puestos de trabajo y conexiones a la Intranet.

1.3 Ubicación de la Intranet

Según las necesidades de los usuarios la Intranet se puede colocar en:

- Un ordenador personal (PC)
- Una red local (LAN)
- Internet

Muy a menudo se combina las tres posibilidades en Intranet, siendo habitual conectar a la red local interna con Internet (con corta fuegos de seguridad).

Para saber qué ubicación es la más adecuada y así satisfacer las necesidades de cada cliente, la clave está en la ubicación de los usuarios de la Intranet.

1.4 Tipos de intranet

El parámetro utilizado para su clasificación desde una perspectiva tecnológica, es la capacidad que se le atribuye para ingresar, modificar y consultar datos dentro del sistema. Bajo este prisma, podemos distinguir dos tipos de intranets: las pasivas y las activas.

Aquellas denominadas pasivas, son interactivas pero no dinámicas, esto quiere decir, que no permiten el acceso a los datos y sólo permiten desplegar información estática en la pantalla.

Por el contrario, las activas son interactivas y son dinámicas, ya que permiten acceso e interacción con los datos por parte del usuario o cliente.

Visto desde una perspectiva funcional, el parámetro de clasificación que se considera es, la función a la que sirve la intranet.

En este caso, encontramos: aquellas que apoyan a la toma de decisiones, control y gestión y, aquellas que apoyan a la parte operativa y administrativa de la empresa.

Las primeras aportan información relevante para el ciclo gerencial de la empresa en sus funciones de decisión, control y gestión. Las segundas en cambio, sirven con mayor propiedad a las funciones operativas de la empresa.

1.5 Servicios de la Intranet

El entorno de software de la Intranet se ejecuta en todos los sistemas operativos y plataformas de hardware de cliente y servidor, en consecuencia produce un entorno de red común capaz de incluir incluso a los entornos de red más heterogéneos.

Los servicios de la Intranet permiten a los usuarios realizar cualquier tipo de tarea: buscar información, enviar y recibir correo electrónico, buscar en directorios, integrar cualquier tipo de aplicación personalizada y de cualquier fabricante y finalmente centralizar la administración de la red incorporando funciones tales como seguridad y directorios.

1.5.1 Tipos de Servicios de la Intranet

1.5.1.1 Servicios de Usuario

Facilidad de crear, compartir y administrar la información.
La Intranet facilita la ubicación y administración transparente y sin problemas de contenidos en toda la red, asegurando que todo aquel que cuente con derechos de acceso estará en posesión de la información más reciente procedente de cualquier parte de la red. Pueden crearse documentos HTML usando intuitivas interfaces y los formatos de documentos ya existentes tales como documentos de tratamiento de textos y hojas de cálculo pueden publicarse con la mayor facilidad. Hiperenlaces, multimedia (imágenes, videos y sonidos), y objetos incrustados, permiten integrar y personalizar contenidos en línea enriquecidos e interactivos. Los documentos se indexan y organizan mientras se publican, y pueden administrarse desde el escritorio y de forma centralizada, en un solo lugar.

Navegación
La Intranet facilita la búsqueda de cualquier información o recurso que se encuentre en la red. Los usuarios, al ejecutar una sola consulta, obtienen una lista organizada de toda la información coincidente en todos los servidores de toda la empresa y en
Internet. Los índices y jerarquías de exploración se crean y mantienen con la mayor facilidad, ofreciendo una interfaz de navegación similar a los mejores buscadores de Internet.

Con servicios de agentes, los usuarios pueden hacer que los servidores estén atentos a la llegada de nueva información o vigilen si se producen cambios en los recursos existentes. El control de acceso sólo permite que accedan los usuarios autorizados a los documentos restringidos. En consecuencia, todos los usuarios tienen un acceso completo y personalizado a toda la información importante de su red interna y de Internet.

Comunicación
Las normas de Internet permiten que las posibilidades del correo electrónico abierto y los groupware sean tan avanzadas y funcionales como las alternativas propietarias tradicionales.

El control de acceso y la seguridad permiten que el correo electrónico y los grupos de discusión sean privados, así como la autentificación de todas las partes en la red.

Los usuarios pueden examinar direcciones de correo electrónico, claves de seguridad y números de teléfono de Internet usando una sencilla interfaz de agenda de direcciones conectada con un servicio de directorio abierto en Internet.

Acceso a bases de datos y aplicaciones

El acceso a bases de datos y aplicaciones ya existentes se realiza fácilmente desde una sola interfaz. Pueden instalarse aplicaciones nuevas una sola vez con JavaScript y Java, y desplegarse rápidamente en cualquier plataforma, en todos los entornos operativos y plataformas de hardware de escritorio y servidor. Las aplicaciones pueden estar asociadas con el contenido y pueden Desplegarse de forma transparente tanto en Internet como en la Intranet.

Todos los servicios de la Intranet están a disposición de las aplicaciones, lo que incluye administración de contenidos, directorios y duplicación. El acceso a las aplicaciones se controla fácilmente y puede basarse en los procesos comerciales, lo que ofrece funciones de flujo de trabajo de fácil uso en toda la empresa.

1.5.1.2 Servicios de red

Directorio

Los servicios de directorio gestionan información referente a personas, control de acceso, configuración de servidores y recursos específicos de las aplicaciones. El protocolo de directorio funciona en todos los entornos operativos y aplicaciones de la Intranet e Internet.

Los usuarios finales pueden obtener información de personas, incluidas direcciones de correo electrónico, claves de seguridad y números de teléfono. Los administradores pueden gestionar de manera centralizada el control de acceso y los parámetros de configuración de los servidores de toda la empresa. Las aplicaciones pueden gestionar información específica de las propias aplicaciones, incluidos directorios ya existentes tales como los de sistemas de correo electrónico propietarios. La información de directorio puede duplicarse en toda la empresa.

Protección

La Protección es omnipresente y fácil de gestionar. Los servicios de seguridad de la Intranet ofrecen métodos para proteger los recursos contra los usuarios no autorizados, para encriptar y autentificar las comunicaciones y para verificar la integridad de la información.
Aplicaciones, páginas Web, directorios, grupos de discusión y bases de datos están sujetos a un control de acceso, que se gestiona de forma centralizada, por el cual la información referente a recursos específicos y a los privilegios de usuario relativos a dichos recursos se gestiona y distribuye a través del servicio de directorio de la Intranet.

El correo electrónico y las comunicaciones en tiempo real pueden estar asegurados, cada parte autentificada y el tráfico de mensajes encriptado.

Las corporaciones pueden crear y administrar una infraestructura de claves de seguridad para ofrecer a sus empleados la capacidad de hacer los negocios de la empresa a través de la red con total seguridad. Asimismo, las aplicaciones de la Intranet pueden ampliarse con total seguridad a través de Internet.

Duplicación

La duplicación eleva al máximo la eficiencia de la red, al permitir que información tal como el contenido de las páginas Web, los mensajes de los grupos de discusión, directorios y tablas de base de datos se distribuyan en la Intranet. La duplicación también facilita recibir recursos de la red tales como grupos de discusión y directorios fuera de línea, de tal manera que se permite a los usuarios seguir efectuando cambios y actualizaciones; cuando el usuario vuelve a estar en línea, todos los cambios se reconcilian correctamente.

Administración

La Intranet proporciona una interfaz de administración común, integrada, sencilla de usar y basada en HTML que permite gestionar con total seguridad los servidores y recursos desde cualquier lugar de la Intranet. Todos los servidores de la Intranet admiten el Protocolo simple de gestión de red (SNMP) y están integrados con entornos de administración de red comunes.

Los servicios de directorio permiten que toda la información referente a los usuarios, parámetros de control de acceso y configuración de servidores sea segura y esté centralizada y duplicada, así como la creación, el borrado y la modificación de cuentas de usuario mediante un solo botón y en toda la empresa. Las aplicaciones pueden integrarse limpiamente con cualquiera de los principios básicos de administración mencionados.

1.6 Administración de servicios para una Intranet.

La importancia de una administración adecuada implica muchos aspectos importantes. Todos los sistemas UNIX son distintos de una forma u otra y cada sistema individual UNIX es distinto en la forma en que debe administrarse. Linux no es una excepción. Las tareas de administración varían dependiendo, entre otras cosas, del número de usuarios a administrar, los tipos de periféricos conectados al conmutador, las conexiones de red y el nivel de seguridad necesaria.

Un administrador de sistema tiene que proporcionar a los usuarios del sistema un entorno eficiente, seguro y fiable. La delegación de las responsabilidades de administración varía de un sistema a otro. En sistemas pequeños se asigna a un simple usuario la tarea de administrador. Si se trabaja en un entorno de red, la administración la realiza un administrador de red. Todos los sistemas Linux tienen un sólo usuario que puede realizar cualquier operación en el computador denominado súper usuario, con un nombre especial de entrada llamado root.

1.7 Uso de la Intranet

El uso de la Intranet es limitado solo por su imaginación. Una Intranet ahorra tiempo y dinero y papel al reducir o eliminar la impresión y re- impresión de información, al poder ser fácil producida, distribuida y accesible electrónicamente.

En una Intranet, la totalidad de la información puede ser actualizada y distribuida inmediatamente, ganando en productividad y competitividad. Y, la más importante, convierte a la universidad en una comunidad, salvando tiempo, zonas y lugares. Los siguientes ejemplos tratan de darle una guía de aplicaciones y formas en que una Intranet puede ayudarle.

Cartas, Memorandos, Circulares

Si usted publica su carta en una o varias páginas de la Intranet, tan pronto como usted haya finalizado de escribirla, puede estar disponible para que todas las lean. Puede aún configurar un enlace que les permita a los lectores responder vía e-mail cualquier publicación nueva. Todo lo que ellos tienen que hacer es clic en el símbolo de e-mail resaltado y su Browser abre una ventana de e-mail y automáticamente inserta su dirección.

Manual de los Empleados

A medida que la política de una institución cambia, el mantenimiento de un manual de empleados actualizado y distribuido se puede volver una operación difícil y costosa. Si el manual es publicado en un sitio de la Intranet cada cambio puede ser incluidos para beneficios en salud, planes de pensión, y acceso a la hoja de vida del empleado (proveyendo seguridad apropiada, claro esta).

Soporte a los Miembros

Podemos estandarizar los problemas más frecuentes de los miembros en publicar las soluciones respectivas. Soporte al personal con procedimientos, manuales, etc. Encontraran los miembros que muchos de los problemas que le quitaban tiempo se verán automáticamente solucionados.

1.8 Principales características de una Intranet

La principal diferencia entre una Intranet e Internet es su rango de operación. Mientras la primera es una red limitada al dominio de la organización, Internet es una red de ancho mundial.

Además, una Intranet puede tener acceso a Internet (aunque no es requerido). Sin embargo, esta última no puede entrar a la Intranet (pero generalmente existe un camino de acceso controlado).

La Intranet ahorra dinero, tiempo y papel al reducir o eliminar la impresión y reimpresión de información. Al poder ser fácilmente producida, distribuida y accesible electrónicamente.

En una Intranet, la totalidad de la información puede ser actualizada y distribuida inmediatamente, ganando en productividad y competitividad. Y, lo más importante, convierte a la institución en una comunidad, salvando tiempo, zonas y lugares.

La Intranet es una nueva alternativa para las empresas que necesiten compartir información que se genera al interior de la organización. En otras palabras, es hacer uso y distribuir la información dentro de la organización pero a la manera de Internet.

1.9 Ventajas de una Intranet

Los beneficios de la implementación de una Intranet son:

- Intranet es una manera rápida y eficaz para realizar transacciones internas.
- Es una herramienta muy útil en la comunicación de sus miembros.
- Puede ser un auxiliar muy eficiente en la planeación de citas y reuniones.
- Intranet representa una nueva forma de relación, ya que promueve el desarrollo del personal y su capacitación, así como también impulsa el trabajo en grupo.
- Es ideal para difundir información tal como lo son las políticas y procedimientos internos, etc.
- Capacidad a acceder a bases de datos sin importar el lugar en donde se encuentre la computadora, ni su arquitectura, ni su sistema operativo.
- Disponibilidad de la información a cualquier hora y desde cualquier lugar.
- Aprovechamiento de recursos tales como:

  Multimedia, el hipertexto y otras facilidades de la red corporativa como Browser, herramientas de Java, etc., para desarrollar aplicaciones en Intranet.

- Mayor eficacia organizacional y productividad.

Un beneficio clave de la tecnología Intranet es la habilidad de entregar información actualizada de manera rápida y costo eficiente a toda la base de usuarios. Una Intranet pone información vital al alcance de todos los empleados con acceso a ella. Otra característica que vale la pena mencionar, es la consistencia, porque la información es la misma a lo largo y ancho de la empresa.

Al darles a las personas la posibilidad de acceder a tiempo a información crítica, esta tecnología mejora el proceso de toma de decisiones. Es posible organizar y mantener información centralizada o distribuida según se requiera o se facilite para la obtención y actualización.

Al proveer información instantánea y segura en formato electrónico, se elimina el tiempo y costo asociado a la publicación, duplicación y distribución asociados a la documentación en papel.

Las tecnología Intranet, también permiten compartir información y conocimientos independientemente de la ubicación.

Los grupos multidisciplinarios y Multi-departamentales, pueden aprovechar grandemente los grupos de discusión virtuales y boletines informativos para preparar reuniones o mejorar la toma de decisiones.

Con anchos de banda suficientes, es posible realizar video-conferencias con audio y video en tiempo real.

Con el apoderamiento que da la Intranet, viene la capacidad (muy deseable por cierto) que los usuarios mismos publiquen por su cuenta información de interés de su grupo de trabajo o de la empresa entera. Esto incrementa la complejidad de la Intranet y sus requerimientos. Capacidad a acceder a bases de datos sin importar el lugar en donde se encuentre la computadora, ni su arquitectura, ni su sistema operativo.

1.10 Cómo trabaja una Intranet

Un computador central típicamente el servidor de red de su compañía, maneja todo el tráfico de datos asociado con el envío y recibo de archivos. Estos archivos pueden ser códigos HTML para ser mostrado por un programa Browser, archivos de datos usados por servidor Web le dice al computador central cómo tratar con los requerimientos y transmisiones tal que cualquier computador se pueda comunicar en una Intranet sin importar de que clase es, o qué sistema operativo utiliza.

Cuando usted inicia su programa Browser, envía un requerimiento al servidor Web. Este le pide al servidor enviar un archivo al Browser, el cual muestra el archivo a usted. Típicamente la primera página mostrada es un departamento o el Home principal que contiene información básica y enlaces a otros archivos y páginas en la Intranet.

Haciendo clic a, por ejemplo, el departamento de recursos humanos, envía un requerimiento al servidor el cual entonces trasmite el home page de dicho Departamento a su Browser. Los archivos HTML y otros que el servidor envía a su Browser, se tienen que originar en el disco duro de su servidor. Hay ventajas y desventajas al tener los archivos centralmente localizados.

Si usted pudiera escribir una página y mantenerla en su computador, sería mucho más fácil para usted hacerle cambios, pero incrementaría el tráfico de la red a su máquina. Ya que los archivos están todos en su computador (o más si su compañía tiene más de un servidor) hay siempre un lugar específico para que los Browser busquen la información, haciendo mucho más fáciles enlazar páginas unas a otras. Una vez que su Intranet está arriba y corriendo, es completamente transparente. Usted ya no tiene que preocuparse de lo que la red está haciendo, sólo apunte y haga clic.

1.11 Importancia de usar una Intranet

Para casi cualquier empresa de hoy en día, y muy especialmente en un futuro muy cercano, la intranet va ha ser un recurso indispensable. Dada la gran cantidad de datos que genera cualquier empresa, se están quedando obsoletos los actuales métodos de inserción y consulta de datos, Una intranet puede resolver estos y otros problemas.

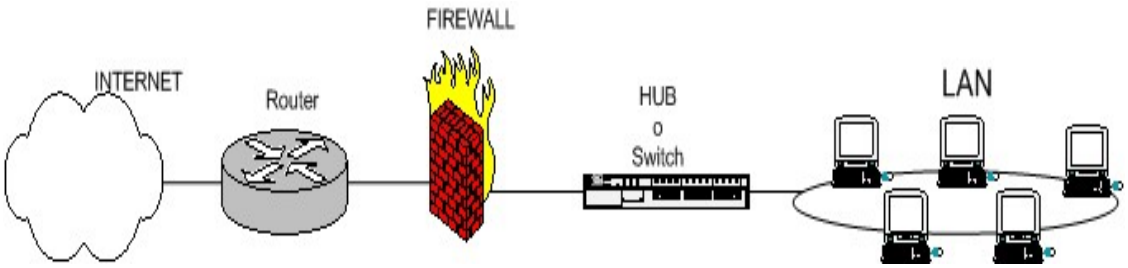
Una Intranet puede resolver, por ejemplo, el problema de la distribución de información para todos los empleados , así pues se pueden publicar manuales, planes de acción, procedimientos, material de formación, listas de precios, información comercial, anuncios, promociones etc. Y son accesibles para el empleado o cliente de forma
Inmediata, y con un ahorro considerable respecto a los métodos clásicos, panfletos, circulares, notas informativas, etc.

Además cualquier actualización de datos es inmediata y no supone ninguna carga para la empresa como los métodos tradicionales.

Una intranet organiza, además, la distribución de una empresa, ya que cada división puede tener su apartado en la intranet. Se puede organizar también una lista de encuentros y reuniones a la que cada empleado podrá acceder rápidamente, planificando así las reuniones de la organización de una forma más eficaz. Se mejora de esta forma la comunicación entre todos los trabajadores, y las sugerencias, peticiones o cualquier comunicación en general, se realiza de una forma más rápida y eficiente.

Se aprovechará también la potencia de una intranet para tener acceso rápido a cualquier documento de la empresa, siempre que se tenga el nivel de privilegios adecuado. Esta es otra de las ventajas de una intranet, su seguridad. Solo tendrán acceso a los recursos aquellos empleados que lo necesiten realmente. Siguiendo con la potencia y velocidad de acceso a datos de una intranet, el tiempo empleado en realizar cualquier búsqueda de datos de cualquier departamento de la empresa se reduce considerablemente, por lo que la productividad de la institución mejora.

1.12 Seguridad de las Intranet



Esquema Básico de Un Firewall en una Red

La seguridad informática es uno de los aspectos más importantes de la instrumentación de una red Intranet en las organizaciones. Su objetivo es asegurar la confidencialidad de los datos y de las transacciones, de forma que un usuario sólo tenga acceso a los datos que está autorizado a visualizar (y no a otros) y que la organización pueda confiar que las transacciones que realice un usuario son las autorizadas y realmente fueron realizadas por él (y no por otro).

La seguridad informática de Intranet es responsabilidad tanto de la institución como de los usuarios. La institución instrumenta encripción de datos para el ingreso de la contraseña, maximizando la seguridad. Los usuarios deben mantener reserva de su contraseña y verificar su último acceso.

Cualquier Intranet es vulnerable a los ataques de personas que tengan el propósito de destruir o robar datos empresariales. La naturaleza sin límites de Internet y los protocolos TCP/IP exponen a una empresa a este tipo de ataques.

Las intranet requieren varias medidas de seguridad, incluyendo las combinaciones de hardware y software que proporcionan el control del tráfico; la encriptación y las contraseñas para convalidar usuarios; y las herramientas del software para evitar y curar de virus, bloquear sitios indeseables, y controlar el tráfico.

El término genérico usado para denominar a una línea de defensa contra intrusos es firewall. Un firewall es una combinación de hardware / software que controla el tipo de servicios permitidos hacia o desde la intranet.

Los servidores sustitutos son otra herramienta común utilizada para construir un firewall. Un servidor sustituto permite a los administradores de sistemas seguir la pista de todo el tráfico que entra y sale de una intranet.

Los Firewall protegen a las Intranet de los ataques iniciados contra ellas desde Internet. Están diseñados para proteger a una Intranet del acceso no autorizado a la información de la empresa, y del daño o rechazo de los recursos y servicios informáticos. También están diseñados para impedir que los usuarios internos accedan a los servicios de Internet que puedan ser peligrosos, como FTP. Las computadoras de las Intranets sólo tienen permiso para acceder a Internet después de atravesar un firewall.

Un firewall de un servidor bastión se configura para oponerse y evitar el acceso a los servicios no autorizados. Normalmente está aislado del resto de la Intranet en su propia subred de perímetro. De este modo si el servidor es "allanado", el resto de la Intranet no estará en peligro. Los sistemas de autenticación son una parte importante en el diseño de la seguridad de cualquier Intranet. Los sistemas de autenticación se emplean para asegurar que cualquiera de sus recursos, es la persona que dice ser. Los sistemas de autenticación normalmente utilizan nombres de usuario, contraseñas y sistemas de encriptación.

El software para el bloqueo de sitios basado en el servidor de sitios basado en el servidor puede prohibir a los usuarios de una Intranet la obtención de material indeseable. EL software de control rastrea dónde ha ido la gente y qué servicios han usado, como HTTP para el acceso a la Web.

El software para detectar virus basado en el servidor puede comprobar cualquier archivo que entra en la Intranet para asegurarse que está libre de virus. Una manera de asegurarse de que las personas impropias o los datos erróneos no pueden acceder a la Intranet es usar un enrutador para filtrar.

