ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TITULO DE INGENIERÍA

"DISEÑO Y GESTIÓN DE SERVICIOS DE COMUNICACIÓN BAJO PLATAFORMA LINUX PARA LA SUPERINTENDENCIA DE BANCOS Y SEGUROS"

Patricio Xavier Zambrano Rodríguez

SANGOLQUÍ – ECUADOR

2006

CERTIFICACIÓN

Certificamos que el Señor PATRICIO XAVIER ZAMBRANO RODRIGUEZ con cédula de identidad 171694296-4, ha culminado con éxito el Proyecto de Grado para la obtención del título en Ingeniería Electrónica.

El tema de grado titulado "**Diseño y Gestión de Servicios de Comunicación bajo plataforma Linux para la Superintendencia de Bancos y Seguros**" ha sido elaborado bajo nuestra dirección y ha cumplido con todas las expectativas.

_____	_____
Ing. Ramiro Ríos	**Ing. Alejandro Castro**
DIRECTOR	**CODIRECTOR**

RESUMEN

El presente proyecto "**Diseño y Gestión de Servicios de Comunicación bajo plataforma Linux para la Superintendencia de Bancos y Seguros**", pretende implementar a futuro, servicios de comunicación VPN LAN-to-LAN y Acceso remoto VPN bajo plataforma Linux, como respaldo a las vías de comunicación que posee actualmente la Entidad (Enlaces Clear Channel y Acceso Remoto VPN - RAS).

Para poner en producción la propuesta de Backup VPN y fortalecer la migración de plataforma Windows a Linux, como primera etapa se migraron los servicios DHCP y DNS que proporcionaba Windows NT Server a Red Hat Enterprise Linux 4AS. Adicionalmente el servidor provee monitoreo de los servicios de comunicación y recursos del sistema vía HTTPS, manifestando así aspectos de seguridad.

Como refuerzo a las seguridades Institucionales se configuró un FIREWALL (IPTABLES) que proporciona accesos exclusivos a funcionarios administradores y remotos a la Red Institucional, sin interferir con los servicios de comunicación de carácter público (DNS) y privado (DHCP).

Se determina finalmente que la migración de plataforma es totalmente factible en la Superintendencia de Bancos y Seguros, pues se ha observado en el desarrollo del proyecto: soporte VPN, estabilidad y compatibilidad de la plataforma, con el entorno en que se desenvuelven las comunicaciones actualmente.

DEDICATORIA

Dedico el presente proyecto de grado a Dios y a mis padres, que pusieron toda su confianza en mí, desde el inicio de la carrera hasta su culminación. A todos mis amigos con quienes compartí diferentes experiencias y me brindaron su apoyo para sobrellevar esta dura tarea.

Patricio Xavier Zambrano Rodríguez

AGRADECIMIENTO

Mi agradecimiento va dirigido a los directivos y personal de la Dirección Nacional de Recursos Tecnológicos, de la Superintendencia de Bancos y Seguros, por el apoyo incondicional desde el inicio hasta la exitosa culminación del proyecto de Tesis.

Un especial agradecimiento a mis padres por su apoyo incondicional, por el ejemplo de lucha diaria que me motiva a superarme día tras día.

Adicionalmente un sincero agradecimiento a todos los profesores de la Escuela Politécnica del Ejército por brindarme sus conocimientos, especialmente al Ingeniero Ramiro Ríos, que por su exigencia como docente, me motivó a elevar mi nivel de exigencia profesional.

Patricio Xavier Zambrano Rodríguez

PRÓLOGO

La Superintendencia de Bancos y Seguros como organismo de control posee constante comunicación con sus Intendencias Regionales por medio de enlaces dedicados Clear Channel y con Funcionarios auditores, directores y administradores de la Red vía Acceso Remoto VPN. Esta tecnología WAN y el acceso remoto VPN vía RAS, provee seguridad a la información, pero en caso no contemplado, llegaran a caer los enlaces o el servidor de acceso remoto VPN, entraría en funcionamiento la propuesta tecnológica de Backup VPN, arquitecturas LAN-to-LAN y Acceso remoto VPN, bajo plataforma Linux.

La arquitectura Acceso Remoto VPN, implementada en la SBS, actualmente, permite el acceso a la Red Institucional exclusivamente vía RAS. La propuesta tecnológica de Backup de esta arquitectura se fundamenta en el procedimiento que sigue un funcionario al ingresar a la Institución (RAS-VPN) y el cliente VPN del sistema operativo Windows XP (L2TP/IPsec). Adicionalmente esta propuesta no contempla únicamente el acceso a la Red Institucional por medio del servidor RAS, sino también desde la Red Pública como el Internet. Estos servicios de comunicación bajo plataforma Linux (VPN) brindan, todas las normas de seguridad (encriptación y entunelamiento) que la información requiere.

Para poner en producción estos servicios de Backup y fortalecer la migración de plataforma Windows a Linux en la SBS, como primera etapa se estableció migrar los servicios de DNS y DHCP proporcionados por un servidor Windows NT a plataforma Linux, en base de los actuales procedimientos de comunicaciones, destacando las características técnicas que debe poseer esta plataforma para su adecuada configuración. Llegando a determinar, en la culminación del proyecto, la factibilidad de la migración de plataforma en base a las configuraciones planteadas en el proyecto y el desempeño de sus servicios de comunicación.

ÍNDICE

CONTENIDO…….……...…PAG.

CAPITULO I

INTRODUCCIÓN

CAPITULO II

EVALUACIÓN DE LA SITUACIÓN ACTUAL DE LA RED Y SERVICIOS DE COMUNICACIÓN DE LA SUPERINTENDENCIA DE BANCOS Y SEGUROS (SBS)

CAPITULO III

FUNDAMENTO TEÓRICO DE LOS SERVICIOS DE COMUNICACIÓN CORRESPONDIENTES A LA PROPUESTA TECNOLÓGICA DE BACKUP

CAPITULO IV

DISEÑO Y CONFIGURACIÓN DE LOS SERVICIOS DE COMUNICACIÓN PARA LA PROPUESTA TECNOLÓGICA DE BACKUP PARA LA SBS

CONFIGURACIÓN DEL SERVICIO DHCP - LINUX

DISEÑO DEL SERVICIO DNS - LINUX

CONFIGURACIÓN DEL SERVICIO DNS - LINUX
CONFIGURACIÓN DE LOS MONITORES SBS

FIREWALL - IPTABLES SBS

DISEÑO DEL SERVICIO VPN - SBS

CONFIGURACIÓN DEL SERVICIO VPN – SBS
ARQUITECTURA LAN-to-LAN

DISEÑO DEL SERVICIO VPN – SBS
ARQUITECTURA ACCESO REMOTO VPN

CONFIGURACIÓN DEL SERVICIO VPN – SBS
ARQUITECTURA ACCESO REMOTO VPN

ÍNDICE DE FIGURAS

FIGURA……..……...…PAG.

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

ÍNDICE DE TABLAS

TABLA……...…….……...…PAG.

CAPÍTULO III

CAPÍTULO IV

GLOSARIO

LETRA	DESCRIPCIÓN
A	
ACPI	Advanced Configuration and Power Interface
ADSL	Asymmetric Digital Subscriber Line
AH	Authentication Header
APIPA	Automatic Private Internet Protocol Addressing
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
B	
BRI	Basic Rate Interface
BSD	Berkeley Software Distribution
C	
CPE	Customer Premise Equipment
D	
DHCP	Dynamic host configuration protocol
DHCPD	DHCP Daemon
DNS	Domain Name Service
DSL	Digital Subscriber Line
E	
ESP	Encapsulated Security Payload
F	
FQDN	Fully Qualified Domain Name
FSF	Free Software Foundation

FTP File Transfer Protocol

G

GPL General Public License
GTDLS Generic Top Level Domains

H

HTTPD Hypertext Transfer Protocol

I

IANA Internet Assigned Number Authority
IANC International Ad Hoc Committee
IP Internet Protocol
IPSEC Internet Protocol security
ISP Internet Service Provider
ISV Independent Software Vendor
IT Information Technologies
ITU International Telecommunication Union

L

L2TP Layer Two Tunneling Protocol

M

MAC Media Access Control address
MTU Maxim Transfer Unit

N

NAMED Domain Name System server named
NAPS Network Access Point
NFS New File System
NIC Network Interface Card
NIS Network Information Service
NS Name Server
NT New Technologies
NTP Network Time Protocol

P

POP Point of Presence
PPP Point to Point Protocol
PPTP Point to Point Tunneling Protocol
PRI Primary Rate Interface
PVC Permanent Virtual Circuit

R

RAM Random Access Memory
RAS Remote Access Service
RFC Request For Comments
RNS Root Name Server
RR Resource Records
RTPC - PSTN Red de Telefonía Pública Conmutada

S

SMP Symmetric Multiprocessing
SMTP Simple Mail Transfer Protocol
SO Sistema Operativo
SSH Secure Shell
SSL Secure Socket Layer

T

TA Terminal Adapter
TCP Transfer Communication Protocol
TFTP Trivial File Transfer Protocol
TTL Tome To Live

U

UDP User Datagram Protocol

V

VPN Virtual Private Network

CAPITULO I

INTRODUCCIÓN

1.1. ANTECEDENTES

La Superintendencia de Bancos y Seguros ha trabajado con la plataforma Windows NT 4.0 los últimos años para proporcionar servicios de comunicación. El 31 de diciembre del 2004 fue la fecha efectiva de finalización del soporte de incidencias y del soporte de actualizaciones de seguridad para Microsoft Windows NT 4.0.

Este sistema operativo se lanzó en septiembre de 1996. No se diseñó con la seguridad y complejidad del entorno IT (Information Technologies) que se requiere actualmente y ha alcanzado el final de su vida efectiva de soporte.

Microsoft ha ido comunicando este hecho desde septiembre de 2001 con el fin de ayudar a sus clientes a migrar sus aplicaciones e infraestructuras desde Windows NT 4.0 a los actuales sistemas operativos Windows Server.

La Dirección Nacional de Recursos Tecnológicos, consciente de los problemas que pueden presentarse debido a la falta del soporte antes mencionado por parte de Microsoft para Windows NT, ha buscado nuevas alternativas más seguras y menos costosas como por ejemplo Linux, que sin ser invulnerable demuestra estabilidad y permite el desarrollo de ingeniería principalmente en las comunicaciones.

El presente proyecto pretende fomentar la migración del Sistema Operativo Windows a Linux, seleccionando una distribución que se adecue a los requerimientos técnicos de la Entidad. Toda esta migración se dará por etapas, siendo la primera el cambio del Servidor Windows NT Server que proporciona los servicios de comunicaciones **DHCP**

y DNS básicamente a un servidor Linux. Adicionalmente se configurarán **MONITORES** de los servicios y del desempeño del servidor y un **CORTAFUEGOS (FIREWALL-filtro)**. Una vez realizado el respectivo análisis y diseño de los servicios de comunicación a migrar se procederá ha analizar los servicios y las necesidades de comunicaciones existentes de la Superintendencia de Bancos y Seguros (SBS) y de ser necesario, proponer soluciones bajo la misma plataforma, afianzando así el proyecto de migración.

A continuación se realizará una breve reseña histórica de Linux, definición del sistema operativo como tal y de sus distribuciones.

1.2. RESEÑA HISTÓRICA LINUX

El nacimiento del sistema operativo Linux no ha sido fruto de la casualidad, sino todo lo contrario. Es el resultado de varios acontecimientos que han sucedido en diferentes momentos a lo largo de las últimas décadas se puede resumir, principalmente, en:

- **Aparición del sistema operativo.**
- **Punto de partida la FSF.**
- **Funcionamiento del sistema operativo.**

1.2.1. Aparición del sistema operativo. La aparición del sistema operativo UNIX cuya gestación se inicia con los trabajos de Dennis Ritchie, durante los años 70, en los laboratorios de AT&T (American Telephone and Telegraph Corporation). En un principio estaba escrito en lenguaje ensamblador, aceptaba tan solo dos usuarios y recibió el nombre de UNICS. En 1973 se reescribió todo el código en lenguaje C, se amplió el número de usuarios y se le bautizó con el nombre de UNIX. Se distribuyó por universidades de todo el mundo. Una de estas llegó a la Universidad de California en Berkeley la cual participó con muchas innovaciones a través de la BSD (Berkeley Software Distribution). Entre todos, se había construido un sistema operativo robusto y estable caracterizado por realizar los trabajos desglosándolos en múltiples y simples tareas que se ejecutan por separado pero de un modo seguro. En el año 1982 salieron al mercado las diferentes versiones. AIX de IBM, XENIX de Microsoft, UNIX BSD, etc. Unos años más tarde se homologaron todas las

distribuciones bajo el mismo estándar UNIX SYSTEM Versión 4. Su interfaz era únicamente en modo texto (alfanumérica). Como parte de sus deficiencias UNIX era un sistema que necesitaba de unos recursos de hardware muy potentes que estaban sólo al alcance de organizaciones militares, administrativas o académicas.

1.2.2. Punto de partida de la FSF. Nacimiento de la FSF (Free Software Foundation, 1984) con carácter no lucrativo. Su objetivo principal era crear un sistema operativo GNU, que se llamaría UNIX y que sería de libre distribución. Otro éxito de la FSF fue el asentamiento de las bases de un nuevo tipo de licencia para el software. Es la llamada GPL (General Public License), que permite distribuir los programas de modo gratuito siempre que éstos se acompañen con el código fuente correspondiente. Hoy en día los términos GNU y GPL son prácticamente equivalentes.

1.2.3. Funcionamiento del sistema operativo. Un paso decisivo se produce en 1987 a raíz de la necesidad del profesor de Sistemas Operativos, Andrews S. Tanenbaum, tenía para explicar a sus alumnos cómo funciona por dentro un sistema operativo. Al no disponer de suficiente información sobre los sistemas de software propietarios que había, por aquellos años, optó por escribir un sistema operativo muy sencillo publicando, al mismo tiempo, todo el código fuente. Le llamó MINIX por su parecido con UNIX y su sistema de archivos "MINIX" todavía se emplea hoy en día debido a su elevada eficacia, sobre todo, en dispositivos de poca capacidad como disquetes o discos-ram. La idea de Tanembaum le gustó mucho a un estudiante finlandés de informática llamado Linus Torvalds quien tenía en mente crear un sistema operativo como UNIX pero que fuese capaz de adaptarse al hardware de un ordenador personal. Linus, además, tuvo otra buena idea: usar la Internet para dar a conocer su proyecto, bajo licencia GPL (5 de octubre de 1991) desde la Universidad de Helsinki. Comienza así la andadura y el desarrollo de un sistema operativo edificado, desde el primer momento, sobre las necesidades, la creatividad y la participación de sus mismos usuarios.

Desde entonces, el crecimiento, uso y aumento de prestaciones de Linux no se ha detenido gracias al elevado número de desarrolladores, colaboradores altruistas y usuarios de todo el mundo. Se utiliza en empresas, administraciones y usuarios domésticos, ofreciendo una alternativa al software comercial de la competencia. Sin embargo, donde

realmente brilla por sus cualidades es en el sector educativo. Hay multitud de información al respecto. Solo la editorial Prentice Hall tiene más de 100 títulos publicados. En la red existen libros enteros gratuitos, así como gran cantidad de documentación que permite hacer cualquier cosa a cualquier usuario que se lo proponga. Se puede afirmar que, en Linux, no hay nada oculto y que toda la información está a disposición de quien la necesite.

1.3. ¿QUÉ ES LINUX?

En principio se puede asumir que este nombre se reserva para nombrar al núcleo, o kernel, del sistema operativo en sí. El núcleo aparece en la mayor parte de los sistemas como un archivo de nombre vmlinuz que se carga en la memoria RAM del ordenador durante el proceso de arranque bien sea a través de disquete, de CDROM o de disco duro.

El kernel es un programa que "envuelve" al conjunto de los elementos físicos, o hardware, que componen el ordenador, haciendo de intermediario, para que el usuario no tenga que preocuparse demasiado por el funcionamiento de éstos. Se encarga también de planificar la ejecución de los procesos o el uso de los recursos del sistema, supervisar la transmisión de los datos entre aplicaciones y los dispositivos periféricos. Una parte importante del núcleo lo constituyen los controladores de dispositivos, o drivers, que pueden incluirse formando parte del mismo durante el proceso de compilación o bien pueden acompañarlo por separado, como archivos binarios de código objeto, que se cargarán después en memoria sólo aquellos que sean necesarios para controlar un dispositivos físico concreto, lo cual hace que el núcleo sea más pequeño y ligero. Como es de esperar, los controladores, deben compilarse al mismo tiempo que el núcleo sobre el que luego funcionarán.

Una particularidad del kernel es la posibilidad de que cualquier usuario pueda utilizar el código fuente escrito en lenguaje C y compilarlo en su mismo ordenador introduciendo las modificaciones que estime necesarias para un uso personalizado. En efecto, durante el proceso de compilación, se pueden seleccionar gran número de opciones, de un modo muy sencillo, a través de un menú gráfico, o en modo texto, y sin necesidad de tener

conocimientos avanzados de programación. Esto permite obtener núcleos de tamaño muy variado, desde los más pequeños de unos 600 MB hasta otros mayores de 1300 MB, y lo que es más importante, ajustados a las exigencias de cada usuario.

El kernel aunque parezca extraño solo no sirve para nada. El primer elemento que resulta imprescindible es el intérprete de comandos, que es otro archivo independiente del núcleo. Recibe el nombre de shell porque actúa como una coraza que envuelve al núcleo. Es una interfaz que permite al usuario comunicarse con el sistema operativo. Al igual que en UNIX, en Linux, hay disponibles varios shell's. El más usual es el bash que es GNU. Utilizando el shell pueden realizarse programas bastante completos que se llaman guiones (scripts). Las órdenes que acepta el shell, a través de la línea de comandos, están básicamente formadas por el nombre de la orden, uno o varios modificadores precedidos por un guión y uno o varios argumentos, por ejemplo, nombres de archivos o directorios. Estos campos deberán ir siempre separados por un espacio.

1.4. ESPECIFICACIONES TÉCNICAS DE LINUX

Resumiendo las principales especificaciones técnicas de Linux, como sistema operativo, se puede decir que es:

1.4.1. Multiusuario. Varios usuarios, bajo la supervisión de un sólo S O, comparten al mismo tiempo todos los recursos del ordenador, microprocesador, RAM, discos, impresora, etc (siempre que cada uno tenga su propio terminal formado por pantalla y teclado).

1.4.2. Multitarea real. Cada uno de los posibles usuarios conectados al sistema, puede ejecutar, a su vez, varios trabajos al mismo tiempo. A mayor número de procesos iniciados, más tardarán en completarse, pero se terminarán bien.

1.4.3. Multiplataforma. Al estar escrito en lenguaje C, se puede compilar para diferentes arquitecturas, por ejemplo: Intel, Motorola, Alpha, Sparc, etc. La versión 3.0 de Linux Debian soporta hasta 11 plataformas distintas.

1.4.4. Multiprocesador. Puede funcionar en ordenadores que tengan una placa base con más de un procesador. Admite arquitecturas de 32 y 64 bits.

1.4.5. Servidor de red. Puede gestionar el acceso y el uso de los recursos compartidos de una red local compuesta por otras máquinas sean Linux o no. Dispone de los servicios necesarios para trabajar con redes externas, como router, prestar servicios de seguridad, o firewall, servidor ftp, etc. Es un sistema orientado hacia las redes.

1.4.6. Interfaz alfanumérica. Sin duda alguna es el sistema operativo más potente en lo que a interfaz en línea de comandos se refiere. Además, puede utilizar interfaz gráfica, llamada X-Windows, sobre la cual podemos instalar dos tipos de escritorios diferentes a elegir: el KDE o el GNOME, ambos tan funcionales e intuitivos como los de los sistemas operativos de la competencia.

1.4.7. Estabilidad y seguridad. Una vez instalado, y correctamente configurado, es el sistema más estable y seguro, característica que comparte junto con su antecesor UNIX.

1.5. ¿QUÉ ES UNA DISTRIBUCIÓN DE LINUX?

Aunque se le suele llamar Linux, palabra reservada para nombrar su núcleo, lo que realmente tenemos instalado en nuestro ordenador es una distribución Linux y, a veces, algunas cosas más. En líneas generales y dada la estructura altamente modularizada de este sistema operativo, podemos decir que una distribución es como un rompecabezas, con mayor o menor número de piezas que encajan perfectamente y entre las que podemos encontrar:

- El kernel o núcleo del sistema operativo.
- Utilidades básicas.
- Controladores de dispositivos.
- Asistentes para facilitar la instalación.
- Aplicaciones.
- Fuentes.

- Documentación.
- Asistencia.
- Coste bajo o nulo.

1.5.1. El kernel o núcleo del sistema operativo. Es imprescindible y viene en todas las distribuciones. Por ejemplo el vmlinuz 2.4.18-4GB de SuSE o el vmlinuz 2.4.18-bf2.4 de Debian.

1.5.2. Las utilidades básicas. Forman un conjunto de herramientas que acompañan al núcleo y permiten realizar las tareas de instalación, administración, reparación, seguridad, etc. Por ejemplo, intérprete de comandos (bash), particionador de disco (fdisk), formato, creación y comprobación de sistemas de archivos (fdformat, mkfs, fsck), gestión de archivos y directorios (mkdir, cp, ls), compresión y descompresión, (gzip, bzip2, gunzip) empaquetado, desempaquetado y copia (cpio, tar, dd), editores de texto sin formato (vi, emacs, nano, pico), filtros (sed, grep), gestores de arranque (lilo, grub), etc.

1.5.3. Controladores de dispositivos. Muchos forman parte del núcleo. Otros, en cambio, se entregan como programas en formato binario con la particularidad de terminar con la extensión .o (de objeto). Ejemplos: rtl8139.o para la tarjeta de red de Realtek, nv.o para una tarjeta gráfica de Nvidia, bttv.o para una tarjeta sintonizadora con el chip BT878, ac97.o para tarjetas de sonido, etc.

1.5.4. Asistentes para facilitar la instalación. La detección del hardware y el ajuste de los parámetros de los diferentes dispositivos, dependen de cada distribución y pueden ser de tipo gráfico o en línea de comandos, libres o no. Por ejemplo es muy conocido el YaST2 de SUSE (no GNU) y el DrakeX de Mandrake, ambos gráficos, o el apt de Debian (GNU) en modo texto.

1.5.5. Aplicaciones. En general es muy variable el número de programas y de paquetes de aplicaciones que entrega cada distribución. La gran mayoría son GNU, pero también pueden no serlo. Es muy conocido el entorno ofimático OpenOffice de Sun, el navegador

Mozilla (el Nestcape de Linux), el editor de imágenes Gimp, el reproductor de audio en todos los formatos Xmms, el visor de televisión xatw, etc.

1.5.6. Fuentes. Es decir los programas originales escritos en lenguaje C antes de su compilación. Por ejemplo el del núcleo del sistema operativo o los de los controladores de dispositivos o aplicaciones, para que cualquier usuario los pueda modificar a su gusto o necesidad o simplemente desea conocer cómo funcionan. Esto, además de ser un requisito en las condiciones de las licencias GPL, repercute en una notable mejora en la calidad de todo el software así distribuido.

1.5.7. Documentación. Por ejemplo: manual de instalación rápida, manual de uso, manual de redes, manual multimedia, etc. Todo esto, además de la amplia información que acompaña de serie al mismo SO o a sus aplicaciones como son las páginas del manual disponibles en pantalla y por supuesto la documentación implícita que existe en los mismos programas fuente.

1.5.8. Asistencia. Ayuda que la empresa distribuidora ofrece a los usuarios para la solución de problemas durante cierto período de tiempo.

1.5.9. Coste bajo o nulo. En algunos casos, como en Debian, la adquisición es totalmente gratuita y en otras el precio es muy bajo si se tiene en cuenta la proporción incluida de los componentes arriba descritos. La mayoría de las distribuciones están disponibles en Internet para su descarga gratis (aunque no se incluye soporte técnico) y en éste caso su copia, por terceros, es legal. La mayoría de los problemas que tienen los usuarios se solucionan a través de las asociaciones de usuarios de Linux, foros y chats que, a tal efecto, existen en la red.

CAPITULO II

EVALUACIÓN DE LA SITUACIÓN ACTUAL DE LA RED Y SERVICIOS DE COMUNICACIÓN DE LA SUPERINTENDENCIA DE BANCOS Y SEGUROS (SBS)

2.1. LA SUPERINTENDENCIA DE BANCOS Y SEGUROS Y SU FUNCIÓN

La Superintendencia de Bancos y Seguros es un organismo técnico con autonomía administrativa, económica y financiera y personería jurídica de derecho público, está dirigida y representada por el Superintendente de Bancos.

Tiene a su cargo la vigilancia y control de las Instituciones del Sistema Financiero Público y Privado, así como de las Compañías de Seguros y reaseguros, determinadas en la Constitución y en la Ley.

Su misión es la de proteger los intereses del público usuario y, en especial, de los pequeños depositantes de las Entidades que conforman el Sistema Financiero del Ecuador. Entre sus funciones contempla que:

- Controlará que la constitución, organización, administración, capitalización, operación, funcionamiento, información, regularización y liquidación de dichas Entidades se encuadre dentro de la normatividad respectiva;

- Pondrá énfasis en el profesionalismo, experiencia e integridad de los administradores de las entidades del Sistema Financiero y demandará su colaboración de auto-

vigilancia, mediante suficientes y adecuados controles internos de políticas y procedimientos a seguir en todas las áreas de riesgo de la Entidad;

- Fortalecerá la autonomía de la Superintendencia, utilizará asistencia técnica externa, modernizará sus sistemas informáticos y mejorará la normatividad;

- Propiciará el carácter técnico y la estabilidad de los recursos humanos de la Superintendencia y requerirá de los mismos un alto nivel ético y moral, trabajo honesto, lealtad institucional y respeto al sigilo bancario, el cual podrá ser transferido, en los casos que permita la Ley, para cooperar en la lucha contra la corrupción. La fuerza impulsora que animará y aglutinará al personal de la Superintendencia, será la motivación de ubicarla en un alto nivel de calificación en Latinoamérica y el Caribe.

- Institucionalizará el Sistema de Planificación Estratégica.

2.1.1. Regulación y supervisión del Sistema Financiero. La Superintendencia de Bancos y Seguros tiene como objetivo constante el avanzar en el cumplimiento de los principios básicos para una supervisión bancaria efectiva emitidos por el Comité de Basilea, a través de la expedición de nuevas normas o el ajuste de las existentes en línea con las recomendaciones Internacionales.

Además se encuentra en constante fortalecimiento de los procesos de supervisión in situ, extra situ, consolidada y transfronteriza mediante el diseño y aplicación de metodologías y prácticas de supervisión prudencial dirigida a: mejorar la calidad de la información financiera; la razonabilidad de reservas y provisiones; y, el cumplimiento de las disposiciones legales, normativas y contables.

Promueve activamente en las instituciones financieras el desarrollo de adecuadas prácticas para la administración y supervisión integral de riesgos, considerando las mejores prácticas internacionales aplicables al caso ecuatoriano.

2.1.2. Sistema de Seguro Privado. La Entidad es encargada de ajustar la regulación prudencial del sector asegurador a estándares internacionales, especialmente en materia de: reservas técnicas, capital adecuado, gestión de riesgos, pólizas y tarifas y reaseguros.

Diseña e implanta un constante proceso de supervisión integral y preventiva que permita garantizar el cumplimiento de las regulaciones existentes.

2.1.3. Sistema Nacional de Seguridad Social. Constate Fortalecimiento de la supervisión del Sistema Nacional de Seguridad Social.

2.2. COMO INTERACTÚA LA INSTITUCIÓN CON LAS DIFERENTES ENTIDADES FINANCIERAS.

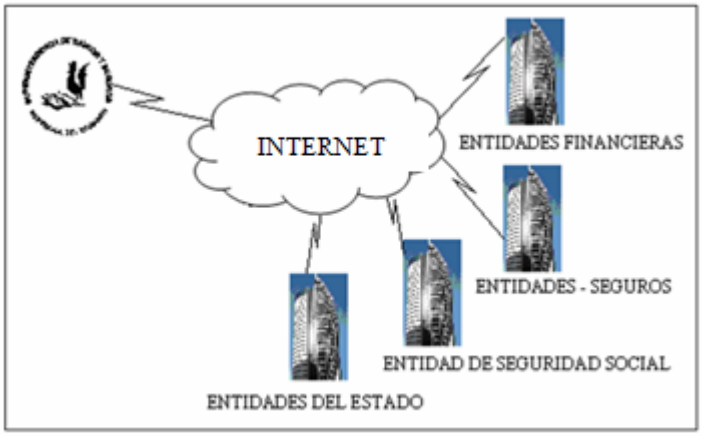

Figura 2.1. Interacción SBS – Entidades Financieras

La Superintendencia de Bancos y Seguros interactúa con Entidades Financieras, Compañías de Seguros y Entidades del Estado. Este intercambio de información (Estructuras de Información, balances, etc.) se transmite a través del Internet de dos formas básicamente: Uno de los medios de transmisión entre las Entidades es vía FTP (Protocolo de Transferencia de Ficheros) y a través de la página Web de la Superintendencia de Bancos y Seguros.

La SBS es la encargada de proveer los niveles de seguridad requeridos para que no se den cambios en la información, puesto que su transferencia es en texto plano. Toda esta información es procesada y validada por funcionarios con ayuda de software propietario de los Sistemas Informáticos de la Entidad que generan acuses de recibo en caso de que la información contenga errores o se haya transferido sin problemas. Las figuras 2.2 y 2.3 detallan estos procedimientos.

Figura 2.2. Módulos del Sistema Integrado

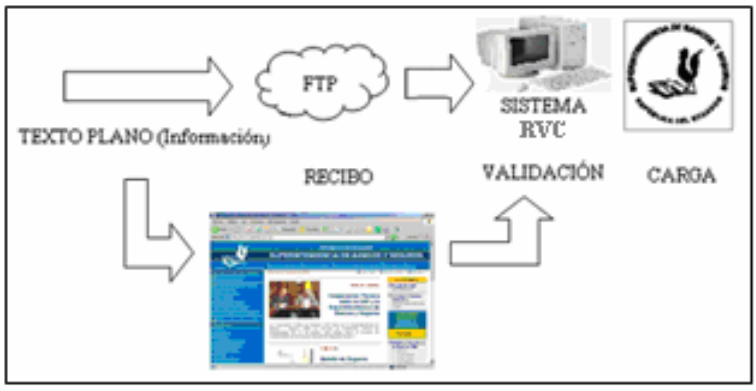

Figura 2.3. Transferencia de Información

Actualmente la información se recibe en un 95 % vía electrónica (sistemas de comunicación) y tan solo un 5 % por formularios.

2.3. INFRAESTRUCTURA TECNOLÓGICA DE LA SBS

Antes de detallar la Infraestructura Tecnológica como tal, se detallará la función que desempeña el Departamento Tecnológico:

- Planificación y desarrollo del Centro de Cómputo, en función de las necesidades de Software y Hardware.

- Diseño de formatos necesarios para recepción de datos enviados por las Entidades controladas a través de medios electrónicos y absolver consultas pertinentes.

- Desarrollo de los sistemas de información requeridos por los usuarios internos Institucionales.

- Asegurar la implantación de los sistemas informáticos desarrollados, mediante el asesoramiento técnico a los usuarios y la capacitación permanente al personal de la Superintendencia de Bancos y Seguros, en coordinación con la Dirección de Recursos Tecnológicos.

- Administración de las Bases de Datos del Sistema Informático Institucional.

- Actualización periódica del Plan de Contingencias Informático y, su ejecución, en caso de ser requerido.