Este es un tipo especial de enrutador que examina la dirección IP y la información de cabecera de cada paquete que entra en la Intranet, y sólo permite el acceso a aquellos paquetes que tengan direcciones u otros datos, como e-mail, que el administrador del sistema ha decidido previamente que pueden acceder a la Intranet.

¿Cómo funciona la encriptación?
Un medio de asegurar una Intranet es usar la encriptación: alterar datos para que sólo alguien con acceso a códigos específicos para descifrar pueda comprender la información.

La encriptación se utiliza para almacenar y enviar contraseña para asegurarse de que ningún fisgón pueda entenderla. La encriptación se emplea también cuando se envían datos entre Intranets en Redes Privadas Muy Seguras (VSPN). Además la encriptación se usa para dirigir el comercio en Internet y proteger la información de la tarjeta de crédito durante la transmisión.

Las claves son el centro de la encriptación. Las claves son formulas matemáticas complejas (algoritmos), que se utilizan para cifrar y descifrar mensajes. Si alguien cifra un mensaje sólo otra persona con la clave exacta será capaz de descifrarlo.

1.13 Aplicaciones para una Intranets

Básicamente, intranet, se enfoca en el uso de aplicaciones concretas para la organización y el intercambio de información de un modo estático, dinámico o interactivo.

Estático: Organizar y compartir la información vital de la empresa, mediante la presentación de documentos publicados en la Intranet.

Dinámico: Aplicaciones presentando información dinámica en la Web a través de bases de datos.

Interactivo: Aplicaciones que hacen posible el intercambio de información desde consultas complejas y actualizaciones automatizadas a bases de datos, hasta programas en lenguaje universal Java.

Para saber qué aplicaciones deba implementar el cliente en su Intranet La clave está en qué información tiene que compartir, y qué uso quiere hacer de esa información**.**

La utilización de la tecnología de Internet, y en especial la tecnología World-Wide Web, para crear una Intranet dentro de una organización, está provocando profundos cambios en la cultura corporativa de las instituciones, que se plasman en la significativa evolución de los modelos actuales de flujo de la información interna y de trabajo en grupo, en los que están comprometidas todas las áreas funcionales de la institución.

Una gran variedad de aplicaciones se ejecutan en el entorno de la intranets, algunas se derivan directamente de los servicios que prestan, otras son desarrollos personalizados de cada empresa y el resto las suministran vendedores de software comercial.
Estas aplicaciones resuelven necesidades y como ejemplos podemos citar las siguientes:

Información actualizada para los miembros de la institución así como un sistema que permita llevar un seguimiento de esta.

Comunicación y compartición de información por los miembros de un equipo de proyecto que pueden estar distribuidos en lugares físicos distintos.
Seguimiento de los problemas de los miembros por el área de Asistencia Técnica con elaboración de un “help" para los usuarios.

Un solo sistema de correo electrónico que aglutine a los varios existentes y que incluya todos los directorios y todas las personas.

Una aplicación para que los nuevos empleados puedan encontrar la información relativa a los procedimientos, la organización y las ventajas de la institución tan pronto como empiecen a trabajar.

Un método de acceso, para el personal, a través de una interfaz uniforme en cualquier escritorio.

La información de Recursos Humanos, debido a la gran cantidad de papeles y gráficas, se puede usar en una Intranet. La Intranet podría también administrar el reclutamiento, promoción, salarios y asistencias de los

empleados, ahorrando gran tiempo y dinero de Recursos Humanos. Además da a los empleados rápido acceso a información de su interés.

Una Intranet puede ayudar a simplificar una variedad de operaciones y funciones administrativas. Una forma de utilizarla es crear una página central dónde publicar gráficas, listas de contactos, boletines, preguntas frecuentes, procedimientos, formas, calendarios, proyectos, aprobaciones en líneas, etc.
Las organizaciones que usan intranets se encuentran con que una combinación de aplicaciones nativas, personalizadas y comerciales, resuelve fácilmente estas necesidades
Las aplicaciones se dividir en las siguientes:

Aplicaciones Nativas

Los servicios de usuario y red que ofrece la Intranet, descritos anteriormente, se convierten directamente en aplicaciones nativas que se proporcionan en el entorno de la Intranet.

Entre dichas aplicaciones se incluyen las siguientes:

- Correo electrónico.
- Colaboración entre equipos y groupware.
- Comunicación con sonido y vídeo en tiempo real.
- Compartición y publicación de la información.
- Navegación, indexación y búsqueda full-text.
- Directorios de personas y objetos.

Aplicaciones Personalizadas

Una ventaja fundamental de la Intranet es que ahora las instituciones pueden construir con total facilidad aplicaciones personalizadas a las que tienen un acceso inmediato los usuarios de cualquier parte de la Intranet, en cualquier plataforma.

Puesto que el desarrollo y el despliegue son mucho más rápidos, el ahorro de costes con respecto a los antiguos modelos centrados en el escritorio es considerable. Más aún, los usuarios no necesitan una extensa formación.

Como ejemplos que se encuentran funcionando en grandes empresas tenemos:

- Acceso a bases de datos en toda la organización.
- Acceso directo a aplicaciones.
- Investigación y desarrollo.
- Aplicaciones en recursos humanos.
- Aplicaciones financieras.

Aplicaciones Comerciales

Prácticamente todos los programadores de software comercial están creando nuevas aplicaciones o adaptando las ya existentes, para que se ejecuten de manera infalible en el entorno de la Intranet.
Son ejemplos:

- Sistemas financieros.
- Aplicaciones de productividad personal.
- Sistemas para lugares de operaciones financieras.
- Aplicaciones de gestión comercial.
- Sistemas de administración de documentos.
- Aplicaciones de Procesamiento analítico on-line.
- Aplicaciones de asistencia y soporte al cliente.
- Puntos de información.

1.14 Intranet y las redes de área local

Los servicios que ofrece la intranet conducen la red hacia el punto focal de la informática en los negocios. El antiguo modelo centrado en el escritorio, dominado por aplicaciones propietarias estáticas, está perdiendo terreno a medida que las empresas descubren que basar el entorno informático de sus negocios en la intranet, y construir aplicaciones sobre ella, son proposiciones mucho más fáciles y avanzadas para los usuarios, administradores y programadores de aplicaciones.

En resumen el entorno de la intranet centrada en red presenta las siguientes ventajas importantes:

Es muy fácil de implantar, no hay que reemplazar todos los sistemas, bases de datos y aplicaciones ya existentes.

Aprovecha las inversiones en infraestructura ya existentes, incluidas las inversiones en ordenadores de sobremesa, servidores, ordenadores centrales, bases de datos, aplicaciones y redes.

Permite a los programadores instalar una vez y ejecutar en cualquier lugar, incluso a través de plataformas cliente y servidor, en lugar de transportar y

personalizar reiteradamente aplicaciones para diferentes plataformas propietarias.

Puede desplegarse y administrarse de forma centralizada, desde el servidor, en lugar de exigir costosas actualizaciones en ordenadores de sobremesa o portátiles estáticos individuales.

Tiene un bajo coste total de implantación y propiedad, donde se incluye software, aplicaciones personalizadas, hardware, formación y asistencia.
Está basada en normas abiertas, lo que ofrece flexibilidad, por lo que las empresas pueden elegir componentes individuales de varios vendedores, actuales y futuros.

1.15 E-mail dentro de una Intranet

Probablemente la parte más usada de una Intranet que no tiene nada que ver con bases de datos de la empresa, páginas Web ostentosas, o contenido multimedia es el uso del correo electrónico. Las Intranets empresariales pueden emplear diferentes programas e-mail, como: Mail Microsoft Mail o Lotus Notes, entre otros.

Pero la arquitectura más común que sirve de base al uso del e-mail de las redes internas es el protocolo llamado Protocolo simple de Transferencia de Correo, o SMTP.

Como se utiliza SMTP para repartir correo dentro de una Intranet:

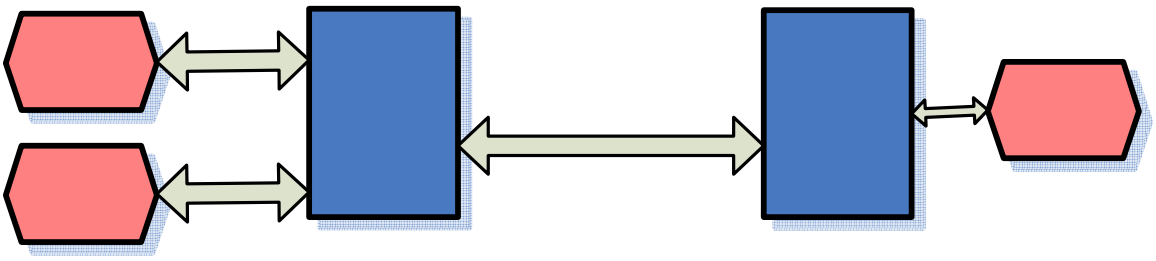
- Como sucede con muchas aplicaciones de Intranets y de Internet, SMTP usa una arquitectura cliente / servidor. Cuando alguien quiere crear un mensaje, usa un agente usuario de correo o agente usuario (MUA o UA), software cliente que se ejecuta en un computador, para crear un fragmento de correo electrónico. Este MUA puede ser cualquiera de los programas e-mail, y puede ejecutarse en varias computadoras diferentes, incluyendo PC, Macintosh, y estaciones de trabajo UNÍX; Pegasus, Eudora. CC: Mail y Microsoft Mail para PC; y Eudora para Macintosh.

- Después de finalizar el mensaje, el MUA lo manda a un programa que se esta ejecutando en un servidor llamado agente de transferencia de correo (MTA) examina la dirección del receptor de mensaje. Si el receptor del mensaje está en la Intranet, el MTA envía el mensaje a otro programa servidor en la red interna denominado agente de entrega de correo (MDA). Si el receptor está ubicado en Internet o en otra red interna, el archivo llegará al receptor a través de Internet. El MDA examina la dirección del receptor, y envía el correo a la bandeja de entrada de la persona adecuada.

- Algunos sistemas de correo emplean otro protocolo e-mail llamado el Protocolo de Oficina de Correos (POP) conjuntamente con SMTP. Con POP, el e-mail no se entrega directamente en tu computadora. En lugar de eso, el correo se echa a un buzón en el servidor. Para conseguir el correo, alguien accede al servidor usando una contraseña y un nombre de usuario, y recupera el mensaje con un agente de correo.

- El receptor del correo puede utilizar ahora un agente usuario de correo para leer el mensaje, archivarlo y responderlo.

- SMTP sólo puede manejar la transferencia de e-mail de archivos de textos ASCII sencillos. Para enviar archivos binarios como hojas de cálculos, dibujos y documentos de procesador de texto, primero deben convertirlos en un formato ASCII codificándolos. Los archivos se pueden codificar usando varios métodos que incluyen codificación y Base.



Muchos software e-mail codificarán automáticamente archivos binarios. Cuando alguien recibe un archivo codificado, lo descodifica y después puede usar o examinar el archivo binario. Además muchos paquetes e-mail descodifican automáticamente archivos codificados.

1.16 Como se reparte E-MAIL entre Intranet

A menudo el e-mail creado en una Intranet no se entregará a una computadora de la Intranet, sino a alguien en Internet, en otra Intranet, o un servidor en línea como América Online, Microsoft Netword, o CompuServe. Aquí están los pasos que un mensaje típico tiene que seguir cuando se envía de una Intranet a otra red o Intranet.

Un mensaje e-mail se crea usando SMTP. Como ocurre con toda la información enviada a través de Internet, el mensaje es dividido por el Protocolo TCP de Internet en paquetes IP. La dirección la examina el agente de

USER

transferencia de correo de la Intranet. Si la dirección se encuentra en otra red, el agente de transferencia de correo enviará el correo a través de la Intranet mediante enrutadores al agente de transferencia de correo en la red receptora.

Antes de que se pueda enviar el correo a través de Internet, puede que primero tenga que atravesar un firewall, una computadora que protege a la Intranet para que los intrusos no puedan acceder a ella. El firewall sigue la pista de los mensajes y los datos que entran y salen de la Intranet.

El mensaje deja la Intranet y se envía a un enrutador Internet. El enrutador examina la dirección, determina dónde debería mandarse el mensaje, y después lo pone en camino.
La red receptora obtiene el mensaje e-mail. Aquí utiliza una pasarela para convertir los paquetes IP en un mensaje completo.

Después la pasarela traduce el mensaje al protocolo particular que emplea la red (como el formato de correo de Compu-Serve), y lo pone en camino. Puede que el mensaje también tenga que atravesar un firewall en la red receptora.

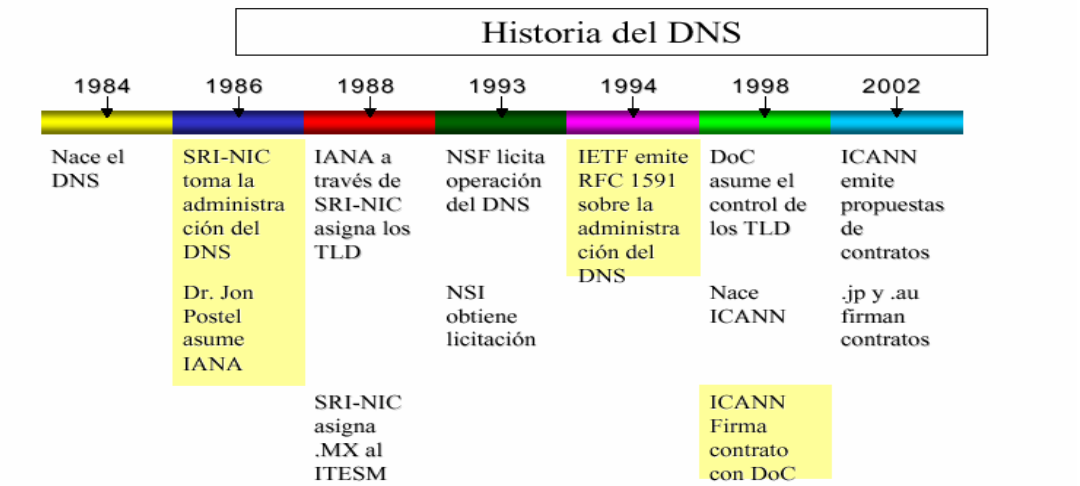
La red receptora examina la dirección e-mail y envía el mensaje al buzón específico donde el mensaje está destinado a ir, o emplea el Protocolo de Oficina de Correo (POP) para entregarlo a un servidor de correo.

Las pasarelas realmente pueden modificar los datos (si se necesita) para la conectividad. Para el e-mail, puede convertir el protocolo Compu-Serve en SMTP. Las pasarelas también se utilizan para conectar PC con sistemas centrales IBM, por ejemplo, ASCII con EBCDIC.

2 DNS (Servidor de nombres de Dominio)

Inicialmente, el DNS nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a Internet. En un inicio, SRI (ahora SRI Internacional) alojaba un archivo llamado HOSTS.TXT que contenía todos los nombres de dominio conocidos. (Técnicamente, este archivo aun existe - la mayoría de los sistemas operativos actuales todavía pueden ser configurados para chequear su archivo hosts.

El crecimiento explosivo de la red causó que el sistema de nombres centralizado en el archivo HOSTS.TXT resultara impráctico y en 1983, Paúl Mockapetris publicó los RFCs 882 y 883 definiendo lo que hoy en día ha



evolucionado al DNS moderno. (Estos RFCs han quedado obsoletos por la publicación en 1987 de los RFCs 1034 y 1035).

DNS es una abreviatura para Sistema de nombres de dominio (Domain Name System), un sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios.

La asignación de nombres DNS se utiliza en las redes TCP/IP, como Internet, para localizar equipos y servicios con nombres descriptivos.

Cuando un usuario escriba un nombre DNS en una aplicación, los servicios DNS podrán traducir el nombre a otra información asociada con el mismo, como una dirección IP.

Un nombre descriptivo resulta más fácil de aprender y recordar. Sin embargo, los equipos se comunican a través de una red mediante direcciones numéricas. Para facilitar el uso de los recursos de red, los sistemas de nombres como DNS proporcionan una forma de asignar estos nombres descriptivos de los equipos o servicios a sus direcciones numéricas.

El DNS consiste en un conjunto jerárquico de servidores DNS. Cada dominio o subdominio tiene una o más zonas de autoridad que publican la información acerca del dominio y los nombres de servicios de cualquier dominio incluido. La jerarquía de las zonas de autoridad coincide con la jerarquía de los dominios. Al inicio de esa jerarquía se encuentra los servidores raíz: los servidores que responden cuando se busca resolver un dominio de primer nivel.

El Sistema de Dominio de Nombres (DNS) es básicamente una base de datos distribuida de computadoras que forman parte de una red. Esto facilita el control local de la totalidad de segmentos de la base de datos, lo que permite, que cada segmento esté disponible a través de la red por un esquema de cliente-servidor (Client/Server).

El servidor de nombres (Name Server) es un programa que forma la parte servidor del mecanismo cliente-servidor del DNS.
Los Servidores de Nombres contienen información sobre un determinado segmento de la base de datos y la hace disponible para clientes (Client), denominados Resolver. Los Resolver muchas veces consisten sólo en rutinas de librerías, que crean interrogaciones y las mandan a través de la red a un Servidor de Nombre.

La totalidad de la base de datos se muestra como un árbol (tree) invertido con la raíz (root) en la punta. El nombre de la raíz es la etiqueta NULL, pero se escribe con un solo punto ("."). Cada nudo del árbol representa tanto una partición de la totalidad de la base de datos, como un Dominio (domain) del Sistema de Dominio de Nombre. En adelante cada dominio puede ser dividido

en particiones que se llaman Subdominios (subdomains), que son derivados como niños de sus nudos paternales.

Cada dominio es marcado de modo que tiene una etiqueta que le identifica relativamente con su dominio paternal. El dominio posee también un nombre de dominio (domain name), que identifica su posición en la base de datos, tal como una ruta absoluta de un directorio especifica su lugar en el sistema de archivos de su computadora.

En el DNS, el nombre de dominio completo es una secuencia de etiquetas, empezando por el dominio hasta la raíz (root), separando las etiquetas por puntos "." (p. Ej.: ipsalle.edu.ni). Permitiendo que cada dominio pueda ser administrado por una organización diferente. Cada organización puede dividir su dominio en varios subdominios, cuya administración puede ser realizada por otras organizaciones.

Las computadoras trabajan perfectamente con cifras como la dirección IP. Cuando entramos a la Internet colocamos una dirección como por ejemplo http: //ipsalle.edu.ni, el navegador dirige una petición (Request) al Servidor de Dominio de su proveedor y este intenta resolver el nombre de dominio con la IP correspondiente. En el caso que su proveedor no está autorizado.

Para esta zona, transmite la petición (Request, Query) al servidor de dominio autorizado hasta llegar al dominio que se indicó. Esto significa que cada servidor de dominio tiene la información completa de la zona para la que esta autorizado y aparte tiene informaciones básicas sobre otras zonas. Cuando una petición (Request) se dirige a una zona que esta fuera de la zona autorizada, el servidor por lo menos sabe por donde buscar. Esto puede significar que la petición (Request) de una dirección tiene que pasar por varios servidores hasta que se haga contacto con el destino solicitado.

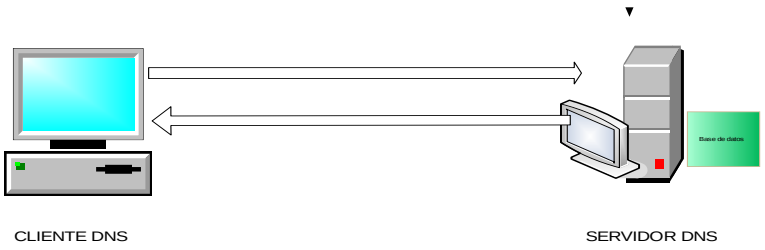
De este modo es fácil de imaginar porque el Sistema de Dominio de Nombre no puede consistir en una sola base de datos centralizada. Primero tardaría demasiado tiempo encontrar un servidor entre millones de otros y segundo habría una cola bastante larga en el caso de miles de peticiones simultáneas de todo el mundo. Adicionalmente no tendría sentido dirigirse a un servidor lejano para comunicar con un host de la misma zona.

Para la operación práctica del sistema DNS se utilizan tres componentes principales:

- Los Clientes DNS *(*resolvers*)*, un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS *(de* la forma: Qué dirección IP corresponde a nombre, dominio).

- Los Servidores DNS *(*name Server*)*, que contestan las peticiones de los clientes, los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada.

- las Zonas de autoridad' (authoritative DNS Server*)*, porciones del espacio de nombres de dominio que manejan las respuestas a las peticiones de los clientes. La zona de autoridad abarcan al menos un dominio e incluyen subdominios, pero estos generalmente se delegan a otros servidores.



Esquema DNS

2.1 El DNS define

1. Un espacio de nombres jerárquico para los hosts y las direcciones IP.
2. Una tabla de hosts implementada como una base de datos distribuida.
3. Un traductor (del inglés, **resolver**) o librería de rutinas que permite realizar consultas a esa base de datos.
4. Enrutamiento mejorado para el correo electrónico.
5. Un mecanismo para encontrar los servicios en una red.
6. Un protocolo para intercambiar información de nombres.

¿Cual es la direccion I

Intranet.lasalle.edu.r

Para ser auténticos ciudadanos de Internet, los sitios necesitan el DNS. Mantener un fichero local */etc/hosts* con un mapeado de todos los hosts que los usuarios puedan querer contactar no es factible.

Cada sitio mantiene una o varias piezas de la base de datos distribuida que posibilita el servicio global del sistema DNS. Su pieza de la base de datos consiste en dos o más ficheros de texto que contienen registros para cada uno de los hosts.

Cada registro es una sencilla línea consistente en un nombre (normalmente el nombre de un host), un tipo de registro y diversos valores o datos.

El DNS es un sistema cliente/servidor. Los servidores (de nombres) cargan los datos de sus ficheros de DNS en memoria y los usan para responder las consultas tanto de los clientes de la red interna como de los clientes y otros

servidores en la red Internet. Todos sus hosts deberían ser clientes del DNS, pero relativamente pocos necesitan ser servidores de DNS.

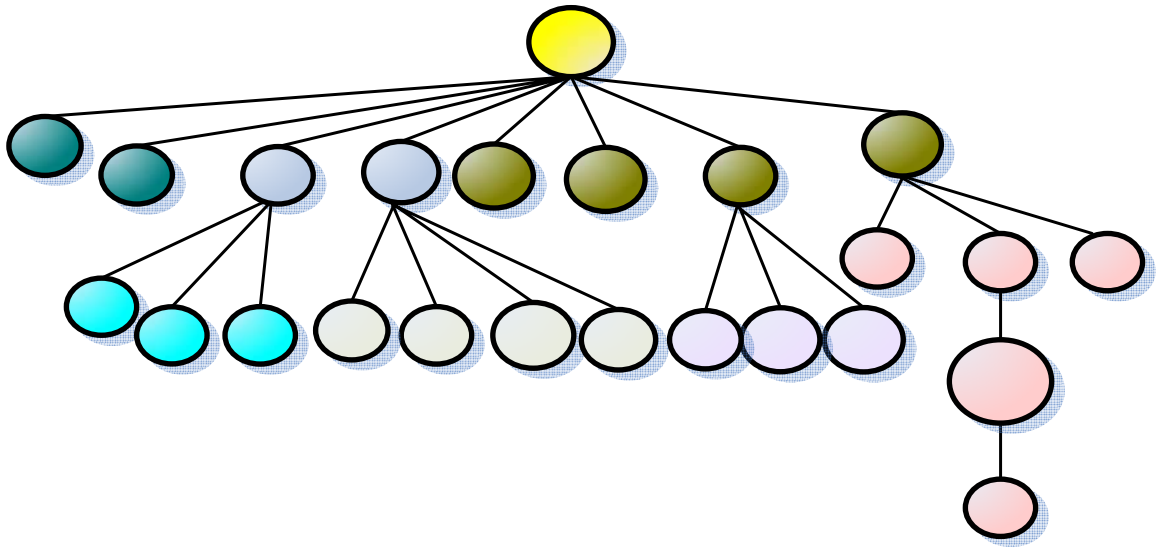
Si su organización es pequeña (unos pocos hosts en una única red), puede ejecutar un servidor en uno de sus equipos o pedirle a su ISP (del inglés, **Internet Services Provider**) que le proporcione ese servicio en su nombre.

Un sitio de tamaño medio con diversas subredes debería tener múltiples servidores de DNS para reducir la latencia de las consultas y mejorar la productividad. Un sistema muy grande puede dividir sus dominios de DNS en subdominios y usar algunos servidores para cada subdominio.

2.2 Jerarquía del DNS

De forma similar a los sistemas de archivos, donde un directorio puede contener subdirectorios, cada dominio tiene un nombre y puede contener subdominios. Igualmente, la raíz de árbol DNS se encuentra en la parte superior y se representa por un punto (·)

Cada subdominio debe tener un nombre único dentro de su dominio padre, lo cual asegura su unicidad dentro del espacio de nombres DNS.



El dominio raíz (root): Este dominio era manejado inicialmente por el gobierno de U.S., específicamente, por un consorcio llamado InterNIC, Actualmente, es administrado por un grupo sin ánimo de lucro llamado ICANN (Internet Corporation for Asigned Names and Numbers).
Es el nodo origen de toda la jerarquía DNS.

2.3 Estándares utilizados en los FQDN

Los nombres de los dominios DNS están formados por su ruta de ubicación en el árbol DNS, empezando desde el nombre del nodo, hasta la raíz.

Los nombres de los nodos se concatenan en secuencia, formando segmentos, y se separan utilizando un punto (·). Al final del nombre puede aparecer un punto que representa a la raíz. Este punto final puede o no especificarse, pero siempre hace parte del nombre del dominio. Estos nombres se conocen como **FQDN** (Fully Qualified Domain Names).

Ej.:net.ipsalle.edu.ni

Los nombres DNS se leen de izquierda a derecha, empezando por el nombre del equipo, hasta llegar al dominio root. Cada segmento de un nombre de dominio puede tener máximo 63 caracteres y todo el nombre puede tener máximo 255 caracteres.

Sólo se pueden usar los siguientes caracteres (RFC 1123): A-Z 0-9 a-z "-" (guión), La estructura básica de un nombre DNS es: Nombre computador. DominioDNS también llamado Sufijo DNS.

Debe tenerse en cuenta que aunque el nombre DNS puede tener un máximo de 255 caracteres, cuando los nombres de los PC's se manejan con NetBIOS, como en Windows 2000, éste sólo toma el primer segmento del nombre DNS y sólo hasta 15 caracteres, Esto podría causar conflictos si al asignar los nombres a los equipos se utilizan identificadores muy extensos.

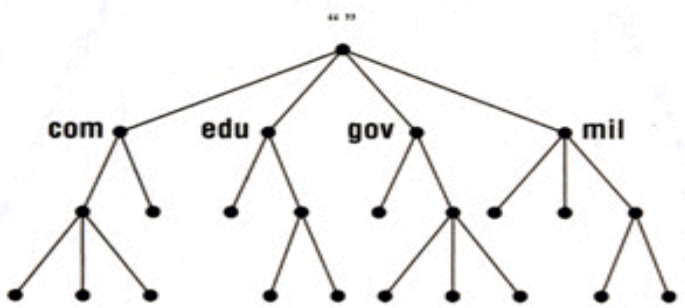
2.4 Bases de datos del DNS

DNS utiliza una gran base de datos distribuida, que cambia todo el tiempo. Desde cualquier computador en Internet es posible encontrar la dirección de otro computador en Internet, utilizando la jerarquía global de nombres DNS o "namespace".

La base de datos del DNS se mantiene de forma que No existe una persona u organización que haga un seguimiento de estos nombres. La responsabilidad de la relación nombre/dirección_IP es local.

2.5 Dominios de alto nivel

Estos dominios, agrupan a las organizaciones, teniendo en cuenta el tipo de servicios que ofrecen. Existen una gran cantidad de dominios de este tipo, entre los cuales, los más utilizados son: Punto com, net, org, gov, edu, mil.



De estos dominios, .com., net y org son administrados por la compañía "Network Solution" (propiedad de Verisign desde 1999).
Igualmente, en este nivel se encuentran los dominios asignados a los países. Por ejemplo:

- ni (Nicaragua)
- u.s (Estados Unidos)
- ca (Canadá)
- es (España)

2.6 Dominios de segundo nivel

Estos son subdominios que pueden crearse dentro de los dominios de alto nivel, y para crearlos no es necesario autorización de los dueños del dominio "padre".
Lo que hay que hacer es "delegar" la responsabilidad de los nombres de este segundo nivel a algún equipo de su red.

2.7 Proceso de resolución de nombres

Cuando una aplicación (cliente) necesita resolver un FQHN envía un requerimiento al *servidor de nombres* configurado en el sistema (normalmente, el provisto por el ISP).

A partir de entonces se desencadena el proceso de resolución del nombre:

1. El servidor de nombres inicial consulta a uno de los *servidores raíz* (cuya dirección IP debe conocer previamente).
2. Este devuelve el nombre del servidor a quien se le ha delegado la sub-zona.
3. El servidor inicial interroga al nuevo servidor.
4. El proceso se repite nuevamente a partir del punto 2 si es que se trata de una sub-zona delegada.
5. Al obtener el nombre del servidor con autoridad sobre la zona en cuestión, el servidor inicial lo interroga.
6. El servidor resuelve el nombre correspondiente, si este existe.
7. El servidor inicial informa al cliente el nombre resuelto.

Para el proceso de resolución, el dominio root debe contener registros llamados NS (Name Server) que delegan la responsabilidad del dominio solicitado a otros servidores (los servidores del dominio que se busca).

Los servidores DNS del dominio solicitado contienen registros NS que delegan la responsabilidad de los servidores del dominio que se busca.

Pero dentro del dominio de segundo nivel, es posible que se deseen crear subdominios, para habilitar a diferentes grupos para usar nombres DNS dentro de su dominio, pero sin tener que hacer el mantenimiento de los registros DNS.

Para crear un subdominio se debe hacer lo siguiente:

El grupo debe habilitar a uno de sus computadores como servidor DNS para el subdominio. Este computador debe estar conectado permanentemente a Internet. El administrador del servidor DNS debe crear un registro NS en su base de datos DNS, que indica “hay un subdominio en el dominio cisco.com, y si usted quiere buscar nombres en ese dominio, no me lo pregunte a mí, pregúntele a este otro servidor DNS (el del grupo)".

2.8 Dominios y Zonas

Dominios

Cada nodo en el árbol de la base de datos de DNS junto con todos sus nodos hijos, es llamado un dominio. Es posible crear subdominios o dominios hijos ("child domain").

Para crear un dominio específico, es necesario registrarlo en un dominio de "alto nivel" (top level). Todos los dominios son hijos de un "dominio raíz" llamado "." (dot).

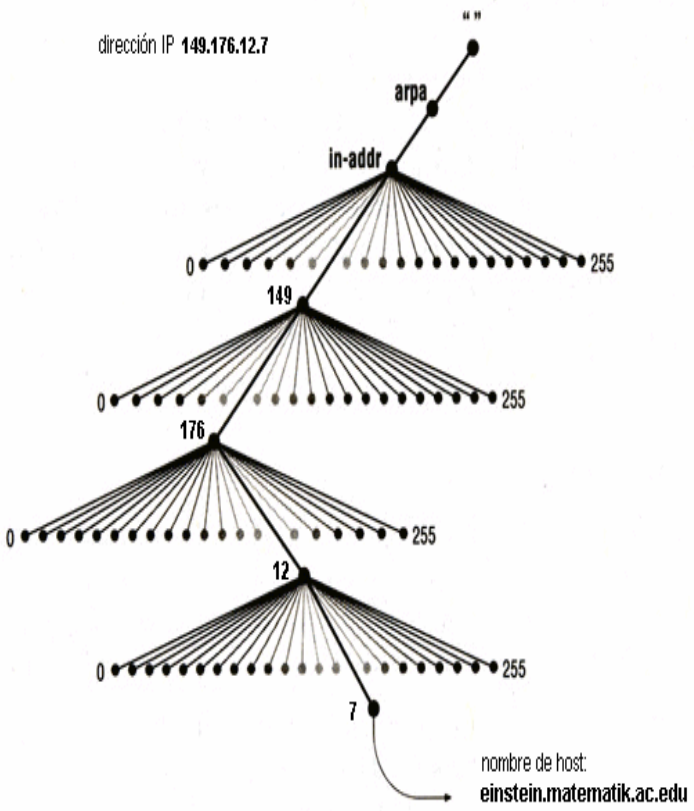
Zonas
Una zona es un archivo físico para almacenar y administrar un conjunto de registros del namespace de DNS. Un solo servidor DNS puede ser configurado para administrar uno o varios archivos de zona, cada zona esta ligada a un nodo de dominio específico conocido como: dominio raíz de la zona.
La zona es el rango de direcciones Internet de las cuales se ocupa un servidor DNS.

2.9 Zonas de búsqueda: "Reverse" y “Forward”

El DNS también puede trabajar en sentido contrario es decir, convertir direcciones IP a nombres. El proceso de convertir un nombre de host a una dirección IP se denomina forward Name resolution (resolución de nombres hacia delante), mientras que el proceso de convertir una dirección IP a su nombre de host correspondiente se denomina reverse name resolution (resolución de nombres en reversa).

Para construir la zona de búsqueda reversa, deben tomarse los segmentos de la dirección IP que identifican a la red, invertirlos y adicionar ".in-addr.arpa" al final del nombre.

Zona Reversa



2.10 Forwarders y Esclavos

Cuando un NS DNS recibe una solicitud DNS, el intenta localizar la información dentro de sus propios archivos de zona. Si falla porque el servidor no tiene autoridad por el dominio solicitado, el se debe comunicar con otros NS para satisfacer la solicitud.

Para resolver este problema, DNS utiliza el concepto de forwarder. Ciertos NS son seleccionados como forwarder, y solamente ciertos forwarder determinados realizan comunicaciones en Internet. Esta configuración se hace por servidor, no por zonas.

Cuando un servidor configurado para usar forwarder recibe una solicitud DNS que es incapaz de resolver, el transfiere la solicitud a uno de sus forwarder determinados. El forwarder entonces lleva a cabo cualquier comunicación necesaria para satisfacer la solicitud y regresar el resultado.

Los esclavos son servidores configurados para utilizar forwarder y para regresar un mensaje de falla si el forwarder no puede satisfacer la solicitud. Los esclavos no intentan contactar a otros NS si el forwarder es incapaz de satisfacer la solicitud.

2.11 Caching-only Servers

Aunque todos los NS almacenan temporalmente (caché) las consultas contestadas, los servidores de Caching-only, son NS cuyo único trabajo es ejecutar consultas, almacenar las respuestas, y regresar resultados. En otras palabras, ellos no tienen autoridad sobre ningún dominio y solamente contienen información que han almacenado al satisfacer consultas.

Para determinar cuándo usar un servidor caching-only, se debe pensar que el servidor al inicializarse no tiene información de nombres y la irá adquiriendo. Sin embargo, para redes muy lentas, se genera menos tráfico que en una transferencia de zona.Algunos servidores de nombres son: Bind • PowerDNS • MaraDNS • djbdns • pdnsd • MyDns.

2.12 Resolución de Nombres

Hay tres tipos de consultas que un cliente puede hacer a un servidor DNS: recursiva, interactiva e inversa. Estas consultas no solo se realizan entre clientes DNS y servidores DNS sino también entre servidores.

- **Consultas Recursivas**

En una consulta recursiva, el NS responde con el dato solicitado o un estado de error. El NS no puede transferir la consulta a otro NS.

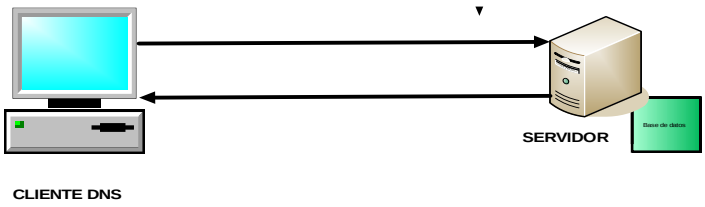
Este tipo de consulta es típicamente hecha por un cliente DNS (un resolver) a un servidor DNS. Y cuando un servidor DNS está configurado para usar un forwarder.

- **Consultas Interactivas**

En una consulta interactiva, el servidor consultado trata de dar la mejor respuesta. Este tipo de consulta es típicamente hecha por un servidor DNS a otro, después de recibir una consulta recursiva desde el resolver (cliente).

- **Consultas Inversa**

Cuando un resolver tiene una dirección IP y desea conocer el nombre del nodo, utiliza una consulta inversa. Debido a que no hay una relación directa entre el espacio de nombres DNS y sus direcciones IP asociadas, solamente una búsqueda en todos los dominios podría garantizar una respuesta correcta.



Para remediar este problema, un dominio especial "in-addr.arpa." en el espacio DNS fue creado. Los nodos en el dominio "in-addr.arpa" son nombrados después de sus números en la representación IP de octetos. Sin embargo, como las direcciones IP son más específicas de derecha a izquierda, y los dominios los son de izquierda a derecha, el orden de los octetos de las direcciones IP debe escribirse al revés. Así, la administración de las "ramas inferiores" del árbol DNS in-addr.arpa pueden otorgarse a las compañías en base a sus clases A, B, o C.

Cuando el árbol de dominios es construido en la base de datos DNS, un registro apuntador especial es añadido a la dirección IP asociada al nombre de

nodo correspondiente. En otras palabras, para encontrar un nombre de nodo en base a una dirección IP, el resolver preguntará por un registro apunto a una dirección IP. Si esta dirección IP esta fuera del dominio local, el servidor DNS comenzará a resolver a otros nodos del dominio.

2.13 Cache y Tiempo de Vida

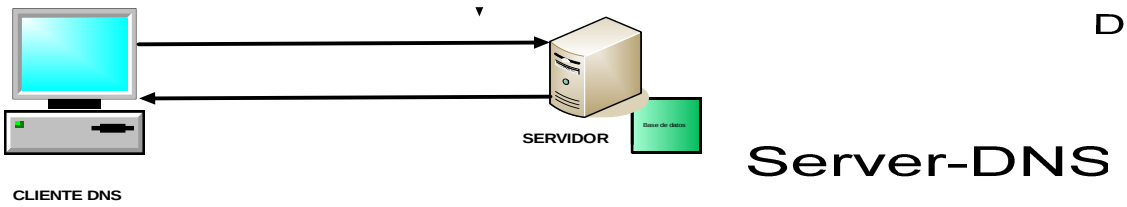
Cuando un servidor de nombres esta procesando una consulta recursiva, posiblemente envíe varias consultas para encontrar una respuesta. El NS almacena en cache toda la información que recibe durante el proceso por cierto tiempo especificado en los datos regresados. Esta cantidad de tiempo se conoce como el: Tiempo de Vida (Time To Live, TTL).

- **Consultas Interactivas**

En una consulta interactiva, el servidor consultado trata de dar la mejor respuesta. Este tipo de consulta es típicamente hecha por un servidor DNS a otro, después de recibir una consulta recursiva desde el resolver (cliente).

- **Consultas Inversa**

Cuando un resolver tiene una dirección IP y desea conocer el nombre del nodo, utiliza una consulta inversa. Debido a que no hay una relación directa entre el espacio de nombres DNS y sus direcciones IP asociadas, solamente una búsqueda en todos los dominios podría garantizar una respuesta correcta.



Para remediar este problema, un dominio especial "in-addr.arpa." en el espacio DNS fue creado. Los nodos en el dominio "in-addr.arpa" son nombrados después de sus números en la representación IP de octetos. Sin embargo, como las direcciones IP son más específicas de derecha a izquierda, y los dominios los son de izquierda a derecha, el orden de los octetos de las direcciones IP debe escribirse al revés. Así, la administración de las "ramas inferiores" del árbol DNS in-addr.arpa pueden otorgarse a las compañías en base a sus clases A, B, o C.

Cuando el árbol de dominios es construido en la base de datos DNS, un registro apuntador especial es añadido a la dirección IP asociada al nombre de nodo correspondiente. En otras palabras, para encontrar un nombre de nodo en base a una dirección IP, el resolver preguntará por un registro apunto a una dirección IP. Si esta dirección IP esta fuera del dominio local, el servidor DNS comenzará a resolver a otros nodos del dominio.

2.13 Cache y Tiempo de Vida

Cuando un servidor de nombres esta procesando una consulta recursiva, posiblemente envíe varias consultas para encontrar una respuesta. El NS almacena en cache toda la información que recibe durante el proceso por cierto tiempo especificado en los datos regresados. Esta cantidad de tiempo se conoce como el: Tiempo de Vida (Time To Live, TTL).

El administrador del NS de una zona decida el TTL para sus datos. Los TTL ayudarán a asegurar la consistencia de los datos, sin embargo, incrementa el trabajo para el NS.

Cuando los datos se almacenan en la cache del servidor DNS, él comienza a decrementar su TTL para saber cuando eliminarlo. Si una consulta se satisface en base a los datos en cache, el TTL devuelto será la cantidad de tiempo restante en la cache del servidor DNS. Así, los clientes también conocen cuando expira un dato.

2.14 Registros de recursos DNS

Cada base de datos DNS contiene registros de recursos. En general, los registros de recursos contienen información relacionada con un determinado equipo host, como su dirección IP, el propietario del host o el tipo de servicios que ofrece.

Tipos comunes de registros de recursos

Tipos de registros de recursos	Descripción	Explicación
SOA	Inicio de autoridad	Este registro designa el principio de una zona. Contiene información como el nombre de la zona, la dirección de correo electrónico del administrador de la zona y opciones para indicar cómo los servidores DNS secundarios deben actualizar los archivos de datos de la zona.
A	Dirección	Este registro enumera las direcciones IP de un nombre de host determinado. Es el registro principal para la resolución de nombres.
CNAME	Nombre canónico	Este registro especifica un alias o un sobrenombre para el nombre de host estándar (canónico).
MX	Intercambiador de correo	Este registro muestra el equipo host responsable de recibir el correo electrónico enviado a un dominio.
NS	Servidores de nombres	Este registro especifica el servidor de nombres responsable de una zona dada.