- Mantenimiento de un registro actualizado del parque informático Institucional, hardware y software de base, aplicaciones, paquetes, instalaciones y otros equipos que dispone la Superintendencia de Bancos.

2.3.1. Detalle de la Infraestructura Tecnológica de la Superintendencia de Bancos y Seguros. Como se puede apreciar en la figura 2.4, la Infraestructura tecnológica de la SBS se desenvuelve en 4 escenarios, los cuales serán desglosados a detalle a continuación.

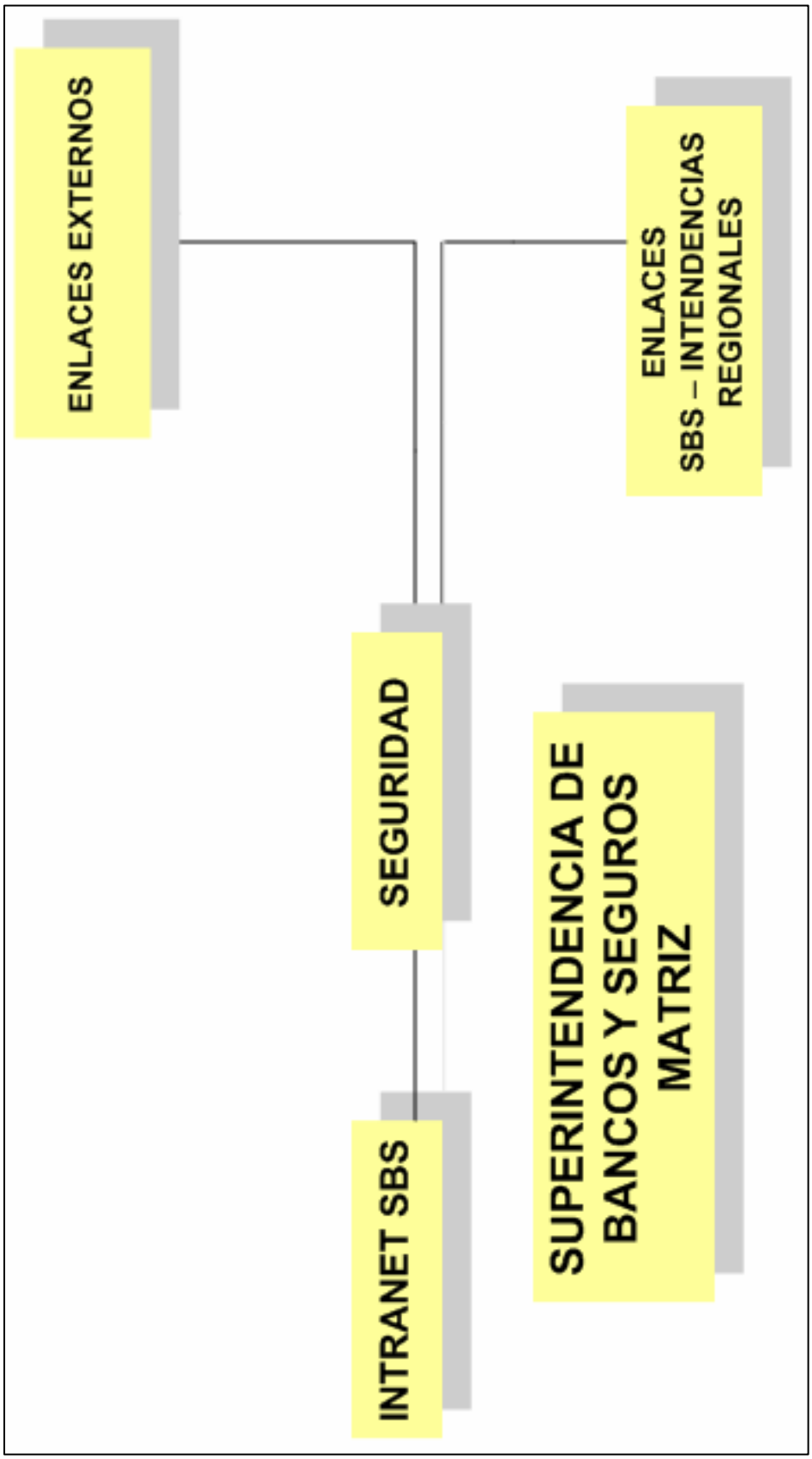

Figura 2.4. Infraestructura Tecnológica

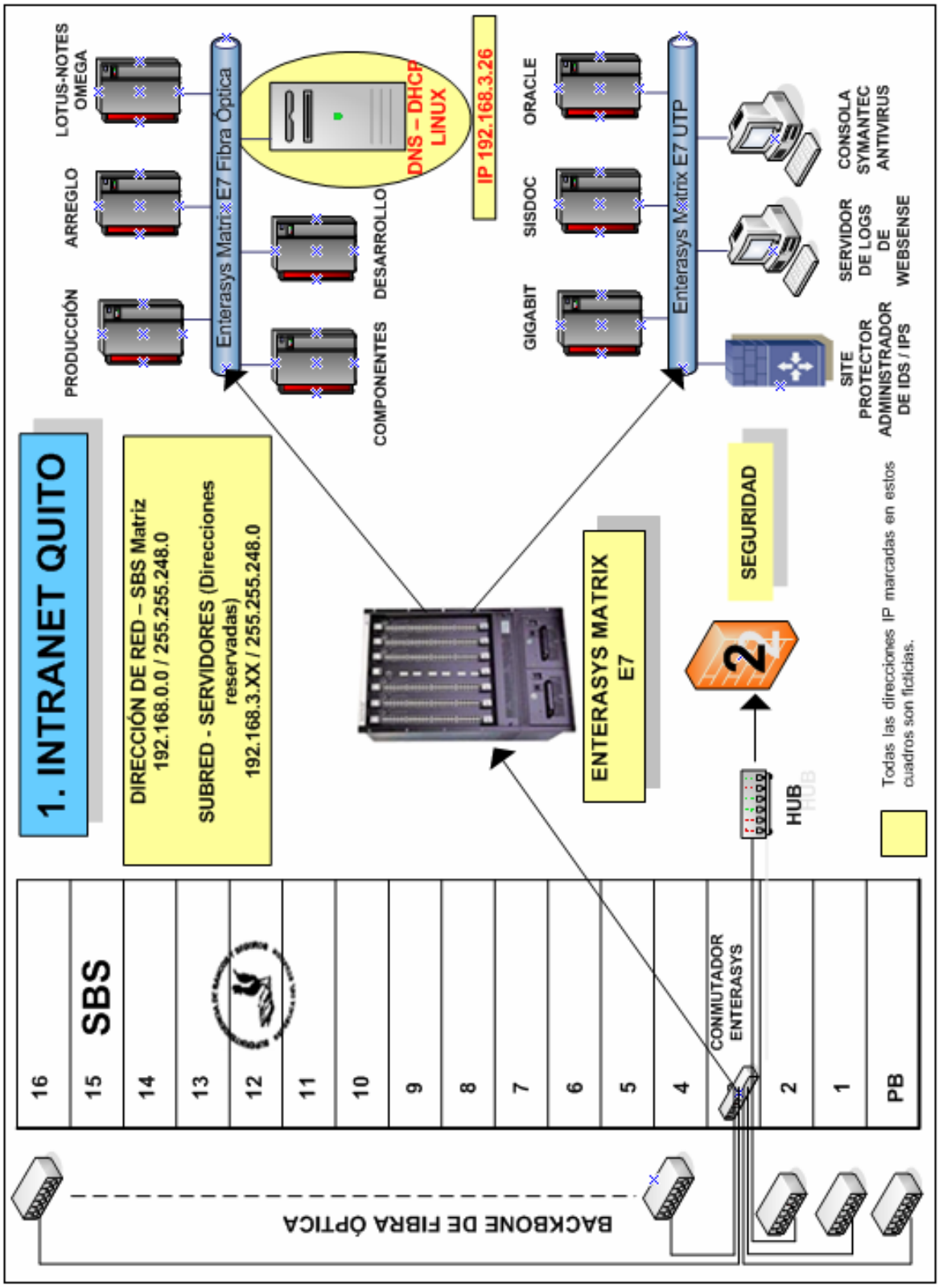

Figura 2.5. Intranet Quito

2.3.2. Intranet Quito. El Backbone de Fibra Óptica del edificio de la Superintendencia de Bancos y Seguros, sostiene una gama de aplicaciones, como la distribución de contenido basado en la WEB y la convergencia de voz, datos y vídeo. Todas estas aplicaciones deben trabajar con una buena calidad de servicio, seguridad y contención del tráfico hacia el escritorio de los usuarios y los servidores de la Entidad, motivo por el cual está provista de un conmutador Enterasys Matriz E7 que trabaja con cableado de Fibra Óptica y UTP.

El Conmutador Enterasys Matrix E7, provee switcheo a los Funcionarios de la Entidad y a los puntos de acceso de los servidores. Como se observa en la Figura 2.5, el conmutador se desempeña en el Centro de Datos y entrega un alto desempeño en el cuarto de cableado de Fibra Óptica y UTP. Este dispositivo integra servicios de Capas 2 y 4.

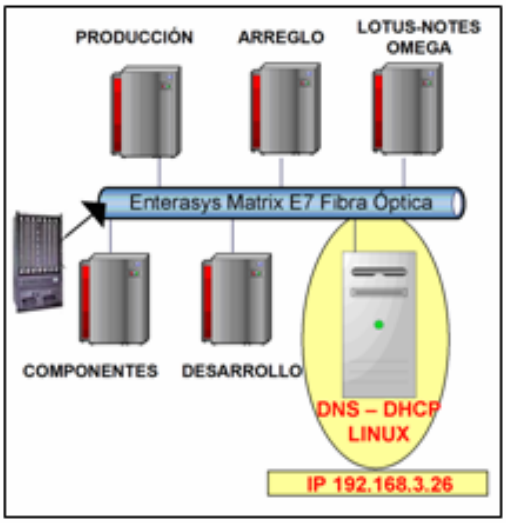

Figura 2.6. Granja de servidores (Interfaz de Fibra Óptica)

El Conmutador Enterasys Matrix E7 opera por medio de Fibra Óptica con diferentes servidores de la Entidad (Fig. 2.6): Servidores de Producción, Correo Electrónico (Lotus-Notes), de Componentes y a futuro el **Servidor del Proyecto Linux (DNS-DHCP).**

Adicionalmente el conmutador opera por medio de cableado UTP (Fig.2.7) con tres servidores (Gigabit, Sisdoc y Oracle F50) y dos computadores de administración.

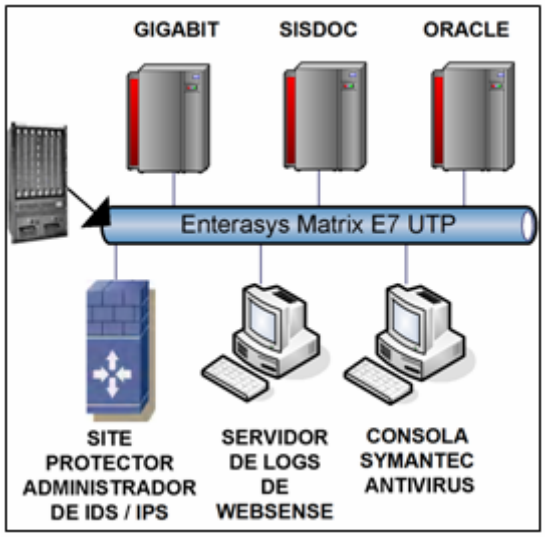

Figura 2.7. Granja de servidores (Interfaz Ethernet)

La **Consola Symantec Antivirus** es la encargada de actualizar y escanear constantemente virus a los ordenadores de la Entidad y el **Servidor de Logs de Websense** almacena la actividad diaria de tráfico URL del servidor Websense (ver **SEGURIDAD**).

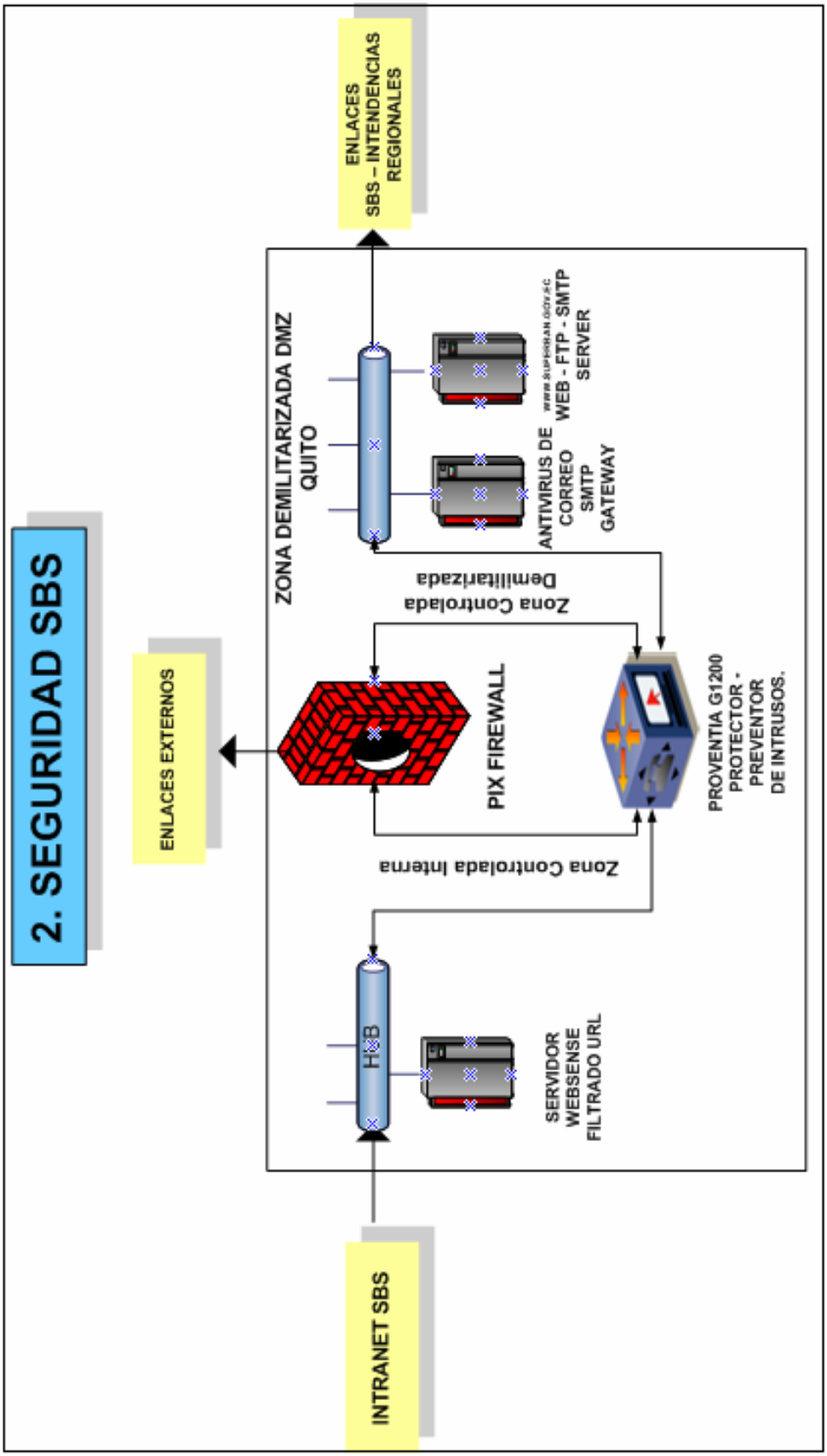

Figura 2.8. Seguridad SBS

2.3.3. Seguridad. La información que procesa la Superintendencia de Bancos y Seguros, como Organismo de Control, es muy sensible, motivo por el cual no se ha escatimado gastos en seguridades de la Red (Fig.2.8).

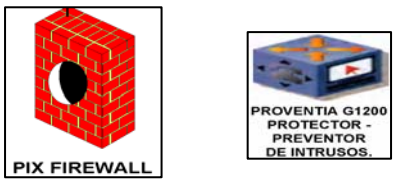

Figura 2.9. Firewall PIX - Preventor de Intrusos

Las seguridades Institucionales integran funciones de control de acceso, autenticación y encriptamiento para garantizar la seguridad de las conexiones de red, la autenticidad de los usuarios locales y remotos, y la privacidad e integridad de la comunicación de datos. Un FIREWALL cisco PIX y un protector - preventor de intrusos (estableciendo reglas de filtrado Fig. 2.9), son los encargados de permitir o no el acceso a puertos de la Red Institucional desde los diferentes enlaces externos (Internet, RAS, etc.), evitando así pérdidas de Información (vulnerabilidad de las seguridades). Adicionalmente también son los encargados de administrar y manejar la zona demilitarizada donde se encuentran servicios tales como FTP, HTTP y SMTP.

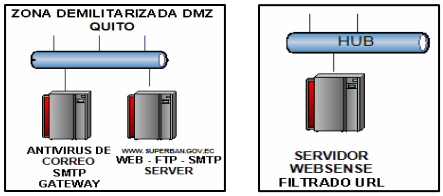

Figura 2.10. Websense - DMZ

Como refuerzo, en las seguridades Institucionales, se encuentra un Servidor de filtro URL Websense (Fig. 2.10), que brinda privilegios de acceso a Internet a los diferentes departamentos y funcionarios de la Entidad, controlando así el uso del mismo, asegurando un servicio rápido de buena calidad pero restringido.

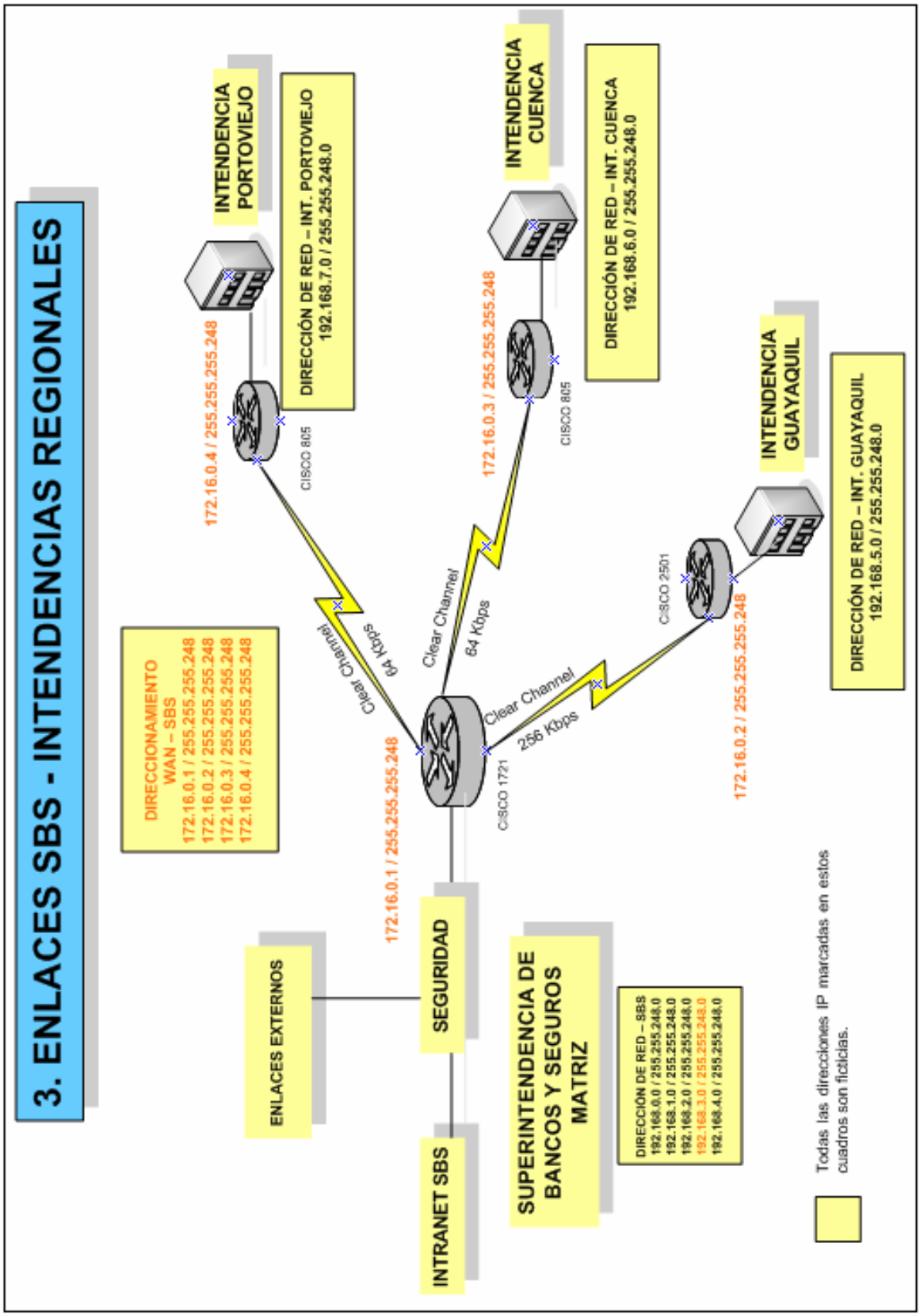

Figura 2.11. Enlaces SBS – Intendencias Regionales

2.3.4. Enlaces SBS – Intendencias Regionales. Los enlaces SBS – INTENDENCIAS REGIONALES o enlaces dedicados son conexiones permanentes punto-multipunto, que se valen de una infraestructura de transporte (Capa 1) comúnmente llamados enlaces Clear Channel.

Actualmente la SBS tiene a su disposición 3 enlaces Clear Channel (Fig. 2.11). Dos enlaces de 64Kbps que la comunica con las Intendencias de Portoviejo – Cuenca y un enlace de 256Kbps con la Intendencia de Guayaquil.

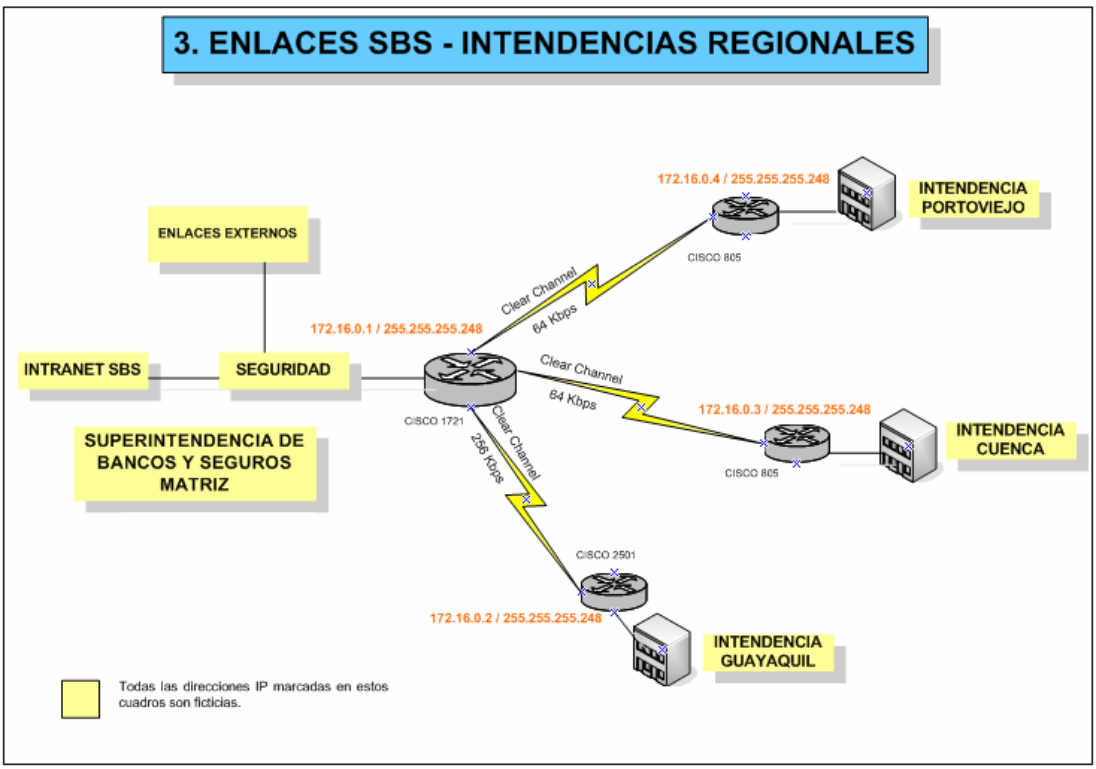

Figura 2.12. Enlaces Clear Channel

Estos enlaces con las Intendencias Regionales permiten integrarlas a la red local (SBS - Matriz) y proceder a comunicar los sitios de forma transparente con los protocolos usados en la misma. Como característica propia del servicio se destaca su alta disponibilidad ya que los administradores hacen uso del ancho de banda total de la forma que deseen.

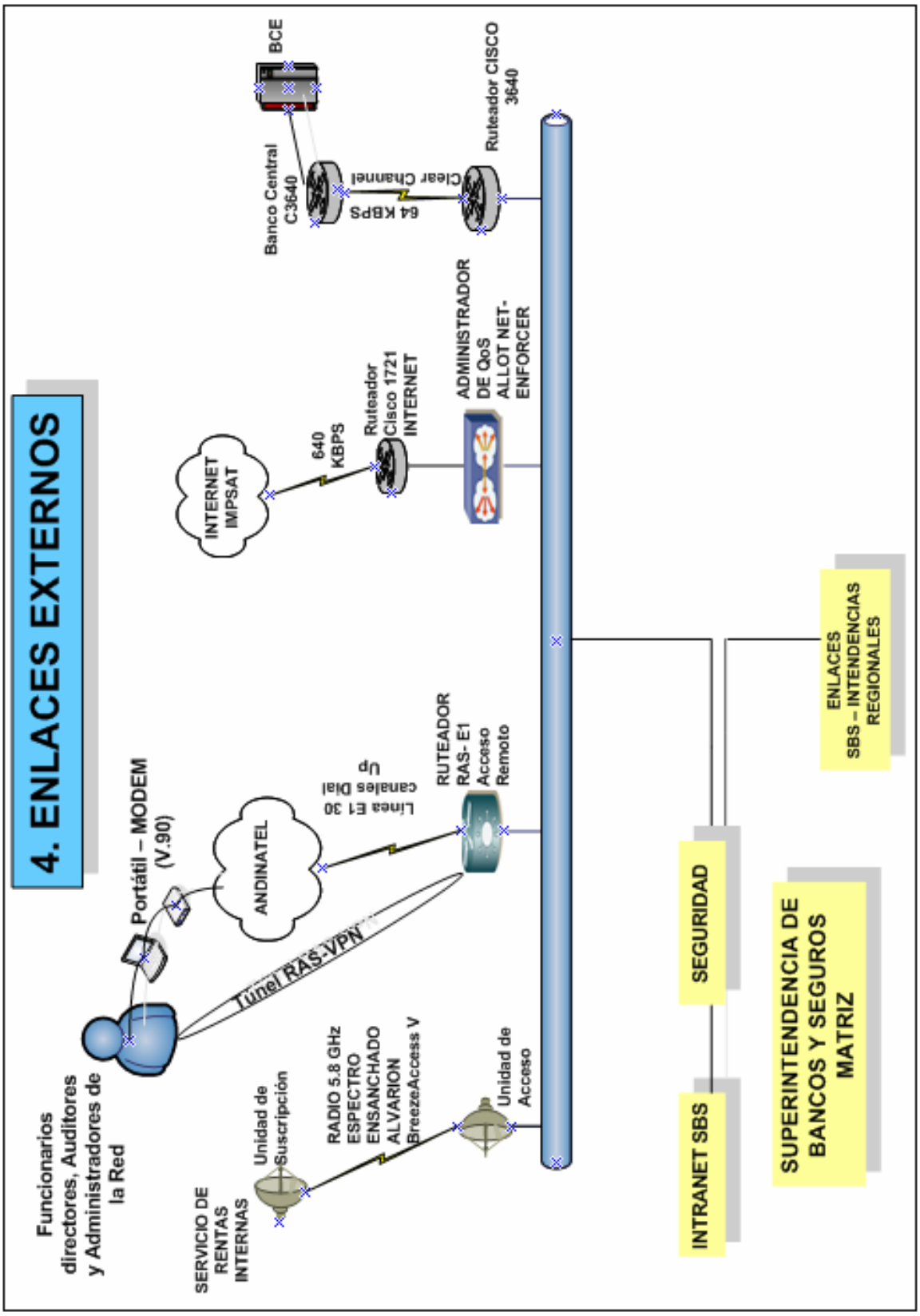

Figura 2.13. Enlaces Externos

2.3.5. Enlaces Externos. La necesidad de enlaces privados con Entidades gubernamentales para interconectarse con la SBS o de enlaces comerciales, con empresas que brinden servicios de comunicaciones (Andinatel e Impsat), nace a partir del intercambio de información Interinstitucional (BCE, SRI) o actualización de bases de datos (auditores de la entidad). La Entidad posee dos tipos de enlaces: comerciales y privados (Fig. 2.13) estos a su vez son requeridos para brindar servicios de comunicaciones a los usuarios internos y externos de la Entidad.

2.3.5.1. Enlaces Comerciales

- **Enlace SBS – ANDINATEL**.- El enlace E1 (2Mbps 30 canales dial up) proporcionado por Andinatel interactúa con el servidor RAS el cual provee el servicio de acceso remoto a los funcionarios de la Entidad (comunicaciones RAS – VPN).

- **Enlace SBS – IMPSAT**.- Enlace de Internet (640 Kbps) proporcionado por IMPSAT a la Superintendencia de Bancos y Seguros.

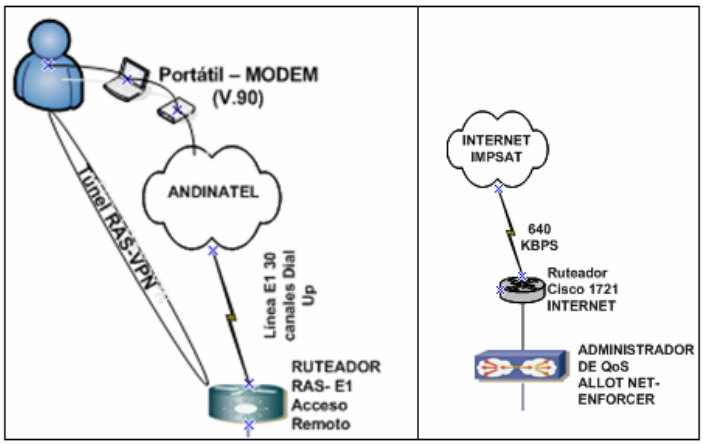

Figura 2.14. Enlaces SBS – Andinatel e Impsat

2.3.5.2. Enlaces Privados

- **Enlace SBS – SRI**.- Radio enlace digital que trabaja en la frecuencia de 5.8 GHz.
- **Enlace SBS – BCE**.- Enlace Clear Channel con el Banco Central del Ecuador.

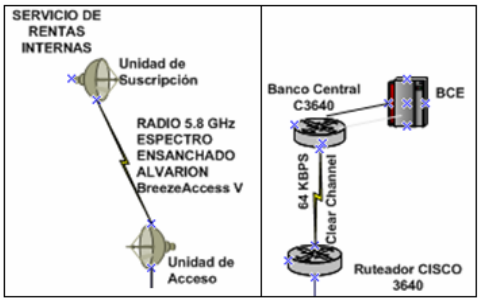

Figura 2.15. Enlaces SBS – SRI y BCE

2.4. USUARIOS INTERNOS Y EXTERNOS DE LA INFORMACIÓN QUE PROCESA LA SBS

Figura 2.16. Información que procesa la SBS

2.4.1. Usuarios Internos. La Superintendencia de Bancos y Seguros, tiene la obligación de velar por la Información a ella entregada. Toda aquella información como Análisis Financiero Técnico, Controles de Patrimonio de las Entidades Controladas, Registro de Instituciones, entre otras (Fig. 2.16), es procesada y almacenada por Funcionarios Internos en las bases de datos de los Sistemas Informáticos que posee la Entidad (por ejemplo Central de Riesgos).

Otro tipo de control son las auditorias externas a Entidades Bancarias y Compañías de Seguros y Reaseguros. Una vez obtenida la Información necesaria, los auditores ingresan a la Red Institucional para almacenar y actualizar la información que poseen las bases de datos. Esta información es canalizada por sistemas de comunicaciones tales como RAS y VPN que autentican a los Funcionarios y proveen altos niveles de seguridad.

2.4.2. Usuarios Externos. La Superintendencia de Bancos y Seguros provee a los usuarios externos una variedad de información y servicios a través de su página Web que se resume en:

- Información sobre la estructura, historia y características de la Superintendencia de Bancos y Seguros.

- Interfase para los procesos de validación y transmisión electrónica de toda la Información requerida por la Institución.

- Información de carácter público con su descripción de: boletines financieros, patrimonio técnico, calificación de activos de riesgos, información de seguros, de grupos financieros, de entidades 0ff shore, resoluciones, boletín de captaciones y colocaciones, cotizaciones, plan de cuentas, etc.

NOTA.- *En caso de ser necesaria información adicional sobre la SBS, su función y procesos que ejecuta, la Institución posee el departamento de ayuda al cliente, el cual facilitará únicamente la Información permitida por las leyes y normas vigentes en la misma actualmente.*

2.5. PROPUESTA TECNOLÓGICA DE BACKUP

La tecnología WAN implementada en la Superintendencia de Bancos y Seguros son los enlaces Clear Channel, estos brindan seguridad permanente en el intercambio de información que se da entre la Matriz y sus Intendencias. Estas comunicaciones buscan asegurar la información que por ellas fluye. Pero siempre es necesario el respaldo, no solo de la información como tal, sino también de los recursos de comunicaciones, motivo por el cual se ha propuesto en el proyecto, una alternativa de comunicación de BACKUP, que busca fortalecer las seguridades en el trayecto de la red pública (Internet) y proveen disponibilidad de la Información.

Es aquí donde entran las redes privadas virtuales (VPN), pues su implementación resulta sencilla y bastante económica puesto que su funcionamiento se apoya en infraestructuras públicas (Internet) ya creadas, evitando costos en la compra de equipos físicos como Routers o en alquiler de enlaces privados o dedicados.

NOTA.- *Se debe recalcar que el proyecto no fomenta la eliminación de estos enlaces dedicados, sino brindar un backup de los mismos, asegurando la disponibilidad y seguridad* constante de la información.

2.5.1. BACKUP DE ENLACES SBS - INTENDENCIAS REGIONALES VÍA VPN (ARQUITECTURA LAN-to-LAN).

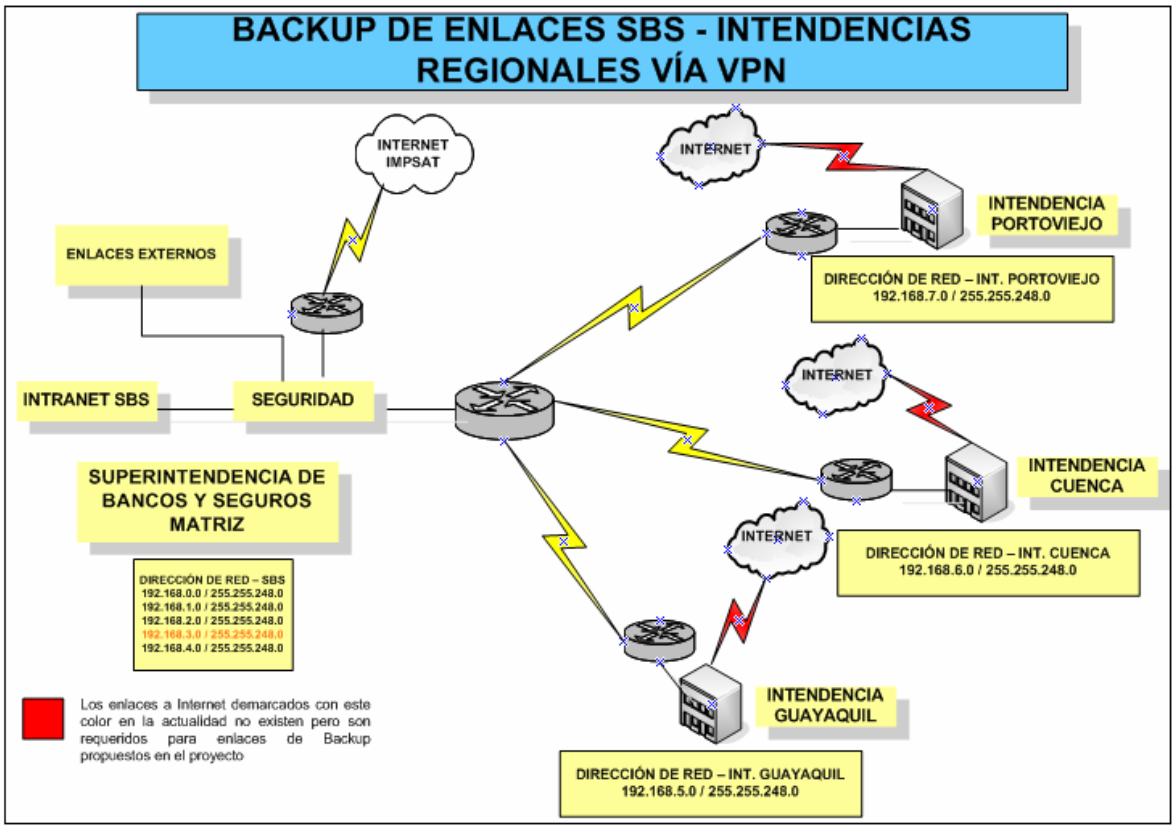

Figura 2.17. Enlaces Individuales de Internet en las Intendencias Regionales

2.5.1.1. REQUERIMIENTOS VPN LAN-to- LAN

Los requerimientos de la alternativa de comunicación de BACKUP (Fig. 2.17), son básicamente:

- Enlaces individuales a Internet en las Intendencias Regionales.
- Un servidor VPN Linux con Firewall en cada uno de los extremos.

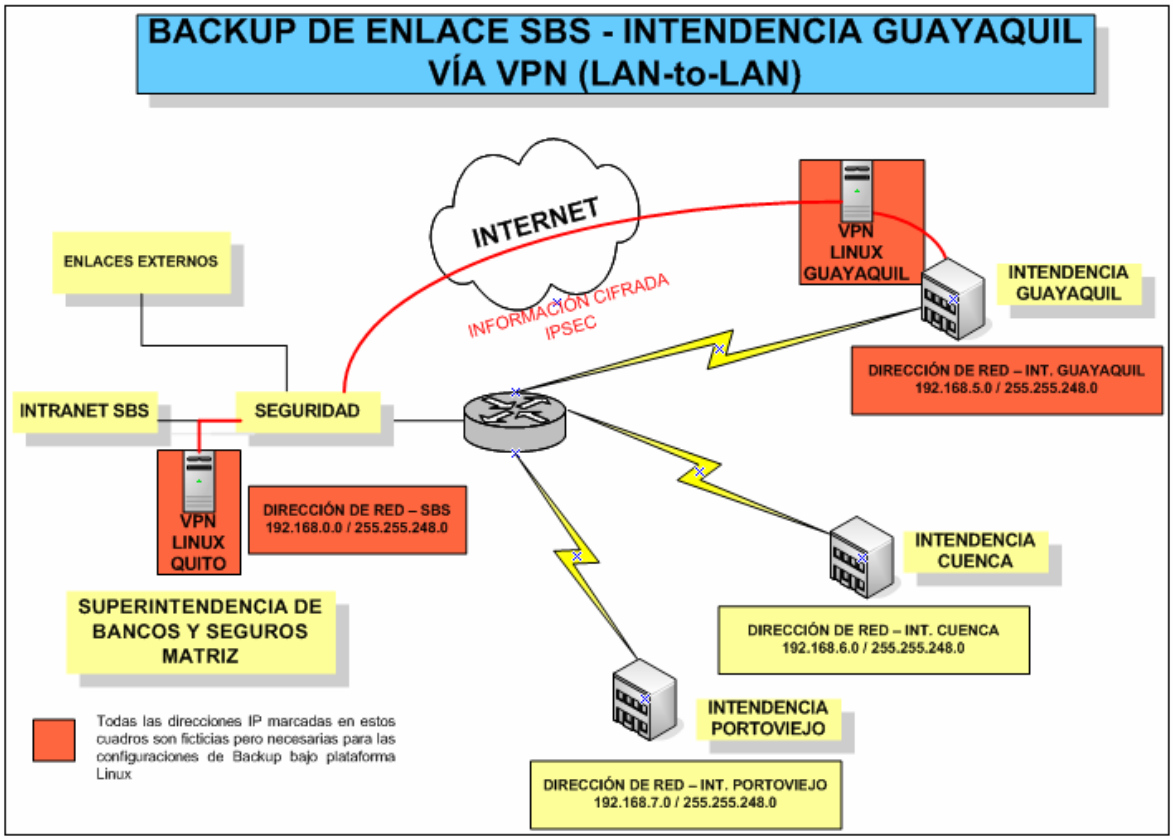

Figura 2.18. Backup de Enlace SBS - Intendencias Guayaquil

La Figura 2.18 muestra una conexión VPN entre la Intendencia de Guayaquil y la Matriz SBS. Este cifrado de información se lo realiza bajo el protocolo IPSEC, el cual se implementa con OPENSWAN (Software adicional) en Linux. Es necesario mencionar que a este protocolo de entunelamiento aún no se le han detectado vulnerabilidades como al protocolo PPTP, y es uno de los más utilizados en las soluciones VPN comerciales como Checkpoint (VPN1-pro).

2.5.2. ACCESO REMOTO VPN - INTERNET

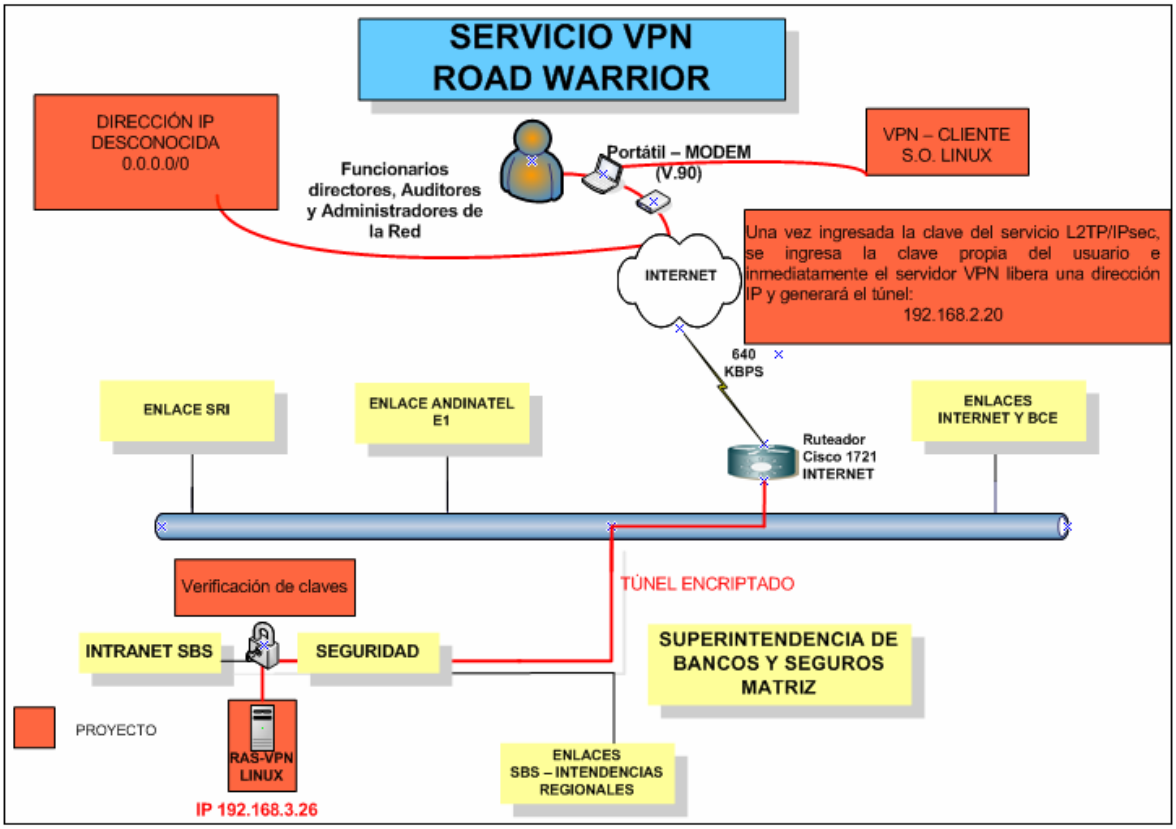

Figura 2.19. Servicio de acceso remoto VPN - Internet

El auge del Internet como el principal medio mundial de comunicación en la actualidad, obliga a la Superintendencia de Bancos y Seguros brindar accesos, a sus Funcionarios, por este medio. Todo este entorno de comunicación debe plasmarse en las configuraciones del servidor LINUX (IPSEC/OPENSWAN) con sus respectivas seguridades.

Desde el punto de vista de la seguridad, es importante tener en cuenta que las claves de los Funcionarios remotos se transmitirán a través del Internet. Motivo por el cual, los administradores del servidor deben proporcionarlas de manera exclusiva a aquellos Funcionarios que requieran este tipo de acceso, puesto que será la única manera que el servidor los reconozca, debido a que ellos pueden tener cualquier tipo de dirección IP (Fig. 2.19).

2.5.3. ACCESO REMOTO VPN – SERVIDOR RAS

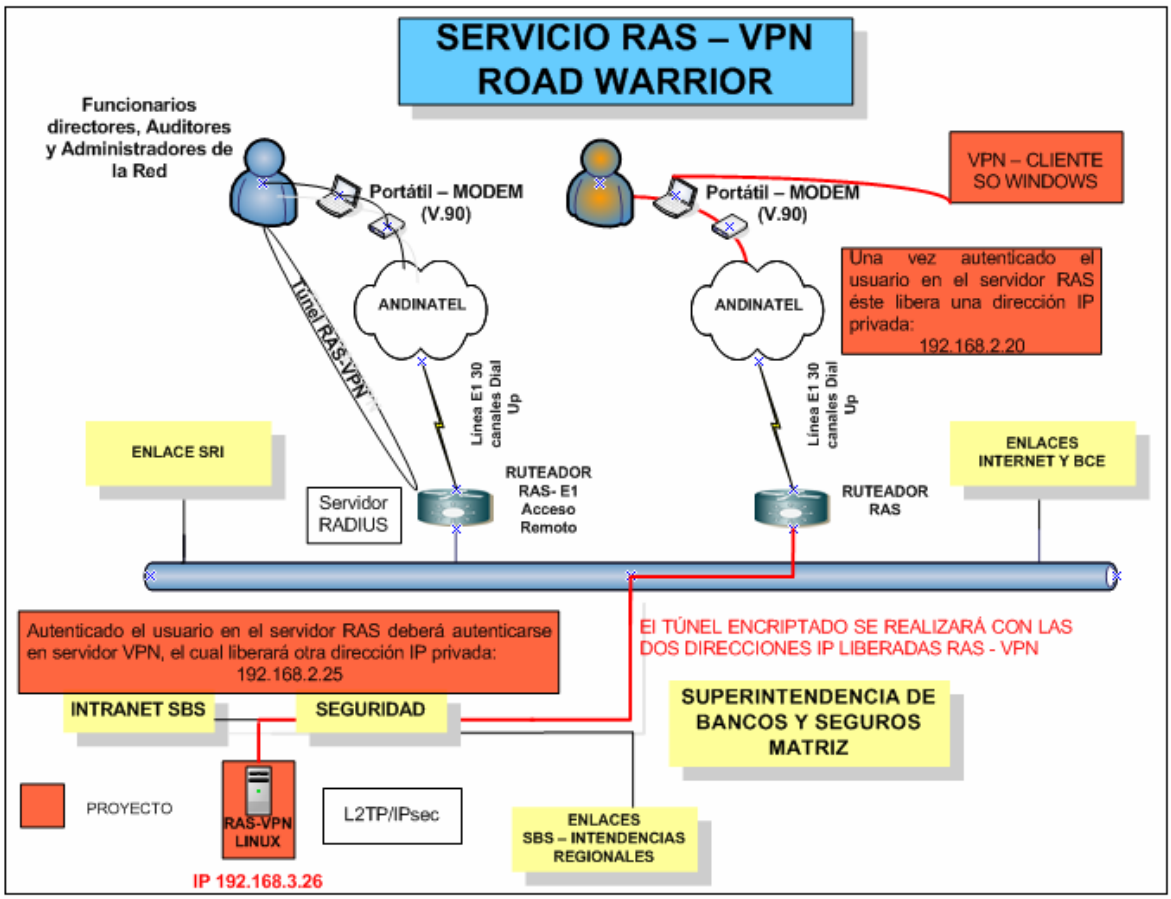

Figura 2.20. Servicio de acceso remoto VPN – Servidor RAS

El servicio RAS que brinda la Entidad está provisto de un servidor RADIUS que se encarga de cifrar la información personal (nombre y clave) del cliente remoto (bajo Linux **ROAD WARRIOR**). Adicionalmente posee un servidor VPN (software comercial) el cual se encarga de cifrar toda la información que los funcionarios deseen ingresar u obtener de las diferentes aplicaciones y bases de datos de la Entidad (Fig. 2.20).

En la propuesta tecnológica se contempló una implementación VPN bajo plataforma Linux que brinde todas estas cualidades de cifrado. Como punto de partida se basó en tomar las cualidades del sistema operativo Windows XP y su cliente VPN (L2TP/IPsec) para que interactúe con el servidor VPN Linux.

2.5.3.1. REQUERIMIENTOS DEL ACCESO REMOTO VPN CON SERVICIO RAS E INTERNET

Los requerimientos para configurar los escenarios VPN (Fig. 2.21 y 2.22) bajo un entorno Linux, son básicamente:

- Un servidor VPN Linux, que actúe como Gateway, con su correspondiente Firewall en el extremo SBS.

- Un computador portátil (S.O. WinXP) con VPN-client (L2TP/IPSec), con conexión remota si el acceso es vía RAS o sin ella si es vía Internet (Fig. 2.21 y 2.22).

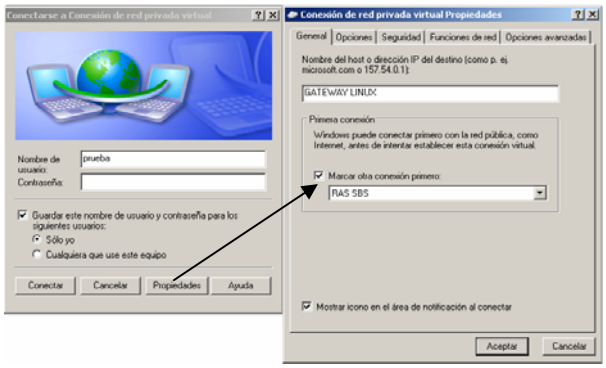

Figura 2.21. Conexión remota CON acceso RAS

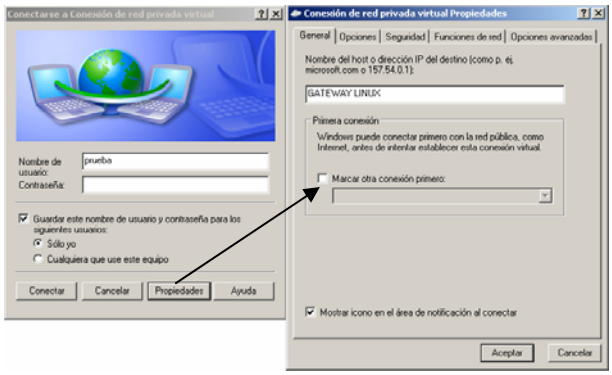

Figura 2.22. Conexión remota SIN acceso RAS

CAPITULO III

FUNDAMENTO TEÓRICO DE LOS SERVICIOS DE COMUNICACIÓN CORRESPONDIENTES A LA PROPUESTA TECNOLÓGICA DE BACKUP

3.1. SERVICIOS SOBRE PLATAFORMA LINUX

Los servicios más relevantes que hacen tan interesante a esta plataforma son los servicios de correo, transferencia de archivos (FTP), de nombres (DNS), DHCP, servidor de archivos compartidos de Microsoft Windows (SAMBA), FIREWALL, Base de Datos, entre otros.

Se debe destacar que cada servicio funciona independientemente del resto. Se puede modificar la dirección IP del equipo, las rutas, añadir, parar o reiniciar un servicio concreto sin que el resto de los servicios se vean afectados.

3.1.1. Distribuciones Linux. Una distribución Linux, o distribución GNU/Linux (distro) es un conjunto de aplicaciones reunidas que permiten brindar mejoras para instalar fácilmente un sistema Linux (también llamado GNU/Linux).

Existen numerosas distribuciones Linux. Cada una de ellas puede incluir cualquier número de software adicional (libre o no), como algunos que facilitan la instalación del sistema y una enorme variedad de aplicaciones.

La base de cada distribución incluye el núcleo Linux, con las bibliotecas y herramientas del proyecto GNU y de muchos otros proyectos/grupos de software, como BSD.

3.1.1.1. Núcleo Linux. El kernel o núcleo de Linux se podría definir como el corazón de la plataforma y es el encargado de que el software y el hardware del equipo puedan trabajar juntos.

Las funciones más importantes del mismo, aunque no las únicas, son:

- Administración de la memoria, para todos los programas en ejecución.
- Administración del tiempo de procesador, que estos programas en ejecución utilizan.
- Es el encargado de que podamos acceder a los periféricos/elementos de nuestro ordenador de una manera cómoda.

Existen dos versiones del kernel Linux:

- **Versión de producción**. Es la versión estable hasta el momento. Esta versión es el resultado final de las versiones de desarrollo o experimentales. Cuando el equipo de desarrollo del kernel experimental, decide que ha conseguido un kernel estable y con la suficiente calidad, se lanza una nueva versión de producción o estable. Esta versión es la que se debería utilizar para un uso normal del sistema, ya que estas son consideradas más estables y libres de fallos en el momento de su lanzamiento.

- **Versión de desarrollo.** Esta versión es experimental y es la que utilizan los desarrolladores para programar, comprobar y verificar nuevas características, correcciones, etc. Estos núcleos suelen ser inestables y no se deberían usar, a no ser que se maneje de manera profesional.

3.1.1.1.1. Interpretación de los números de las versiones del Kernel Linux. Las versiones del kernel se numeran con 3 números, de la siguiente forma: XX.YY.ZZ

- ***XX***: Indica la serie principal del kernel. Hasta el momento solo existen la 1 y 2. Este número cambia cuando la manera de funcionamiento del kernel ha sufrido un cambio muy importante.

- ***YY***: Indica si la versión es de desarrollo o de producción. Un número impar, significa que es de desarrollo, uno par, que es de producción.

- ***ZZ:*** Indica nuevas revisiones dentro de una versión, en las que lo único que se ha modificado, son fallos de programación/bugs.

3.1.1.1.2. Estándares Interdistribuciones Linux. Linux Standard Base (Fundación de estándares Linux) es una organización consagrada a desarrollar una cooperación estrecha entre diferentes distribuciones. El Filesystem Hierarchy Standard (Estándar jerárquico de sistema de ficheros) es una importante herramienta de la organización para lograr una cierta normalización oficial.

El Sistema de ficheros es el método mediante el cual se almacena la información en las unidades de disco. Los distintos sistemas operativos normalmente usan diferentes sistemas de ficheros, lo que dificulta compartir los contenidos de una unidad de disco entre ellos. Sin embargo, Linux admite múltiples sistemas de ficheros (Filesystem), lo cual hace posible la lectura/escritura de particiones dedicadas a MS-Windows.

Distribuciones no comerciales y comerciales Linux. Las diferencias entre las distribuciones Linux son muy amplias, motivo por el cual, se detallarán exclusivamente ciertas características de software (Tabla 3.1 y 3.2)

Tabla 3.1. Tabla General de distribuciones Linux

	Empresa	Fecha de la primera P.R.	Predecesor	Última versión estable	Licencia	Público	País
Debian GNU/Linux	Debian Project	Agosto 1993	N/A	3.1r2 (*sarge*)	cualquier DFSG (*)	Desktop, Workstation, Server	Mundial
Fedora Core	Fedora Project	Noviembre 2003	Fedora Linux, Red Hat Linux	Ver. 5 / Marzo 2006	GPL (*)	Workstation, Server, Público	EEUU
Gentoo	Gentoo Foundation	Marzo 2002	Enoch	2006.0	GPL	Workstation, Server, Público	Mundial
Mandriva Linux	Mandriva	Julio 1998	Mandrakelinux/Conectiva y Lycoris Xls	Mandriva 2006	GPL	Desktop, Workstation, Server	Mundial
Rxart	Pixart	octubre 2001	rxart, rxart Linux	Rxart 2.0	GPL	Workstation, Server	América Spanish
Slackware Linux	Patrick Volkerding	Julio 1993	SLS	10.2	GPL	Workstation, Server, Público	EEUU
SUSE Linux	Novell	Marzo 1994	Jurix	10.1	GPL	Workstation, Server, Público	Mundial

Tabla 3.2. Tabla Técnica de distribuciones Linux

	Kernel	Sistema de ficheros	Arquitectura	Herramienta de Actualización online	Administrador de Paquetes
Debian GNU/Linux	Linux 2.4.27/2.6.8	ext3	x86, IA64, PPC, SPARC, SPARC64, Alpha, MIPS, ARM, PA-RISC, Mac/VME 68k, S/390	APT	dpkg, Synaptic, y APT
Fedora Core	Linux 2.6.15 Fed.Core. Ver 5	ext3	x86, x86-64, i386, PowerPC	up2date, yum, APT (limited)	RPM, yum
Rxart	Linux 2.6.11	ext3	x86, x86-64, i386, PowerPC	up2date, net, APT (limited)	DEB, ASK
Mandriva Linux	Linux 2.6.12.12	ext3	x86 (i586), x86-64, PPC	urpmi	RpmDrake
Slackware Linux	Linux 2.4.29	ReiserFS, ext3/ext2	x86, IA64, S/390	Swaret, Slapt-get, many other not official	installpkg and upgradepkg
SUSE Linux	Linux 2.6.11.4	ReiserFS	x86, IA64, x86-64, PPC	YaST2	RPM, YaST

Distribuciones NO Comerciales.

- ***Aurox*** Basada en Red Hat Linux.
- ***Debian*** x86/PPC.

- ***CentOS*** Basada en Red Hat Enterprise Linux.
- ***Fedora Core*** x86/PPC y basada en Red Hat Linux.
- ***Gentoo Linux*** x86/PPC.
- ***Gnoppix*** Basada en Ubuntu, antes en Debian.
- ***Knoppix*** Basada en Debian, de tipo CD autónomo.
- ***Kubuntu*** x86/PPC/x86-64 y Ubuntu con KDE.
- ***Mandriva Linux*** x86/PPC/x86-64 (antes Mandrake Linux).
- ***Pardus*** Basada en Debian.
- ***Slackware***
- ***OpenSuSE***
- ***Trinux*** Basada en Debian, de tipo CD autónomo.
- ***Trustix Secure Linux***
- ***Ubuntu Linux*** Basada en Debian.
- ***VectorLinux*** Basada en Slackware.
- ***White Box*** Basada en Red Hat Enterprise Linux.
- ***Jarro Negro*** Basada en Slackware, entre otras.

Distribuciones NO Comerciales Hispanoamericanas.

- ***ASLinux Desktop*** Distribución para escritorios de descarga gratuita basada en Debian y KDE, mantenida por la empresa andaluza Activa Sistemas.
- ***EduLinux*** Una distribución educativa chilena.
- ***Gobierno GDF*** Creada por la Delegación Tlalpan del Gobierno del Distrito Federal (México), basada en Fedora.
- ***Jarro Negro*** Creada por la Comunidad Linux UNAM Naucalpan CLUN, por estudiantes del Colegio de Ciencias y Humanidades plantel Naucalpan, basada en Slackware y Debian.
- ***GuadaLinex*** (x86) Impulsada por la Junta de Andalucía (España), basada en Ubuntu, antes en Debian.
- ***JuegaLinex*** (x86) Hermana de Guadalinex, pero con muchos juegos.

- ***gnUAMix*** Patrocinada por la Universidad Autónoma de Madrid, basada en Debian y de tipo CD autónomo.
- ***LinEspa*** Creada por el foro Linux en español, basada en Debian.
- ***LinEx*** Creada por la Junta de Extremadura (España).
- ***Linuxin*** Basada en Debian GNU/Linux 3.0 (Woody) y realizada para novatos.
- ***LliureX*** Creada por la Generalitat Valenciana (España) y orientada al sistema educativo, basada en Knoppix. Soporta 2 idiomas: español y valenciano.
- ***LUC3M*** Distribución de la Universidad Carlos III de Madrid.
- ***Molinux*** Creada por la Comunidad Autónoma de Castilla-La Mancha (España), basada en Ubuntu.
- ***Pequelin*** Distribución educativa para niños y jóvenes, basada en Knoppix.
- ***Ututo-e*** Distribución 100% libre creada en Argentina y basada en Gentoo, entre otras.

Distribuciones Comerciales

- ***ASLinux Desktop*** Distribución para escritorios de descarga gratuita basada en Debian y KDE mantenida por la empresa andaluza Activa Sistemas.
- ***Conectiva Linux*** Distribución hecha especialmente para América Latina Soporta 3 idiomas: español, portugués e inglés.
- ***Corel Linux*** Basada en Debian.
- ***Linspire*** Basada en Debian (antes Lindows).
- ***Mandriva***
- ***Tumix GNu/linux***
- ***Red Hat Enterprise***
- ***SUSE Linux (x86)***
- ***Turbolinux***
- ***Xandros*** Basada en Corel Linux e inspirada en Debian
- ***Yellow Dog Linux*** Para PPC, basada en Fedora Core PPC.

3.1.1.2. Selección de la distribución Linux. La propuesta inicial de los directivos de la Dirección de Recursos Tecnológicos fue trabajar con Red Hat Enterprise 3, pero una vez realizada la investigación pertinente, enfocándose a las necesidades actuales y futuras de seguridades en las comunicaciones de la Entidad, se procedió a sugerir la versión 4 del mismo sistema operativo.

Obtenidas las bases y requerimientos de software, detalladas en la tabla 3.3, se buscó la versión Linux que permita trabajar con los protocolos y servicios de comunicación propuestos en el proyecto de tesis, tales como: DHCP, DNS y VPN (protocolo IPSEC) entre los más importantes. La versión 4 de Red Hat proporciona el soporte necesario para levantar todos y cada uno de los servicios. A continuación se detallará las características básicas de Red Hat Enterprise 4, que pueden ser de mucha ayuda en caso que se desee implementar algún servicio adicional por parte de los desarrolladores de la Entidad.

Tabla 3.3. Requerimientos de seguridad del kernel Linux.

PF_KEY	**Sockets**
IP	AH transformations
IP	ESP transformations
IP	IPComp transformations
IP	Tunnel transformations
IPsec	User configuration interface
Soporte de criptografía Administración de Key	3DES, AES, SHA1, MD5 Preshared Keys, RSA Keys, X.509 Digital Certificates.