2.15 Beneficios del DNS

El uso de DNS sobre computadores permite:

- Acceso a diferentes tipos de sistemas (Unix, NT, etc.) UNIX, utilizando nombres "amigables".
- Conexión a Internet, utilizando convenciones de nombres.
- Mantener un esquema consistente de nombres jerárquicos dentro de la organización.

2.16 Servidores DNS primario, secundario y Maestro.

Para garantizar la alta disponibilidad del servicio, DNS requiere que más de un servidor de nombres admita de forma redundante cada zona.

Los registros de recursos de una zona concreta se actualizan manual o automáticamente en un único servidor de nombres maestro, denominado servidor DNS primario. Un servidor DNS primario puede tener autorización para una o varias zonas. Un nombre de servidores primario, obtiene los datos de sus zonas de sus archivos locales. Los cambios a la zona, como añadir otros dominios o nodos, se hacen en el NS Primario.

Otros servidores de nombres redundantes, denominados servidores DNS secundarios, actúan como servidores de reserva para el servidor principal de la misma zona, en caso de que no se pueda tener acceso al servidor principal o esté inactivo.

Los servidores DNS secundarios se comunican periódicamente con el servidor DNS principal para asegurarse de que su información de zona está actualizada. De lo contrario, los servidores DNS secundarios obtendrían una copia de los archivos de datos de zona más recientes existentes en el servidor principal.

Este proceso de replicación de archivos de zona en varios servidores de nombres se denomina transferencia de zona.
Hay tres razones para tener NS secundarios. Estas razones son:

- Redundancia. Se necesitan al menos dos NS en cada zona, un primario y al menos un secundario por redundancia. Como cualquier sistema de tolerancia a fallas, las máquinas deben ser independientes, por ejemplo, diferentes redes.
- Localidades Remotas. Para reducir la cantidad de trabajo en el servidor primario, Como la información de cada zona es almacenada en archivos independientes, la designación de primario o secundario, está definida a un nivel de zona.
- El uso de servidores secundarios como servidores maestros ayuda mucho, cuando el servidor primario esta muy ocupado, o cuando la forma de comunicación es mas eficiente.

2.17 Como funcionan los servidores DNS en las Intranet

Cuando hay que conectar con un URL particular, la dirección con el URL debe ser igual que la dirección IP verdadera. Tu navegador para Web irá primero a un servidor DNS local en la Intranet de la empresa o universidad para obtener esta información si la

Dirección IP es local, el servidor DNS podrá resolver el URL con la dirección IP. Este enviará la dirección IP auténtica a tu computadora.
Tu navegador para Web tiene ahora la dirección IP verdadera del lugar que estás intentando localizar. Utiliza esa dirección IP y contacta con el sitio. EL sitio te envía la información que has solicitado.

Si la información que has solicitado no está en tu Intranet, y si tu servidor DBS local no tiene la dirección IP, el servidor DNS de Intranets debe obtener la información desde un servidor DNS en Internet.

EL servidor DNS de Intranets contacta con lo que se denomina servidor de dominio raíz, que se mantiene por un grupo llamado InterNiC. EL servidor raíz de dominio l dice al servidor de Intranets qué servidor primario de nombres y qué servidor secundario de nombres tiene la información sobre el URL solicitado.

El servidor de Intranets contacta ahora con el servidor primario de nombres. Si la información no se puede encontrar en el servidor primario de nombres, el servidor DNS de Intranets contacta con el servidor secundario. Uno de esos servidores de nombres tendrá la información exacta.
Después devolverá la información al servidor DNS de Intranets. El servidor DNS de Intranets te devuelve la información, tu navegador para Web usa ahora la dirección IP para contactar con el sitio exacto.

Cuando alguien en una Intranet quiere contactar con una localización, por ejemplo, visitar un sitio Web, escribirá una dirección, como www.net.ipsalle.edu.ni. Aunque de hecho, Internet no utiliza realmente estas direcciones alfanuméricas.

En lugar de eso, emplea direcciones IP, que son direcciones numéricas, en cuatro números de 8 bits separados por puntos, como 10.6.1.1 Un servidor DNS, llamado también un servidor de nombres, empareja, direcciones alfanuméricas con sus direcciones IP, y te permite contactar con la localización exacta.

2.18 Sistema Bind

La solución más empleada en Linux y Unix para resolver nombres de DNS es BIND
El servidor de nombres BIND (Berkeley Internet Name Domain) ya está preconfigurado en suse Linux.

La configuración de BIND se realiza por completo con el archivo /etc/named.conf. Los datos propios de la zona, que son los nombres de los ordenadores, direcciones IP, etc. de los dominios administrados, se han de anotar en archivos adicionales dentro del directorio /var/lib/named.

3. Servidor Web Apache

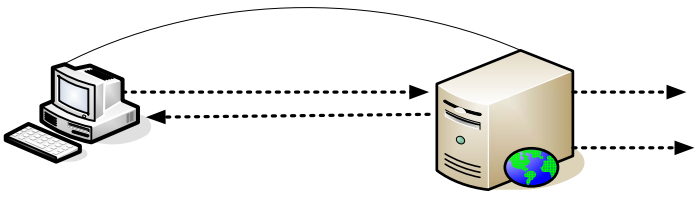
Servidor Web

Un servidor Web es un programa que sirve datos en forma de páginas Web, hipertextos o páginas HTML (HyperText Markup Language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de sonidos.

La comunicación de estos datos entre cliente y servidor se hace por medio un protocolo*, concretamente del protocolo HTTP.

Con esto, un servidor Web se mantiene a la espera de peticiones HTTP, que son ejecutadas por un cliente HTTP; lo que solemos conocer como un navegador Web.
A modo de ejemplo: al teclear http://www.ipsalle.edu.ni en un navegador, éste realizará una petición HTTP al servidor que tiene asociada dicha URL**. El servidor responde al cliente enviando el código HTML de la página; el navegador cuando recibe el código, lo interpreta y lo muestra en pantalla.

El cliente es el encargado de interpretar el código HTML, es decir, de mostrar las fuentes, los colores y la disposición de los textos y objetos de la página. El servidor se encarga de transferir el código de la página sin llevar a cabo ninguna interpretación de la misma.



3.1 Apache

Es u programa de servidor http Web de código abierto, desarrollado en 1995, es actualmente unos de los servidores Web mas usados en la red. Este corre en UNIX, Linux, BSD y Windows.
Es un poderoso paquete de servidor Web con diversos módulos que se le agregan y que se consiguen de forma gratis en Internet.

3.2 HTTP

Los clientes suelen ser navegadores Web como Konqueror o Mozilla. La comunicación entre el navegador y el servidor Web se produce a través del protocolo de transferencia de hipertexto (Hypertext Transfer Protocol).

El Protocolo de Transferencia de Hipertexto (Hypertext Transfer Protocol) es un sencillo protocolo cliente-servidor que articula los intercambios de información entre los clientes Web y los servidores HTTP. La especificación completa del protocolo HTTP está recogida en el RFC 1945. Fue propuesto por Tim Berners-Lee, atendiendo a las necesidades de un sistema global de distribución de información como el World Wide Web.

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 (por defecto, el 80), 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 un 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.

3.3 Etapas de una transacción http

Cada vez que un cliente realiza una petición a un servidor, se ejecutan los siguientes pasos:

- Un usuario accede a una URL, seleccionando un enlace de un documento HTML o introduciéndola directamente en el campo Location del cliente Web.

El cliente Web descodifica la URL, separando sus diferentes partes. Así identifica el protocolo de acceso, la dirección DNS o IP del servidor, el

VIII. METODOLOGIA DEL TRABAJO

1 Diseño Metodológico

Para lograr los objetivos de la investigación desarrollamos diferentes métodos como:

- Recopilación de la información.
- Análisis de la estructura de la red.
- Pruebas experimentales.

Recursos Disponibles

Software

- Sistema Operativo Linux suse 10.0.
  Es un sistema basado en el núcleo Linux.

- Sistema Operativo Windows XP Profesional con S.P/2.

Hardware

- Disco Duro de 40 GB.
- Disco Duro de 40 GB
- Memoria de 256 de RAM.
- Memoria de 128 de RAM.
- Procesador de 2.4 MHz.
- Procesador de 1.5 MHz.

Hardware Adicional

- Un HUB.
- Cables de red con conectores RJ45.
- 2 tarjetas de red (Asrock).

2. Especificación de requisitos para los servicios de red

El presente trabajo se llevó a cabo en el Instituto Politécnico La Salle-León (La Salle - León), desarrollándolo como proyecto piloto en las instalaciones de dicho centro estudiantil.
Según las necesidades de los usuarios la Intranet se puede colocar en:

- Un ordenador personal (PC)
- Una red local (LAN)
- Internet

En nuestro proyecto combinaremos las tres posibilidades, siendo lo habitual conectar la red local interna con Internet a través de firewall (con corta fuegos de seguridad).

Las aplicaciones que tendrá la Intranet serán aplicaciones concretas para Organizar y compartir la información de vital importancia de la institución, mediante la presentación de documentos publicados en la Intranet así como controlar la entrada a la Web mediante claves y contraseñas, logrando de este modo que sólo los usuarios autorizados tengan acceso a recursos e información privada, esté donde esté la ubicación de sus puestos de trabajo y conexiones a la Intranet.

Un computador central el servidor de la Intranet (net.ipsalle.edu.ni) de la institución educativa, maneja todo el tráfico de datos asociado con el envío y recibo de archivos. Estos archivos pueden ser códigos HTML para ser mostrado por un programa Browser, archivos de datos usados por servidor Web le dice al computador central (net.ipsalle.edu.ni) cómo tratar con los requerimientos y transmisiones tal que cualquier computador se pueda comunicar en una Intranet sin importar de que clase es, o qué sistema operativo utiliza.

Cuando usted inicia su programa Browser, envía un requerimiento al servidor Web. Este le pide al servidor enviar un archivo al Browser, el cual muestra el archivo a usted. Típicamente lo primero que se mostrara será una página principal que contiene información básica y enlaces a otros archivos y páginas en la Intranet.

2.1 Los servicios de usuario son

Intercambio y creación
Podrá crear y publicar fácilmente documentos en línea. A todos aquellos que tienen acceso les permite obtener y editar la última información publicada a lo largo de la red Por ejemplo, la información sobre los estudiantes del técnico medio puede ser creada y publicada, disponible mundialmente a todos aquellos con acceso.

Comunicación y colaboración

Correo electrónico y trabajo en grupo de carácter abierto. Con control de acceso y seguridad de identificación, se puede crear grupos de trabajo y correo electrónico privados en línea abierta o cerrada.

Acceso a información
Acceso directo a bases de datos. Se pueden obtener datos, a través de una simple ventana.

2.2 Factibilidad de tener la intranet dentro del Instituto Politécnico La salle

Factibilidad técnica

Se ha determinado que la implementación de la Intranet en el Instituto Politécnico La Salle - León puede realizarse con el equipo que se dispone actualmente, son equipos que cuentan con la tecnología requerida (hardware) para la implementación de dicha Intranet; además el software que se necesita la mayoría de ellos se tiene a mano o se pueden obtener vía Internet.

El personal técnico que tiene el Politécnico La Salle-León esta capacitado para la implementación de éste sistema de Intranet.

Factibilidad económica

La red interna que se maneja en los departamentos y la red Internet serán utilizadas como vía de comunicación de la Intranet, lo cual no ocasionaría ningún costo adicional, se tiene actualmente un servidor disponible el cual podría ser utilizado como servidor Intranet.
Además que se realizara bajo una plataforma de Software Libre (Linux-Suse 10.0) lo que directamente beneficiara el aspecto económico del Instituto Politécnico, por lo tanto este trabajo será una alternativa para reducir costes siendo esto una razón importante para aprobar este proyecto.

Factibilidad operacional

Si se desarrolla e implementa este sistema de información, será utilizado por personas encargadas de tomar decisiones importantes para el desarrollo del Centro Politécnico la salle (aparato administrativo, Dirección, proyectos, etc.), los cuales son parte integral de la información que se genera, así como por la comunidad estudiantil.

3. Diseño Lógico de la Red

El diseño de una red de comunicaciones implica la elección de una topología y una arquitectura que guíe la interconexión de los componentes.

En el Instituto Politécnico la Salle se cuenta con tres laboratorios con 180 equipos en total para aplicaciones en el área académica y alrededor de 13 equipos en biblioteca.

El acceso a Internet no es igual para todos, es decir que no todos pueden navegar, descargar archivos, chatear, etc. ya que cada laboratorio tiene permisos distintos de acceso al servicio de Internet.

En el instituto Politécnico la Salle, existe un dominio “ipsalle.edu.ni”. En torno a este dominio existen 4 grupos llamados “grupos de trabajo”, esto se hizo por razones de seguridad para el sistema. Los grupos de trabajo son:

- Ipsalle0
- Ipsalle1
- Ipsalle2
- Ipsalle3

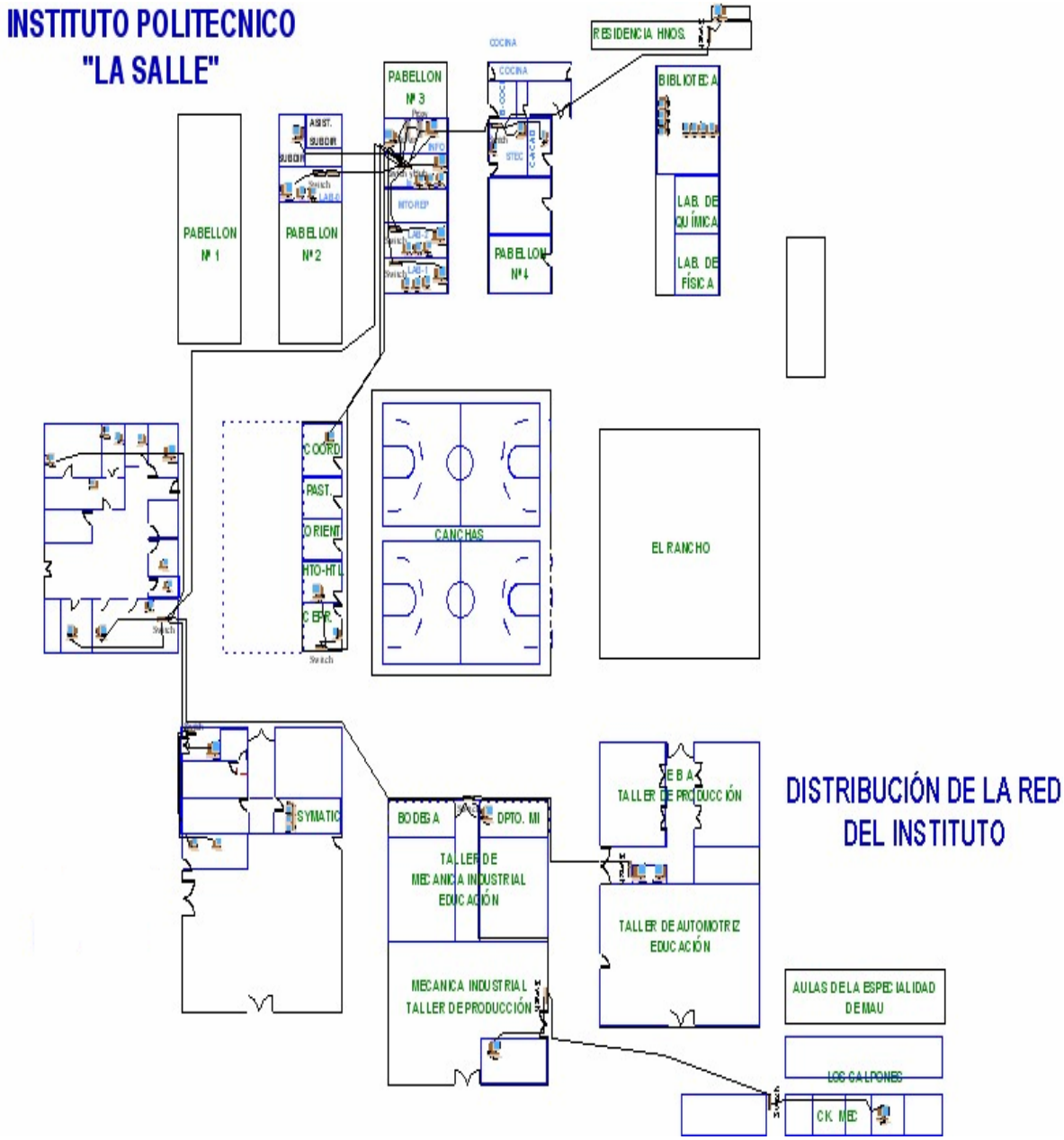
La señal de Internet es distribuida por un Proxy configurado en Linux (coyote). La asignación de IP es estática, solo para las PC que tienen conexión a Internet.

La topología de la red es en estrella con switch, existe un hub principal del cual se derivan 4 segmentos, de estos 4 segmentos hay otros switch que van en cascada.

El proveedor de Internet o ISP es Alfanuméric, con un ancho de banda de 512 de subida y 512 de bajada, todos sus hosts son clientes del DNS pero ninguno es servidor DNS.

La topología empleada para el sistema de red Intranet que utilizaremos será la de estrella ya que es con la que se cuenta actualmente. El servidor estará conectado al nodo central Internet para la salida al exterior de la red.

4. Diseño Físico de la Red



IX. Configuración de los Servicios Básicos de Red

1. Instalación de Suse Linux 10.0

Pantalla de arranque

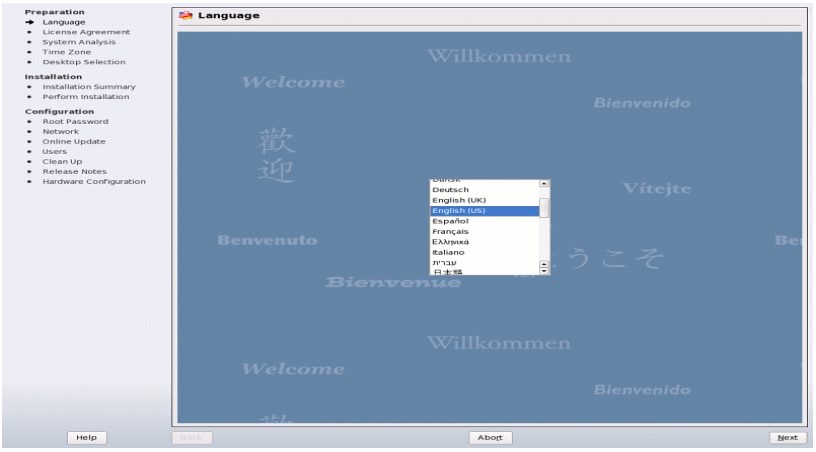
La pantalla de arranque muestra varias opciones para el proceso de instalación. La opción

Arrancar del disco duro permite arrancar el sistema instalado. Este elemento está seleccionado por defecto. Para instalar el sistema, seleccione una de las opciones de instalación con las teclas direccionales. Las opciones relevantes son:

Instalación El modo de instalación normal. Todas las funciones de hardware modernas están habilitadas.

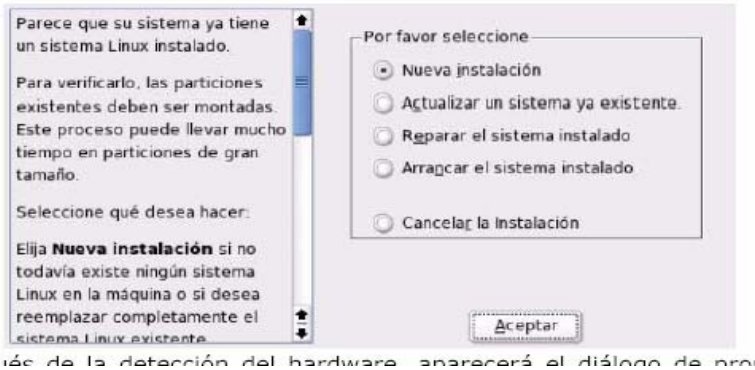
Selección de idioma

Es posible configurar YaST, y SUSE Linux en general, para que emplee distintos idiomas según sus necesidades. El idioma que seleccione aquí se utilizará para la distribución del teclado. Asimismo, YaST utiliza este valor para establecer la zona horaria del reloj del sistema.



Modo Instalación

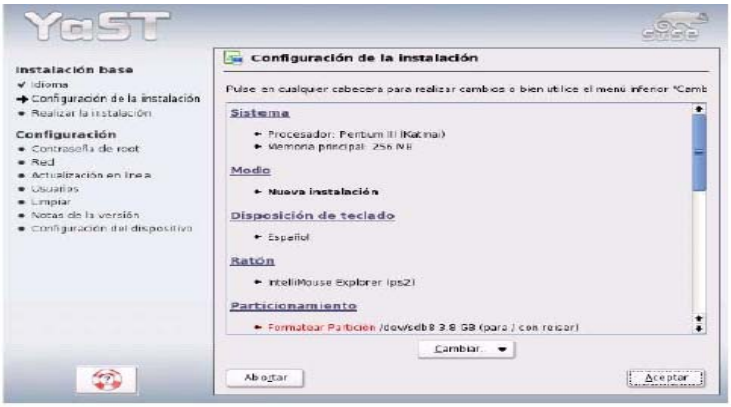
La opción es nueva instalación por lo que es la primera vez que se instala este sistema operativo.



...ués de la detección del hardware, aparecerá el diálogo de propu...

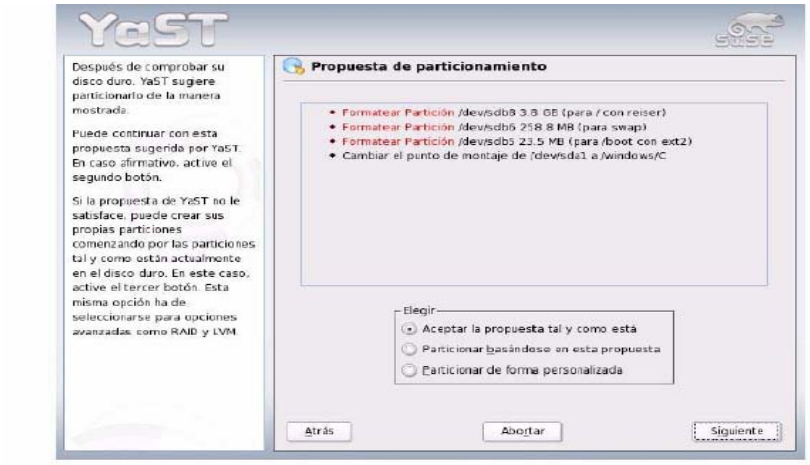
Configuración de la instalación

En este paso la configuración ofrece una serie de opciones los mas importantes son software o paquetes a instalar, particionamiento que es las particiones a tener (Swap, Boot, Root, Windows).

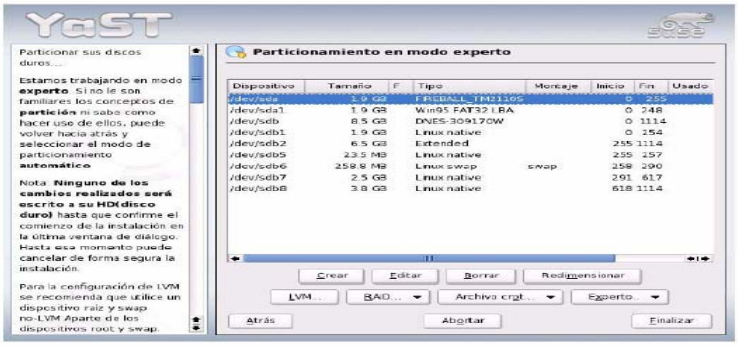


Modo de Particionamiento

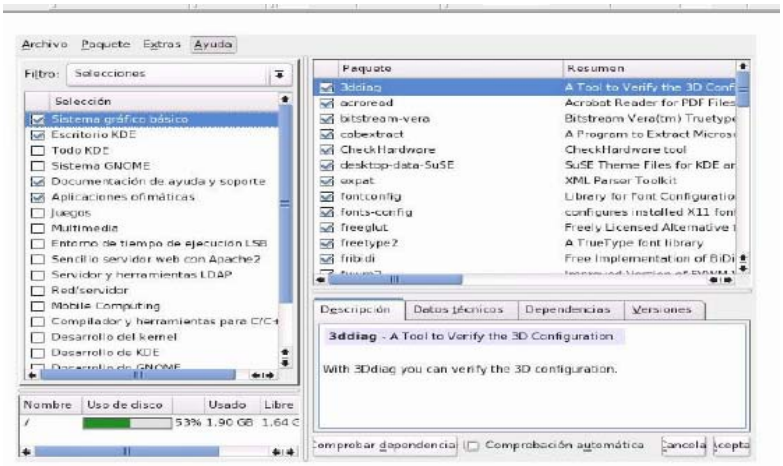
Es la forma como quedara distribuida las particiones del disco duro.



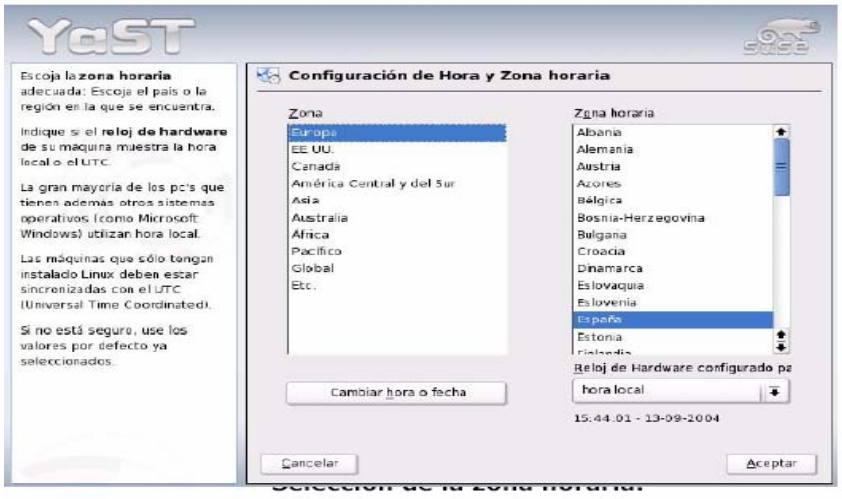
En el dialogo para experto se puede modificar el particionamiento:



En la opción de software podemos elegir los paquetes a instala.



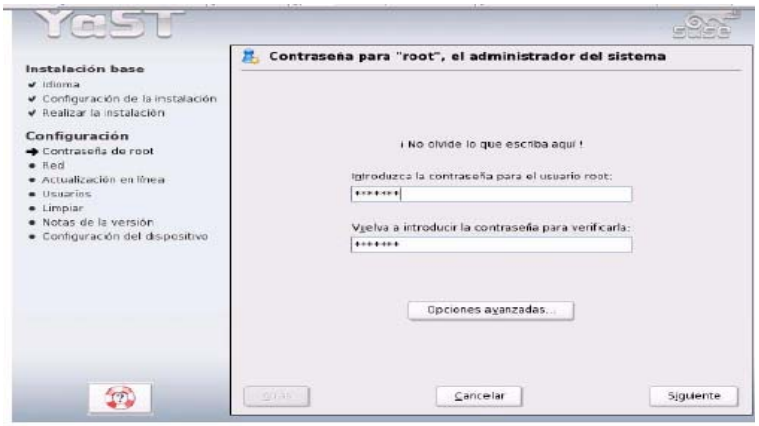
Selección de la zona horaria



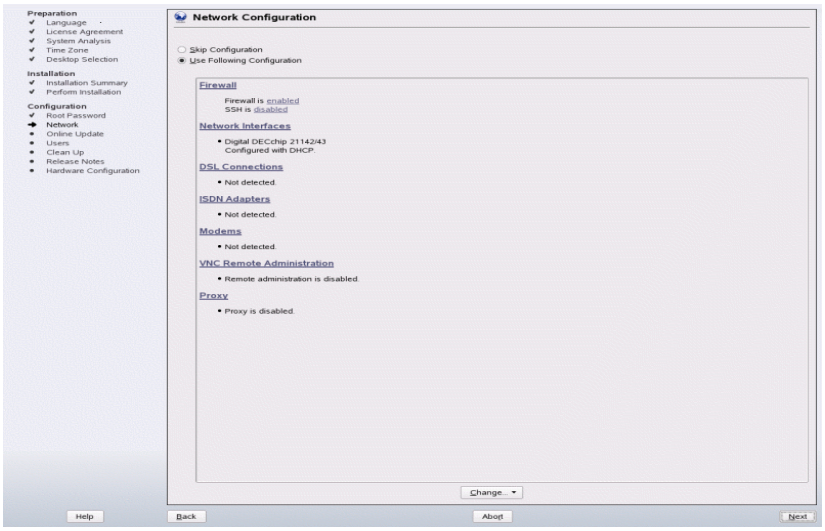
Aquí lo que se hace es seleccionar la hora y país.

Configuración de root

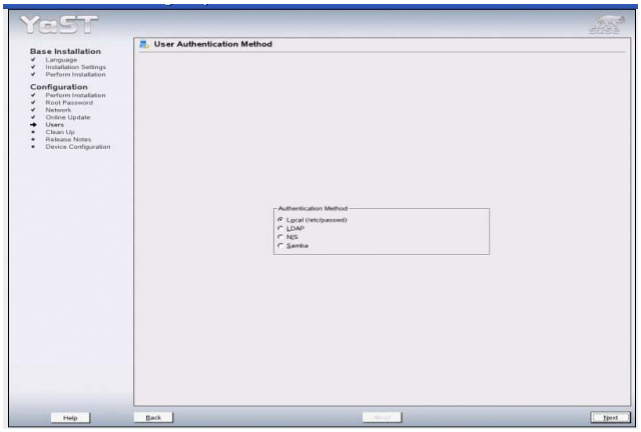
Se pone la contraseña o password del usuario root.



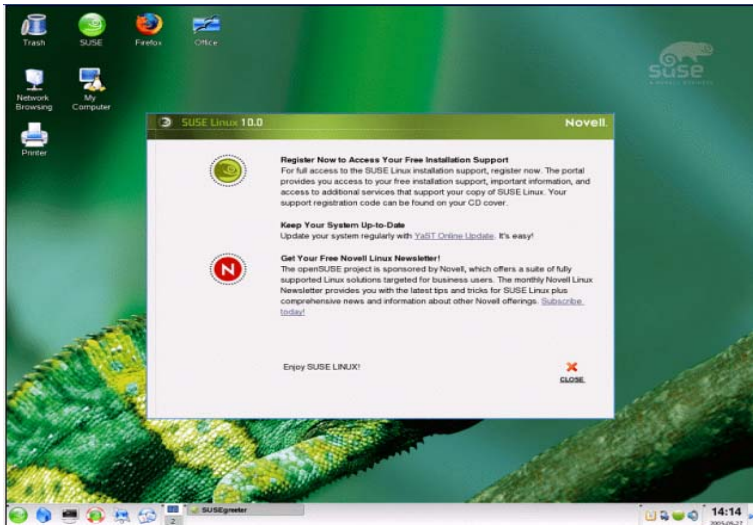
Configuración de la red



Método de Autenticación de Usuario



Finalmente podemos reiniciar Suse 10.0 con éxito.



2. Configuración del servidor DNS

El archivo de configuración /etc/named.conf

La configuración de BIND se realiza por completo con el archivo /etc/named.conf. Los datos propios de la zona, que son los nombres de los ordenadores, direcciones IP, etc. de los dominios administrados, se han de anotar en archivos adicionales dentro del directorio /var/lib/named.

El Archivo /etc/named.conf se estructura en dos secciones; la primera es options para la configuración general y la siguiente es la que contiene las entradas zone para los diferentes dominios. También es posible utilizar una sección logging o una con entradas del tipo ACL (Access Control List). Las líneas comentadas comienzan con el símbolo '#' o '//'.

Comandos Importantes dentro del named.conf

Directory "/var/lib/named"; indica el directorio que contiene los archivos con los datos de zona.

Type master; master significa que esta zona se administra en este servidor de nombres. Es algo que requiere un archivo de zona muy bien configurado.

Type hint; La zona del tipo hint se utiliza para indicar los root name Server. Es una definición de zona que no se modifica.

Sintaxis de los archivos de zona

Existen dos tipos de archivos de zona; el primero sirve para asignar la dirección IP a un nombre de ordenador y el segundo proporciona el nombre del ordenador en función de una dirección IP. El símbolo del punto ('.') tiene un significado importante en los archivos de zona. A todos los nombres de ordenadores que se indican sin el punto por detrás, se les añade la zona.

Por eso es importante terminar con un '.' los nombres de las máquinas que se hayan anotado con el dominio completo. La falta o la posición equivocada de un punto suele ser la causa de error más frecuente en la configuración de un servidor de nombres.

Sección Options
En una ventana shell se hace primero una copia del archivo de configuración Central del DNS (toda la configuración del DNS tiene que ser hecha usando la identidad de "Root").

Intranet: / # **cp /etc/named.conf /etc/named.conf.original**

Se debe de dejar ahora totalmente vacío el archive "named.conf"

Intranet: / # cp /dev/null /etc/named.conf

Iniciamos el editor de texto vi

Intranet: / # **vi /etc/named.conf**

Editamos la sección de options a como se muestra en el ejemplo:

// Sección de Opciones

Options {

directory "/var/lib/named";

dump-file "/var/log/named_dump.db";
statistics-file "/var/log/named.stats";

};

Sección de Zonas

Después de la sección de opciones se encuentran las entradas para la zona. Al menos siempre deberían existir las entradas de localhost, 0.0.127.in-addr.arpa y "." Las cuales deberían ser ubicadas siempre dentro del directorio de zona de cada servidor.

Primero tendrá que crear físicamente el directorio que contendrá la zona privada del servidor. Esto lo puede hacer sin necesidad de abandonar el archivo que esta editando con el vi:

:!mkdir /var/lib/named/salle
Pero también necesitamos el archivo que contendrá los datos de la zona pública:

A continuación siga editando el archivo named.conf colocando lo siguiente:

// Inicio Zona

```
zone "." in {
        type hint;
        file "salle/root.hint";
};

zone "localhost" in {
        type master;
        file "salle/localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "salle/127.0.0.zone";
};
```

Sin embargo seguramente podrá deducir que la zona publica que acaba de crear no contiene las zonas “.”, “localhost” y "0.0.127.in-addr.arpa". Esto lo puede verificar ejecutando un comando “ls” desde el “vi”.

:!ls -agl /var/lib/named/salle

Esto se debe a que estas zonas vienen creadas por defecto en /var/lib/named. Lo que hay que hacer es moverlas al directorio de la zona pública. Esto lo puede hacer también sin salir del “vi” :

:!mv /var/lib/named/127.0.0.zone /var/lib/named/salle
:!mv /var/lib/named/root.hint /var/lib/named/salle
:!mv /var/lib/named/localhost.zone /var/lib/named/salle

Antes de escribir la zona privada se deben de crear los directorios que contendrán los archivos para dicha zona. Esto lo puede hacer siempre desde el “vi”:

~
:! mkdir /var/lib/named/lasalle
~
:! touch /var/lib/named/lasalle/net.ipsalle.edu.ni
~
:! touch /var/lib/named/lasalle/50.168.192

Ahora estamos listos para comenzar a escribir la parte correspondiente a la zona privada o zona Interna.

// Zona de Intranet de la salle

```
zone "net.ipsalle.edu.ni" in {
        type master;
        file "lasalle/net.ipsalle.edu.ni";
};
```

Para la resolución inversa de direcciones IP (reverse lookup) de la zona privada, se utiliza el pseudo-dominio in-addr.arpa. Éste se añade por detrás a la parte de red de la dirección IP escrita al revés. En nuestro ejemplo la dirección de la tarjeta de red privada que es 10.1.6.1 se convertiría en 6.1.10

Ahora hay que ingresar la reversa de la zona privada:

```
zone "50.168.192.in-addr.arpa" in {
        type master;
        file "lasalle/50.168.192";
};
```

Con esto completamos la edición de la zona privada. Nos salimos del “vi” guardando cambios para regresar al shell de comandos.

A continuación se describe el significado de c/u de los términos que seran usados en las configuración de las zonas para el Dominio net.ipsalle.edu.ni.

Línea 1: $TTL define el TTL estándar, que vale para todas las anotaciones en este archivo y es en este caso de 2 días (2D = 2 days). TTL"time to live" es el tiempo de vencimiento.

Línea 2: Aquí comienza la parte del SOA control record:

- En primer lugar figura el nombre del dominio a administrar net.ipsalle.edu.ni, terminado con un '.' para que no se añada otra vez el nombre de la zona. La alternativa es la de anotar el símbolo '@' para que se busque el nombre de la zona en /etc/named.conf.

- Por detrás de IN SOA se anota el nombre del servidor de nombres que actúa como master para esta zona.

- A continuación aparece la dirección de correo electrónico de la persona que se encarga de este servidor de nombres. Como el símbolo '@' ya tiene un significado especial, se le reemplaza por un '.' - en lugar de root@net.ipsalle.edu.ni se escribe entonces root.net.ipsalle.edu.ni. . No se debe olvidar el punto al final para que no se añada la zona.

- Al final hay un '(', para incorporar las siguientes líneas hasta el ')' con todo el SOA-Record.

Línea 3: El número de serie en la línea serial es un número al azar que debe aumentarse después de cada modificación del archivo. El cambio del número informa a los servidores de nombres secundarios sobre la modificación. Es típico utilizar una cifra de diez dígitos formada por la fecha y un número de orden en la forma AAAAMMDDNN.

Línea 4: El intervalo de refresco en la línea refresh indica al servidor de nombres secundario cuándo debe comprobar nuevamente la zona. En este caso es un día (1D = 1 day).

Línea 5: El intervalo de reintento en la línea retry indica cuánto tiempo después el servidor de nombres secundario debe intentar conectar nuevamente con el primario. En este caso son 2 horas (2H = 2 hours).

Línea 6: El tiempo de expiración en la línea expiry indica el tiempo después del cual el servidor de nombres secundario debe descartar los datos dentro de la caché, cuando la conexión con el servidor primario haya dejado de funcionar. En este caso es una semana (1W = 1 week).

Línea 7: La última entrada en SOA es el negative caching TTL que indica cuánto tiempo pueden mantener los otros servidores en la caché las consultas DNS hechas que no se han podido resolver.

Línea 8: IN NS indica el servidor de nombres que se encarga de este dominio.

Puede haber varias líneas de este tipo, una para el servidor de nombres primario y otra para cada servidor de nombres secundario.

Si la variable notify de /etc/named.conf tiene el valor “yes”, se informará de todos los servidores de nombres aquí mencionados y de los cambios en los datos de zona.

Línea 9: El MX-Record indica el servidor de correo que recibe, procesa o traspasa los mensajes para el dominio. En este ejemplo se trata del mismo ordenador net.ipsalle.edu.ni. La cifra por delante del nombre de ordenador es el valor de preferencia.

Si existen varias entradas MX, primero se utiliza el servidor de correo con el valor de preferencia más bajo y si la entrega del correo a este servidor falla, se utiliza el servidor con el siguiente valor más alto.

“A” es un puntero que se utilice para enlazar un nombre de dominio con un numero IP.

Con esto completamos la edición de la zona privada. Salimos del “vi” guardando los cambios:

Comenzaremos ahora a editar los archivos correspondientes a la zona privada. El primer archivo que editamos es el que contentara la zona privada de nombres. Lo que tenemos que hacer primero es trasladarnos al directorio que habíamos creado previamente para contener los archivos de zona privada (/var/lib/named/salle) :

 # cd /var/lib/named/lasalle
Entonces editamos el archivo de zona de nombre:
intranet:/var/lib/named/lasalle **# vi net.ipsalle.edu.ni**

Entonces editamos lo siguiente:

```
$TTL 2D
@           IN    SOA   net.ipsalle.edu.ni.  root.net.ipsalle.edu.ni. (
                                               2007030502 ; Serial
                                               1D         ; Refresh
                                               2H         ; Retry
                                               1W         ; Expire
                                               2D )       ; Minimum
```

```
                    NS      net.ipsalle.edu.ni.      ; Primary DNS Server
                    MX  5   net.ipsalle.edu.ni.      ; Primary Mail

net                 A       192.168.50.44
net.ipsalle.edu.ni. A       192.168.50.44
pc1                 A       192.168.50.45
index.html          A       192.168.50.44
```

A como se observa la creación de la zona privada de nombres es prácticamente Sencilla.
Terminamos entonces de editar el archivo guardando los cambios que hasta ahora hemos hecho:

El siguiente paso es editar el archivo de reversa correspondiente a la zona privada (/var/lib/named/lasalle/50.168.192) que ya habíamos creado con anterioridad:

test:/var/lib/named/intranet # **vi 50.168.192**

Ingresamos entonces la siguiente información:

```
$TTL 2D
@       IN      SOA    net.ipsalle.edu.ni.  root.net.ipsalle.edu.ni.  (
                                             2007030502 ; Serial
                                             1D         ; Refresh
                                             2H         ; Retry
                                             1W         ; Expire
                                             2D     )   ; Minimum


                    NS      net.ipsalle.edu.ni.      ; Primary DNS Server
                    MX 5    net.ipsalle.edu.ni.      ; Primary Mail

44                  PTR     net
44                  PTR     net.ipsalle.edu.ni.
45                  PTR     pc1.net.ipsalle.edu.ni.
44                  PTR     index.html
```

Lo ultimo que quedar por hacer para completar la edición de la zona privada es guardar los cambios que hasta ahora hemos hecho:

:wq!

Con esto ya quedan totalmente editadas las zonas públicas y privadas. Solo resta ya hacer pruebas con el DNS para verificar que funcione correctamente.

Es decir que cargue sin errores y resuelva correctamente los nombres de dominio a números IP y los números IP a nombres de dominio.

Para comprobar su correcto funcionamiento Abrimos dos consolas y ponemos lo siguiente:

- En la primera shell /etc/init.d/named start
- En la siguiente ponemos:

  cp /dev/null /var/log/messages
  clear
  tail –f /var/log/messages

Esta nos mostrara los errores o si nuestro servidor DNS funciona correctamente para luego probar mediante un nslookup y haciendo ping si todo funciona perfectamente.

Ahora que ya tenemos el named instalado y configurado podemos ejecutarlo y hacer las pruebas necesarias mediante nslookup para ver si esta funcionado correctamente.