3.1.1.2.1. Red Hat Enterprise Linux 4. Esta versión Enterprise fue introducida en Febrero del 2005, proporciona importantes mejoras tecnológicas sobre la versión 3. Entre las áreas de desarrollo específico se incluyen mejoras en las capacidades de seguridad, incremento en el rendimiento y escalabilidad del servidor, y mejoras en la capacidad del escritorio. Red Hat Enterprise Linux 4 soporta una amplia gama de aplicaciones de hardware y de software.

3.1.1.2.2. Infraestructura del Kernel de Linux 2.6. Red Hat Enterprise Linux 4 es un producto comercial estable y robusto basado en el kernel 2.6.9 de la comunidad Linux.

Los proyectos de código abiertos, como Fedora, proporcionaron un entorno de maduración al kernel Linux 2.6 durante el 2004. Como resultado, el kernel de Red Hat Enterprise Linux 4 ofrece numerosas ventajas sobre los kernels anteriores, estas incluyen mejoras en algoritmos y características:

- Planificador CPU genérico lógico: maneja núcleos múltiples y CPU con tecnología hyper-thread.
- Object-based Reverse Mapping VM: incrementa el rendimiento en los sistemas de memoria reducida.
- Read Copy Update: mejora del algoritmo SMP para las estructuras de datos del sistema operativo.
- Planificador múltiple de E/S: capacidad de selección basada en las aplicaciones del entorno.
- Soporte mejorado de SMP y NUMA: Incrementa el rendimiento y escalabilidad de grandes servidores.
- Network interrupt mitigation (NAPI): incrementa el rendimiento en pesados procesos de transferencia a través de la red.

3.1.1.2.3. Características varias de RHEL 4. Al ser una nueva versión casi todos los aspectos de Red Hat Enterprise Linux han sido mejorados. Algunas de las más importantes mejoras son:

- Compatibilidad con versiones anteriores: Red Hat Enterprise Linux 4 incluye librerías de compatibilidad que permiten a la mayoría de aplicaciones de las versiones 3 y 2.1 ser ejecutadas sin necesidad de ser modificadas.

- Idiomas: enfocados en estándares internacionales, tales como OpenI18N y GB 18030, Red Hat Enterprise Linux dispone de documentación y software en 15 idiomas: inglés, japonés, alemán, portugués, coreano, italiano, francés, chino simplificado, chino tradicional, español, devanagari, bangla, punjabi, tamil, guajarati.

- Servidor de archivos: la inclusión de NFSv4 proporciona características tales como mejoras de seguridad, unión de operaciones y cierre integrado de archivos; mientras Samba proporciona fácil acceso a impresoras y archivos compartidos bajo Microsoft Windows.

- Desarrollo de Software: proporciona la última cadena de compiladores GCC 3.4 y un adelanto de GCC 4.0 para ofrecer la maleabilidad estándar de los entornos de desarrollo C/C++ y Fortran 95.

- Interfaz de energía y configuración avanzada: el soporte del estándar ACPI permite un amplio rango de capacidades de administración de energía (monitoreo de la batería, apagado automático, suspensión), y provee una base para el incremento de sofisticadas características en el futuro.

- El ciclo de vida de Red Hat Enterprise Linux proporciona siete años de asistencia a cada versión. Nuevas versiones son introducidas en un periodo previsto en 18 meses.

- Plataforma Certificada: Red Hat trabaja activamente para tener certificaciones de la industria ISVs y OEMs para Aplicaciones Integrales y soporte de hardware para los productos Red Hat Enterprise Linux. Como ejemplo se detallará algunos fabricantes que soportan Red Hat Enterprise Linux: Oracle, Checkpoint, Dell, Novell, IBM: Tivoli, Lotus, DB2, Webspshere, entre otros.

3.1.1.2.4. Costos del software. La Superintendencia de Bancos y Seguros ha trabajado los últimos años con HP (Hewlett-Packard), empresa que se ha destacado por brindar soporte técnico y constante preocupación del óptimo funcionamiento de los equipos adquiridos. Motivo por el cual se ha tomado en cuenta para la adquisición de Red Hat Enterprise 4 AS. Los costos de esta plataforma oscilan entre $2000.oo y $7000.oo (dólares americanos) más gastos de envío. La diferencia de costos radica básicamente en el tiempo y el tipo de soporte que se desee.

3.1.2. Servicio DHCP. DHCP son las siglas en inglés de Protocolo de configuración dinámica de usuario (Dynamic Host Configuration Protocol). Es un protocolo de red en el que un servidor provee los parámetros de configuración a los ordenadores conectados a la red informática (máscara de subred, puerta de enlace y otros) y también incluye un mecanismo de asignación de direcciones de IP.

Este protocolo apareció como un protocolo estándar en octubre de 1993. En **RFC 2131** se puede encontrar la definición más actualizada. Los últimos esfuerzos describiendo DHCPv6, DHCP en una red IPv6, fue publicado como **RFC 3315.**

Entre las características más relevantes de este protocolo se encuentran:

- Asignación de direcciones IP.
- Parámetros configurables.
- Anatomía del protocolo:
  - DHCP Discover
  - DHCP Offer
  - DHCP Request
  - DHCP Acknowledge
  - DHCP Inform
  - DHCP Release

3.1.2.1. Asignación de direcciones IP. Sin DHCP, cada dirección IP debe configurarse manualmente en cada ordenador y, si el ordenador se mueve a otro lugar en otra parte de la red, se debe configurar otra dirección IP diferente. El DHCP le permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva IP, si el ordenador es conectado en un lugar diferente de la red.
El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

3.1.2.1.1. Asignación manual. Donde la asignación se basa en una tabla con direcciones MAC (pares de direcciones IP ingresados manualmente por el

administrador). Sólo las computadoras con una dirección MAC que figure en dicha tabla recibirá el IP que le asigna dicha tabla.

3.1.2.1.2. Asignación automática. Donde una dirección de IP libre obtenida de un rango determinado por el administrador se le asigna permanentemente a la computadora que la requiere.

3.1.2.1.3. Asignación dinámica. El único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada computadora conectada a la red está configurada para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes a la red.

Algunas implementaciones de DHCP pueden actualizar el DNS asociado con los servidores para reflejar las nuevas direcciones IP mediante el protocolo de actualización de DNS establecido en **RFC 2136**.

El DHCP es una alternativa a otros protocolos de gestión de direcciones IP de red, como el BOOTP (Bootstrap Protocol). DHCP es un protocolo más avanzado, pero ambos son los usados normalmente.

Cuando el DHCP es incapaz de asignar una dirección IP, se utiliza un proceso llamado APIPA (Automatic Private Internet Protocol Addressing).

3.1.2.2. Parámetros configurables. Un servidor DHCP puede proveer de una configuración opcional a la computadora cliente. Dichas opciones están definidas en **RFC 2132**. Entre las opciones configurables se detallan:

- *Dirección del servidor DNS*
- *Nombre DNS*

- *Puerta de enlace de la dirección IP*
- *Dirección de Publicación Masiva (broadcast address)*
- *Máscara de subred*
- *Tiempo máximo de espera del ARP (Protocolo de Resolución de Direcciones)*
- *MTU (Unidad de Transferencia Máxima) para la interfaz*
- *Servidores NIS (Servicio de Información de Red)*
- *Dominios NIS*
- *Servidores NTP (Protocolo de Tiempo de Red)*
- *Servidor SMTP*
- *Servidor TFTP*
- *Nombre del servidor WINS*

3.1.2.3. Anatomía del protocolo. DHCP usa los mismos puertos asignados por el IANA (Autoridad de Números Asignados en Internet) en BOOTP: 67/udp para las computadoras servidor y 68/udp para las computadoras cliente.

3.1.2.3.1. DHCP Discover. La computadora cliente emite peticiones masivamente en la subred local para encontrar un servidor disponible, por medio de un paquete de broadcast. El router puede ser configurado para redireccionar los paquetes DHCP a un servidor DHCP en una subred diferente. La implementación cliente crea un paquete UDP (Protocolo de Datagramas de Usuario) con destino 255.255.255.255 y requiere también su última dirección IP conocida, aunque esto no es necesario y puede llegar a ser ignorado por el servidor.

3.1.2.3.2. DHCP Offer. El servidor determina la configuración basándose en la dirección del soporte físico de la computadora cliente especificada en el registro CHADDRvbnv. El servidor especifica la dirección IP en el registro YIADDR. El cliente recibe uno o más mensajes DHCP OFFER de uno o más servidores. Elige uno basándose en los parámetros de configuración ofertados y hace un broadcast de un mensaje DHCP REQUEST que incluye la opción identificadora del servidor para indicar qué mensaje ha seleccionado.

3.1.2.3.3. DHCP Request. El cliente selecciona la configuración de los paquetes recibidos de DHCP Offer. Una vez más, el cliente solicita una dirección IP específica que indicó el servidor.

3.1.2.3.4. DHCP Acknowledge. El servidor confirma el pedido y lo publica masivamente en la subred. Se espera que el cliente configure su interfaz de red con las opciones que se les otorgo.

3.1.2.3.5. DHCP Inform. El cliente envía una petición al servidor DHCP para solicitar más información que la que el servidor ha enviado con el DHCPACK original, o para repetir los datos para un uso particular. Dichas peticiones no hacen que el servidor de DHCP refresque el tiempo de vencimiento de IP en su base de datos

3.1.2.3.6. DHCP Release. El cliente envía una petición al servidor DHCP para liberar su dirección de hardware y red. Como los clientes generalmente no saben cuando los usuarios pueden desconectarles de la red, el protocolo no define el envío del DHCP Release como obligatorio.

3.1.3. Servicio DNS

3.1.3.1. Antecedentes. En las redes TCP/IP cada interfaz de red es identificada a través de una dirección IP única de 32 bits. A cada interfaz de red se le puede asociar un nombre o hostname.

Los nombres son asignados a los dispositivos puesto que son más fáciles de manejar que los números IP, es decir, permiten a las personas un uso más amigable de la red. En la mayoría de los casos se pueden utilizar indiferentemente los nombres o las direcciones.

Cuando un comando es introducido con una dirección IP o con un nombre, la conexión siempre se realiza utilizando la dirección IP. Por esta razón el sistema debe convertir el nombre a la dirección IP, de forma transparente al usuario, antes de realizar la conexión.

Existen dos técnicas para traducir nombres a direcciones:

- Mediante la utilización de una tabla llamada host table.
- Mediante la utilización de un sistema de base de datos distribuida llamada Domain Name Service (DNS).

La técnica host table, es un archivo de texto que asocia direcciones IP a nombres. En la mayoría de los sistemas UNIX se encuentra en el archivo /etc/hosts. Esta técnica era utilizada en los comienzos de lo que es hoy Internet. Para ese tiempo existía una comunidad pequeña de unos cientos de máquinas, lo que permitía que se mantuviese toda la información necesaria de cada máquina en un solo archivo.

Sin embargo, con la utilización de los protocolos TCP/IP, la población de la red aumento considerablemente y con ello surgieron los siguientes problemas:

3.1.3.2. Problemas de Host Table

Carencia de escalabilidad. La tabla que mantenía la equivalencia de nombres a direcciones IP creció de tal manera que se convirtió en una forma ineficiente para resolver el problema.

Carencia de un proceso automático de actualización. Las máquinas registradas recientemente, pueden ser referenciadas por su nombre sólo cuando el sitio recibe la actualización de la tabla. Sin embargo no hay forma de garantizar que la host table sea distribuida a los sitios. Antes de adaptar DNS, el Network Information Center (NIC) era el organismo encargado de mantener la información de todas las máquinas registradas. El NIC no sabía que sitio tenía la versión actualizada de la tabla y cual no. Esta falta de consistencia en la host table es la mayor debilidad de esta técnica. Las debilidades inherentes a la host table son solventadas con la utilización del DNS.

El sistema de dominio de nombres (Domain Name System) es una base de datos distribuida, la cual forma un sistema jerárquico para traducir de nombres (hostnames) a direcciones IP. En el DNS no existe una base de datos central con toda la información de los hosts de Internet. Por el contrario la información es distribuida entre cientos de servidores de nombres (name servers). Esto permite controlar por segmentos toda la base de datos en general, logrando que la información de cada uno de estos segmentos esté disponible a través de toda la red, utilizando un esquema cliente - servidor.

Los programas llamados name servers (servidores de nombres) forman la parte del servidor en el mecanismo cliente-servidor de DNS. Los name servers contienen la información de un segmento de la base de datos y la ponen a disposición de los clientes.

Los clientes son llamados “resolvers”, los cuales no son más que rutinas de librería que crean preguntas y las envían a través de la red a los servidores.

La estructura de DNS se asemeja a la estructura jerárquica de los sistemas de archivos de UNIX, la cual se representa con un árbol invertido. El tope de esta jerarquía

se representa por un punto "." y cada nodo del árbol, en general, representa una partición de la base de datos. Cada una de estas particiones es llamada domain (dominio), los cuales a su vez pueden ser divididos en subdomains (subdominios).
En la figura 3.1 se puede apreciar parte de la estructura DNS.

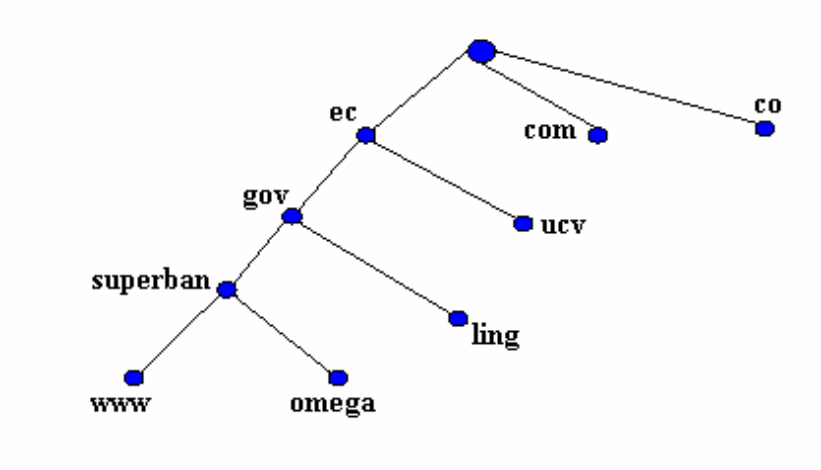

Figura 3.1. Estructura DNS

3.1.3.3. Dominios. Cada unidad de datos en el DNS está indicada por un nombre. Estos nombres son esencialmente rutas en el árbol invertido, llamado espacio de dominio de nombres.

Cada nodo en el árbol es etiquetado con un nombre simple, el cual puede tener hasta ***63 caracteres*** de longitud. El dominio raíz tiene una etiqueta de tamaño cero la cual es reservada. Un nombre completo de cualquier nodo en el árbol es la secuencia de etiquetas separadas por "." las cuales se encuentran en el camino del nodo hasta la raíz.

Por conveniencia cuando el dominio raíz aparece por si mismo, éste es escrito con un punto ".". De esta manera cuando se escribe un nombre de dominio que termina en punto, éste es interpretado como absoluto. Por el contrario cuando se escribe un nombre que no termina en punto, es interpretado como relativo a otro dominio diferente al dominio raíz. Un nombre de dominio absoluto es también referido como nombre de dominio completamente calificado (fully-qualified domain name), algunas veces abreviado FQDN. En la figura anterior, se muestran dos nodos debajo del dominio superban: **www** y **omega** los cuales corresponden a dos máquinas que pertenecen al

dominio **superban.gov.ec.**; el punto al final del dominio indica que es FQDN. Así, los nombres FQDN son **www.superban.gov.ec.** Y **omega.superban.gov.ec.**

Directamente bajo el dominio raíz están los dominios de nivel superior (top-level domains). Existen básicamente dos tipos de dominios de nivel superior: geográficos y organizacionales.

Los dominios geográficos son identificados por dos letras y son asignados a cada país del mundo. Por ejemplo, y como se muestra en la figura **Ecuador** es el dominio **ec** y **Colombia** es **co**.

3.1.3.3.1. Dominios Organizacionales. Los dominios organizacionales están basados como su nombre lo indican en el tipo de organización (comercial, militar, etc.) a la cual pertenece el sistema. Estos dominios son los siguientes:

- com.- Organizaciones comerciales como sun.com, sybase.com.
- edu.- Instituciones educativas como espe.edu, berkeley.edu
- gov.- Agencias gubernamentales como superban.gov
- mil.- Organizaciones militares como navy.mil
- net.- Organizaciones relacionadas con la red como andinanet.net
- org.- Organizaciones que no entran en ninguna de las categorías anteriores como son las organizaciones sin fines de lucro.

Recientemente se han realizado algunas propuestas para incrementar el número de dominios de nivel superior. Los dominios propuestos son llamados dominios de nivel superior genéricos (generic top level domains) o gTLDs. La proposición más conocida fue hecha por el IAHC (International Ad Hoc Commitee). El IAHC propuso los siguientes nuevos gTLDs:

- film.- Negocios o filmaciones.
- store.- Negocios que ofrecen bienes.
- Web.- Organizaciones que hace énfasis en el WEB.

- arts.- Organizaciones culturales y de entretenimiento.
- rec.- Organizaciones recreacionales y de entretenimiento.
- info.- Entidades que proveen servicios de información.
- nom.- Individuos u organizaciones que desean definir una nomenclatura personal.

3.1.3.4. Delegación. La delegación de dominios permite alcanzar uno de los objetivos primordiales del DNS; la administración descentralizada. Una organización que administra un dominio lo puede dividir en subdominios y delegarlos a otras organizaciones. De esta forma cada organización que maneja un subdominio se encarga de mantener toda la data correspondiente a ese subdominio. Ellos pueden cambiar libremente la data e incluso dividir su subdominio en más subdominios. De esta manera el dominio padre en lugar de contener información acerca del subdominio que está delegando, contiene sólo apuntadores a la fuente de la data del subdominio, es decir, a los servidores de nombres. De esta manera si un servidor de nombres de un dominio es interrogado acerca de una máquina que pertenece a uno de sus subdominios, éste devolverá la dirección del servidor que le puede contestar.

Como ejemplo de la delegación, se puede considerar el dominio **gov.ec**. En este dominio se realizan varias delegaciones tal como **ling.gov.ec**. De esta manera los desarrolladores de ingeniería están encargados de agregar, eliminar y modificar los datos del nuevo dominio independientemente de los datos que se tienen en el dominio padre, **gov.ec**.

3.1.3.5. Servidores de Nombres (Name Servers). Los programas que guardan la información acerca del espacio de dominio de nombres son llamados servidores de nombres (name servers). Los servidores generalmente mantienen la información completa acerca de una parte del espacio de dominio de nombres llamado zona. Se dice entonces que el servidor de nombres tiene autoridad para esa zona.

El término zona es algunas veces usado indiferentemente con la palabra dominio, pero debe hacerse una distinción entre estos términos. Una zona se refiere a la información que contiene el archivo de datos, mientras el término dominio se utiliza en

un contexto más general, es decir un dominio es parte de la jerarquía de dominios identificada por un nombre de dominio.

Las especificaciones de DNS definen dos tipos de servidores de nombres: maestros primarios y maestros secundarios. Un servidor primario maestro obtiene los datos de la zona sobre la cual tiene autoridad desde archivos que están en la misma máquina del servidor de nombres, mientras que un maestro secundario obtiene los datos de la zona de otro servidor autorizado para la misma; esto es llamado transferencia de zona.

3.1.3.6. Archivos de Datos. Los datos asociados con cada dominio de nombres está contenida en los llamados registro de recursos (resource records) o simplemente RR. Los RR describen todos los hosts en la zona y marcan toda delegación de subdominios. Los archivos que los servidores de nombres primarios utilizan son llamados archivos de datos (data files). Estos archivos de datos contienen registro de recursos que describen la zona.

3.1.3.7. Resolvers. “Resolvers” son los clientes que acceden a los servidores de nombres. Los programas que necesitan la información de un dominio de espacio de nombres utilizan el “resolver”.

Estos a su vez realizan las siguientes tareas:

- Interrogan al servidor de nombres.
- Interpretan las respuestas (las cuales pueden ser RR o errores).
- Devuelven la información al programa que la solicita.

3.1.3.8. Resolución de nombres. Los servidores de nombres tienden a buscar datos en el espacio de dominio de nombres. Tienen que comportarse de esa manera dada la inteligencia limitada de los “resolvers”.

No sólo pueden dar datos acerca de la zona (puede ser más de una) sobre la que tienen autoridad, sino que pueden buscar a través del espacio del dominio de nombres para encontrar datos sobre los cuales no poseen autoridad. A este proceso se le conoce como resolución. Debido a que el espacio de nombres es estructurado, un servidor de nombres solo necesita una pieza de información para encontrar el camino a cualquier punto en el árbol, los nombres y direcciones de los servidores de nombre raíz.

3.1.3.9. Servidores Raíz Primarios (Root Name Servers, RNS). Los RNS saben que servidores de nombres tienen autoridad para los dominios superiores. Si se les hace una pregunta acerca de un subdominio, los servidores raíz maestros pueden al menos proveer los nombres y direcciones de los servidores de nombres con autoridad para el segundo nivel de dominios a los cuales un dominio pertenece. Cada servidor interrogado da, al que pregunta, información de cómo “estar más cerca” de la respuesta que está buscando o provee él mismo una respuesta. Lo que hacen los RNS es proveer punteros desde los dominios superiores a los servidores de nombres de los dominios inferiores. Por ejemplo para conseguir el servidor de nombres del dominio ve. se debe interrogar a los servidores raíz.

Los RNS, así como los NS normales, son muy importantes en la resolución de un nombre dentro de un dominio particular. Debido a que son tan importantes, DNS provee mecanismos para asegurar siempre el servicio utilizando redundancia (servidores secundarios) o aliviando la carga de los servidores primarios y root (usando caching). Sin embargo, en ausencia de mecanismos como el caching, la resolución debe empezar en los servidores de raíz maestros.

3.1.3.10. Métodos de búsqueda. En el momento que un cliente desea obtener la dirección IP de una máquina, interroga al servidor de nombres de su dominio. Luego el servidor de nombres verifica sus tablas de máquinas a ver si allí consigue el nombre por el cual le están preguntando. Si es así, entonces retorna la dirección IP asociada con ese nombre. Si la información pertenece a otro dominio, el servidor de nombres busca en su caché y si no está allí entonces comienza el proceso de resolución que se puede comportar de las siguientes dos formas:

3.1.3.10.1. Recurrente. Un servidor de nombres envía una respuesta recurrente cuando es el servidor y no el cliente el que pregunta a otros servidores de nombres por la información solicitada del dominio. Esto ocurre cuando el servidor de nombres sabe que el "resolver" no tiene la inteligencia para manejar una referencia a otro servidor de nombres (Es decir, el "resolver" hace explícitamente una pregunta recurrente). A medida que un servidor de nombres pregunta (obtenga respuesta o no) va guardando los nombres encontrados en su caché para evitarse búsquedas innecesarias.

3.1.3.10.2. Iterativa. El servidor de nombres da la mejor respuesta, que ya sabe, a quien preguntó (es decir, da una referencia al servidor de nombres más cercano a la información de dominio interrogado). Primero consulta sus datos locales, si no está allí busca entonces en su caché y si aún no encuentra nada devuelve la respuesta al servidor más cercano al dominio buscado. Si el servidor falla, no lo vuelve a reintentar.

Las bibliotecas del "resolver" hacen búsquedas recurrentes e iterativas, mientras que entre servidores de nombres solo se hacen búsquedas iterativas.

3.1.3.11. Equivalencia de direcciones a nombres. Una vez conceptualizada la conversión de nombres a direcciones, se debe detallar la conversión de una dirección IP a nombres. Cuando se usan las tablas de hosts de las máquinas (hosts tables), la conversión es fácil y requiere de una búsqueda secuencial a lo largo de la tabla usando una dirección.

En DNS, sin embargo, el espacio de dominio de nombres está indexado por nombres y no por números (como es el caso de una dirección IP). DNS soluciona esto, valiéndose de un dominio, el cual usa números como nombres, el dominio in-addr.arpa. Los nodos en el dominio in-addr.arpa son nombrados después de los números en una representación de octetos separados por puntos.

En este dominio la dirección IP se lee desde lo más específico a lo más general; por ejemplo, **superban.gov.ec**. (192.168.3.26) se leería 3.168.192.in-addr.arpa, lo cual

retorna en una búsqueda a **superban.gov.ec**. La razón por la que se escribe así, es porque una dirección IP también es jerárquica.

3.1.3.12. Caching. Podría parecer que el proceso de buscar un nombre es sumamente lento, sin embargo no es así. Una de las razones de la rapidez es el uso de caching. Este mecanismo trabaja de la siguiente manera: Un servidor de nombres que está ejecutando una búsqueda recurrente podría enviar unas cuantas preguntas para encontrar una respuesta acerca de un dominio. Sin embargo, el servidor descubre información acerca del nombre del dominio a medida que explora. Cada vez que es referido a otro servidor, aprende que esos servidores son autoridades de las zonas interrogadas y retiene esas direcciones. Si encuentra el dato buscado, lo guarda para usarlo en una futura referencia. La próxima vez que un “resolver” haga una pregunta acerca de un nombre de un dominio que el servidor conozca, el proceso es acortado, ya que el servidor primero revisará en su caché para dar la respuesta.

El caché solamente se guarda en memoria temporal la cual se borra cuando el servidor reactualiza su memoria (por ejemplo, cuando se apaga la máquina en la que corre el servidor).

3.1.3.13. Tiempo de vida (TTL -Time To Live). Estos tiempos son los que le dicen a un servidor secundario cuanto tiempo debe mantener en memoria sus datos antes de buscar datos actualizados del servidor maestro. Los servidores de nombres no mantienen los datos en caché por siempre. El administrador de una zona decide el tiempo de vida de los datos, buscando un balance entre la veracidad de la información y la cantidad de tiempo perdido en transferir una zona. Una vez que el tiempo de vida expira, el servidor busca de nuevo los datos del dominio, del cual es servidor secundario.

3.2. SERVICIO DE ACCESO REMOTO (RAS)

Antes de dar un concepto de lo que es el servicio de acceso remoto (RAS), primero se debe tener en cuenta los conceptos de los diferentes enlaces conmutados que existen.

3.2.1. Enlaces Conmutados. Los enlaces conmutados se dividen en dos tipos: análogos y digitales. Los primeros llegan hasta tasas de 53 kbit/s para downlink (descarga de información) y hasta de 48 kbit/s para uplink (subida de información), los segundos transmiten y reciben a 64 kbit/s o 128 kbit/s. Estos últimos son conocidos como enlaces RDSI (o ISDN, en inglés) que son las siglas de Red Digital de Servicios Integrados.

3.2.1.1. Enlaces Conmutados Análogos. Fue quizá la primera tecnología de transmisión de datos que usó el hombre para construir redes privadas entre dos sitios remotos. Esto lo hizo aprovechando la Red de Telefonía Pública Conmutada – RTPC (PSTN, en inglés), dicha red ha tenido muchos desarrollos en los últimos 20 años. El servicio tradicional que la RTPC ha prestado ha sido comunicación de voz, y solo recientemente se empezó a usar para soportar un creciente mercado de transferencia de datos.

El rango de frecuencia de la voz humana va desde los 20Hz hasta los 20Khz, pero casi toda la energía espectral se encuentra entre los 300Hz y 3.4Khz, por ende, la ITU ha definido un canal de voz (speech channel) para telefonía en esta banda. Por cuestiones prácticas, y para evitar efectos aliasing se maneja el canal desde los 0Hz hasta los 4KHz, dejando unos pocos Hz como bandas de guarda.

De este criterio partió todo el desarrollo que se ha hecho sobre las redes de telefonía, todos los equipos fueron diseñados para transmitir señales en este rango. Las investigaciones que se hicieron en el campo de las comunicaciones han demostrado que transportar cualquier señal, incluso la voz, en formato digital tiene inmensas ventajas

comparado con una transmisión análoga, de allí que nuestra voz sea convertida en una señal digital en las centrales telefónicas y transportada de la misma manera entre ellas.

Apoyándose un poco en la teoría, el criterio de muestreo de Nyquist dice que para recuperar una señal análoga partiendo de ella misma, pero digitalizada, se tiene que muestrear al doble de la frecuencia máxima, es decir que para la voz humana la tasa de muestreo debe ser 8Khz. Si se usan conversores A/D – D/A de 8 bits se necesita un canal de transporte de 64 kbit/s, de allí proviene la tasa básica de transmisión de voz, y que hoy prácticamente ha sido una limitante para las comunicaciones de datos sobre redes telefónicas, que se pensaron inicialmente solo para voz.

En un enlace conmutado de datos, intervienen varios equipos desde el usuario inicial hasta el punto o equipo destino. La figura 3.2 muestra los componentes de un enlace típico de datos sobre la red telefónica pública, se puede notar la necesidad de realizar una conversión A/D y otra D/A. La inercia resultante de todo este proceso electrónico es la limitante en la velocidad de las comunicaciones analógicas (56 kbit/s), que incluso puede llegar a 33.6 kbit/s cuando aparece una tercera y cuarta conversión entre la Central Telefónica 2 y el terminador de la llamada.

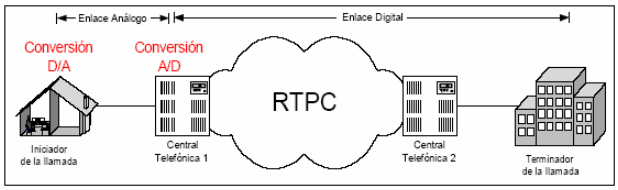

Figura 3.2. Componentes de un enlace de datos sobre la red telefónica pública

Se puede notar que la conexión entre el iniciador de la llamada y la central telefónica es análoga, y se lleva a cabo usando el mismo par de cobre de la línea telefónica, para esto se usa un MODEM análogo. Mientras que en el lado del sitio remoto la conexión es digital, y para esto se usan enlaces RDSI PRI o BRI. Por lo general los equipos que intervienen en este lado son servidores de acceso remoto (Remote Access Server – RAS). Cuando este enlace es también análogo, entonces se puede notar que en el proceso total de la conexión intervienen cuatro conversiones, dos

A/D y dos D/A, esto hace que la tasa de transmisión y de recepción máximas sean apenas de 33.6 kbit/s.

Servicio de Acceso Remoto. El servicio de acceso remoto (RAS) conecta al usuario con una red remota a través de una línea telefónica. Una vez hecha la conexión, la línea telefónica se hace transparente y el acceso a los recursos de red se efectúa como si la computadora estuviera conectada directamente a la red. Con RAS el módem actúa como una tarjeta de red añadiendo al computador a la red.

3.2.2. Características del servicio. Entre las características de mayor relevancia de estos sistemas se encuentran:

3.2.2.1. Limitaciones de las conexiones RAS. El servicio de acceso remoto debe soportar conexiones simultáneas, lo que exige del equipo mayor capacidad de procesamiento y puertos a los que accederán los usuarios remotos, elevando así su costo.

3.2.2.2. Compresión de datos en RAS. Esta compresión se da a nivel de software basándose en los algoritmos, como por ejemplo de ***DRVSPACE*** con un promedio de 2 a 1. Esta compresión puede mejorar la velocidad de las conexiones.

3.2.2.3. Escalabilidad. El servidor RAS es multithreaded y puede soportar multiprocesamiento. Esto permite a los threas del RAS ejecutarse en los varios procesadores de una computadora, mejorando el rendimiento del RAS.

3.2.2.4. Soporte a Redes de Área Amplia. El servicio de acceso remoto debe soportar los siguientes métodos para establecer una conexión entre clientes y servidores:

- Líneas públicas estándares.
- X.25
- ISDN (Integrated Services Digital Network)

3.2.2.5. Seguridad. El servicio RAS debe implementar varias medidas de seguridad para asegurar el acceso de los usuarios remotos a la red. En ciertos aspectos, la conexión con RAS es más segura que trabajar en la red local.

3.2.2.6. Validación y autentificación Encriptada. La información de la autentificación y validación debe ser encriptada cuando se transmite a través de la línea telefónica. El resto de la sesión no es encriptada a menos que se configura manualmente.

3.2.2.7. Auditoria. Con la auditoria habilitada, RAS registrará todas las conexiones remotas incluyendo actividades como la autentificación, validación, etc.

3.2.2.8. Hosts intermedios de Seguridad. Es posible añadir otro nivel de seguridad a la configuración de RAS conectando un host intermedio de seguridad, el usuario escribirá una clave de acceso o un código antes de establecer la conexión con el servidor RAS.

3.2.2.9. Call Back Security. El servidor RAS debe poder ser configurado para proveer call backs (regresar llamadas) como un medio para incrementar la seguridad. El call back puede ser al teléfono de donde se marcó o a un número especificado. El método de call back se define por usuario.

3.3. SERVICIO DE RED PRIVADA VIRTUAL (VPN)

3.3.1. Introducción. Es comúnmente aceptado el hecho que las tecnologías de información en Internet han cambiado la forma como las compañías se mantienen comunicadas con sus clientes, socios de negocios, empleados y proveedores.

Inicialmente las compañías eran conservadoras con la información que publicaban en Internet, tal como, productos, disponibilidad de los mismos u otros ítems comerciales. Pero recientemente, con el auge que ha tenido Internet por la reducción de costos que la gente tiene que pagar para acceder a esta gran red y con el significado que ha adquirido como el principal medio mundial de comunicación, las redes privadas virtuales han hecho su aparición con más fuerza que nunca y se han ganado un espacio dentro del tan cambiante mundo de las redes de información.

Tradicionalmente, un enlace privado se ha hecho por medio de tecnologías WAN como X.25, Frame Relay, ATM, enlaces Clear Channel o enlaces conmutados. Ahora con el gran crecimiento de Internet, es posible usar un protocolo como IP, sin importar la tecnología WAN que lo soporte, para disfrutar de los servicios y ventajas que ofrecen las redes privadas. Y mientras que las tradicionales redes privadas se han hecho fuertes en las conexiones LAN-to-LAN, no han sido capaces de atacar el mercado de los usuarios individuales o pequeñas oficinas sucursales, y es aquí principalmente donde han surgido con fuerza las soluciones basadas en VPNs sobre IP, pues su implementación resulta sencilla y bastante económica.

Además el hecho que las VPNs se construyan sobre infraestructuras públicas ya creadas, ha hecho que las empresas ahorren más del 50% del costo que antes tenían que pagar en llamadas de larga distancia y en equipos físicos de acceso remoto o en alquiler de enlaces privados o dedicados.

Las formas en que se pueden implementar VPNs pueden ser basadas en HARDWARE o a través de SOFTWARE, pero lo más importante es el protocolo que se utilice para la implementación.

Las VPNs basadas en HARDWARE utilizan básicamente equipos dedicados como por ejemplo los routers, son seguros y fáciles de usar, ofreciendo gran rendimiento ya que todos los procesos están dedicados al funcionamiento de la red a diferencia de un sistema operativo el cual utiliza muchos recursos del procesador para brindar otros servicios, en síntesis, los equipos dedicados son de fácil implementación y buen rendimiento, solo que las desventajas que tienen son su alto costo y que poseen sistemas operativos propios y a veces también protocolos que son PROPIETARIOS.

Existen diferentes tecnologías para armar VPNs:

- DLSW: Data Link Switching(SNA over IP)
- IPX for Novell Netware over IP
- GRE: Generic Routing Encapsulation
- ATMP: Ascend Tunnel Management Protocol
- IPSEC: Internet Protocol Security Tunnel Mode
- PPTP: Point to Point Tunneling Protocol
- L2TP: Layer Two Tunneling Protocol

3.3.2. ¿Qué son las redes privadas virtuales – VPNs? Una VPN es una conexión que tiene la apariencia de un enlace dedicado pero trabaja sobre una red pública. Para este propósito usa una técnica llamada entunelamiento (**tunneling**), los paquetes de datos son enrutados por la red pública, tal como Internet o alguna otra red comercial, en un túnel privado que simula una conexión punto a punto. Este recurso hace que por la misma red puedan crearse muchos enlaces por diferentes túneles virtuales a través de la misma infraestructura.

También hace universales para su transporte los diferentes protocolos LAN entre los que se encuentran IP, IPX, Appletalk y Netbeui, de allí la característica de multiprotocolo que hace sumamente universal la tecnología de las redes virtuales privadas. La Figura 3.3 muestra los distintos escenarios que se pueden manejar con la tecnología de Redes Privadas Virtuales (Dial-Up, Intranet VPN y Extranet VPN).

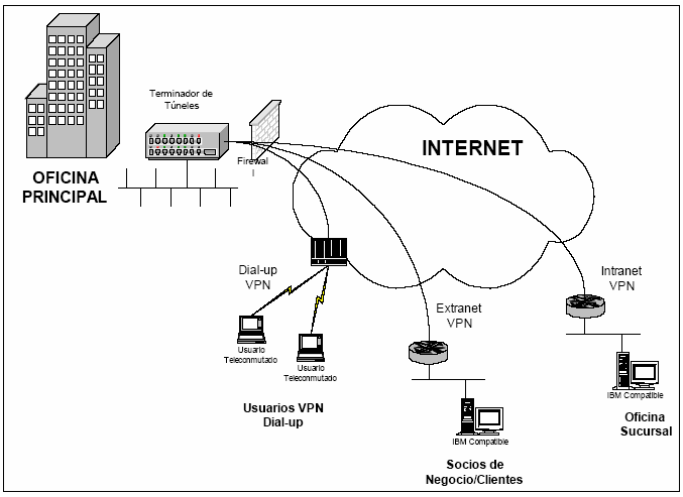

Figura 3.3. Escenarios VPN

Las técnicas de entunelamiento básicamente consisten en encapsular los paquetes de datos que salen de una LAN o del equipo del usuario remoto dentro de protocolos que trabajan a nivel 2 de la capa OSI.

Los componentes básicos de un túnel (Fig. 3.4) son:

- Un iniciador del túnel.
- Uno o varios dispositivos de enrutamiento.
- Un conmutador de túneles (opcional).
- Uno o varios terminadores de túneles.

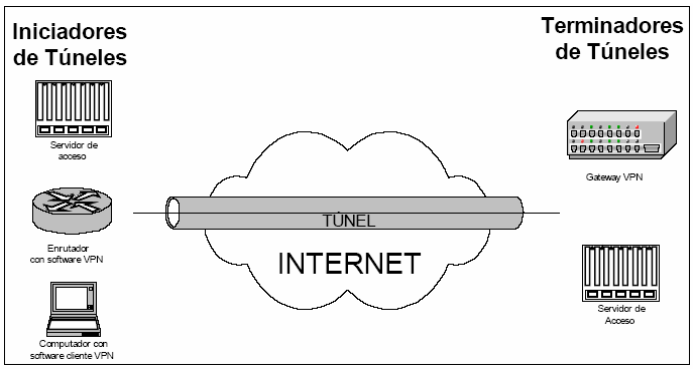

Figura 3.4. Elementos básicos de un túnel VPN

El inicio y la terminación del túnel pueden ser hechos por una amplia variedad de equipos o software. Un túnel puede ser empezado, por ejemplo, por un usuario remoto con un computador portátil equipado con un MODEM análogo y un software de conexión telefónica para hacer una VPN, también puede haber un enrutador de una extranet en una oficina remota o en una LAN pequeña. Un túnel puede ser terminado por otro enrutador habilitado para tal fin, por un switch con esta característica o por un software que haga tal fin.

Adicionalmente y para completar una solución VPN deben existir uno o más dispositivos o paquetes de software que brinden cifrado, autenticación y autorización a los usuarios del túnel. Además muchos de estos equipos brindan información sobre el ancho de banda, el estado del canal y muchos más datos de gestión y de servicio.

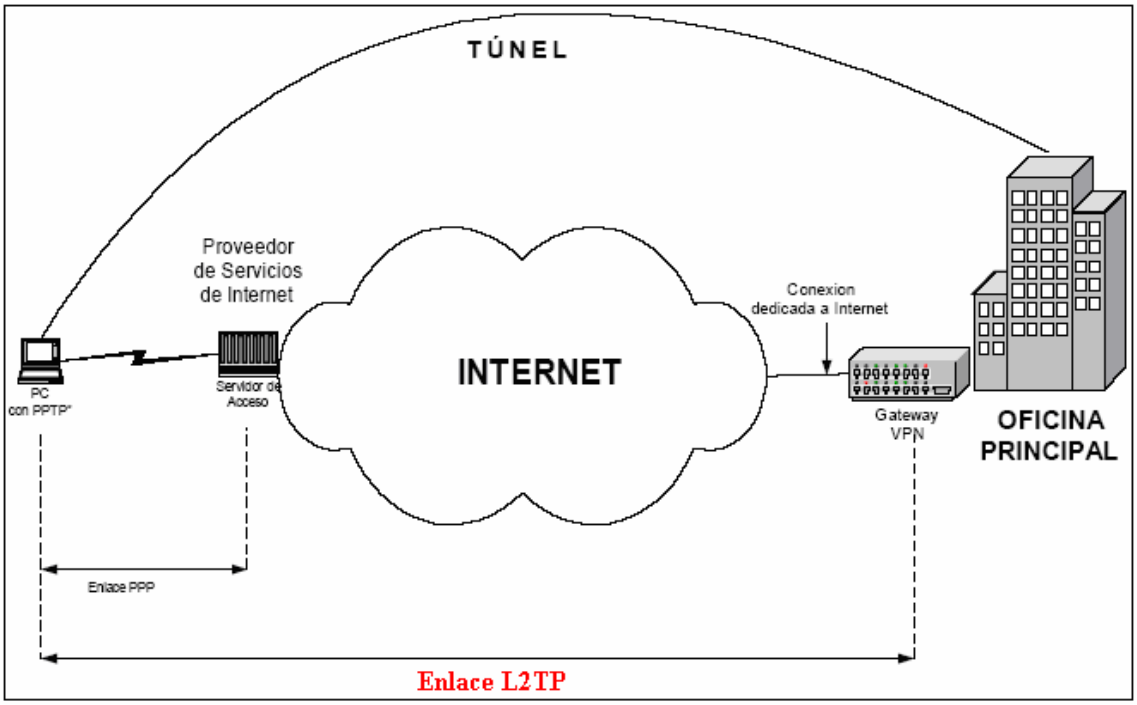

Figura 3.5. Topología VPN (L2TP/IPSec)

La figura 3.5 muestra un diagrama más detallado de una VPN dial-up usando como protocolo de entunelamiento a L2TP. Se notan los trayectos en los cuales el

protocolo que encapsula los datos es PPP y la parte del recorrido que es tunelizada usando L2TP.

En muchos casos las características que les permiten a los dispositivos ser iniciadores o terminadores del túnel se pueden adicionar con una simple actualización del sistema operativo o de sus tarjetas. Una buena solución VPN requiere la combinación de tres componentes tecnológicos críticos: seguridad, control de tráfico y manejo empresarial.

3.3.2.1. Seguridad. Dentro de este punto se destacan: el control de acceso para garantizar la seguridad de las conexiones de la red, el cifrado para proteger la privacidad de los datos y la autenticación para poder verificar acertadamente tanto la identidad de los usuarios como la integridad misma de la información.

3.3.2.2. Control de tráfico. El segundo componente crítico en la implementación de una efectiva VPN es el control de tráfico que garantice solidez, calidad del servicio y un desempeño veloz. Las comunicaciones en Internet pueden llegar a ser excesivamente lentas, lo que las convertirían en soluciones inadecuadas en aplicaciones de negocios donde la rapidez es casi un imperativo. Aquí es donde entran a jugar parámetros como la prioridad de los datos y la garantía del ancho de banda.

3.3.2.3. Manejo empresarial. El componente final crítico en una VPN es el manejo empresarial que la misma posea. Esto se mide en una adecuada integración con la política de seguridad de la empresa, un manejo centralizado desde el punto inicial hasta el final, y la escalabilidad de la tecnología.

Las VPNs se caracterizan también por su flexibilidad. Pueden ser conexiones punto-punto o punto-multipunto. Reemplazando una red privada con muchos y costosos enlaces dedicados, por un solo enlace a un ISP que brinde un punto de presencia en la red (POP por sus siglas en inglés), una compañía puede tener fácilmente toda una infraestructura de acceso remoto, sin la necesidad de tener una gran cantidad de líneas telefónicas análogas o digitales, y de tener costosos pools de módems o servidores de

acceso, o de pagar costosas facturas por llamadas de larga distancia. En algunos casos los ISP se hacen cargo del costo que les genera a los usuarios remotos su conexión a Internet local, pues ven en este tipo de negocio un mayor interés por los dividendos del acceso.

El objetivo final de una VPN es brindarle una conexión al usuario remoto como si estuviera disfrutando directamente de su red privada y de los beneficios y servicios que dentro de ella dispone, aunque esta conexión se realice sobre una infraestructura pública.

3.3.3. Arquitecturas VPN. El éxito de una VPN depende de una adecuada elección de la tecnología y del escenario, siempre acordes a las necesidades que se tengan. La tecnología implica: técnicas de entunelamiento, autenticación, control de acceso, y seguridad de los datos; y los escenarios que se pueden construir son:

- **Intranet VPN (LAN-to-LAN VPN).-** En este escenario, múltiples redes remotas de la misma compañía son conectadas entre si usando una red pública, convirtiéndolas en una sola LAN corporativa lógica, y con todas las ventajas de la misma.

- **Acceso Remoto VPN.-** En este caso, un host remoto crea un túnel para conectarse a la Intranet corporativa. El dispositivo remoto puede ser un computador personal con un software cliente para crear una VPN, y usar una conexión conmutada, o una conexión de banda ancha permanente.

- **Extranet VPN**.- Esta arquitectura permite que ciertos recursos de la red corporativa estén disponibles por redes de otras compañías, tales como clientes o proveedores, sin dejar a un lado el control de acceso.

3.3.3.1. Intranet VPN LAN-to-LAN. Tradicionalmente, para conectar dos o más oficinas remotas de una misma compañía se han necesitado contratar enlaces dedicados Clear Channels o Circuitos Virtuales Permanentes (PVCs) Frame Relay.

Las empresas adoptan diferentes topologías de red WAN para interconectar todos sus sitios remotos, entre estas se encuentran: Enlaces punto-a-punto, de estrella, de malla parcial y de malla completa. Las Figuras 3.6, 3.7, 3.8 y 3.9 detallan cada una de las topologías anteriormente mencionadas.

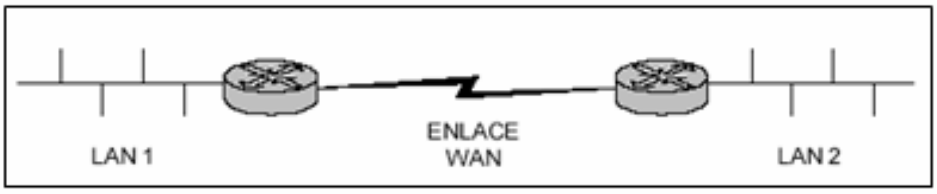

Figura 3.6. Enlace Punto a punto

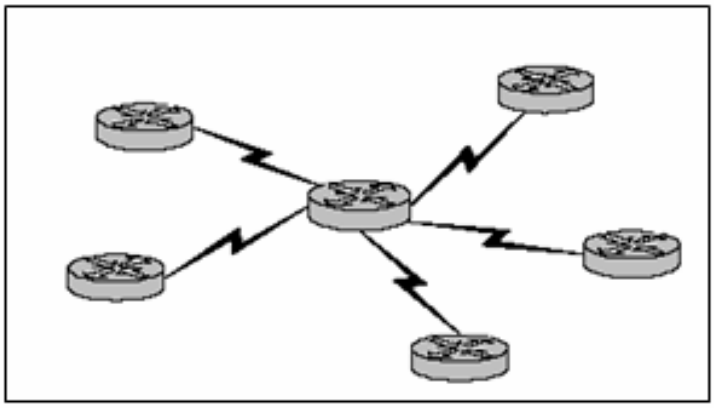

Figura 3.7. Topología en Estrella

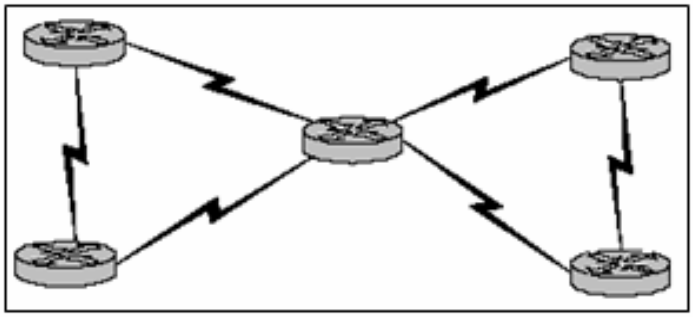

Figura 3.8. Topología de malla parcial

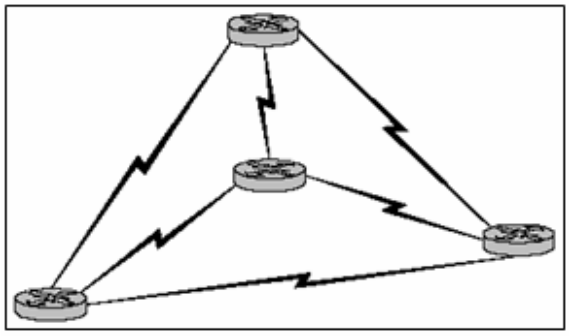

Figura 3.9. Topología de malla completa

En general, cuando se necesita concentrar tráfico en al menos un nodo, es preferible usar tecnologías como Frame Relay pues solo se necesita un canal de última milla por el cual viajan todos los PVCs contratados con el proveedor de servicio; pero económicamente sigue siendo igual de costosa, porque las compañías que prestan el servicio de interconexión Frame Relay cobran por PVC activado, así usen la misma solución de última milla. Si se observa bien, la mayoría de escenarios de enlaces WAN corporativos tienen más de dos nodos interconectados, por tanto habrá al menos un nodo donde existan al menos dos PVCs compartiendo un canal de última milla, esto sería por ejemplo, en la topología de estrella. Si cambiamos a malla completa o parcial, el número de PVCs aumentará considerablemente y con ellos los costos de la solución de transporte de datos. En la Figura 3.10 se observa con más detalle una solución Frame Relay usando topología de estrella.

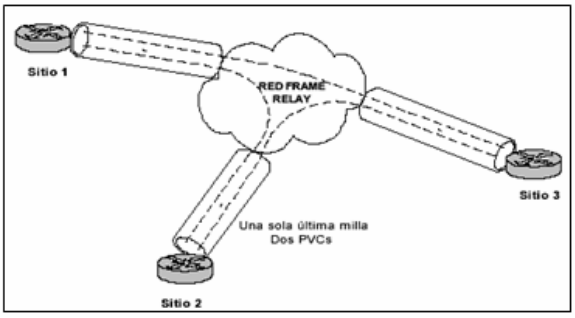

Figura 3.10. Detalle de 4 nodos en estrella con 2 PVCs

A parte del alto precio que tiene una solución Frame Relay o Clear Channel, hay otros factores (Tabla 3.4) a tener en cuenta para decidir cambiar este tipo de tecnologías a una solución usando VPNs, y son entre otras, la disponibilidad, la seguridad, la

eficiencia en el manejo del ancho de banda y la amplia cobertura que ha logrado Internet.

Tabla 3.4. Tabla básica comparativa entre enlaces Clear Channel y Frame Relay

Clear Channel	Frame Relay
Conexión dedicada y exclusiva Enlace permanente entre dos puntos	Enlace seguro y veloz en todo momento previa planificación del caudal de la Información a transmitir
Características	
Ideal para aplicaciones que necesitan: flujo constante de información y calidad del enlace por largos períodos.	Por cada nuevo enlace se define un PVC, asignándole a éste, una velocidad de transferencia de Información mínima (CIR)
Parámetros que definen el servicio	
Ancho de banda	La velocidad del canal de acceso al cliente
Narrowband (64Kbps a 2 Mbps) Broadband (2/34/45/155/622 Mbps)	64/128/256/512/1024 Kbps y 2Mbps
Aplicaciones	
Interconexión Redes LAN. Interconexión de Redes de Voz. Interconexión entre centros de cómputo	Interconexión de Redes LAN (soporta la mayoría de protocolos existentes). Soporte de Redes que utilicen protocolos SNA. Servicio de Correo Electrónico. Internetworking (requiere. Alta velocidad).
Beneficios	
Exclusividad: Circuitos totalmente dedicados. Seguridad: Garantizada por la continuidad del servicio. Capacidad: Transmisión constante y escalable. Disponibilidad: Total	Múltiples: Locaciones enlazadas sin importar la distancia. Flexibilidad: Para optimizar las capacidades de las comunicaciones. Eficiencia: Menores costos por enlace de distintos puntos a través del mismo acceso. Adaptabilidad: A la evolución y crecimiento de las Redes de las Empresas.

La ventaja que han sustentado los tradicionales enlaces dedicados es la disponibilidad, sin embargo, estos enlaces también son susceptibles de caídas, y su montaje, en cuanto a hardware se refiere, es tan complejo que es prácticamente imposible cambiar a otro proveedor mientras el enlace se reestablece. Con un escenario **LAN-to-LAN VPN**, cuando un enlace a Internet del ISP que le presta el servicio a la empresa que tiene montada la VPN se cae, la conmutación a otro proveedor es prácticamente transparente para la empresa, ya que el enrutador de frontera del ISP (que

sirve de gateway de toda la red) se encarga de seleccionar otro enlace que se encuentra arriba.

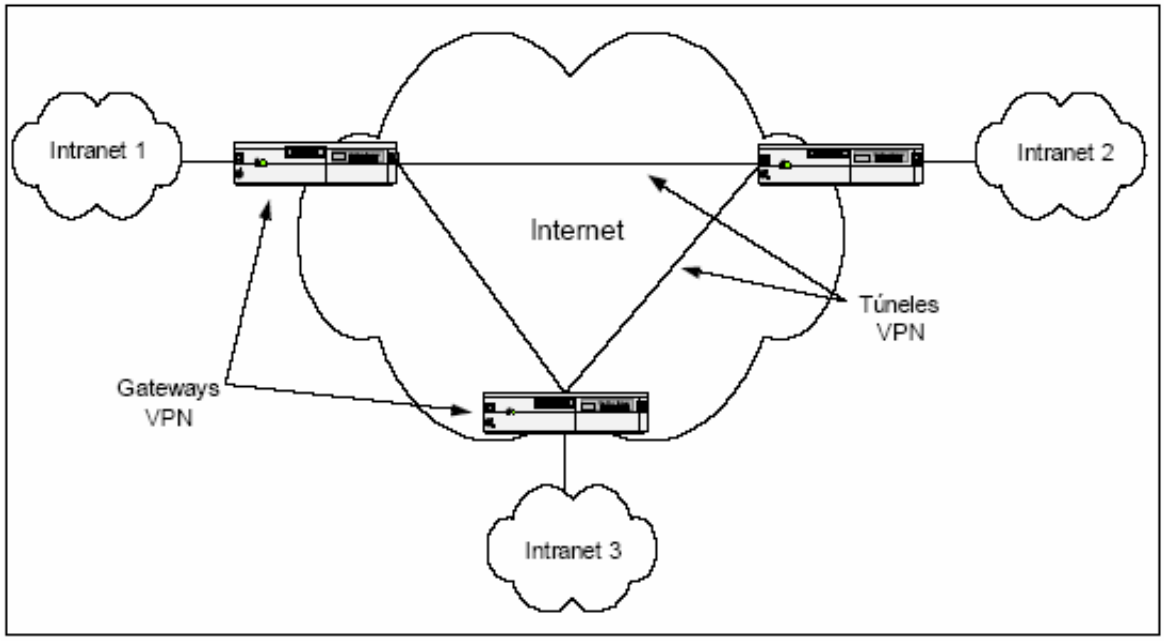

Figura 3.11. Esquema de una solución Intranet VPN (LAN-to-LAN VPN)

La figura 3.11 ilustra la conexión de tres oficinas de una misma compañía usando una arquitectura LAN-to-LAN (IPSEC) VPN. Nótese que los túneles VPN que aparecen señalados no son enlaces físicos sino lógicos que viajan por Internet. El único equipo que tiene que adquirir la compañía para cada oficina a conectar es un gateway VPN que tiene, por lo general, un puerto LAN (Ethernet o Fast Ethernet) para conectarse a la LAN Corporativa, y un puerto LAN o WAN para conectarse hacia el ISP. Muchos de estos gateways VPN trabajan como firewalls. Solo se necesita un canal de última milla por oficina, por ahí viajan todos los túneles VPN que se necesiten.

Si el enlace hacia Internet de la compañía no es dedicado sino conmutado, el mecanismo para cambiar de proveedor es mucho más sencillo, basta con configurar el gateway dial-up VPN con el número telefónico del otro ISP. Si se cuenta con un servicio de cable módem o ADSL solo se necesita conectar el cable del otro ISP al CPE (Customer Premise Equipment o Equipamiento terminal del cliente).

Con una arquitectura Intranet VPN (o LAN-to-LAN VPN) se puede lograr el mismo objetivo de interconectar dos o más sitios de una red corporativa y a un costo mucho menor. La economía se ve reflejada tanto en equipos que se tienen que adquirir o arrendar para el montaje inicial de la topología, como en cargos fijos que se tienen que pagar mes a mes.

Otro factor decisivo que ha hecho que las empresas comiencen a ver en las VPNs otra opción para el montaje de sus redes WAN usando esta tecnología es la aparición de los NAPs (o Puntos de acceso a la Red), que son lugares donde varias redes autónomas de sitios cercanos se conectan para intercambiar tráfico a alta velocidad, y así evitar que paquetes de información que se cruzan entre sitios en un mismo lugar geográfico tengan que ir hasta otros países o continentes, disminuyendo así los costos.

3.3.3.2. Acceso Remoto VPN. Fue la primera aplicación que se le dio a la emergente tecnología de las VPNs.

Consiste en usar cualquier RAS que preste servicio de conexión a Internet, como punto de acceso a una red corporativa, también conectada a Internet por medio de un gateway VPN. Esta solución nació de la necesidad de poder acceder a la red corporativa desde cualquier ubicación, incluso a nivel mundial. Con el Acceso Remoto VPN, los RAS corporativos quedaron olvidados, pues su mantenimiento era costoso y además las conexiones que tenían que hacer los trabajadores de planta externa, como vendedores y personal de soporte técnico, cuando viajaban fuera de la ciudad, y más aun, a otros países eran demasiado costosas.

El acceso remoto VPN se vio claramente impulsado por el auge de la Internet que ha hecho que prácticamente en todas partes del mundo se obtenga fácil acceso a la misma. Con este acceso VPN un trabajador que se haya desplazado a otro país, por ejemplo, y que quiere acceder a la base de datos de su compañía, al correo interno, o a cualquier otro recurso de su red corporativa, solo tiene que conectarse a Internet con una simple llamada local al ISP de la ciudad en la que se encuentre, y ejecutar su cliente de marcación VPN. A partir de la versión Windows98, Microsoft incluyó un cliente de

marcación VPN que funciona con el protocolo de entunelamiento PPTP, en Windows XP existe adicionalmente un cliente de marcación L2TP/IPsec. Todos los gateways VPN vienen con software VPN clientes para ser instalados en los distintos sistemas operativos presentes en el mercado.

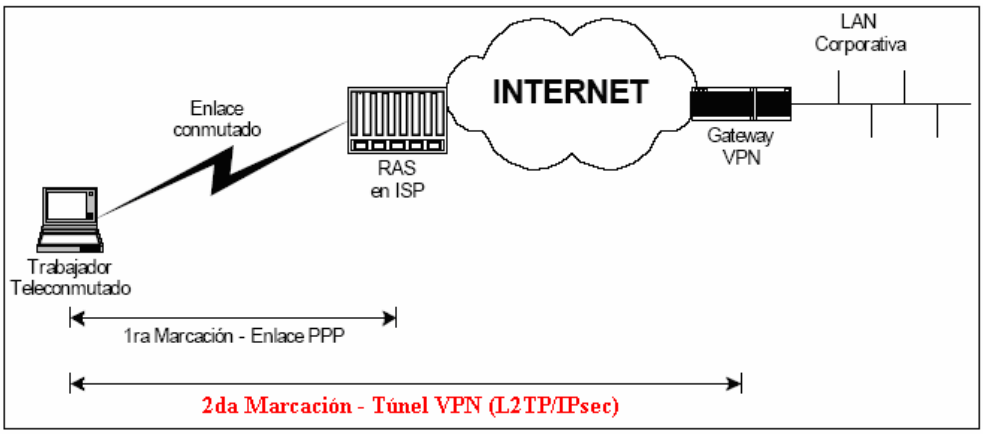

Figura 3.12. Escenario de Acceso remoto VPN.

La Figura 3.12 muestra la creación de un túnel conmutado VPN usando un cliente L2TP/IPsec instalado en el computador del trabajador remoto. Nótese que se realizan dos conexiones, una PPP al ISP, y una L2TP/IPsec al gateway VPN de la compañía que se encuentra conectado a Internet. La conexión PPP puede ser análoga o digital RDSI.

3.3.3.2.1. Protocolo IPSEC. El protocolo IPSec consiste en la "reimplementación" para IPV4 de las medidas de seguridad originalmente diseñadas para IPV6. IPSec define los siguientes protocolos:

- **AH (AUTHENTICATION HEADER).** Este protocolo consiste en incluir en los paquetes enviados una "firma" o hash, como se muestra en la figura 4.13, que permitirá verificar su autenticidad, sin modificar el paquete original (salvo el agregado de la "firma"). De la misma manera que el protocolo TCP se designa con el número 6, y UDP con el 17, este protocolo utiliza el número de protocolo IP 51 para ser identificado. Existen dos modos de conformar un paquete AH: el modo transporte y el modo túnel. Estos modos serán explicados más adelante dentro del protocolo ESP.

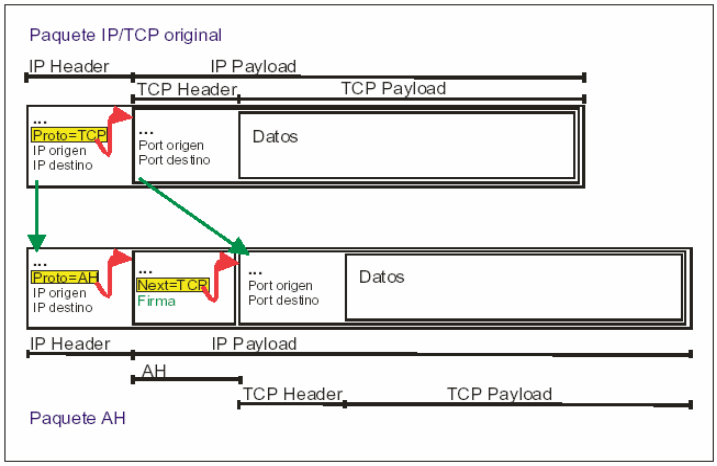

Figura 3.13. Conformación de un paquete AH en modo transporte

- **ESP (ENCAPSUTALED SECURITY PAYLOAD).** Este protocolo servirá para cifrar todo el contenido de los paquetes IP, además de poder verificar su autenticidad. A su vez, este protocolo, posee dos modos principales de operación: El modo transporte (**figura 4.14**), donde simplemente es cifrado el contenido de los paquetes que intercambian dos extremos, y el modo túnel (**figura 4.15**), donde un paquete IP es encapsulado dentro de otro, creando lo que normalmente se conoce como un túnel. Usualmente el modo transporte es utilizado para el cifrado de paquetes entre dos equipos, y el modo túnel entre dos redes. El protocolo ESP utiliza el número de protocolo 50.