Pruebas de funcionamiento del DNS mediante el uso del comando nslookup.

net:~ # /etc/init.d/named start
Starting name server BIND done

net:~ # nslookup

> net
Server: 192.168.50.44
Address: 192.168.50.44 #53

Name: net.net.ipsalle.edu.ni
Address: 192.168.50.44

> net.ipsalle.edu.ni
Server: 192.168.50.44
Address: 192.168.50.44 #53

Name: net.ipsalle.edu.ni
Address: 192.168.50.44

> 192.168.50.44

Server: 192.168.50.44
Address: 192.168.50.44 #53

44.50.168.192.in-addr.arpa name = net.ipsalle.edu.ni.
44.50.168.192.in-addr.arpa name = index.html.

> pc1.net.ipsalle.edu.ni
Server: 192.168.50.44
Address: 192.168.50.44#53

Name: pc1.net.ipsalle.edu.ni
Address: 192.168.50.45

> google.com.ni
Server: 192.168.50.44
Address: 192.168.50.44#53

Non-authoritative answer:
Name: google.com.ni
Address: 64.233.161.104
Name: google.com.ni
Address: 64.233.187.104

Name: google.com.ni
Address: 66.102.7.104

> 66.233.161.104
Server: 192.168.50.44
Address: 192.168.50.44#53

Non-authoritative answer:
104.161.233.66.in-addr.arpa name = 66-233-161-104.gsb.clearwire-dns.net.

Authoritative answers can be found from:
233.66.in-addr.arpa nameserver = ns2.clearwire-dns.net.
233.66.in-addr.arpa nameserver = ns1.clearwire-dns.net.
ns1.clearwire-dns.net internet address = 64.13.112.149
ns2.clearwire-dns.net internet address = 65.77.164.5

> 64.233.187.104
Server: 192.168.50.44
Address: 192.168.50.44#53

Non-authoritative answer:

104.187.233.64.in-addr.arpa name = jc-in-f104.google.com.

Authoritative answers can be found from:
187.233.64.in-addr.arpa nameserver = ns1.google.com.
187.233.64.in-addr.arpa nameserver = ns2.google.com.
187.233.64.in-addr.arpa nameserver = ns3.google.com.
187.233.64.in-addr.arpa nameserver = ns4.google.com.
ns1.google.com internet address = 216.239.32.10
ns2.google.com internet address = 216.239.34.10

> net:~ #
net:~ #

3. Configuración de un sistema Apache2

La configuración de apache es sumamente sencilla. Ya se que use un IP publico o uno privado. Lo único que tiene que hacer para empezarlo a usar es introducir la entrada correspondiente del servidor en el DNS tanto en las zonas de nombre a número como en los punteros de reversa:

.
Index.html A 192.168.50.44
…
..
44 PTR index.html

Sin embargo algunas veces el archivo índice principal necesita ser variado ya que se puede dar el caso que este se pueda llamar diferente a lo usual o a lo que viene por defecto en la configuración del apache (index.html). Si este fuera el caso necesita hacer lo siguiente:

Abra una ventana shell y otra al directorio apache2 (toda la configuración del Apache tiene que ser hecha usando la identidad de “Root”).

:/ # cd /etc/apache2

Editamos el archivo httpd.conf y valla a la línea 163

: **/etc/apache2 # vi httpd.conf**

/etc/apache2/httpd.conf
This is the main Apache server configuration file. It contains the
configuration directives that give the server its instructions.
See <URL:http://httpd.apache.org/docs-2.0/> for detailed information about
the directives.

.
:163
.

List of resources to look for when the client requests a directory
DirectoryIndex index.html index.html.var
.
Dominios Virtuales

Este es el caso de usar dominios virtudes. Es decir que una maquina sea reconocida con diferentes nombres pero que estos nombres estén asociados al mismo numero IP. Esto con el objetivo de que cuando acceda a esta computadora esta presente diferentes paginas Web dependiendo del nombre que se halla usado.

Para configurar los dominios virtuales tiene que hacer lo siguiente:
:/ # cd /etc/apache2

Edite el archivo listen.conf y vallase a la línea 41

Listen: Allows you to bind Apache to specific IP addresses and/or
ports. See also the <VirtualHost> directive.
#
http://httpd.apache.org/docs-2.0/mod/mpm_common.html#listen
#
:41
#
#**NameVirtualHost *:80**
#
Descomente el término de NameVirtualHost. Este se usa para habilitar las conexiones de dominios virtuales.

Sálgase de este archivo de configuración, salvando los cambios hechos.
:wq!

Ahora vámos al directorio donde se van a crear los archivos de configuración de los dominios virtuales :

://etc/apache2 # **cd vhosts.d/**

En nuestro ejemplo crearemos dos dominios virtuales. Si se usa al menos un dominio virtual, siempre tendrá que ser creado otro para el sitio principal.

Tiene que hacer dos copias de un archivo llamado vhost.template ya que será en esas copias donde tendremos que configurar los dominios virtuales.

Las dos copias que haga tendrán que terminar con la extensión .conf. Y cada una empezara con el nombre que quiera darle a ese dominio. En nuestro ejemplo la primera copia tendrá el nombre de intranet y la segunda el nombre de net.

:/etc/apache2/vhosts.d # **cp vhost.template net.conf**

Ahora tendremos que editar el archivo para introducir los datos propios de este. Comenzamos:

:/etc/apache2/vhosts.d **# vi net.conf**

En la línea #14 se encuentra el termino ServerAdmin. Este término define la dirección de correo de la persona que se va a encargar de darle mantenimiento al dominio virtual.
ServerAdmin hazzell2682@yahoo.com

En la línea 15 se encuentra el termino ServerName. Este define el nombre para este dominio virtual. Aquí colocaremos:
ServerName net.ipsalle.edu.ni

Por ultimo se va la línea 20 donde esta la directiva DocumentRoot. Aquí se definirá el lugar donde residirán las páginas para este dominio virtual. En nuestro caso utilizaremos la ruta por defecto para el sitio principal (/srv/www/htdocs).

DocumentRoot /srv/www/htdocs

Solo le resta salirse y guardar cambios.
.:wq!

Con eso terminaríamos la edición para el dominio virtual que representara al sitio principal.

Ahora ya podemos poner a funcionar nuestro http mediante una pequeña página Web tanto para el sitio principal como para el dominio virtual.

Hay que usar siempre un nombre de archivo índice principal valido (Ej. Index.html). Estos dos index.html residirán en lugares distintos. El del dominio principal será depositado en /srv/www/htdocs y el del dominio virtual en /srv/www/htdocs/).

Ya solo resta iniciar el apache y hacer las pruebas o ajustes necesarios a través de los comandos necesarios.

linux:~ # /etc/init.d/apache2 start

Starting apache2 …… done

En la Url ponemos http:// net.ipsalle.edu.ni y nos mostrara la página de nuestro sitio Web.

4. Configuración de Qmail

La configurará del servidor de correo estará bajo el dominio “net.ipsalle.edu.ni” con FQDN 'net.net.ipsalle.edu.ni' y cliente de correo Web “Squirrelmail”, este servidor se encargará de gestionar cualquier dominio virtual que se desee agregar incluyendo “net.net.ipsalle.edu.ni”, para ello el sistema de correo cuenta con las siguientes características:

- Agente de Transporte de Correo qmail, con todos sus parches actualizados.
- Manejo de dominios y cuentas virtuales a través de vpopmail.
- Servidor pop3 e imap para lectura de correos.
- Control anti-spam y anti virus.
- Filtrado de correos a través de maildrop
- Gestión de listas de correo.
- Cliente de correo Web bajo HTML 4.0 puro, para asegurar la mayor compatibilidad con browsers existentes.
- Herramientas administrativas para gestión de cuentas y administración vía Web del servidor de correo

Paquetes que se utilizan la configuración

Qmail: Es el MTA (Agente de Transporte de Correos) ideal para sustitución de Sendmail, este utiliza el SMTP (Protocolo Simple de Transferencia de Correo) para intercambiar mensajes con otros MTA.

Ucspi-tcp: Es un servidor que maneja conexiones smtp, es una solución alternativa al uso de *Xinetd* para manejar conexiones.

Qmail's daemontools: Herramientas útiles para mantenimiento o gestión de demonios.

Qmail's pop3d: Maneja el Servicio pop3d para qmail.

Qmail SMTP authentication patch: Se necesita de este parche para obligar autenticación smtp, es importante para evitar el relay.

Qmail SMTP TLS patch: Parche para encriptado de conexiones smtpd remotas.

Ezmlm: Administración y gestión de listas de correo.

Autoresponder: Genera reglas que permiten autoresponder correos, en caso de ausencias temporales.

Vpopmail: Herramienta para manejar cuentas y dominios virtuales.

Vqadmin: Interfaz Web para administrar las cuentas y dominios vpopmail.

Maildrop: Para aplicar filtros de correos, téngase en cuenta que es una herramienta difícil de utilizar.

Qmailadmin: Es una Interfaz Web semejante a vqadmin para el manejo detallado de dominios virtuales vpopmail.

Courier IMAP & IMAP SSL: Servidor IMAP e IMAP seguro.

Squirrelmail webmail client: Es un cliente de correo Web ampliamente personalizable, además cuenta con gran cantidad de plugins.

Spamassassin – Herramienta desarrollada en perl para el control del spam, brinda un 95% de eficiencia.

Clam anti-virus -Explora todo el correo entrante, a través de lectura de cabeceras determina si se esta infectado con virus, además mantiene una base de datos con actualizaciones en línea.

Dependencias del Sistema
Es necesario antes de proceder con la instalación de los paquetes mencionados anteriormente, hacer un chequeo de las dependencias, en este

sentido se debe de tener previamente instalado y configurado el siguiente software:

- Servidor Web Apache – httpd-2.0.52-3.1.
- php-4.3.11-2.5 o cualquier versión estable
- perl-5.8.5 o cualquier versión estable
- Compilador gcc-3.2.3 o superior, debe incluir compilador para C++
- Openssl-0.9.5a o superior
- openssl-devel
- patch y patch-utils, herramientas

Chequear que estén instalados los siguientes módulos perl:

Time::HiRes
Net::DNS
Digest::SHA1
Digest::HMAC
HTML::Tagset
HTML::Parser
Mail::SpamAssassin
Pod::Usage
Parse::Syslog
Statistics::Distributions

Debe de tener bien claro los puertos utilizados por cada uno de los servicios que vamos a utilizar.

Portocolo	**Puerto de Salida**	**Puerto de Entrada**
SMTP	25	25
POP services	110	110
IMAP	143	143
Spamassasin	783	783
IMAPS	993	993
HTTP		80
HTTPS		443

Puertos utilizados

Para la comprobación de los módulos perl, se ejecuta el script: '/downloads/qmailrocks/scripts/util/check_perlmods.script', posterior al desempaquetado del paquete qmailrocks.tar.gz

Descarga del software necesario:

En el sitio www.qmailrocks.com se ha hecho una colección de todos los paquetes necesarios para la instalación y configuración de un completo servidor de correo. Con la cuenta root del sistema se siguen los pasos:

Descarga del conjunto de paquetes

```
[root@linux ~]# mkdir /downloads
[root@linux ~]# cd /downloads/
[root@linux downloads]# wget http://www.qmailrocks.org/downloads/qmailrocks.tar .gz
[root@linux downloads]# tar xvzf qmailrocks.tar.gz
```

En la carpeta descomprimida se encuentra un script que nos permitirá crear los directorios, grupos y usuarios de qmail, a la vez desempaquetara las *daemontools y el uscpi-tcp,* para establecer parámetros iniciales, para ello se ejecuta lo siguiente:

Establecer parámetros iniciales de Configuración
[root@linux downloads]# ./qmailrocks/scripts/install/qmr_install_linux-s1.script

Antes de continuar con la instalación, es necesario aplicar los parches correspondientes para qmail, *daemontools y ucspi-tcp*. Se cuenta con una lista actualizada de todos los parches, los cuales se instalan a través del script:

Aplicando parches
[root@linux downloads]# ./qmailrocks/scripts/util/qmail_big_patches.script

Instalación de qmail, daemontools y ucspi-tcp
En este momento ya podemos seguir con la compilación de qmail, ejecutando:
[root@linux downloads]# cd /usr/src/qmail/qmail-1.03/
[root@linux qmail-1.03]# make man && make setup check
[root@linux qmail-1.03]# ./config-fast net.ipsalle.edu.ni

Con esto ya tenemos qmail instalado en nuestro sistema, es importante generar un certificado de seguridad que será usado para cifrar las sesiones SMTP de nuestro servidor a través de TLS, esto lo hacemos con los comandos mostrados a continuación.

Ahora generamos el certificado de seguridad
[root@linux qmail-1.03]# **make cert**
Country Name (2 letter code) [GB]:**NI**
State or Province Name (full name) [Berkshire]:**Leon**
Locality Name (eg, city) [Newbury]:**Leon**
Organization Name (eg, company) [My Company Ltd]:**Proyecto La Salle**
Organizational Unit Name (eg, section) []: **Instituto Politecnico La Salle**
Common Name (eg, your name or your server's hostname) []:**net.ipsalle.edu.ni**

Email Address []:postmaster@net.ipsalle.edu.ni
chmod 640 /var/qmail/control/servercert.pem

y luego nos aparece lo siguiente.

chown qmaild.qmail /var/qmail/control/servercert.pem
ln -s /var/qmail/control/servercert.pem /var/qmail/control/clientcert.pem
Generar Certificado de seguridad

Si el certificado se generó con éxito, automáticamente se crearan los archivos *'/var/qmail/control/servercert.perm'* y *'/var/qmail/control/clientcert.pem'*, con lo que ya podemos definir el propietario de dichos ficheros:

Establecer derechos de propiedad
[root@linux qmail-1.03]# chown -R vpopmail:qmail /var/qmail/control/clientcert.pem /var/qmail/control/servercert.pem

Para la instalación de ucspi-tcp ejecutar:
[root@linux qmail-1.03]# cd /usr/src/qmail/ucspi-tcp-0.88/
[root@linux ucspi-tcp-0.88]# patch < /downloads/qmailrocks/patches/ucspi-tcp-0.88.errno.patch
[root@linux ucspi-tcp-0.88]# make && make setup check

Ahora procedemos a la instalación de los daemonstools:
Compilando daemontools
[root@linux daemontools-0.76]# cd /package/admin/daemontools-0.76/src/
[root@linux src]# patch < /downloads/qmailrocks/patches/daemontools-0.76.errno.patch
[root@linux src]# cd /package/admin/daemontools-0.76/
[root@linux daemontools-0.76]# ./package/install

Si las compilaciones hasta el momento hechas no han presentado errores, al ejecutar el siguiente comando se observara el demonio 'svscanboot', esto significa que todo marcha a la perfección.

[root@linux daemontools-0.76]# **ps -aux | grep svs**
Warning: bad syntax, perhaps a bogus '-'? See /usr/share/doc/procps-3.2.3/FAQ
root 11606 0.0 0.4 2212 1044 ? Ss 13:13 0:00 /bin/sh /command/svscanboot
root 11608 0.0 0.1 1552 308 ? S 13:13 0:00 svscan /service
root 11612 0.0 0.2 5200 728 pts/2 S+ 13:20 0:00 grep svs

Con esto tenemos instalado qmail, en los apartados siguientes se instalan herramientas que ampliaran las funciones del servidor de correo.

Instalación de ezmlm

Ezmlm aumenta las capacidades de nuestro servidor dándole la funcionalidad de manejar listas de correo, Cuando instalemos qmailadmin se, observara una interfaz grafica en ambiente Web para la administración de las listas de correo.

Para la compilación de ezmlm:
[root@slavedns ~]# cd /downloads/qmailrocks
[root@slavedns qmailrocks]# tar xvzf ezmlm-0.53-idx-0.41.tar.gz
[root@slavedns ezmlm-0.53-idx-0.41]# cd ezmlm-0.53-idx-0.41
[root@slavedns ezmlm-0.53-idx-0.41]# make && make setup

Instalación de Autoresponder
Este programa nos permite ejecutar auto respuestas para los mailbox de los usuarios.
Para su instalación y ejecución se hace lo siguiente:

[root@linux ezmlm-0.53-idx-0.41]# cd /downloads/qmailrocks

[root@linux qmailrocks]# tar xvzf autorespond-2.0.5.tar.gz
[root@linux qmailrocks]# cd autorespond-2.0.5
[root@linux autorespond-2.0.5]# make && make install

Vpopmail

Es uno de los componentes fundamentales del sistema, este software permite la recepción de correo en dominios virtuales. Además podemos agregar usuarios virtuales, es decir usuarios que no podrán logearse al sistema a través de telnet, por ejemplo.
Para su instalación ejecute:
[root@linux autorespond-2.0.5]# cd /downloads/qmailrocks
[root@linux qmailrocks]# tar xvzf vpopmail-5.4.9.tar.gz
[root@linux qmailrocks]# cd vpopmail-5.4.9
[root@linux vpopmail-5.4.9]# ./configure –enable-logging=p
[root@linux vpopmail-5.4.9]# make && make install-strip

Vqadmin

Vqadmin es una interfaz simple basada en Web que nos permitirá manejar el Vpopmal. A través de esta interfaz podremos crear dominios virtuales, nuevos usuarios y establecer propiedades sobre los buzones de correo de cuentas individualmente. La figura 13 muestra los comandos para su instalación:
[root@linux vpopmail-5.4.9]# cd /downloads/qmailrocks
[root@linux qmailrocks]# tar xvzf vqadmin-2.3.6.tar.gz
[root@linux qmailrocks]# cd vqadmin-2.3.6
[root@linux vqadmin-2.3.6]# ./configure --enable-cgibindir=/srv/www/cgi-bin –enable-htmldir=/srv/www/html
  Current settings
---
vpopmail directory = /home/vpopmail
            uid = 1008
            gid = 1003
     cgi-bin dir = /srv/www/cgi-bin
     vqadmin dir = /srv/www/cgi-bin/vqadmin
     mysql features = disabled

[root@linux vqadmin-2.3.6]# make && make install-strip
Con esto ya tenemos instalado vqadmin en ‘/srv/www/cgi-bin’, habrá que hacer las siguientes modificaciones al *'*/etc/apache2/default-server.conf*':*

La ruta del directorio cgi-bin

```
<Directory "/srv/www/cgi-bin">
      AllowOverride All
      Options +ExecCGI -Includes
      Order allow,deny
      Allow from all
</Directory>
```

La ruta del directorio cgi-bin

```
<Directory "/srv/www/cgi-bin/vqadmin">
        AllowOverride All
        Options +ExecCGI -Includes
        Order allow,deny
        Allow from all
</Directory>
```

Ahora se edita el fichero *'*.htaccess' al directorio cgi-bin para protegerlo con contraseña:

```
[root@linux vqadmin-2.3.6]# vi /srv/www/cgi-bin/vqadmin/.htaccess
AuthType Basic
AuthUserFile /etc/apache2/vqadmin.passwd
AuthName vQadmin
```

Editando el fichero '/srv/www/cgi-bin/vqadmin/.htaccess'. Es de mucha importancia establecer los permisos del fichero:

```
[root@linux vqadmin-2.3.6]# chown wwwrun /srv/www/cgi-bin/vqadmin/.htaccess
[root@linux vqadmin-2.3.6]# chmod 644 /srv/www/cgi-bin/vqadmin/.htaccess
```

Estableciendo permisos sobre el fichero '/var/www/cgi-bin/vqadmin/.htaccess'

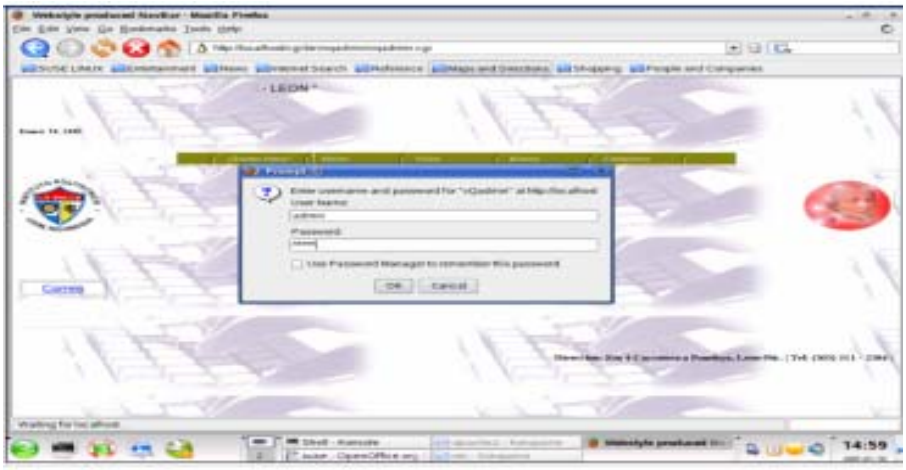
Ahora hay que crear el correspondiente fichero *'*.htpassword' que contendrá la cuenta y contraseña (cifrada) con la que ingresaremos a la administración del vqadmin.

```
[root@linux vqadmin-2.3.6]# htpasswd2 -bc /etc/apache2/vqadmin.passwd admin admin
[root@linux vqadmin-2.3.6]# chmod 644 /etc/apache2/vqadmin.passwd
```

Para finalizar reiniciamos apache, para que los cambios tengan efecto.

```
[root@linux vqadmin-2.3.6]# /etc/init.d/apache2 restart
Syntax OK                                  [  OK  ]
Starting httpd2 (prefork)                  [  OK  ]
```

Después podremos ingresar a *vqadmin,* a través del browser tecleando el URL http://localhost/cgi-bin/vqadmin/vqadmin.cgi.