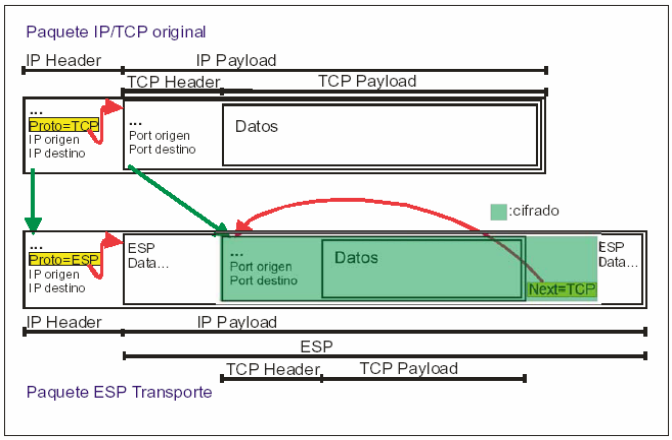

Figura 3.14. Conformación de un paquete ESP en modo transporte

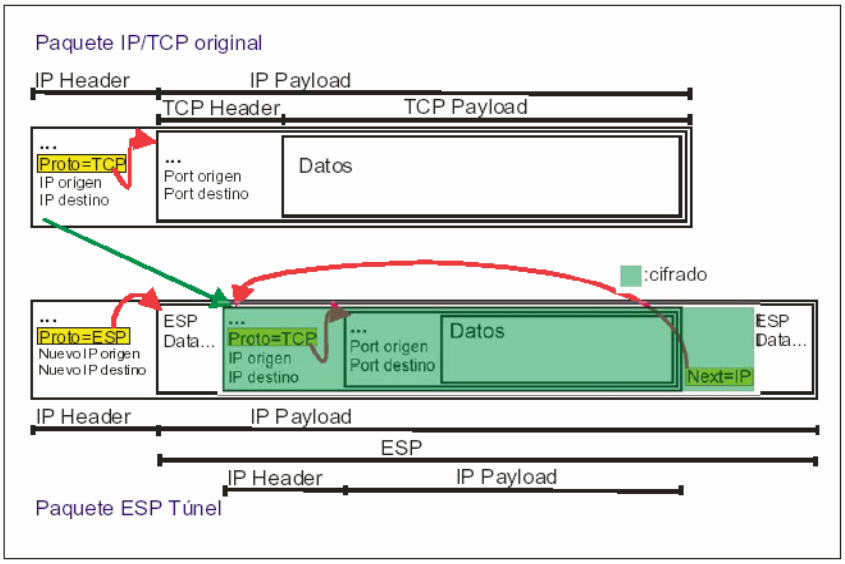

Figura 3.15. Conformación de un paquete ESP en modo túnel

- **PSK.** Las claves compartidas son un método válido de autenticación cuando sólo dos extremos la conocen, y además se utilizan claves suficientemente "fuertes". Las principales desventajas que posee son: que no son seguras, por un problema de diseño y que en el caso de ser compartidas por más de un extremo (por ejemplo, si las queremos utilizar para "usuarios remotos"), no podemos identificar cual de los "usuarios" es el que se conecta.

- **NAT-T.** Originalmente IPSec no fue pensado para convivir con NAT. Es por ello que posteriormente se definió el protocolo Nat-T, o Nat-Trasversal. Este protocolo, que recientemente pasó de la etapa de "Proponed Standard" a "Internet Standard" (bajo las **RFC 3947 y 3948**), facilita la convivencia de IPSec con la traducción de direcciones. OpenSwan Soporta Nat-t tanto en modo transporte como en modo túnel.

3.3.3.2.2. L2TP (LAYER 2 TUNNEL PROTOCOL). Es un protocolo definido como Estándar de Internet en la **RFC 2661**. Su trabajo es encapsular frames de un protocolo de capa 2 (ISO/OSI), para ser transportados a través de una red de conmutación de paquetes (por ejemplo, TCP/IP). En particular, se encapsularán frames PPP (Point to Point Protocol, habitualmente utilizado en las conexiones seriales, por ejemplo en un

dial-up), y se transportarán entre los extremos del túnel mediante el protocolo UDP. El extremo definido como servidor, o concentrador de túneles, utilizará el puerto 1701 para enviar y recibir paquetes UDP. En la Figura 3.16 puede verse una esquematización del encapsulamiento realizado.

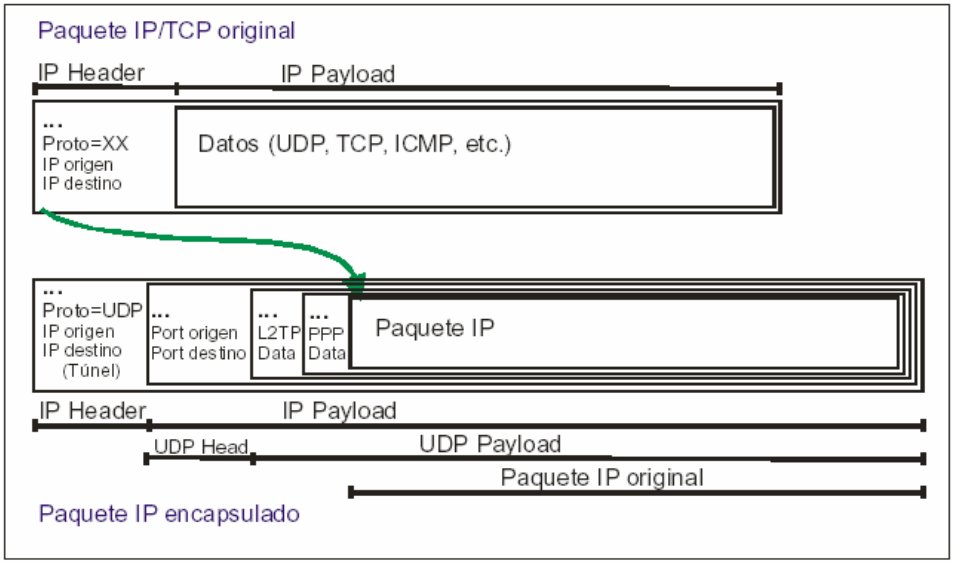

Figura 3.16. Encapsulamiento utilizando L2TP

Otra de las grandes ventajas del acceso remoto VPN sobre el tradicional acceso remoto es poder usar tecnologías de acceso de banda ancha como xDSL y cable módem. Para una empresa seria costoso e inconveniente tener un concentrador xDSL en sus instalaciones para permitirle a sus trabajadores teleconmutados el acceso a su red. Mientras que las VPNs usan la infraestructura existente de los proveedores del mercado para acceder a gran velocidad a la red corporativa.

El mejor intento de una empresa por tener su propia infraestructura de acceso tradicional (no VPN) sería montar un RAS con capacidad para recibir conexiones RDSI-BRI, es decir velocidades de 64 kbit/s o 128 kbit/s, además si la llamada la origina un trabajador en otra ciudad o país se tienen que sumar los cargos de esas llamadas.

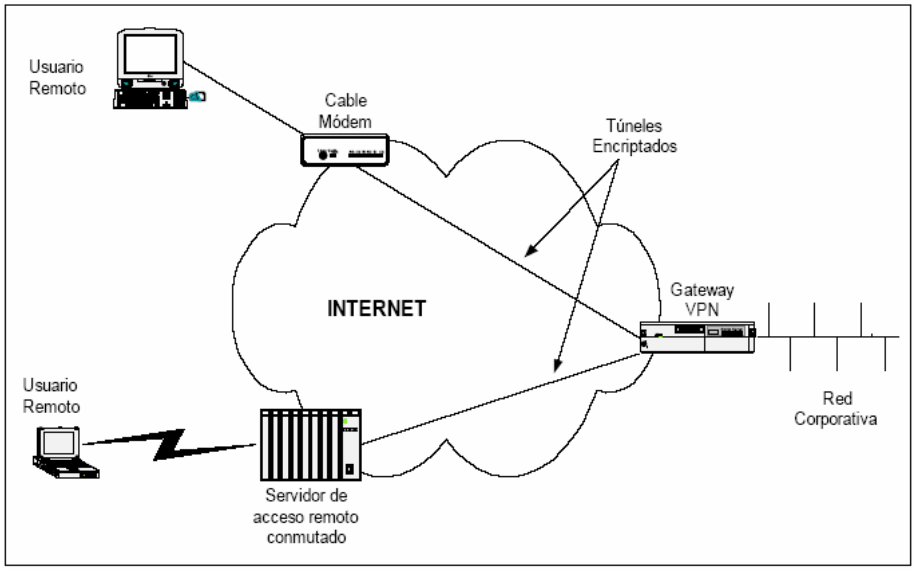

Figura 3.17. Dos montajes típicos de un acceso remoto VPN

La Figura 3.17 ilustra dos tipos de accesos remotos VPN, uno de banda ancha, donde el usuario remoto que crea el túnel tiene una conexión cable módem (también aplica xDSL) hacia el ISP; y otro acceso por medio de un módem análogo común, en este caso el usuario remoto podría estar en otra ciudad o incluso en otro país.

3.3.3.3. Extranet VPN. Las empresas necesitan intercambiar información y realizar transacciones no solamente entre sitios de su misma organización sino también con otras compañías. Hoy en día todas las empresas están haciendo presencia en la Internet y esto hace casi imperativo la comunicación con las otras empresas por este medio.

Ciertamente con una arquitectura de Extranet VPNs cada empresa tiene que controlar muy meticulosamente el acceso a los recursos de su red corporativa y a los datos que van a intercambiar con sus socios de negocios. Implementar una topología Extranet VPN implica incrementar la complejidad de los sistemas de control de acceso y de autenticación. Adicionalmente la tendencia de los mercados hacen que un cambio en la topología se pueda realizar fácilmente, para esto una Extranet VPN debe poder adicionar y eliminar dinámicamente acceso seguro a otras compañías.

La presencia de una compañía en Internet y el uso de la arquitectura de Extranet VPN, hace posible crear conexiones dinámicas seguras a otras redes sin necesidad de cambiar la infraestructura física. Al igual que en una arquitectura LAN to LAN VPN es necesario un gateway VPN que se instala en la frontera de la red corporativa. Los túneles son creados a través de Internet entre este gateway y el gateway VPN situado en la red de la otra empresa. De otro modo un cliente VPN en un computador independiente podría acceder a la red corporativa como un cliente, usando cualquier acceso remoto.

En la actualidad la mayoría de los gateways VPN pueden establecer múltiples túneles seguros a múltiples empresas. Sin embargo, es importante que una empresa no sea capaz de obtener acceso a la información de otra compañía que está accediendo por medio de Extranet VPNs. Un nivel más de seguridad puede ser adicionado, ubicando recursos exclusivos a cada una de las compañías que va a acceder a la red de interés en diferentes servidores.

3.3.4. Modelos de entunelamiento. En las VPN los sitios de terminación (terminadores) de los túneles son aquellos donde se toman las decisiones de autenticación y las políticas de control de acceso y donde los servicios de seguridad son negociados y otorgados. En la práctica hay tres tipos posibles de servicios de seguridad que dependen de la ubicación de los terminadores:

- **El primer caso** es aquel donde el terminador está en el mismo host, donde los datos se originan y terminan.
- **En el segundo caso** el terminador está en el gateway de la LAN corporativa donde todo el tráfico converge en un solo enlace.
- **El tercer caso** es aquel donde el terminador está localizado fuera de la red corporativa, es decir en un Punto de Presencia (POP) del ISP.

Dado que un túnel VPN se compone de dos terminadores, se pueden obtener seis tipos de modelos de seguridad derivados de la posible combinación de las diferentes

localizaciones: End-to-End, End-to-LAN, End-to-POP, LAN-to-LAN, LAN-to-POP y POP-to-POP, en la figura 3.18 se notan cada uno de ellos.

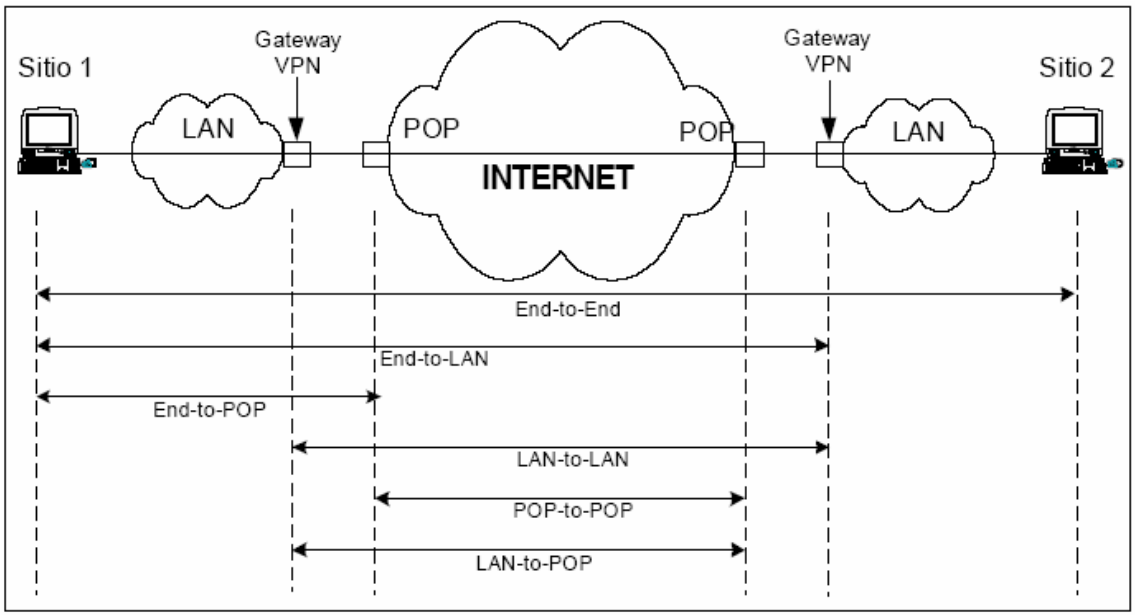

Figura 3.18. Modelos de entunelamiento VPN

3.3.4.1. Modelo End-to-End. En el modelo End-to-End el túnel va desde un extremo hasta el otro del sistema. Por lo tanto, los servicios de seguridad son negociados y obtenidos en la fuente y en el destino de la comunicación. Este escenario presenta el más alto nivel de seguridad dado que los datos siempre están seguros en todos los segmentos de la red, bien sea pública o privada. Sin embargo, el total de túneles que puede haber en una empresa grande, dificulta el manejo de los servicios de seguridad requeridos por dichos host. Este modelo de seguridad es comúnmente visto en implementaciones de capas superiores, como es el caso de SSL (Secure Sockets Layer). Tales implementaciones no son consideradas como modelos de entunelamiento.

3.3.4.2. Modelo End-to-LAN. En el modelo End-to-LAN, el túnel comienza en un host y termina en el perímetro de una LAN en la cual reside el host destino. Un dispositivo VPN localizado en el perímetro de la red es el responsable de la negociación y obtención de los servicios de seguridad de los host remotos. De esta manera, la

seguridad de un gran número de dispositivos en una red corporativa puede ser manejada en un único punto, facilitando así la escalabilidad del mismo.

Dado que la red corporativa es considerada un sitio seguro, comúnmente no hay necesidad de encriptar la información que transita dentro de ella. La mayoría de implementaciones de acceso remoto VPN trabajan con este modelo.

3.3.4.3. Modelo de entunelamiento End-to-POP. El modelo de entunelamiento End-to-POP es aquel en el cual un host remoto termina el túnel en un POP del ISP. Un dispositivo VPN o un equipo con funciones de terminador VPN y que se encuentra en la red del ISP es el responsable por la negociación y concesión de los servicios de seguridad. La entrega de los datos desde el POP hasta el host destino es por lo general asegurada con infraestructura física, la cual separa el tráfico del resto de la red pública. Por lo general en este caso el ISP administra los permisos y controla el acceso según las directivas de los administradores de red de las empresas clientes. La arquitectura de acceso remoto VPN también usa este modelo.

3.3.4.4. Modelo LAN-to-LAN. En el modelo LAN-to-LAN ambos hosts usan dispositivos VPNs situados en la frontera de la red corporativa para negociar y conceder servicios de seguridad. De esta manera, las funciones de seguridad no necesitan ser implementadas en los hosts finales donde los datos son generados y recibidos. La implementación de los servicios de seguridad es completamente transparente para los hosts. Esta implementación reduce drásticamente la complejidad en el manejo de las políticas de seguridad. La arquitectura Intranet VPN encaja en este modelo.

3.3.4.5. Modelo LAN-to-POP. En el modelo de LAN-to-POP el túnel comienza en un dispositivo VPN localizado en la frontera de la red corporativa y termina en un dispositivo VPN el cual se encuentra en un POP del ISP. En la actualidad prácticamente este modelo de entunelamiento no es aplicado.

3.3.4.6. Modelo POP-to-POP. Finalmente, en el modelo POP-to-POP ambos dispositivos VPN son localizados en la propia red del ISP. Por lo tanto los servicios de

seguridad son completamente transparentes para los usuarios finales del túnel. Este modelo permite a los proveedores de servicio implementar valores agregados a los clientes sin que estos alteren la infraestructura de sus redes.

De los seis modelos anteriores el End-to-LAN y el LAN-to-LAN son los más extensamente usados en las soluciones VPN. Sin embargo, el POP-to-POP o modelo de seguridad basado en red, ha cobrado vigencia últimamente dado que permite a los ISPs implementar servicios de valores agregados para sus clientes.

CAPITULO IV

DISEÑO Y CONFIGURACIÓN DE LOS SERVICIOS DE COMUNICACIÓN PARA LA PROPUESTA TECNOLÓGICA DE BACKUP PARA LA SBS

4.1. SERVICIOS SOBRE PLATAFORMA LINUX

4.1.1. Plan de direccionamiento IP – SBS. Como se mencionó en capítulos anteriores el propósito principal del proyecto es migrar los servicios de comunicación que proporciona el servidor Windows NT a un servidor Linux, para lo cual es necesario evaluar el direccionamiento IP configurado en el mismo. Las subredes detalladas en la tabla 4.1 (direcciones ficticias) permiten observar la estructura y difusión de las direcciones IP proporcionadas por el servidor NT hacia los usuarios de la red Institucional de la Superintendencia de Bancos y Seguros.

En esta estructura se reserva la subred 192.168.3.XX y las direcciones 192.168.0.119 y 192.168.0.120, ya que son de uso exclusivo de los servidores propios de la Red Institucional.

LA DIRECCIÓN IP IMPLEMENTADA EN TODOS LOS ARCHIVOS DE CONFIGURACIÓN DEL SERVIDOR LINUX DE LA SUPERINTENDENCIA DE BANCOS Y SEGUROS ES LA 192.168.3.26 /255.255.248.0 (dirección ficticia pero que se encuentra en el rango de las direcciones reservadas para uso exclusivo de servidores).

Tabla 4.1. Direccionamiento IP

192.168.0.1	192.168.0.118
192.168.0.121	192.168.0.254
192.168.1.0	192.168.1.254
192.168.2.0	192.168.2.254
192.168.3.0	192.168.3.254
192.168.4.0	192.168.4.254
MÁSCARADE SUBRED **255.255.248.0**	

4.1.2. Configuración de los servicios de comunicaciones bajo plataforma Linux. Una vez obtenido y evaluado el plan de direccionamiento IP de la Entidad se procede a configurar los servicios que proporcionará el servidor Linux, tales como DHCP, DNS, Monitores, Cortafuegos y VPN. Para este propósito la SBS proporcionó un servidor marca DELL, cuyas características técnicas serán ampliadas en el servicio VPN.

Entre los protocolos y servicios que brindará el mismo, a futuro, se destaca los demonios **NAMED, HTTPD, DHCPD e IPTABLES** y el protocolo **SSH.**

- **NAMED-** El demonio NAMED es el encargado de activar el servicio DNS del servidor Linux.

- **HTTPD.-** La necesidad de activar este demonio nace a partir de la implementación de monitores de servicios que brinda el servidor Linux vía WEB. Uno los monitores es un servicio adicional de Webmin (software de administración de sistemas operativos Linux). En caso de ser administrado el servidor Linux por dicho software, el intercambio de información deberá ser encriptado, razón por la cual se implementó un servidor WEB seguro el cual necesita del demonio HTTPD para ejecutarse.

- **DHCPD.-** El demonio DHCPD es el encargado de activar el servicio DHCP del servidor Linux.

- **SSH.-** Este protocolo proporcionará al administrador una adecuada comunicación (encriptada) en ***modo texto*** con el servidor Linux desde cualquier equipo (S.O. Windows - PUTTY o Linux) y lugar, fuera o dentro de la Institución, siempre y cuando sea autenticado por su dirección IP fija o remota en el Firewall implementado en el servidor.

Todos los protocolos y demonios mencionados anteriormente deberán ser activados, este procedimiento se realiza con **ntsysv** (Herramienta propia del Sistema Fig. 4.1) por medio del intérprete de comandos de shell de la siguiente manera: **# ntsysv**

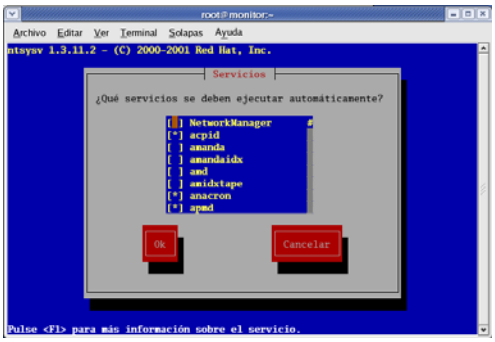

Figura 4.1. Ntsysv (software de administración)

Para una adecuada inicialización y arranque de los mismos, es necesario reiniciarlos. Este procedimiento es realizado con el comando:

[root@monitor /] # service <<*servicio*>> restart

Adicionalmente es recomendable que los servicios inicien en nivel 3 (Ambiente Texto) puesto que el servidor siempre va a trabajar en el mismo. Tanto el ambiente gráfico como el texto son de uso exclusivo del administrador por razones de seguridad. La exclusividad de ingreso y administración al sistema evita manipulación inadecuada del servidor, aumentando su seguridad. El cambio antes mencionado se realiza con:

[root@monitor /] # chkconfig –level 345 <<*servicio*>> on

CONFIGURACIÓN DEL SERVICIO DHCP - LINUX

4.1.2.1. Servicio DHCP. El Protocolo de configuración dinámica, es un protocolo de red para asignar automáticamente información TCP/IP a equipos cliente. Cada usuario DHCP se conecta al servidor DHCP centralizado (192.168.3.26 - SBS) que devuelve la configuración de red del usuario, incluyendo dirección IP, puerta de enlace y el servidor DNS (Tabla. 4.2).

Tabla 4.2. Información base DHCP

Dirección IP	192.168.X.X
Máscara	255.255.248.0
Gateway	192.168.3.10
Dns	192.168.3.26

4.1.2.1.1. Configuración del servidor DHCP. Para levantar el servicio DHCP-SBS se modifica el archivo de configuración que se encuentra en **/etc/dhcpd.conf.** Dhcp.conf es el encargado de almacenar la información de la Estructura y Direccionamiento IP de la Red Institucional (Tabla 4.1 y 4.2) para los ordenadores internos de la Entidad. En caso de no hallarse dicho archivo se deberá crear desde el intérprete de comandos de **shell** (Fig. 4.2) de la siguiente manera:

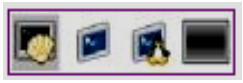

Figura 4.2. Intérprete de Comandos de Shell

[root@monitor /] # vi /etc/dhcpd.conf

El servicio DHCP también usa el archivo **/var/lib/dhcp/dhcpd.leases** para almacenar la base de datos de arrendamiento de clientes, en dhcp.leases se puede observar la información sobre el arrendamiento de DHCP de cada dirección IP asignada recientemente. Toda esta información se almacena de modo automático en la base de datos del arrendamiento e incluye la longitud del mismo, a quién se ha asignado la dirección IP, las fechas iniciales y finales de la renta, y la dirección MAC de la tarjeta de interfaz de red.

La administración del archivo deberá ser de uso exclusivo del administrador y es importante tener conocimiento de su ubicación, puesto que en muchos casos se ha podido observar conflictos entre los arrendamientos del servidor (Windows NT) y software específico de la Entidad, que proporciona privilegios de acceso a Internet a nivel de direcciones IP (WEBSENSE).

4.1.2.1.2. Fichero de configuración de la SBS. El archivo de configuración del servicio DHCP – SBS, contiene la línea de configuración de la forma:

parámetro valor;

y línea de la forma:

option parámetro valor;

El valor dependerá del parámetro que se quiera configurar; podrá ser un valor lógico (on u off), una dirección, un nombre predefinido u otro valor**.**

En dhcpd.conf se encuentran definidas las subredes en las que actúa el servidor DHCP (Tabla 4.1) y rangos de difusión de direcciones IP a asignar a los ordenadores de la Entidad. Existen parámetros que pueden ser globales o ser especificados dentro de una declaración de subred. Cualquier parámetro especificado en una subred tiene preferencia sobre los establecidos de forma global.

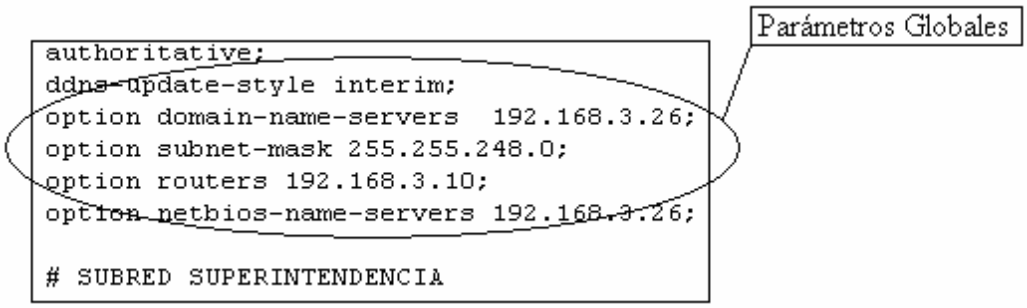

Figura 4.3. Parámetros Globales – DHCP

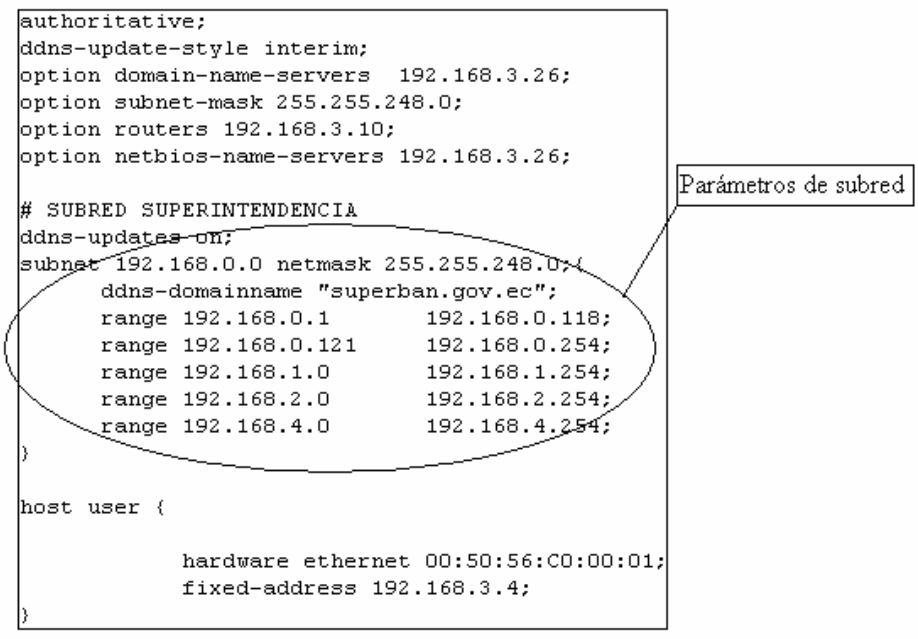

Figura 4.4. Parámetros de subred - DHCP

4.1.2.1.3. Descripción de parámetros del servidor DHCP.

- ***Authoritative***.- Esta función define que la configuración correcta para la Red Institucional es la configurada en el servidor DHCP y tratará de reasignar datos a los usuarios mal configurados. El parámetro puede ser global o asignado a una declaración de subred. Los cambios realizados en el servidor marcado como authoritative tienen una rápida propagación en la subred.

- ***ddns-update-style interim.-*** Esta línea indica el método de actualización DNS automática con los valores de la IP asignados por DHCP.

- ***option domain-name-servers 192.168.3.26.-*** Define la dirección del servidor DNS CENTRAL.

- ***option subnet-mask 255.255.248.0.-*** Define la máscara general de red en la que trabajarán todos los ordenadores de la Institución.

- ***option routers 192.168.3.10.-*** Define el gateway (puerta de enlace) de la Red Institucional, esta dirección (ficticia) le pertenece al servidor encargado de proveer Internet a todos los ordenadores de la Entidad.

- ***ddns-updates on.-*** Activa la actualización DNS con los valores asignados mediante DHCP.

- ***Subnet y netmask.-*** En estos campos se define la arquitectura o diseño de la Red Institucional.

- ***ddns-domainname superban.gov.ec.-*** Indica el dominio en el que se actualizan los DNS.

- ***default-lease-time 604800.-*** Indica el tiempo de asignación en segundos.

- ***max-lease-time 604800.-*** Indica el tiempo máximo de asignación en segundos.

- ***Host***.- Comienza una declaración de host. Esta declaración por lo general se realizará entre llaves **{}**.

- ***Hardware - tipo_hardware - dirección.-*** En estos campos se especifica que tipo de hardware se utiliza, Ethernet o token ring en nuestro caso Ethernet con su respectiva dirección física (MAC).

- ***fixed-address lista_direcciones_IP.-*** Este campo define direcciones estáticas para asignar a un ordenador. Por niveles de seguridad se deberá utilizar esta opción para asignar direcciones IP al administrador del servidor, puesto que como detallará más adelante el Firewall implementado permite accesos a ciertos puertos (SSH (22) – FTP (21), etc.) a las direcciones IP configuradas en este campo.

- ***range ip-menor ip-mayor.-*** En este campo se define las direcciones que se asignarán en la correspondiente subred.

4.1.2.1.4. Parámetros no requeridos del servidor dhcp.

- ***Group.-*** Declaración de grupo.

- ***one-lease-per-client on.-*** Cuando se encuentra en "on" y un cliente solicita una asignación, el servidor libera automáticamente cualquier otra asignación que tenga ese cliente. Se supone que si el cliente hace una solicitud es porque ha olvidado que tuviera alguna, es decir tiene una sola interfaz de red.

- ***server-identifier 192.168.3.26.-*** Este parámetro identifica el nodo que alberga el servicio DHCP. Sólo se deber usar cuando el nodo tenga más de una dirección IP asignada al interfaz.

- ***option netbios-name-servers 192.168.3.26.-*** Se define la dirección del servidor WINS para NetBios. El servidor actual bajo Windows NT no proporciona este servicio, motivo por el cual no se contemplo en la configuración.

- ***routers lista_IP.-*** Lista de IP de Gateways. En la estructura Tecnológica de la Superintendencia de Bancos y Seguros se especifica un solo Gateway o puerta de enlace.

NOTA.- *Todos los cambios realizados en el archivo de configuración no se aplicarán hasta reiniciar el demonio DHCP.*

DISEÑO DEL SERVICIO DNS - LINUX

4.1.2.2. Servicio DNS

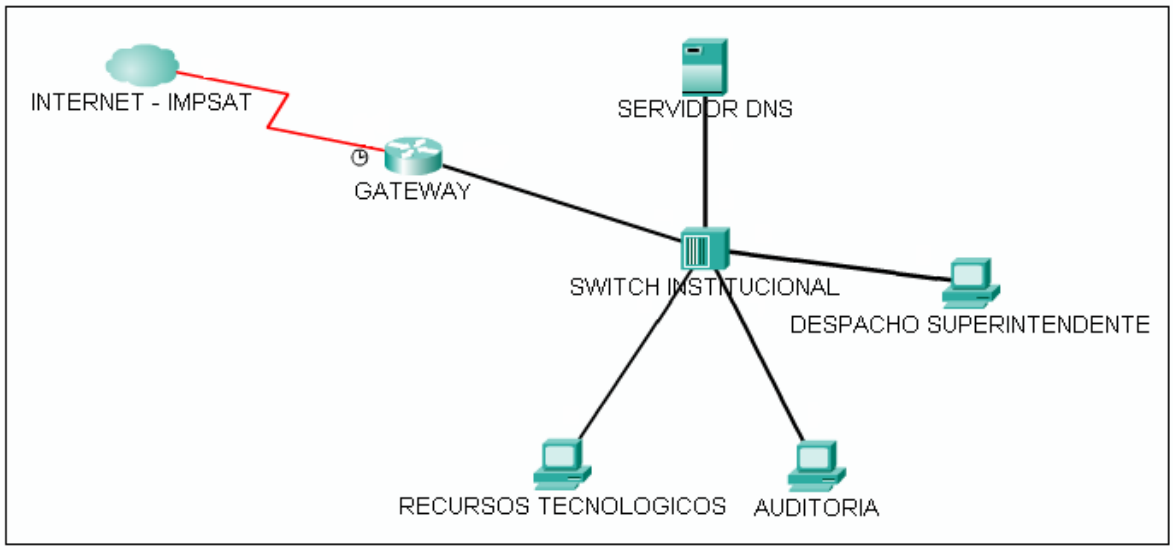

Figura 4.5. Servicio DNS IMPSAT - SBS

En la configuración del servicio DNS se detallará la forma de resolución de nombres o zonas pertenecientes a la SBS. Dicho proceso (Fig. 4.5) debe brindar una adecuada resolución tanto interna (Red Institucional) como externa (Red Pública - INTERNET).

Entre la granja de servidores observados en el capítulo II, a futuro, operará el servidor Linux (Interfaz de Fibra Óptica y Ethernet), proporcionando el servicio DNS con la dirección IP 192.168.3.26 (direcciones reservadas).

Como elemento importante en toda Red Institucional, se encuentra un Firewall, que provee las funciones necesarias para evitar accesos no permitidos a la red y consecuentemente al servidor DNS. En el proyecto se contempló la implementación de un Cortafuegos como filtro, el cual permitirá acceso público al puerto 53 (servicio DNS).

4.1.2.2.1. Zona SBS. La zona principal SBS (**superban.gov.ec**) especificada en todo el proceso de configuración está provista de una dirección IP fija (**Servidor Central 192.168.3.26**). Adicionalmente esta zona se deberá resolver en el proveedor de Internet

(IMPSAT), para que el público externo pueda acceder a los servicios que provee la Entidad (Fig. 4.6 - 4.7).

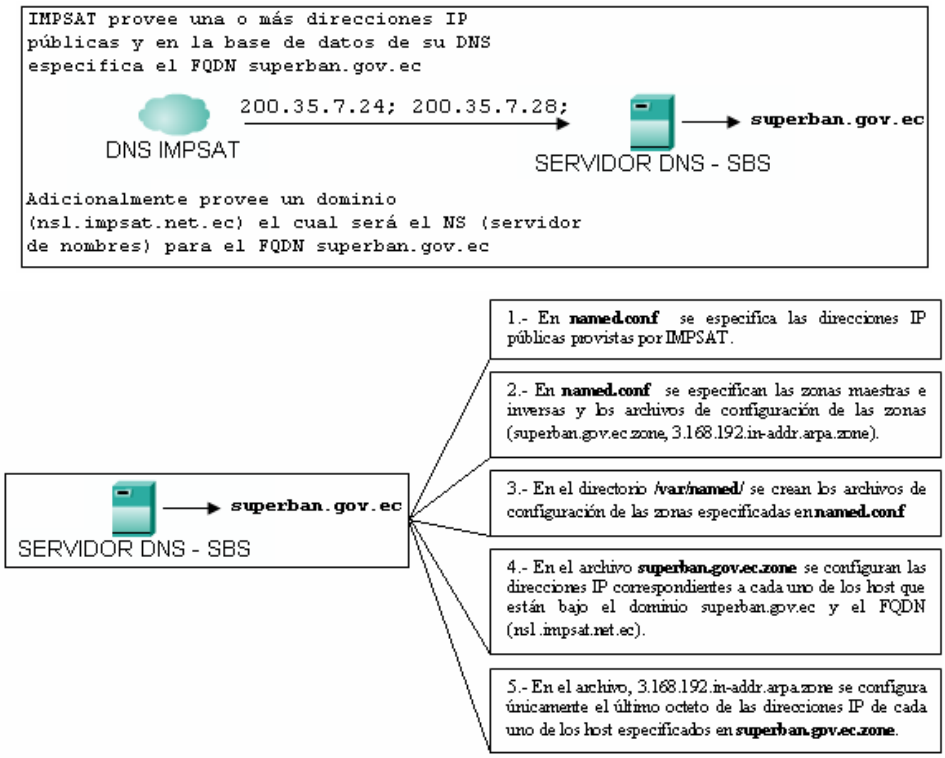

Figura 4.6. Zona SBS

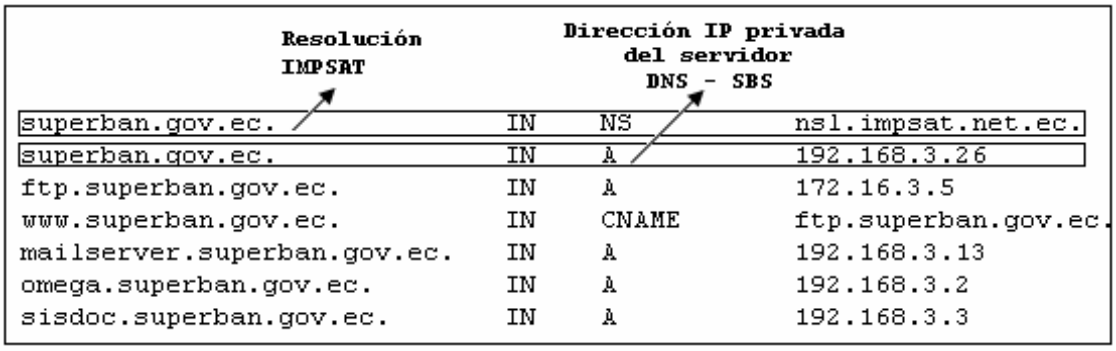

Figura 4.7. Dominios

El proveedor de Internet facilita una o más direcciones públicas (Fig. 4.8) a las cuales se reenviarán las peticiones DNS externas a la Entidad, estas direcciones deben especificarse en los archivos de configuración de **BIND** (herramienta Linux que permite levantar el servicio DNS).

```
options {
      directory "/var/named";
      query-source address * port 53;
      transfers-in 300;
      forwarders {
            200.35.7.24;
            200.35.7.28;
            };
};
```

Figura 4.8. Direcciones Públicas

4.1.2.2.2. Introducción a DNS – BIND. En UNIX, DNS es implementado por el Berkeley Internet Name Domain (BIND). Existen principalmente tres versiones de BIND: 4, 8 y 9, las cuales poseen cierta diferencia en la sintaxis de los archivos de configuración de los servidores. Existen cuatro tipos de configuración de servidores de nombres primarios en BIND:

- **Maestro.-** Almacena los registros de las zonas originales y de autoridad para un cierto espacio de nombres y responde a consultas sobre el espacio de nombres de otros servidores de nombres.

- **Esclavo.-** Responde a las peticiones que provienen de otros servidores de nombres y que se refieren a los espacios de nombres sobre los que tiene autoridad. Sin embargo, los servidores esclavos obtienen la información de sus espacios de nombres desde los servidores maestros.

- **Sólo caché.-** Ofrece servicios de resolución de nombres a direcciones IP pero no tiene ninguna autoridad sobre ninguna zona. Las respuestas en general se introducen en un caché por un período de tiempo fijo, la cual es especificada por el registro de zona recuperado.

- **Reenvío.-** Reenvía las peticiones a una lista específica de servidores de nombres para la resolución de nombres. Si ninguno de los servidores de nombres especificados puede resolver los nombres, la resolución falla.

4.1.2.2.3. Utilidades de Administración y Seguridad BIND. BIND realiza la resolución de nombres a través del demonio **named**. También incluye dos utilidades de administración y seguridad llamados **rndc y chroot**.

- **Rndc.** Rndc permite la administración de línea de comandos del demonio named desde el ordenador local o desde un ordenador remoto. Para prevenir el acceso no autorizado al demonio named, se utiliza un método de autenticación de llave secreta compartida para otorgar privilegios a ordenadores. Esto significa que una llave idéntica debe estar presente en los archivos de configuración /etc/named.conf y en el rndc, /etc/rndc.conf.

- **Chroot**. Red Hat Enterprise 4 proporciona este entorno que permite trabajar "como si" se tuviera un árbol diferente de ficheros. Su importancia radica en que si el servicio DNS se corrompe o logra ser vulnerado, evita que se afecte el resto de servicios disponibles o al mismo sistema operativo del servidor. El directorio de trabajo named, dentro de chroot se localiza en **cd var/named/chroot/var/named**

4.1.2.2.4. Zonas de servidores de nombres BIND. Estas zonas son definidas en servidores de nombres autorizados a través del uso de archivos de zona (Fig. 4.9). Los archivos de zona son almacenados en servidores de nombres primarios (también llamados servidores de nombres maestro), los cuales son verdaderamente autorizados y adicionalmente es donde se realizan cambios a los archivos.

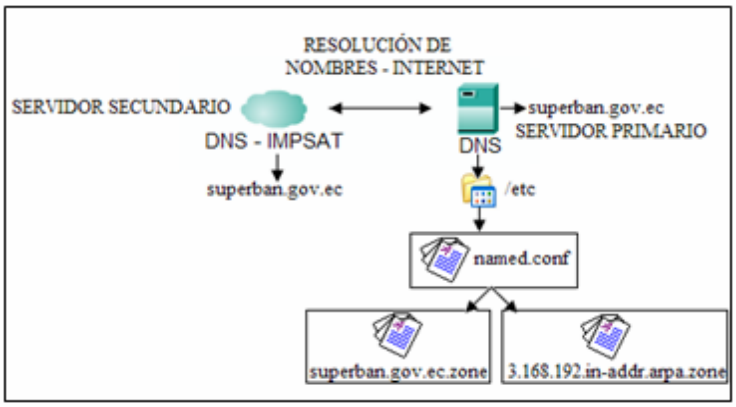

Figura 4.9. Archivos de Zona

4.1.2.2.5. Archivo de Configuración BIND - named.conf

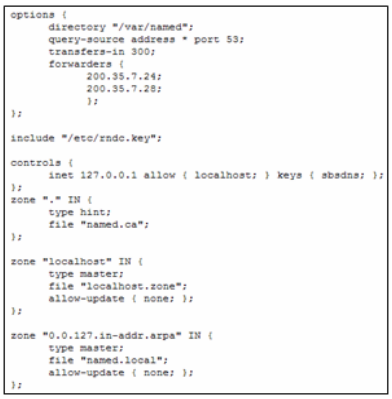

Figura 4.10. Named.conf

Named.conf es el fichero de configuración principal de BIND (Fig.4.10). Es una conjunto de declaraciones, usando opciones anidadas rodeadas por caracteres de llaves, { }. Además de estas declaraciones, el archivo de configuración permite comentarios al estilo de C++; es decir, se puede utilizar /* y */ para encerrar un comentario; o se puede utilizar // para colocar un comentario hasta el final de la línea.

4.1.2.2.6. Descripción de la Estructura named.conf.

- **Declaración options**. Esta declaración define y configura opciones globales y por defecto, del servicio (Fig.4.11). En este apartado se especifica la ubicación del directorio de trabajo named, número máximo de transferencias de zona simultáneas, las direcciones IP públicas provistas por IMPSAT, entre otras.

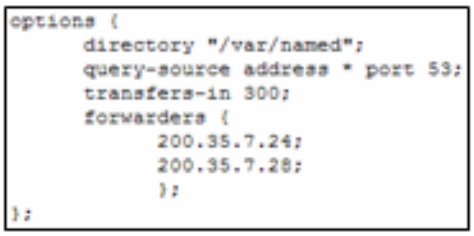

Figura 4.11. Declaración options - named.conf

- **Declaración Include.** La declaración include permite incluir archivos en named.conf. De esta forma los datos de configuración confidenciales (tales como llaves) se pueden colocar en un archivo separado con permisos restringidos. En la configuración del servidor DNS - SBS se realiza una llamada a la utilidad rndc.key.

- **Estadísticas named.** Especifica la localización alternativa de los archivos de estadísticas. Por defecto, las estadísticas de named son guardadas en el archivo: **/var/named/chroot/var/named/data/named_stats.txt**.

- **Declaración Zone.** Una declaración zone define las características de una zona tal como la ubicación de su archivo de configuración (**ARCHIVO DE ZONA**) y opciones específicas de la zona (Fig. 4.12). La declaración Zone SBS se define a continuación:

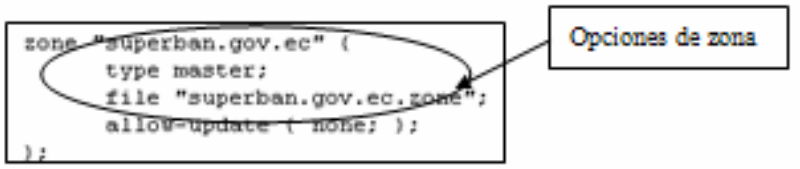

Figura 4.12. Zona SBS en named.conf

- **Type.-** Define el tipo de zona. .

- **Hint.-** Tipo especial de zona que se usa para orientar hacia los servidores de nombres root que sirven para resolver peticiones de una zona que no se conoce. No se requiere mayor configuración que la establecida por defecto con una zona hint.

- **Master.-** Designa el servidor de nombres actual como el que tiene la autoridad para esa zona. Una zona se puede configurar como tipo master si los archivos de configuración de la zona residen en el sistema.

El atributo “superban.gov.ec” para la declaración de la zona es particularmente importante, pues es el valor por defecto asignado para la directriz **$ORIGIN** (Fig. 4.13)

usada dentro del archivo de zona correspondiente localizado en el directorio **/var/named/chroot/var/named/.** Named anexa el nombre de la zona a cualquier nombre de dominio que no esté completamente cualificado listado en el archivo de zona.

```
$ORIGIN superban.gov.ec.
$TTL 86400
@
```

Figura 4.13. Directiva ORIGIN

4.1.2.2.7. Archivos de Zona. Los Archivos de zona SBS contienen información sobre un espacio de nombres particular y son almacenados en el directorio de trabajo named**.** Cada archivo de zona es nombrado de acuerdo a la opción file en la declaración zone, definida. En otras palabras relaciona a los dominios configurados en named.conf con sus correspondiente archivos de zona incluidos en **/var/named/chroot/var/named/.**

Cada archivo de zona contiene **directivas** y **registros de recursos (Fig. 4.14)**. Las directivas le dicen al servidor de nombres que realice tareas o aplique configuraciones especiales a la zona. Los registros de recursos definen los parámetros de la zona y asignan identidades a ordenadores individuales. Las directivas son opcionales, pero los registros de recursos se requieren para proporcionar servicios de nombres a la zona.

```
$ORIGIN superban.gov.ec.
$TTL 86400
@                           IN    SOA   @     root (
                        9 ; serie
                        28800 ;
                        7200 ;
                        604800 ;
                        86400 ; ttl
                        )
superban.gov.ec.            IN    NS          @
superban.gov.ec.            IN    NS          ns1.impsat.net.ec.
superban.gov.ec.            IN    A           192.168.3.26
ftp.superban.gov.ec.        IN    A           172.16.3.5
www.superban.gov.ec.        IN    CNAME       ftp.superban.gov.ec.
```

Figura 4.14. Directivas y Registros de Recursos

4.1.2.2.8. Directivas de archivos de Zona. Las directivas comienzan con el símbolo de dólar ($) seguido del nombre de la directiva. Usualmente aparecen en la parte superior del archivo de zona. A continuación se detallan las directivas utilizadas en las configuraciones:

- **$Origin.-** Anexa el nombre del dominio a registros no cualificados, tales como aquellos con el nombre de ordenador solamente. Cualquier nombre utilizado en registros de recursos que no terminen en un punto (.) tendrán el dominio anexado.

- **$TTL.-** Ajusta el valor Time to Live (TTL) predeterminado para la zona. Cada recurso puede contener su propio valor TTL y al aumentarlo, permite a los servidores de nombres remotos hacer caché a la información de zona para un período más largo de tiempo, reduciendo el número de consultas para la zona y alargando la cantidad de tiempo requerido para proliferar cambios de registros de recursos.

4.1.2.2.9. Registros de recursos de archivos de Zona. El componente principal del archivo de zona es su registro de recursos. Hay muchos tipos de registros de recursos de archivos de zona. A continuación se muestra a detalle los tipos de registros utilizados:

- **SOA.-** Registro de recursos Start Of Authority, que declara información importante de autoridad relacionada con espacios de nombres al servidor nombres. Está situado detrás de las directivas, un registro SOA es el primer registro en un archivo de zona. El siguiente ejemplo (Fig. 4.15) muestra la estructura básica de un registro de recursos SOA:

```
$ORIGIN superban.gov.ec.
$TTL 86400
@                               IN    SOA   @     root (
                          9 ; serie
                          28800 ;
                          7200 ;
                          604800 ;
                          86400 ; ttl
                          )
```

Figura 4.15. Registro SOA

El símbolo @ coloca la directiva $ORIGIN como el espacio de nombres que está siendo definido por este registro de recursos SOA. El nombre del host del servidor de

nombres que tiene autoridad para este dominio es la directiva, **localhost.superban.gov.ec.** o **@**, y el correo electrónico de la persona a contactar sobre este espacio de nombres es la directiva **root@superban.gov.ec.** o **root** sin punto simplemente.

- **NS.-** Registro NameServer (Fig. 4.16), el cual anuncia los nombres de servidores con autoridad para una zona particular (***ns1.impsat.net.ec - FQDN*** *en IMPSAT).*

```
superban.gov.ec.  IN  NS   ns1.impsat.net.ec.
```

Figura 4.16. Registro NameServer

- **A.-** Registro de dirección que especifica una dirección IP que se debe asignar a un nombre. Si el valor **superban.gov.ec** (Fig. 4.17) es omitido, el registro **A** apunta a una dirección IP por defecto para la parte superior del espacio de nombres.

```
superban.gov.ec.  IN  A  192.168.3.26
```

Figura 4.17. Registro A

- **CNAME.-** Registro del nombre canónico, que enlaza un nombre con otro, también conocido como un alias. En la figura 4.18 se indica a named que cualquier petición enviada a www.superban.gov.ec apunte al host, ftp.superban.gov.ec.

```
www.superban.gov.ec.  IN  CNAME  ftp.superban.gov.ec.
```

Figura 4.18. Registro CNAME

En la Figura 4.19 un registro **A** vincula un nombre de ordenador a una dirección IP, mientras que un registro **CNAME** apunta al nombre del ordenador comúnmente usado para WWW.

```
ftp.superban.gov.ec.   IN    A       192.168.3.26
www.superban.gov.ec.   IN    CNAME   ftp.superban.gov.ec.
```

Figura 4.19. Vínculo de registro A a registro CNAME

- **PTR.-** Registro Pointer o puntero, diseñado para apuntar a otra parte del espacio de nombres, la utilidad de este registro se ve con mayor énfasis en la zona inversa.

4.1.2.2.10. Directivas adicionales. Los tiempos (en segundos) definidos en estos registros, indican a los servidores secundarios cuando actualizar los datos que ellos poseen.

- S**erial-number=9.** Valor numérico que es incrementado cada vez que se cambia el archivo de zona para así indicar a named que debería recargar esta zona.

- **Time-to-refresh=28800**. Valor numérico que los servidores esclavos utilizan para determinar cuánto tiempo debe esperar antes de preguntar al servidor de nombres maestro si se han realizado cambios a la zona.

- T**ime-to-retry=7200.** Valor numérico usado por los servidores esclavo para determinar el intervalo de tiempo que tienen que esperar antes de emitir una petición de actualización de datos en caso de que el servidor de nombres maestro no responda.

- **Minimum-TTL=86400.** Cantidad de tiempo que otros servidores de nombres guardan en caché la información de zona. Cuando se configura BIND, todos los tiempos son siempre referenciados en segundos. Sin embargo, es posible usar abreviaciones cuando se especifiquen unidades de tiempo además de segundos, tales como minutos (M), horas (H), días (D) y semanas (W). A continuación se muestra la cantidad de tiempo en segundos y el tiempo equivalente en otro formato.

Tabla 4.3. Unidades de tiempo para BIND

60	1M
3600	1H
43200	12H
86400	1D
604800	1W

Archivos de Zona Inversa

La SBS posee un archivo de zona de resolución inversa de nombres para traducir la dirección IP 192.168.3.26 en un espacio de nombres particular en un FQDN (**superban.gov.ec**). Este archivo es de forma similar al archivo de zona explicado anteriormente, excepto que usa registros de recursos PTR para enlazar las direcciones IP a un nombre de dominio completamente cualificado.

Registro PTR de la SBS:

last-IP-digit IN PTR FQDN-of-system

```
26  IN    PTR   superban.gov.ec.
```

El valor **last-IP-digit (26)** se refiere al último número en la dirección IP que apunta al **FQDN** (superban.gov.ec). A continuación (Fig. 4.20) se detallará un archivo de configuración de una zona inversa.

```
$TTL 86400
3.168.192.in-addr.arpa. IN    SOA   @     root.superban.gov.ec.   (
                        4 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttl
                        )
3.168.192.in-addr.arpa.             IN    NS    @

26                      IN    PTR   superban.gov.ec.
13                      IN    PTR   mailserver.superban.gov.ec.
2                       IN    PTR   omega.superban.gov.ec.
3                       IN    PTR   sisdoc.superban.gov.ec.
110                     IN    PTR   dcuio01.superban.gov.ec.
4                       IN    PTR   gigabit.superban.gov.ec.
1                       IN    PTR   componentes.superban.gov.ec.
9                       IN    PTR   desarrollo.superban.gov.ec.
22                      IN    PTR   riesgos.superban.gov.ec.
24                      IN    PTR   infra4.superban.gov.ec.
12                      IN    PTR   portal.superban.gov.ec.
```

Figura 4.20. Zona Inversa

Este archivo de zona se colocará en funcionamiento con una declaración zone en el archivo **named.conf (Fig. 4.21).**

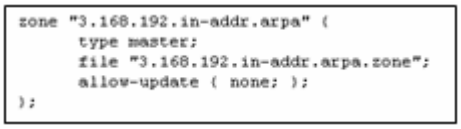

Figura 4.21. Zona SBS Inversa en named.conf

Hay muy poca diferencia entre el ejemplo y una declaración de zone estándar, excepto por el nombre de la zona. Una zona de resolución de nombres inversa requiere que los primeros tres octetos de la dirección IP estén invertidos seguido por .in-addr.arpa. Esto permite asociar con la zona a un bloque único de números IP usados en el archivo de zona de resolución de nombres inversa.

CONFIGURACIÓN DEL SERVICIO DNS - LINUX

1.- Configuración de Zonas SBS en /etc/named.conf

```
zone "superban.gov.ec" {
      type master;
      file "superban.gov.ec.zone";
      allow-update { none; };
};

zone "3.168.192.in-addr.arpa" {
      type master;
      file "3.168.192.in-addr.arpa.zone";
      allow-update { none; };
};

zone "3.23.172.in-addr.arpa" {
      type master;
      file "3.23.172.in-addr.arpa.zone";
      allow-update { none; };

};
```

Figura 4.22. Configuración de Zonas SBS

2.- Creación y configuración de cada archivo de zona en var/named/chroot/var/named/.

[root@monitor /] # vi /var/named/superban.gov.ec.zone

```
$ORIGIN superban.gov.ec.
$TTL 86400
@                           IN     SOA    @ root (
                            9 ; serie
                            28800 ;
                            7200 ;
                            604800 ;
                            86400 ; ttl
                            )
superban.gov.ec.                   IN     NS       @
superban.gov.ec.                   IN     NS       ns1.impsat.net.ec.
superban.gov.ec.                   IN     A        192.168.3.26
ftp.superban.gov.ec.               IN     A        172.16.3.5
www.superban.gov.ec.               IN     CNAME    ftp.superban.gov.ec.
mailserver.superban.gov.ec.        IN     A        192.168.3.13
omega.superban.gov.ec.             IN     A        192.168.3.2
sisdoc.superban.gov.ec.            IN     A        192.168.3.3
dcuio01.superban.gov.ec.           IN     A        192.168.3.110
gigabit.superban.gov.ec.           IN     A        192.168.3.4
server.superban.gov.ec.            IN     A        172.16.3.8
serv.superban.gov.ec.              IN     CNAME    server.superban.gov.ec.
componentes.superban.gov.ec.       IN     A        192.168.3.1
compo.superban.gov.ec.             IN     CNAME    componentes.superban.gov.ec.
desarrollo.superban.gov.ec.        IN     A        192.168.3.9
riesgos.superban.gov.ec.           IN     A        192.168.3.22
infra4.superban.gov.ec.            IN     A        192.168.3.24
portal.superban.gov.ec.            IN     A        192.168.3.12
```

Figura 4.23. Creación y configuración de cada archivo de zona en var/named/chroot/var/named/

3.- Creación y configuración del archivo de zona inversa en var/named/chroot/var/named/.

[root@monitor /] # vi /var/named/3.168.192.in-addr.arpa.zone

```
$TTL 86400
3.168.192.in-addr.arpa.  IN    SOA   @      root.superban.gov.ec.    (
                         4 ; serial
                         28800 ; refresh
                         7200 ; retry
                         604800 ; expire
                         86400 ; ttl
                         )
3.168.192.in-addr.arpa.                IN    NS    @

26                       IN    PTR   superban.gov.ec.
13                       IN    PTR   mailserver.superban.gov.ec.
2                        IN    PTR   omega.superban.gov.ec.
3                        IN    PTR   sisdoc.superban.gov.ec.
110                      IN    PTR   dcuio01.superban.gov.ec.
4                        IN    PTR   gigabit.superban.gov.ec.
1                        IN    PTR   componentes.superban.gov.ec.
9                        IN    PTR   desarrollo.superban.gov.ec.
22                       IN    PTR   riesgos.superban.gov.ec.
24                       IN    PTR   infra4.superban.gov.ec.
12                       IN    PTR   portal.superban.gov.ec.
```

Figura 4.24. Creación y configuración del archivo de zona inversa

4. – Pruebas del Servicio DNS – SBS

Nslookup.- Es una herramienta de depuración que permite interrogar directamente el servidor de nombres y consigue cualquier información conocida del DNS. Este programa se utiliza para resolver preguntas directamente desde la línea de comandos. Como se demuestra a continuación:

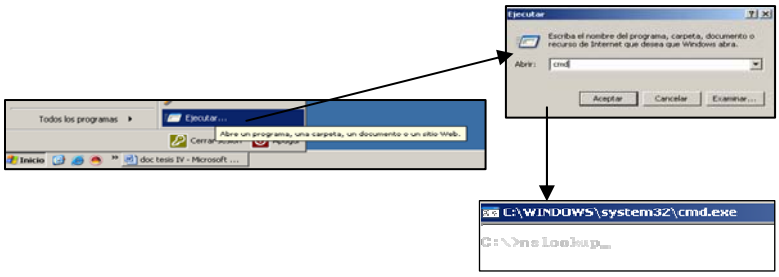

Figura 4.25. Pruebas del Servicio DNS - SBS

Posteriormente se escribe el dominio que se haya configurado, en el caso SBS, **superban.gov.ec**, el cual deberá entregar la dirección IP del servidor sin errores:

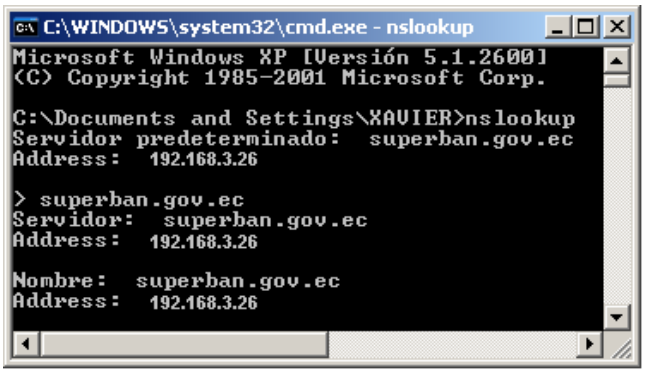

Figura 4.26. Pruebas DNS Nslookup

En caso de existir errores se recomienda usar **nslint (software de verificación del servicio DNS)**, que al ejecutarla entrega detalles de los problemas que no permiten el correcto funcionamiento del servicio DNS.

5.- Configuración RNDC

En /var/named/chroot/etc/named.conf, por motivos de seguridad se cambia la dirección 127.0.0.1 por la dirección del servidor, su nombre y un nombre en el cual se especifique la clave **dnskey** dentro de rndc.key, para que solo éste pueda controlar el demonio de named.

```
include "/etc/rndc.key";

controls {
      inet 192.168.3.26 allow { monitor; } keys { dnskey; };
};
```

Figura 4.27. Configuración RNDC

En el archivo /var/named/chroot/etc/**rndc.key** se copia la clave generada (directorio de root) con: **dnssec-keygen -a hmac-md5 -b 1024 -n HOST monitor**

```
key "dnskey" {
                  algorithm       hmac-md5;

secret "Bg9sdB2tIMnq6QhQSzQdi56aTr4Vazyb/t2CFykU
};
```

Figura 4.28. Rndc.key

En **/etc/rndc.conf** especificamos el nombre del servidor (SBS - monitor), definimos el nombre de la función que contiene la clave de rndc (dnskey).

```
include "/etc/rndc.key";
options {
        default-server  monitor;
        default-key     "dnskey";
      };

server monitor {
             key "dnskey";
             };
```

Figura 4.29. Rndc.conf

Una vez configurado rndc, probamos que solo la dirección IP del servidor pueda detener el demonio named o determinar el estado actual del mismo (named_stats.txt) de la siguiente manera.

[root@monitor /] # rndc –s 192.168.3.26 stop
[root@monitor /] # rndc –s 192.168.3.26 stats

Si no se dan errores se encuentra bien configurado el rndc. Es importante recalcar que la configuración del rndc y las estadísticas de named_stats.txt nos servirán posteriormente para la configuración del monitor del servicio DNS con la herramienta MRTG.