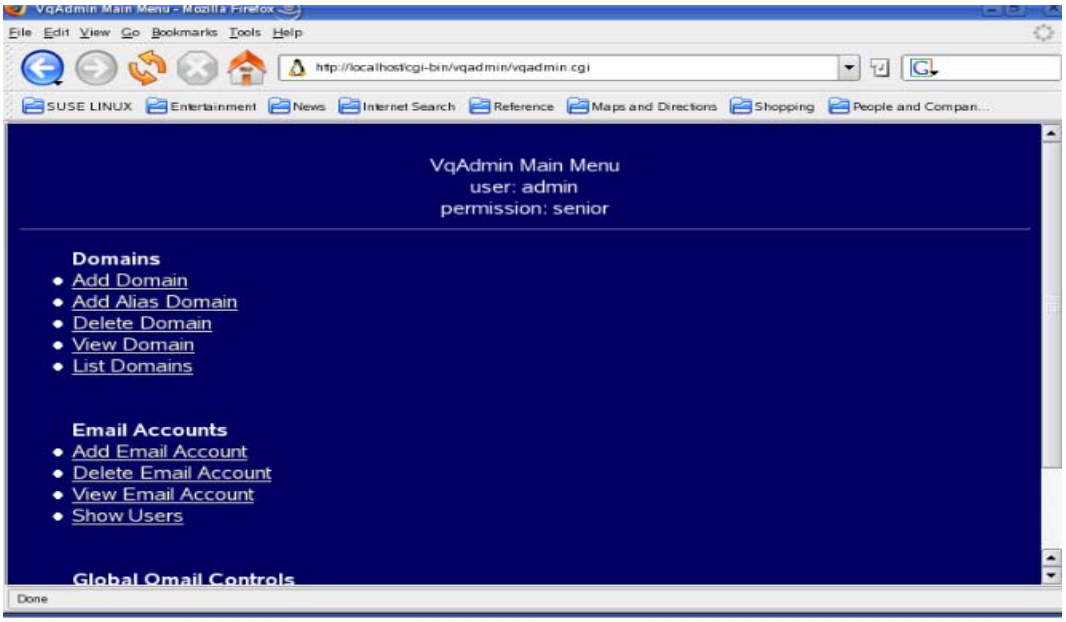
Instalación de Maildrop

Con maildrop podremos filtrar los mensajes que lleguen al servidor por medio de reglas establecidas por el usuario, para su instalación se siguen los siguientes pasos.

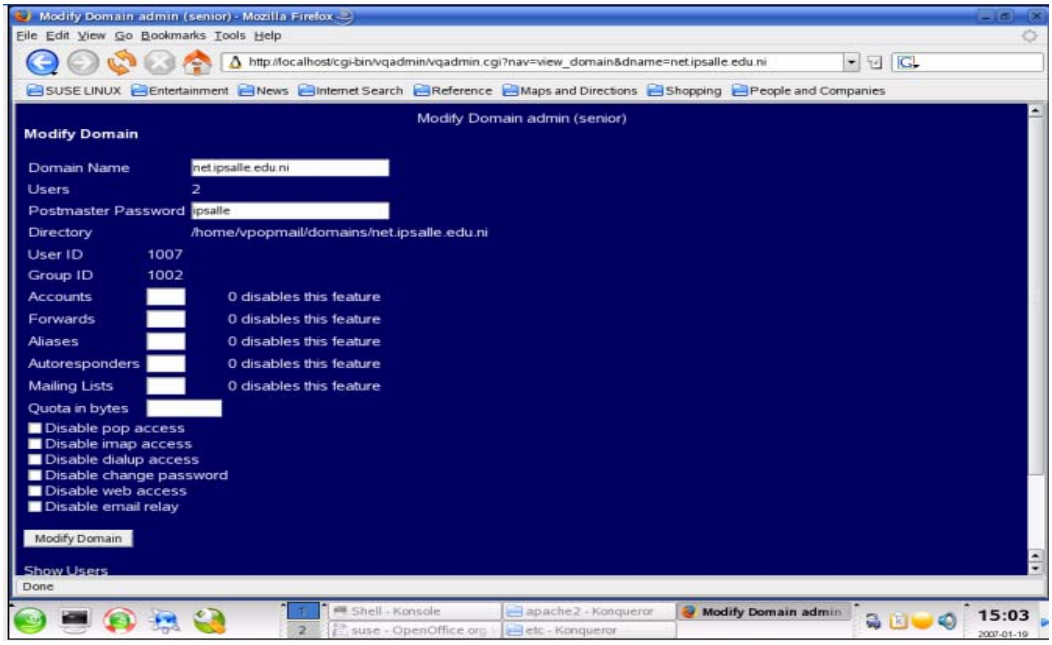
[root@linux vqadmin-2.3.6]# cd /downloads/qmailrocks
[root@linux maildrop-1.6.3]# tar xvzf maildrop-1.6.3.tar.gz
[root@linux maildrop-1.6.3]# cd maildrop-1.6.3
[root@linux maildrop-1.6.3]# ./configure --prefix=/usr/local --exec-prefix=/usr/local --enable-maildrop-uid=root --enable-maildrop-gid=vchkpw --enable-maildirquota
[root@linux maildrop-1.6.3]# make && make install-strip && make install-man

Instalación de qmailadmin
Qmailadmin nos brindará funcionalidades para crear mailbox, alias, forwards, listas de correo, etc. Para instalarlo ejecutamos:
[root@linux maildrop-1.6.3]# cd /downloads/qmailrocks
[root@linux qmailadmin-1.2.3]# tar xvzf qmailadmin-1.2.3.tar.gz
[root@linux qmailadmin-1.2.3]# cd qmailadmin-1.2.3
[root@linux qmailadmin-1.2.3]# ./configure --enable-cgibindir=/srv/www/cgi-bin -enable-htmldir=/srv/www/htdocs
[root@linux qmailadmin-1.2.3]# make && make install-strip

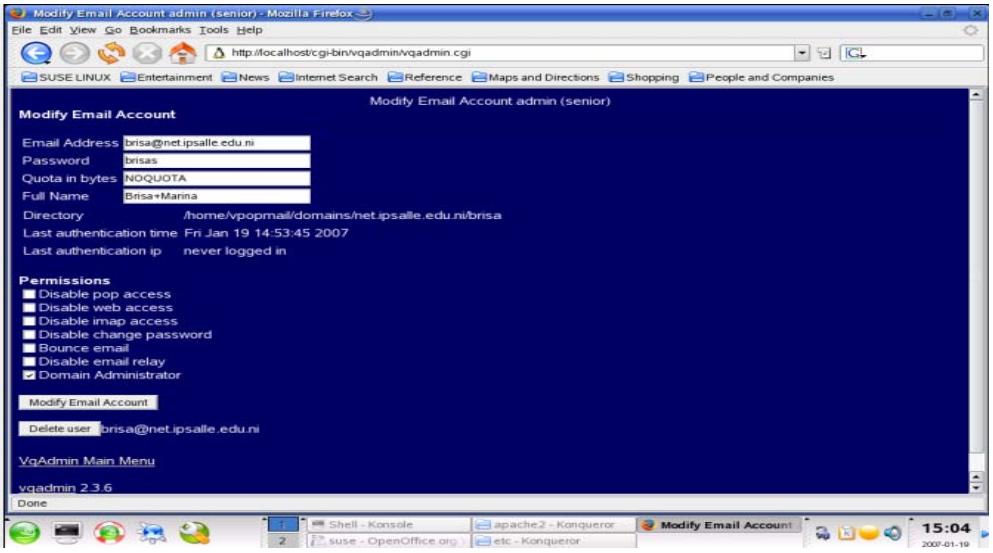
Con esto ya contamos con Qmailadmin en nuestro sistema, a continuación teclee el url **http://localhost/cgi-bin/qmailadmin** en su navegador web, para logearse ingrese el dominio virtual que tendrá que haber creado previamente con vqadmin. Y nos mostrara la siguiente ventana para crear las cuentas de usuario.



Ahora Creamos la cuenta para del nombre del dominio principal net.ipsalle.edu.ni



También aquí creamos la cuenta de administrador del sistema en este caso lo hemos llamado brisa@net.ipsalle.edu.ni.



Instalación de Maildrop

Con maildrop podremos filtrar los mensajes que lleguen al servidor por medio de reglas establecidas por el usuario, para su instalación se siguen los siguientes pasos.

[root@linux vqadmin-2.3.6]# cd /downloads/qmailrocks
[root@linux maildrop-1.6.3]# tar xvzf maildrop-1.6.3.tar.gz
[root@linux maildrop-1.6.3]# cd maildrop-1.6.3
[root@linux maildrop-1.6.3]# ./configure --prefix=/usr/local --exec-prefix=/usr/local --enable-maildrop-uid=root --enable-maildrop-gid=vchkpw --enable-maildirquota
[root@linux maildrop-1.6.3]# make && make install-strip && make install-man

Instalación de qmailadmin

Qmailadmin nos brindará funcionalidades para crear mailbox, alias, forwards, listas de correo, etc. Para instalarlo ejecutemos:

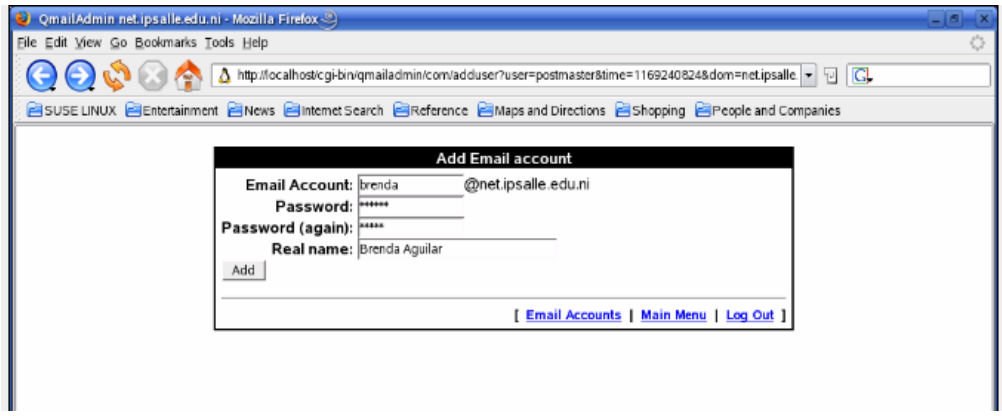
[root@linux maildrop-1.6.3]# cd /downloads/qmailrocks
[root@linux qmailadmin-1.2.3]# tar xvzf qmailadmin-1.2.3.tar.gz
[root@linux qmailadmin-1.2.3]# cd qmailadmin-1.2.3
[root@linux qmailadmin-1.2.3]# ./configure --enable-cgibindir=/srv/www/cgi-bin -enable-htmldir=/srv/www/htdocs
[root@linux qmailadmin-1.2.3]# make && make install-strip

Con esto ya contamos con Qmailadmin en nuestro sistema, a continuación teclee el url **http://localhost/cgi-bin/qmailadmin** en su navegador web, para logearse ingrese el dominio virtual que tendrá que haber creado previamente con vqadmin.

Y nos mostrara la siguiente ventana de autenticación para entrar al sistema., aquí se crean todas las cuentas de correo para los usuarios del qmail. La cuenta para ingresar será postmaster@net.ipsalle.edu.ni y la contraseña respectiva a este.

Luego de autenticar al postmaster nos desplegara una ventana en donde se crean todas las cuentas con el nombre del usuario más su respectivo dominio.

A continuación un ejemplo de cómo se crean las cuentas de los usuarios en qmailadmin.



Ajustes en la Configuración de Qmail

Previo a los ajustes finales de qmail y de su puesta a punto, es necesario desinstalar el MTA por defecto para Suse *(postfix)*.

Lo primero que harémos será ejecutar un script, éste se encargará de crear y otorgar los permisos necesarios a los ficheros supervise y luego ejecutarlo*:*
[root@linux qmailadmin-1.2.3]# cd downloads/qmailrocks/scripts/finalize/linux/
[root@linux linux]# ./finalize_linux.script

Ahora editaremos el fichero '/var/qmail/supervise/qmail-pop3d/run' e ingresamos el nombre de nuestro servidor de correo:
#!/bin/sh
exec tcpserver -H -R -v -c100 0 110 qmail-popup **net.ipsalle.edu.ni** \

Igualmente establecemos el fqdn de nuestro servidor en el fichero '/var/qmail/supervise/qmail-smtpd/run'*:*
#!/bin/sh
/var/qmail/bin/qmail-smtpd **net.ipsalle.edu.ni** \

A continuación, mataremos todos los procesos en ejecución de qmail:
[root@linux linux]# qmailctl stop
Stopping qmail...
qmail-smtpd
qmail-send
qmail-pop3d
[root@linux linux]#

Permitimos al localhost hacer relay en el servidor:
[root@linux linux]# echo '127.:allow,RELAYCLIENT="" >> /etc/tcp.smtp
[root@linux linux]# qmailctl cdb

Ahora creáremos los alias del sistema, estos le dirán a qmail que hacer con los correos comunes, nosotros definiremos al usuario 'brisa' (previamente creado con el comando 'useradd'*)* como administrador del sistema y del correo:

[root@linux linux]# echo brisa > /var/qmail/alias/.qmail-root
[root@linux linux]# echo brisa > /var/qmail/alias/.qmail-postmaster
[root@linux linux]# echo brisa > /var/qmail/alias/.qmail-mailer-daemon

Hacemos un enlace simbólico y establecemos los permisos adecuados:
[root@linux linux]# ln -s /var/qmail/alias/.qmail-root /var/qmail/alias/.qmail-anonymous
[root@linux linux]# chmod 644 /var/qmail/alias/.qmail*

Desinstalando Sendmail y Postfix

Con todo lo anterior ya realizado correctamente, estamos listos para poner a funcionar el servidor de correo. En este caso solo se desinstala postfix ya que Suse no incorpora Sendmail, sin embargo es necesario colocar un reemplazo de este:

[root@linux linux]# rpm -qa | grep postfix
postfix-2.1.5-5
[root@linux linux]# rpm -e postfix-2.2.5-5

Reemplazando Sendmail
[root@linux linux]# ln -s /var/qmail/bin/sendmail /usr/lib/sendmail
[root@linux linux]# ln -s /var/qmail/bin/sendmail /usr/sbin/sendmail

Inicio y Prueba de qmail
En el conjunto del software qmailrocks se encuentra un script que nos permitirá hacer un test de toda la configuración realizada hasta el momento, para asegurarse que todo se hizo bien se realiza lo siguiente.
[root@linux linux]# /downloads/qmailrocks/scripts/util/qmr_inst_check
Si obtenemos un mensaje de felicitaciones, significa que el servidor esta listo para ponerse en marcha.
[root@linux linux]# qmailctl start
Starting qmail...
Starting qmail-send
Starting qmail-smtpd
Starting qmail-pop3d

[root@linux linux]# qmailctl stat
/service/qmail-send: up (pid 9312) 4 seconds
/service/qmail-send/log: up (pid 9313) 4 seconds
/service/qmail-smtpd: up (pid 9314) 4 seconds
/service/qmail-smtpd/log: up (pid 9316) 4 seconds
/service/qmail-pop3d: up (pid 9315) 4 seconds
/service/qmail-pop3d/log: up (pid 9322) 4 seconds
messages in queue: 0
messages in queue but not yet preprocessed: 0
[root@linux linux]#
Ahora comprobamos que cada uno de los servicios esté escuchando el puerto que debe escuchar, utilizáremos la cuenta *'brisa' (*Cuenta virtual, creada con el

comando 'useradd'*)* previamente creada a través de vqadmin*.* Y agregamos user y pass.
Useradd brisa
Passwd brisa brisa

Prueba del pop3
[root@linux linux]# telnet localhost 110
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
+OK 9381.1118336482@net.ipsalle.edu.ni
user brisa@net.ipsalle.edu.ni
+OK
pass brisa
+OK
quit
+OK
Connection closed by foreign host.

Se comprueba el servicio smtp para cerciorarnos de que TLS esta funcionando bien:
[root@linux linux]# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
220 net.ipsalle.edu.ni ESMTP
ehlo localhost
250-linux.regacad.unanleon.edu.ni
250-AUTH LOGIN CRAM-MD5 PLAIN
250-AUTH=LOGIN CRAM-MD5 PLAIN
250-STARTTLS
250-PIPELINING
250 8BITMIME
starttls
220 ready for tls
quit
quit
Connection closed by foreign host.
[root@linux linux]#

Instalando Courier IMAP e IMAP SSL

Ya se cuenta con el servicio qmail, ahora agregamos algunos complementos que brindarán mayor seguridad, vamos a instalar courier-imap/imaps y courierpassd*.* También instalaremos Courier-authlib para permitir autenticación a través de *Courier-imap.* Con la instalación de IMAP no solo permitiremos conexiones IMAP al servidor de correo, sino que también será importante para el funcionamiento del webmail *(*squirrelmail*),* además facilita el manejo de las

cuentas virtuales a través de *vpopmai*l. Con couierpassd incorporamos una funcionalidad para cambio de contraseñas de los usuarios remotamente.

Empezamos instalando el *Courier-Authlib*:
[root@linux qmailrocks]# cd /downloads/qmailrocks
[root@linux qmailrocks]# tar jxvf courier-authlib-0.55.tar.bz2
[root@linux qmailrocks]# cd courier-authlib-0.55
[root@linux courier-authlib-0.55]# ./configure --prefix=/usr/local --exec-prefix=/usr/local --with-authvchkpw --without-authldap --without-authmysql --disable-root-check --with-ssl --with-authchangepwdir=/usr/local/libexec/authlib
[root@linux courier-authlib-0.55]# make && make check
[root@linux courier-authlib-0.55]# make install-strip && make install-configure

Agregamos el demonio authdaemon al fichero '/etc/init.d/boot.local' para que se ejecute siempre al inicio:
[root@linux courier-authlib-0.55]# vi /etc/init.d/boot.local
Agregamos la siguiente linea
/usr/local/sbin/authdaemond start
La compilación del IMAP debe ser realizada por un usuario no-root, en esta guía utilizamos al usuario *'*brisa'*:*

[root@linux courier-authlib-0.55]# cd /downloads/qmailrocks
[root@linux qmailrocks]# tar jxvf courier-imap-4.0.2.tar.bz2
[root@linux qmailrocks]# chown -R brisa:wheel courier-imap-4.0.2
[root@linux qmailrocks]#cd courier-imap-4.0.2
[root@linux courier-imap-4.0.2]#su brisa

[brisa@linux courier-imap-4.0.2]$ ./configure --prefix=/usr/local --exec-prefix=/usr/local --with-authvchkpw --without-authldap --without-authmysql --disable-root-check --with-ssl --with-authchangepwdir=/usr/local/libexec/authlib
[brisa@linux courier-imap-4.0.2]$ make && make check

Ahora abandone el usuario root y ejecute:
[brisa@linux courier-imap-4.0.2]$ exit
[root@linux courier-imap-4.0.2]# make install-strip && make install-configure

El servidor IMAP-SSL también necesita tener un certificado SSL. El comando siguiente, iniciara un proceso automático que generara un certificado firmado por nosotros mismos bajo X.509 impad.pem.
[root@linux courier-imap-4.0.2]# /usr/local/sbin/mkimapdcert

Modificamos la línea mostrada en la *figura 39* en el fichero '/usr/local/etc/imapd.cnf', el valor que pondremos será el de la cuenta de administrador postmaster definida anteriormente.
emailAddress=brisa@net.ipsalle.edu.ni

Asegúrese de que el fichero '/usr/local/etc/imapd-ssl' tenga la variable "IMAPDSTART=YES", y en el *'/usr/local/etc/imapd-ssl'* exista la configuración

“IMAPDSSLSTART=YES”, también debe estar definida la variable “TLS_CERTIFILE=/usr/local/share/imapd.pem” en este mismo fichero.

En el archivo '/usr/local/etc/authlib/authdaemonrc' debe de aparecer la siguiente línea:
authmodulelist="authvchkpw"

Ahora copiamos los scripts de inicio para los demonios imap e imaps:
[root@linux courier-imap-4.0.2]# cp /usr/local/libexec/imapd.rc /etc/init.d/imap
[root@linux courier-imap-4.0.2]# cp /usr/local/libexec/imapd-ssl.rc /etc/init.d/imaps

Y levantamos cada uno de los servicios, antes nos aseguramos de que todo este detenido:
[root@linux courier-imap-4.0.2]# /usr/local/sbin/authdaemond stop
[root@linux courier-imap-4.0.2]# /etc/init.d/imap stop
[root@linux courier-imap-4.0.2]# /etc/init.d/imaps stop
[root@linux courier-imap-4.0.2]# /usr/local/sbin/authdaemond start
[root@linux courier-imap-4.0.2]# /etc/init.d/imap start
[root@linux courier-imap-4.0.2]# /etc/init.d/imaps start

Ejecute ′nmap localhost′ para asegúrese de que los puertos 143 y 993 estén abiertos y escuchando.

Realizamos un test a través del comando *'telnet'*, empezamos con el puerto 143, el texto en negrilla son los comandos que nosotros tecleamos.

[root@linux courier-imap-4.0.2]# telnet localhost 143
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION STARTTLS] Courier-IMAP ready. Copyright 1998-2005 Double Precision, Inc. See COPYING for distribution information.
a login brisa@net.ipsalle.edu.ni brisa
a OK LOGIN Ok.
a logout
* BYE Courier-IMAP server shutting down
a OK LOGOUT completed
Connection closed by foreign host.
[root@linux courier-imap-4.0.2]#

La prueba del Puerto 993 se hará con un cliente de correo Web (Squirrelmail).
Ahora que ya tenemos instalado el Courier-imap podemos instalar el *Courierpassd,* recuerde que el *Courierpassd* le permitirá cambiar la contraseña a los usuarios desde su correo Web.

Courierpassd requiere que el puerto 106 este abierto para el tráfico local, para su instalación siga los pasos siguientes.

```
[root@linux courier-imap-4.0.2]# cd /downloads/qmailrocks
[root@linux courierpassd-1.1.0-RC1]# tar xvzf courierpassd-1.1.0-RC1.tar.gz
[root@linux courierpassd-1.1.0-RC1]# cd courierpassd-1.1.0-RC1
[root@linux courierpassd-1.1.0-RC1]# ./configure
[root@linux courierpassd-1.1.0-RC1]# make && make install
```

Courierpassd corre bajo Xinetd, por lo que tendremos que crear el siguiente fichero y agregarlo al directorio '/etc/xinetd.d'

```
[root@linux courierpassd-1.1.0-RC1]# vi /etc/xinetd.d/courierpassd
service courierpassd
{
port = 106
socket_type = stream
protocol = tcp
user = root
server = /usr/local/sbin/courierpassd
server_args = -s imap
wait = no
only_from = 127.0.0.1
instances = 4
disable = no
}
```

Posteriormente agregar la línea mostrada en la siguiente figura en el fichero de configuración de Xinetd

```
[root@linux courierpassd-1.1.0-RC1]# vi /etc/xinetd.conf

## Agregamos la siguiente linea al final fichero /etc/xinetd.conf
courierpassd stream tcp nowait root /usr/local/sbin/courierpassd -s imap
```

Ahora agregamos el servicio Courierpassd al archivo de sistema *'/etc/services'*:

```
[root@linux courierpassd-1.1.0-RC1]# vi /etc/services
## Esta línea manejara el servicio Courierpassd
courierpassd    106/tcp
```

Reiniciamos el demonio de Xinetd:

```
[root@linux courierpassd-1.1.0-RC1]# /etc/init.d/xinetd restart
```

Finalmente hacemos el respectivo test para el servicio courierpassd.

```
[root@linux courierpassd-1.1.0-RC1]# telnet localhost 106
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).

Escape character is '^]'.
```

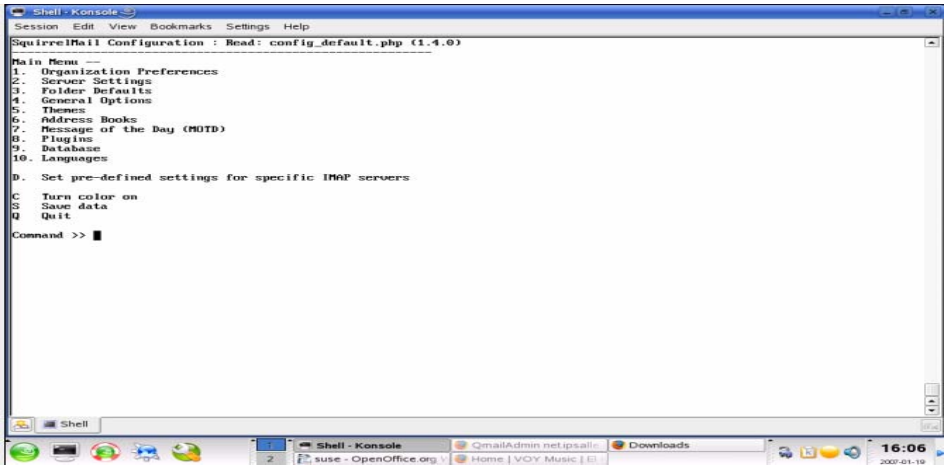
200 courierpassd v1.1.0-RC1 hello, who are you?
user brisa@ net.ipsalle.edu.ni
200 Your password please.
pass brisa
200 Your new password please.
newpass brisa
200 Password changed, thank-you.
quit
200 Bye.
Connection closed by foreign host.
[root@linux courierpassd-1.1.0-RC1]
Si el sistema responde igual a lo mostrado en la figura anterior significa que *Courierpassd* esta trabajando correctamente.

Instalación de SquirrelMail
Ahora que tenemos Qmail trabajando con IMAP podemos instalar Squirrelmail para manejar el correo vía Web. Antes de su instalación hay que cerciorarse que tiene funcionando correctamente el modulo de PHP con el servidor Web Apache y Mysql.

La siguiente figura indica de manera sencilla los pasos para descargar e instalar Squirrelmail.
[root@linux courierpassd-1.1.0-RC1]# cd /srv/www/htdocs
[root@linuxhtdocs]#wgethttp://superbwest.dl.sourceforge.net/sourceforge/squirrelmail/squirrelmail-1.4.7.tar.gz
[root@linux htdocs]# tar xvzf squirrelmail-1.4.7.tar.gz

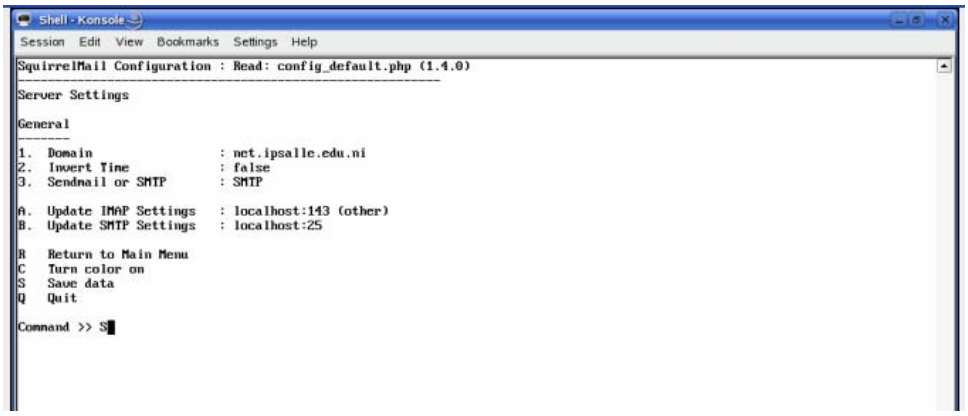
[root@linux htdocs s]# mv squirrelmail-1.4.7 webmail
[root@linux htdocs]# cd webmail
[root@linux webmail]# mkdir /var/sqattachements
[root@linux webmail]# chown -R wwwrun: /var/sqattachements/
[root@linux webmail]# chown -R wwwrun: data/

[root@linux webmail]# cd config
[root@linux config]# ./conf.pl
Una de las características mas importantes de Squirrelmail es la gran cantidad de plugins con que cuenta, estos pueden ser descargados desde su sitio oficial (www.squirrelmail.org) y cargados a través del menú de configuración mostrado al ejecutar el comando '/var/www/htdocs/webmail/config/conf.pl'.



Para cambiar el idioma debe de bajar los paquetes extras desde: http://sourceforge.net/project/showfiles.php?group_id=311.

Dentro de las opciones nos muestra la configuración squirrelmail.



El correo Web lo utilizaremos mediante un dominio virtual 'net.ipsalle.edu.ni'. Solo nos queda abrir nuestro navegador y logearnos con alguna cuenta, claro esta que antes debemos darla de alta.

X. Conclusiones

Hemos cumplido con los objetivos propuestos de configurar un servidor DNS y los Servicios Básicos de Red para la Intranet del Instituto Politécnico la Salle de León, y además dejar una documentación amplia de nuestro trabajo que sirva como guía para otros proyectos Monográficos o prácticos dentro y fuera del instituto.

Este trabajo se llevo a cabo como un Dominio Interno de ipsalle.edu.ni, al que llamamos net.ipsalle.edu.ni que funcionara como servidor principal de intranet dentro del instituto o donde se desee tener ya que funciona igual para cualquier institución u universidad.

XI. Recomendaciones

Luego de haber concluido nuestro trabajo, y de analizar la mejor manera de administrar nuestro servidor podemos dar las siguientes recomendaciones:

- El DNS administrado por el Alfanuméric (ISP), sea administrado por el Personal Instituto Politécnico La Salle.

- El Servidor DNS y Apache deben estar en un mismo PC.

- El Correo debe estar separado en un solo PC debido a que el necesita mayor espacio en disco por la cantidad de cuentas de usuario que hay que crear y por seguridad.

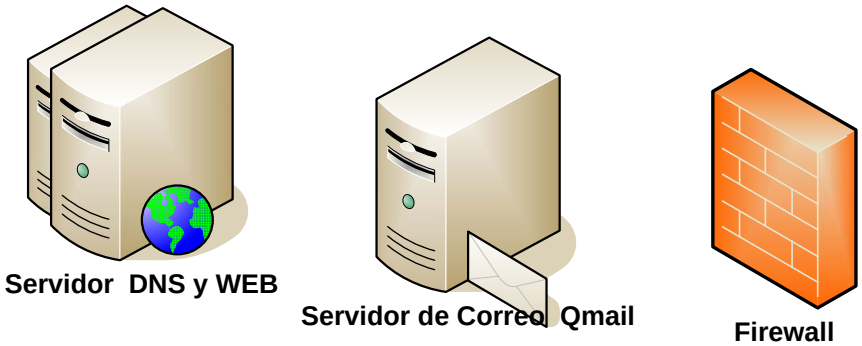
- Debe existir un Hardware Antispam para mayor protección de los servicios de la Intranet, especialmente para el Servidor de Correo Qmail.

- Debe existir un firewall ya sea software o hardware para la protección de los servidores, así como se demuestra en el diagrama idóneo para una red.

Debido a que no tenemos un IP publica, el correo que enviamos a correos con dominios distintos como por ejemplo: yahoo.com, hotmail.com, entre otros no puede ser reenviado hacia nuestro dominio, es decir que todas las direcciones IP de la red local son privadas y no corresponden a direcciones IP reales, globalmente localizables, así que sin enmascaramiento no podrían emplear Internet.

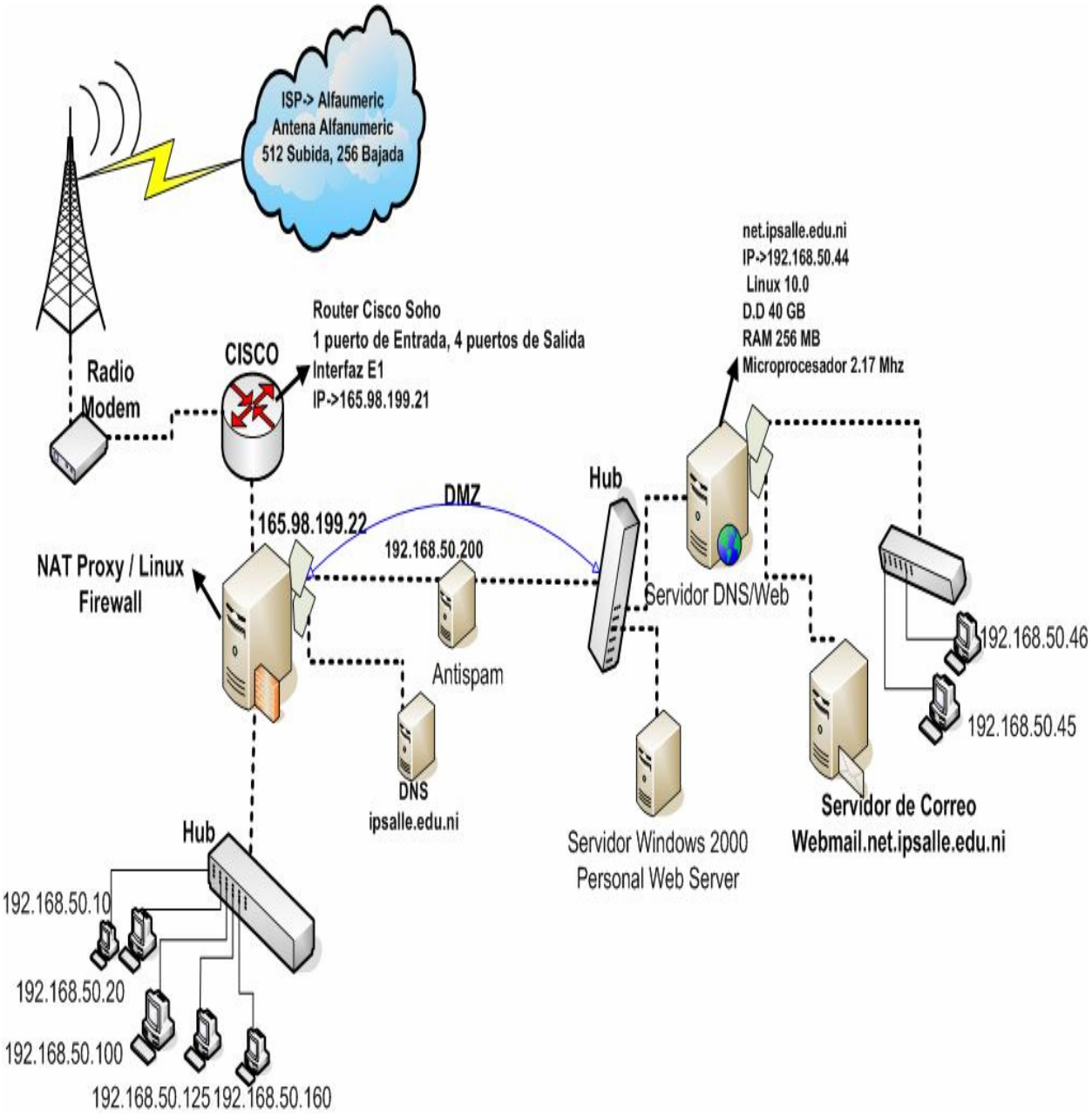
Al emplear enmascaramiento las conexiones iniciadas en un computador de la red privada pasarán por el servidor, el cual cambiará la dirección del computador que inicia la conexión por la del mismo servidor y reenviará la información a Internet.

De esta forma el computador que conteste en Internet responderá al servidor, el cual podrá ajustar la dirección de la información que reciba para que llegue al computador dentro de la Intranet.
También se puede hacer este enmascaramiento desde el Firewall con la misma funcionalidad que la anterior.



ANEXOS

Diagrama Idóneo de Seguridad de la Red para la Intranet



GLOSARIO

ALIAS: Nombre usualmente corto y fácil de recordar que se utiliza en lugar de otro nombre usualmente largo y difícil de recordar.

BIND: (Berkeley Internet Name Daemon): Demonio de Nombres Internet de Berkeley. Este contiene el archivo de configuración named que es el demonio del servidor.

Cliente: Cualquier elemento de un sistema de información que requiere un servicio mediante el envío de solicitudes al servidor.

CGI: Acrónimo de Common Getaway Interface. Interface Común de Pasarela. Interface de intercambio de datos estándar en WWW a través del cual se organiza el envío de recepción de datos entre visualizadores y programas residentes en servidores WWW.

CACHE: Un caché es un sistema especial de almacenamiento de alta velocidad. Puede ser tanto un área reservada de la memoria principal como un dispositivo de almacenamiento de alta velocidad independiente. Hay dos tipos de caché frecuentemente usados en los ordenadores personales: memoria caché y caché de disco.

DNS: Acrónimo de Domain Name System. Sistema de Nombres de Dominio. El DNS un servicio de búsqueda de datos de uso general, distribuido y multiplicado. Su utilidad principal es la búsqueda de direcciones IP de sistemas centrales ("hosts") basándose en los nombres de estos.

DOS: Un sistema operativo para PC, monousuario y monotarea, del que deriva el Windows 95 y sucesivos. Existen versiones distintas del DOS.

DHCP: Acrónimo de Dynamíc Host Confíguration Protocol. Protocolo de configuración dinámica de host. Protocolo que usan los ordenadores para obtener información de configuración.

E-mail: Electronic Mail. Correo electrónico. Sistema mediante el cual un ordenador puede intercambiar mensajes con otros usuarios de ordenadores (o grupos de usuarios) mediante redes de comunicación.

Encriptación: Cifrado. Técnica por la que la información se hace ilegible para terceras personas. Proteger archivos expresando su contenido en un lenguaje cifrado. Los lenguajes cifrados simples consisten, por ejemplo, en la sustitución de letras por números.

Enrutador: Bloque de construcción básico de una interred. Un enrutador es un ordenador que se conecta a dos o más redes y reenvía paquetes de acuerdo con la información encontrada en su tabla de enrutamiento. Los enrutadores de la Ethernet ejecutan el protocolo IP.

Ethernet: nombre de una tecnología de área local que definen las características de cableado y señalización del nivel físico y los formatos de tramas de nivel de datos del modelo OSI.

FireWall: Cortafuegos. Mecanismo de seguridad que impide el acceso a una red.
La regla básica es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autentificación, etc.

GNU: Licencia Publica General. Software desarrollado para distribución sin fines de lucro. El proyecto GNU (GNU es un Acrónimo recursivo para "Gnu No es Unix") comenzó en 1984 para desarrollar un sistema operativo tipo Unix completo, que fuera Software Libre.

Consiste en una serie de pequeños subproyectos mantenidos por voluntarios o corporaciones, normalmente con el objetivo de crear o mantener un componente funcional.

GNU/GPL: licencia publica general, creada por la free software foundation y orientada principalmente a los términos de distribución, modificación y uso de software. Su propósito es declarar que el software cubierto por esta licencia es software libre.

Hub: Dispositivo que integra distintas clases de cables y arquitecturas o tipos de redes de área local. Existe una palabra castellana para identificar un Hub, Concentrador.

IMAP: (Internet Message Access Protocol) Protocolo de Acceso a Mensajes de Internet. Protocolo diseñado para leer correo electrónico almacenado en un servidor.

El modo habitual de gestionar el correo electrónico mediante este protocolo mantiene los mensajes en el ordenador servidor. Además permite la creación de carpetas en el propio servidor donde se pueden ordenar los mensajes enviados y recibidos.

LINUX: Un sistema operativo multiusuario y multitarea basado en UNIX.

Lan: Acrónimo de Local Area Network. Red de área local. El término LAN define la conexión física y lógica de ordenadores en un entorno generalmente de oficina. Su objetivo es compartir recursos (como acceder a una misma impresora o base de datos) y permite el intercambio de ficheros entre los ordenadores que componen la red.

MTA: Acrónimo de Mail Transfer Agent. Agente de transferencia de correo.

MUA: Acrónimo de Mail User Agent. Agente de usuario de correo.

MDA: Acrónimo de Mail Delivery Agent. Agente de entrega de correo.

MIME : Acrónimo de Multipurpose Internet Mail Extensions. Es un protocolo que no especifica los mecanismos de transmisión o recepción de la información, sino la codificación y formato de los contenidos de los mensajes.

MYSQL: El software MySQL proporciona un servidor de base de datos SQL (Structured Query Language) veloz, multi-hilo, multiusuario y robusto.

El servidor esta proyectado tanto para sistemas críticos en producción soportando intensas cargas de trabajo como para empotrarse en sistemas de desarrollo masivo de software.

OpenSSL: es una implementación libre, de código abierto, de los protocolos SSL (Secure Sockets Layer o Nivel de Zócalo Seguro).

Plataforma: El fundamento tecnológico de un sistema de cómputo. En general, una combinación específica de equipo de cómputo (hardware) y sistema operativo.

Plataforma tecnológica: Acervo de tecnología de la información con que cuenta una organización. Comprende todo el equipo de cómputo (hardware), programas (software), bases de datos, personales y políticas que sustentan la política de las acciones en materia de administración de sistemas de información.

POP: Acrónimo de Post Office Protocol. Protocolo de Oficina de Correos. Protocolo diseñado para permitir a sistemas de usuario individual leer correo electrónico almacenado en un servidor.

PERL: Lenguaje de programación muy utilizado para la elaboración de aplicaciones CGI. Es multiplataforma y funciona bajo UNIX.

Ping: Es un comando que se usa para comprobar si hay señal al momento de conectar el servidor al cliente.

Red: En tecnología de la información, una red es un conjunto de dos o más ordenadores interconectados.

Servidor: Ordenador central de un sistema de red que provee servicios y programas a otros ordenadores conectados.

Servidor de correo: es una aplicación que nos permite enviar mensajes (correos) de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando.

Servicios de red: Son todas las prestaciones que ofrece el sistema operativo para la configuración de los servicios más importantes para la comunicación, emisión y recepción de información (ftp, http, dns.).

TLS: (Transport Layer Security, o Seguridad para Nivel de Transporte), Está basado sobre el extinto proyecto SSLeay, iniciado por Eric Young y Tim Hudson, hasta que éstos comenzaron a trabajar para la división de seguridad de EMC Corporation

Topología: Se refiere a la forma en la cual están interconectados físicamente los nodos.
Firewall: combinaciones de hardware y software que sólo permiten a ciertas personas acceder a ella para propósitos específicos

UNIX: un sistema operativo multiusuario y multitarea.