CONFIGURACIÓN DE LOS MONITORES SBS

4.1.2.3. Monitoreo de servicios. En el servidor configurado para la Superintendencia de Bancos y Seguros se procedió a trabajar con dos monitores MRTG-MRTG-sys y SYSSTATS de WEBMIN, estos monitores realizan gráficas del estado de los servicios, actividad, uso de recursos del sistema, entre otros. Estas gráficas son presentadas en páginas Web, motivo por el cual se configuró un servidor Web seguro (https).

4.1.2.3.1. Justificación de los monitores de la SBS. La migración de algunos servicios de comunicación de la Superintendencia de Bancos y Seguros a Linux, busca fortalecer este cambio de plataforma, razón por la que se debe explotar la mayoría de herramientas que permitan no solo levantar los servicios sino mantenerlos constantemente controlados para brindar la mejor calidad de los mismos a través de una adecuada administración. Esto se logra únicamente bajo monitoreo u observación de dichos servicios ya sea por uso o recursos que ocupan del sistema.

Los monitores permitirán, exclusivamente, revisar la actividad de procesos del servidor configurado en la SBS vía WEB, como dato interesante presenta la cantidad de veces que el servicio DNS ha sido requerido, o la actividad de los servicios en el sistema. Estas estadísticas pueden ser de gran uso por parte de los administradores de la red, puesto que si un servicio o más utilizan mayores recursos del servidor puede ser un respaldo para solicitar nuevos equipos de mayores capacidades que brinden una correcta calidad de los mismos.

Como se mencionó con anterioridad, todo el monitoreo será vía WEB, por lo que se procedió a implementar un servidor (básico) WEB seguro (https), con sus respectivas seguridades como se muestra a continuación.

4.1.2.3.2. HTTPS. La combinación del servidor Apache, mod_ssl (módulo de seguridad) y las herramientas de OpenSSL forman el servidor Web seguro o simplemente como el servidor seguro.

El módulo mod_ssl es un módulo de seguridad para el Servidor Apache HTTP. Este módulo usa las herramientas proporcionadas por el Proyecto OpenSSL para añadir una

característica muy importante al Servidor Apache HTTP ó la habilidad de tener comunicaciones encriptadas, requerimiento base de la institución. En contraste, usando HTTP normal, las comunicaciones entre los usuarios y el servidor Web son enviadas en texto plano, lo cual puede ser interceptado y leído por personas no autorizadas.

En los siguientes apartados se mostrará como instalar estos programas y los pasos necesarios para generar una clave privada y una petición de certificado, cómo generar un propio certificado firmado, y cómo instalar un certificado para usarlo con su servidor WEB seguro.

El archivo de configuración mod_ssl está ubicado en:

/etc/httpd/conf.d/ssl.conf.

Para que este archivo sea cargado, y por ende para que mod_ssl funcione, debe tener la sentencia:

Include
conf.d/*.conf en /etc/httpd/conf/httpd.conf.

Esta sentencia es incluida por defecto en el archivo de configuración de Servidor Apache HTTP.

4.1.2.3.2.1. Paquetes necesarios para levantar HTTPS. Los paquetes básicos necesarios para levantar un servidor Web seguro son:

- **httpd.-** Este paquete contiene el demonio httpd y otras utilidades relacionadas, archivos de configuración, iconos, Servidor Apache http, módulos, páginas de manual y otros archivos utilizados por Servidor Apache HTTP.

- **mod_ssl.-** Mod_ssl incluye el módulo mod_ssl, que proporciona criptografía fuerte para el servidor Web, Servidor Apache http, a través de los protocolos SSL, Secure Sockets Layer y TLS, Transport Layer Security.

- **Openssl.-** El conjunto de herramientas de OpenSSL implementa los protocolos SSL y TLS y también incluye una librería criptográfica de propósito general. Adicionalmente, otros paquetes de software pueden proporcionar ciertas funcionalidades de seguridad (pero que no son requeridas para que funcione el servidor seguro).

4.1.2.3.2.2. Certificados y Seguridad. El servidor seguro proporciona seguridad usando una combinación del protocolo de Capa de conexión segura (Secure Sockets Layer, SSL) y (en la mayoría de los casos) un certificado digital de una Autoridad de Certificación (CA). Para el caso de la SBS se creó un certificado propio pero no existiría ningún problema en implementar un certificado de una empresa certificadora.

SSL maneja las comunicaciones encriptadas y la mutua autenticación entre navegadores y su servidor seguro. El certificado digital aprobado por una CA proporciona autenticación para un servidor seguro (el CA pone su reputación detrás de su certificación de la identidad de la organización). Cuando un navegador se esté comunicando usando la encriptación SSL, se observará el prefijo **https://** al principio de la URL (Localizador de Recursos Uniforme - la dirección de Internet) en la barra de navegación.

La encriptación depende del uso de claves (Como anillos codificador/decodificador en formato de datos). En criptografía convencional o simétrica, ambas partes de la transacción tienen la misma clave, la cual usan para decodificar la transmisión del otro. En criptografía pública o asimétrica, coexisten dos claves: una pública y una privada. La SBS guarda su clave privada en secreto, y publica su clave pública. Los datos codificados con la llave pública solo pueden ser decodificados con la clave privada; y los datos codificados con la clave privada sólo pueden ser decodificados con la llave pública.

Para configurar un servidor seguro se usará criptografía pública para crear un par de claves pública y privada. En muchos casos, enviará su petición de certificado (incluyendo

su clave pública), demostrando la identidad de la Superintendencia de Bancos y Seguros. Para la generación del certificado SBS el primer paso fue la generación de una clave.

4.1.2.3.2.3. Generación de clave. Primero se explora el directorio **/etc/httpd/conf,** y posteriormente se eliminan la llave y el certificado simulados que se generaron durante la instalación. A continuación, se necesita crear una llave aleatoria, para lo cual se debe de cambiar al directorio (modo texto) **/usr/share/ssl/certs** y a continuación se escribe el siguiente comando **make genkey**. El sistema mostrará un mensaje (Fig. 4.30) similar al siguiente:

```
umask 77 ; \
/usr/bin/openssl genrsa -des3 1024 > /etc/httpd/conf/ssl.key/server.key
Generating RSA private key, 1024 bit long modulus
.......++++++
.....................................................................++++++
e is 65537 (0x10001)
Enter pass phrase:
```

Figura 4.30. Mensaje de generación de certificado

A continuación se deberá incluir una palabra de paso no menor a 8 caracteres, incluyendo números y símbolos, por seguridad:

NOTA.- *Se debe recordar que la palabra de paso es sensible a las mayúsculas. Adicionalmente existen dos formas de reiniciar el servidor Web seguro el primero se obtiene tecleando la palabra de paso configurada y el segundo incluyendo esta clave a otro archivo. En las configuraciones realizadas se prefirió teclear dicha clave por razones de seguridad.*

Continuando con la instalación se solicitará que se reintroduzca la contraseña, para verificar que es correcta y una vez que se haya tecleado correctamente, será creado un archivo llamado: /etc/httpd/conf/ssl.key/**server.key**, que contendrá dicha clave.

4.1.2.3.2.4. Creación de un certificado Autoafirmado. Como mencionan los desarrolladores del paquete Openssl, éste permite crear un certificado autofirmado propio pero se debe tener en cuenta que un certificado autofirmado no proporciona las garantías

de seguridad que un certificado firmado por una CA sí proporciona. Una vez obtenida la llave de paso, se debe asegurar de estar en el directorio /usr/share/ssl/certs, y a continuación escribir el siguiente comando: **make testcert.** Se observará la siguiente salida y a continuación se solicitará que introducir la palabra de paso (Fig. 4.31):

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-x509 -days 365 -out /etc/httpd/conf/ssl.crt/server.crt
Using configuration from /usr/share/ssl/openssl.cnf
Enter pass phrase:
```

Figura 4.31. Ingreso de clave para crear certificado autofirmado

Después de introducir la contraseña, se solicitará más información. La salida del ordenador y el conjunto de entradas será parecida a lo siguiente (Fig. 4.32):

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:EC
State or Province Name (full name) [Berkshire]: PICHINCHA
Locality Name (eg, city) [Newbury]:QUITO
Organization Name (eg, company) [My Company Ltd]: SUPERINTENDENCIA DE BANCOS Y SEGUROS
Organizational Unit Name (eg, section) []: DIRECCIÓN NACIONAL DE RECURSOS TECNOLÓGICOS
Common Name (your name or server's hostname) []: monitor.superban.gov.ec
Email Address []: pzambrano@superban.gov.ec
```

Figura 4.32. Certificado SBS

Después de proporcionar la información correcta, un certificado autofirmado será creado y colocado en **/etc/httpd/conf/ssl.crt/server.crt**. Finalmente se necesitará reiniciar el servidor seguro.

4.1.2.3.3. MRTG (Multi Router Traffic Grapher). MRTG, como otros grandes proyectos Open Source, es una herramienta para supervisar la carga de tráfico en los enlaces de red. Genera páginas HTML que contienen imágenes gráficas que proporcionan una representación visual VIVA de este tráfico, basado en Perl y C. MRTG funciona bajo UNIX y Windows.

En el caso más general, MRTG usa SNMP (Simple Network Management Protocol) para recolectar los datos de tráfico de un determinado dispositivo (routers o servidores). Los gráficos generados con MRTG, además de una vista diaria detallada, representan también el tráfico de los últimos siete días, las cuatro últimas semanas y los últimos doce meses. Esto es posible porque MRTG mantiene un archivo de todos los datos que ha obtenido del dispositivo de red. Este archivo es consolidado automáticamente, así que no crece con el tiempo, pero contiene todos los datos relevantes del tráfico de los últimos dos años. Todo esto se realiza de una manera eficiente. Por lo tanto, se puede monitorear 200 o más sistemas de red desde cualquier máquina Unix.

SNMP (Simple Network Management Protocol), o protocolo simple de administración de redes, es el protocolo de gestión de red más importante y usado en la actualidad. Forma parte del conjunto de protocolos TCP/IP y está definido en la capa de aplicación del mismo. SNMP busca la sencillez y es por ello que en la capa de transporte está soportado por el protocolo UDP (caracterizado por su rapidez y su falta de fiabilidad) a través del puerto 170.

La configuración inicial de MRTG básicamente realiza estadísticas gráficas del ancho de banda de la interfaz de red, pero en las configuraciones realizadas en el servidor DNS de la Superintendencia de Bancos y Seguros, se tomaron algunos scrips de mrtg-sys.

El conjunto de scrips que contiene MRTG-SYS se encargan de tomar datos de ciertos archivos del sistema (logs, named_stats.txt, etc.) y los representa gráficamente ayudando así a monitorear los servicios como el DNS por ejemplo.

4.1.2.3.3.1. Configuración de MRTG y SNMP. Aunque esta configuración no es parte del proyecto es importante conocer el procedimiento de configuración, en caso que algún administrador lo requiera implementar.

NOTA.- *Todos los programas antes mencionados están incluidos en los cd's de instalación de Red Hat Enterprise 4, por lo que es necesario saber si están instalados. Esta verificación se la realiza de la siguiente manera:*

```
[root@monitor ~]# rpm -qa | grep snmp
net-snmp-5.1.2-11
net-snmp-utils-5.1.2-11
net-snmp-libs-5.1.2-11
[root@monitor ~]# rpm -qa | grep mrtg
mrtg-2.10.15-1
[root@monitor ~]#
```

Figura 4.33. Comandos de comprobación de software

4.1.2.3.3.2. Configuración SNMP. Como requerimiento, en la instalación y configuración de MRTG con SNMP es necesario que esté activado el demonio **snmpd.** En **/etc/snmp/snmpd.conf** se debe cambiar o modificar las siguientes líneas de configuración como se muestra a continuación:

```
com2sec local     localhost                       public
com2sec mynetwork 192.168.3.0/255.255.248.0       public
group MyRWGroup v1         local
group MyRWGroup v2c        local
group MyRWGroup usm        local
group MyROGroup v1         mynetwork
group MyROGroup v2c        mynetwork
group MyROGroup usm        mynetwork

view all    included  .1      80

#       group  context sec.model sec.level  prefix  read   write notif
access MyROGroup ""      any       noauth    exact  all    none   none
access MyRWGroup ""      any       noauth    exact  all    all    none

syslocation Linux (RH3_UP2), SUPERINTENDENCIA DE BANCOS.
syscontact Root <roo@192.168.3.26>
```

Luego de realizar los cambios sugeridos se debe probar el servicio SNMP. Este nos deberá retornar la dirección IP del servidor y la dirección de loopback (Fig. 4.34).

```
[root@monitor snmp]# snmpwalk -v 1 -c public localhost IP-MIB::ipAdEntIfIndex
IP-MIB::ipAdEntIfIndex.192.168.3.26 = INTEGER: 2
IP-MIB::ipAdEntIfIndex.127.0.0.1 = INTEGER: 1
[root@monitor snmp]#
```

Figura 4.34. Prueba de configuración SNMP

4.1.2.3.3.3. Configuración MRTG. MRTG es una herramienta que genera gráficas y las presenta en páginas Web por lo que es necesario crear un directorio donde se accederá a consultar el estado de los servicios o Ancho de Banda del servidor. Luego de crear el directorio se especifica el nombre del archivo de configuración (para la SBS, mymrtg.cfg) el cual contendrá la configuración necesaria para realizar las gráficas dentro de **/var/www/html/monitorsbs.**

```
[root@monitor /]# mkdir -p /var/www/html/monitorsbs/
[root@monitor /]#
```

```
[root@monitor /]# cfgmaker --global 'WorkDir: /var/www/html/monitorsbs' --output /etc/mrtg/mymrtg
.cfg public@localhost
```

Figura 4.35. Creación del directorio WEB – MRTG y archivo de configuración

NOTA.- *Esta configuración es automática no se deberán realizar cambios manuales.*

A continuación se debe crear la página principal o índice que se presentará en el servidor http. Como se puede observar el comando indexmaker genera una página index a partir del archivo de configuración mymrtg.cfg (Fig. 4.36).

```
[root@monitor /]# indexmaker --output=/var/www/html/monitorsbs/index.html /etc/mrtg/mymrtg.cfg
```

Figura 4.36. Generación de la página WEB índice de MRTG

NOTA.- *Como el servicio HTTP no es un servicio propuesto en el proyecto de tesis se generó la página Web con el nombre Index que es fácilmente reconocido en el servicio, pero también se podría configurar otros nombres realizando los cambios pertinentes en los archivos de configuración de Apache.*

Como último paso se debe correr el servicio de MRTG con el comando: # mrtg /etc/mrtg/mymrtg.cfg

NOTA.- *Al ejecutar el comando MRTG aparecerán varios errores, según el autor estos errores deben ser ignorados puesto que en ejecuciones posteriores del mismo comando ya no volverán aparecer.*

Para que el monitor entregue o genere gráficas cada 5 minutos es importante utilizar la herramienta de los sistemas unix el crontab que se encarga de ejecutar ciertos programas o procesos a determinado tiempo en nuestro caso 5 minutos.

4.1.2.3.3.4. Configuración de MRTG - SYS. MRTG-SYS en un conjunto de scripts que permiten graficar diferentes elementos fluctuantes del servidor en función del tiempo (uso de memoria, espacio de disco, uso CPU, etc.). Este paquete generalmente se descarga en formato TAR de la dirección ftp://ftp.ovh.net/made-in-ovh/mrtg-sys/. A continuación se detallará el procedimiento de instalación:

- Instalación MRTG-SYS.
- Modificación del Crontab.

Una vez descargado el paquete en formato TAR se debe de desempaquetar en:

/var/www/mrtg/

NOTA.- *Los procesos de instalación o descompresión de paquetes TAR o RPM pueden ser con herramientas propias del sistema (RHEL4, modo gráfico) o desde línea de comandos*.

Para su instalación y configuración se siguen los siguientes pasos:

1.- Ingresamos a mrtg-sys

```
[root@monitor mrtg]# cd /var/www/mrtg/mrtg-sys
[root@monitor mrtg-sys]#
```

Figura 4.37. Ingreso a MRTG-SYS

2.- Procedemos a instalarlo

```
[root@monitor mrtg-sys]# ls
install.pl  mrtg-sys
[root@monitor mrtg-sys]# ./install.pl
```

Figura 4.38. Instalación de MRTG-SYS

Una vez realizada la instalación se creará un archivo de configuración (Ej. mrtg_monitor.superban.gov.ec.cfg) el cual llama a cada uno de los scripts que posteriormente proveerán los datos requeridos por MRTG para incluirlos en sus gráficas.

Este archivo puede ser renombrado sin ningún problema (para el caso particular de la SBS se renombró a mymrtg.cfg) y se debe copiar en /etc/mrtg/. Como MRTG-SYS proporciona un archivo de configuración con sus respectivos scripts podemos configurar que gráficas vamos a mostrar solo eliminando o adicionando líneas de programación en el mismo (mrtg_monitor.superban.gov.ec.cfg = mymrtg.cfg). Entre los cambios importantes que se pueden realizar al archivo de configuración está el cambio del path.

4.1.2.3.3.5. Gráficas adicionales para MRTG. El sistema MRTG es un proceso que genera a intervalos regulares uno o varios gráficos. Cada gráfico necesita una serie de 4 valores para estar siempre al día. El sistema MRTG hace uso a través de un fichero de configuración, a un script que se encarga de interrogar el valor que necesitamos monitorizar y devuelve la serie de 4 valores a partir de él.

Instalado MRTG y MRTG-sys procedeos a modificar el fichero de configuración (Fig.4.39): **vi /etc/mrtg/mymrtg.cfg.** Para cada nuevo elemento que desee añadir al gráfico, basta con anexar una sección del tipo:

```
Target[monitor.superban.gov.ec_lo]: `/var/www/mrtg/mrtg-sys/mrtg-sys/lo.pl`
PageTop[monitor.superban.gov.ec_lo]: <h1>bits recuperados/emitidos de monitor.superban.gov.ec</h1>
Options[monitor.superban.gov.ec_lo]: growright
MaxBytes[monitor.superban.gov.ec_lo]: 100000000000000000000
Title[monitor.superban.gov.ec_lo]: Paquetes recuperados/emitidos de monitor.superban.gov.ec
Ylegend[monitor.superban.gov.ec_lo]: Paquetes recuperados/emitidos
Legend1[monitor.superban.gov.ec_lo]: bits recuperados
Legend2[monitor.superban.gov.ec_lo]: bits emitidos
LegendI[monitor.superban.gov.ec_lo]: bits recuperados
LegendO[monitor.superban.gov.ec_lo]: bits emitidos
ShortLegend[monitor.superban.gov.ec_lo]: bits

Target[monitor.superban.gov.ec_dns]: `/var/www/mrtg/mrtg-sys/mrtg-sys/dns.pl`
PageTop[monitor.superban.gov.ec_dns]: <h1>Peticiones DNS</h1>
Options[monitor.superban.gov.ec_dns]: growright, perhour, noi
MaxBytes[monitor.superban.gov.ec_dns]: 1000000
Title[monitor.superban.gov.ec_dns]: Peticiones DNS
YLegend[monitor.superban.gov.ec_dns]: pet/hora
LegendO[monitor.superban.gov.ec_dns]: Peticiones DNS
Legend2[monitor.superban.gov.ec_dns]: Peticiones DNS a la hora
ShortLegend[monitor.superban.gov.ec_dns]: /hora
```

Figura 4.39. Archivo de configuración de MRTG – MRTG SYS

El gráfico aparecerá en la página índice de MRTG. El script (Fig.4.40) que hace referencia nuestro ejemplo llama a named_stats.txt de la siguiente manera:

```
#!/usr/bin/perl

#$dummy = `rm -rf /var/named/chroot/var/named/data/named_stats.txt`;
$dummy = `/usr/sbin/rndc stats`;
$data = `tail -3 /var/named/chroot/var/named/data/named_stats.txt` | head -1 | cut -f 2 -d " "`;
print $data;
print $data;
print "0\n0"
```

Figura 4.40. Script que interactúa con named_stats.txt

Para que los gráficos añadidos en MRTG se muestren a través de la página habitual (Fig.4.41), se deberá regenerar el index a cada nueva modificación.

NOTA.- *Como este script necesita ejecutarse constantemente se deberá cambiar en los permisos, que únicamente root o algún administrador con privilegios pueda ejecutarlo.*

Gráficas realizadas

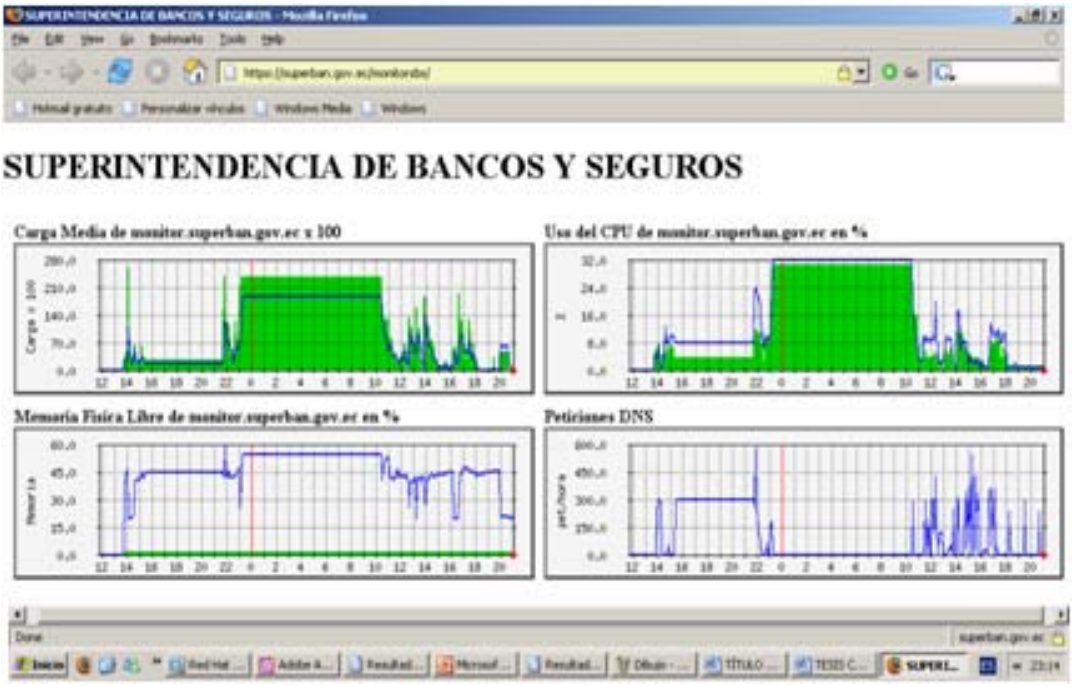

Figura 4.41. Gráficas MRTG del Servidor

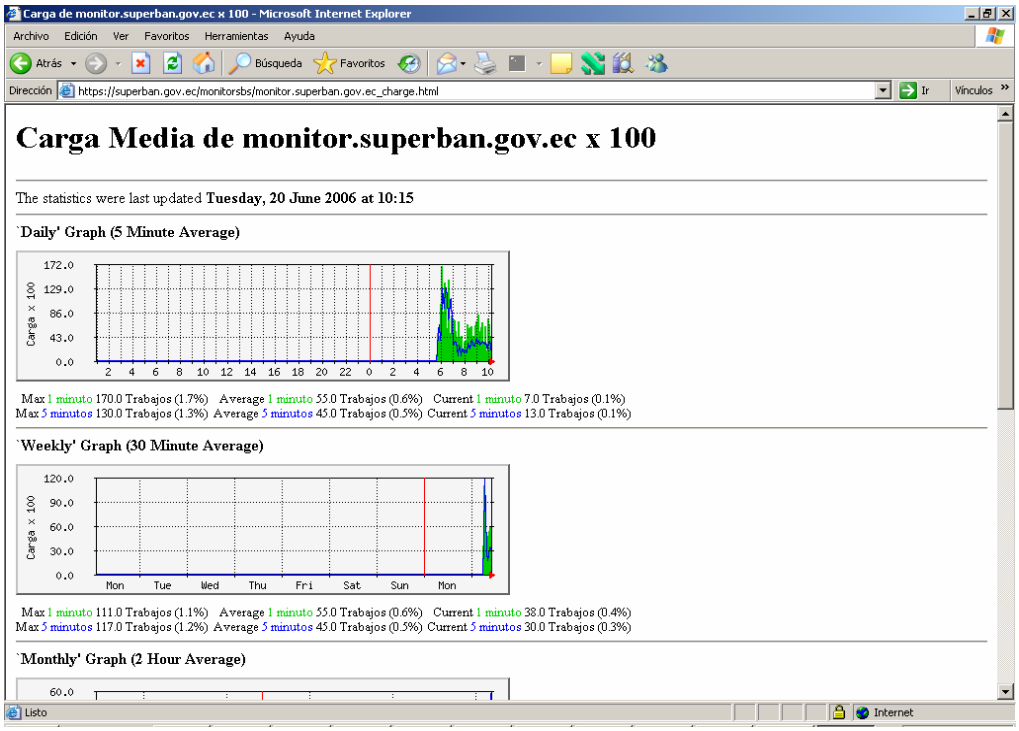

Figura 4.42. Gráficas de Carga Media del Servidor

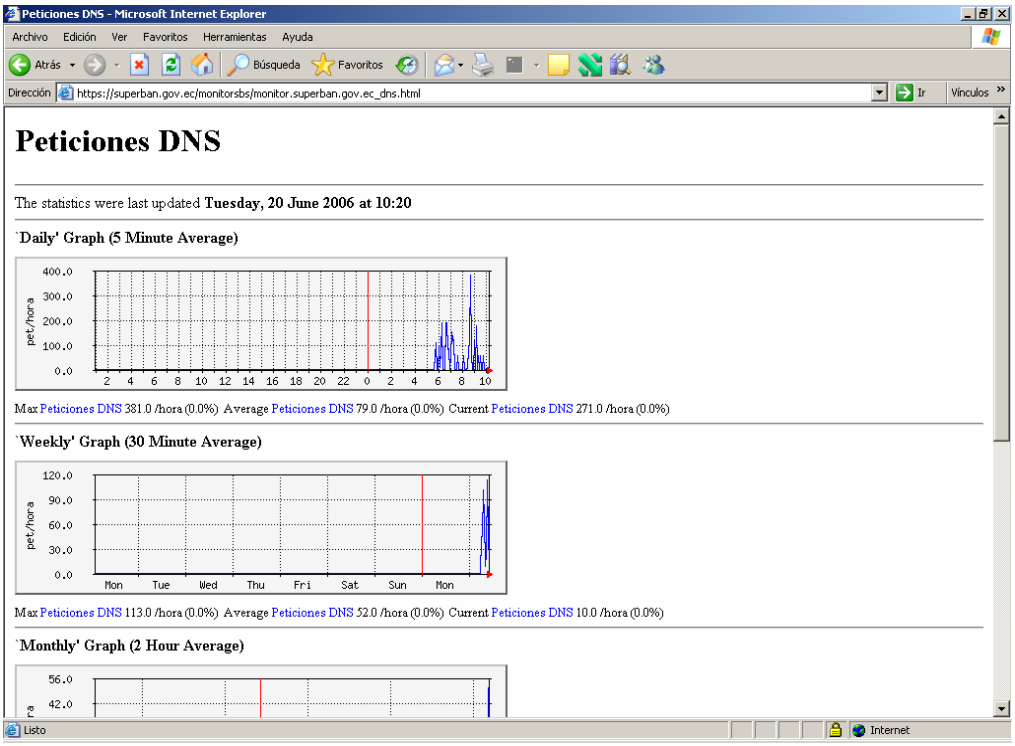

Figura 4.43. Monitoreo del servicio DNS

4.1.2.3.4. SYSSTATS de WEBMIN. La instalación de Webmin es el requerimiento principal para la ejecución de este software (SYSSTATS). Webmin es un administrador del sistema operativo Linux, facultado para realizar configuraciones y cambios al servidor en entorno gráfico. Por este motivo se contempló disponer del servidor HTTPS, para así asegurar las comunicaciones entre el administrador y el servidor.

Los paquetes necesarios para la correcta instalación y un adecuado funcionamiento de WEBMIN – SYSSTATS son:

- **openssl** (secure socket layer).

- **Net::SSleay.-** Es un módulo que permite que los scripts escritos en perl llamen a las funciones en la biblioteca de OpenSSL.

- **RRDtool.-** Es un sistema para almacenar y mostrar datos a través del tiempo. Ej. Tráfico de red, temperatura de la sala de máquinas, carga de servidores. Otra ventaja de este paquete es que los datos se almacenan de manera compacta, la base de datos no crece con el tiempo y permite mostrar fácilmente en forma de gráficos los datos en distintos periodos de tiempo.

4.1.2.3.4.1. Instalación de NET::SSLEAY. Este paquete se encuentra disponible en la Web, es recomendable descargarlo para el sistema Linux en el cual se instale. En el caso de la SBS-RHEL4 se descargó **perl-Net-SSLeay-1.25-1.2.el4.rf.i386.rpm**. Una vez realizada la instalación se debe comprobar el funcionamiento del paquete, esto se realiza de la siguiente manera (Fig. 4.44):

```
[root@monitor ~]# rpm -Uvh perl-Net-SSLeay-1.25-1.2.el4.rf.i386.rpm
[root@monitor mrtg]# perl -e 'use Net::SSLeay'
```

Figura 4.44. Instalación y comprobación de NET::SSLEAY

Si no se da ningún mensaje erróneo, al ejecutar el comando anterior, procedemos con el siguiente paso de instalación.

4.1.2.3.4.2. Instalación de RRDTOOL. Este paquete como otros binarios, pueden ejecutarse e instalarse en modo gráfico o comando.

4.1.2.3.4.3. Instalación de WEBMIN. La distribución de Webmin instalada en el servidor de la Superintendecia de Bancos y Seguros se descargó en formato RPM por lo que su instalación es exactamente igual a la de los paquetes antes mencionados. Una vez realizada la instalación procedemos a ingresar al software (Fig.4.45), esto se realiza a través de un browser (en el caso de Linux Mozilla o Konqueror)

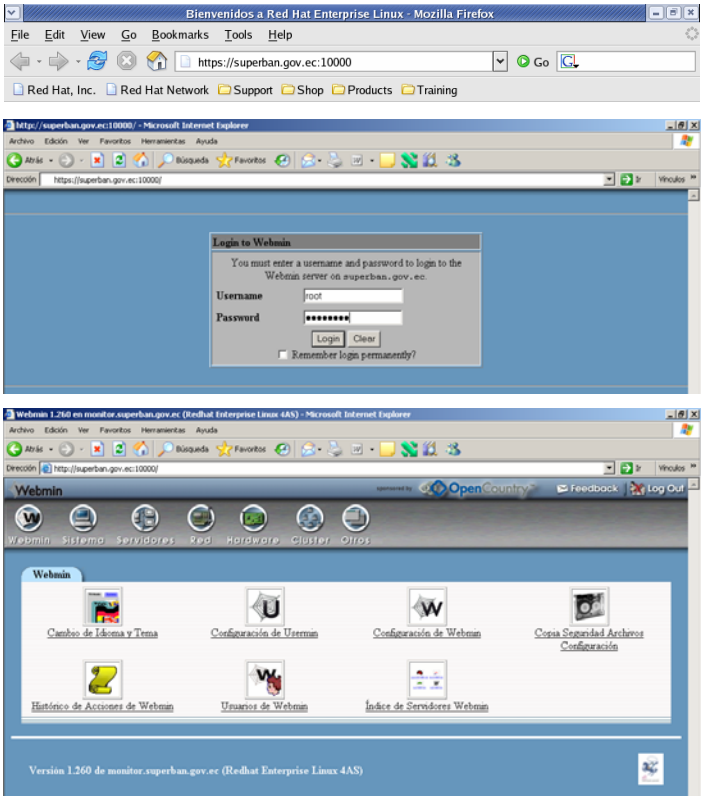

Figura 4.45. Ingreso a WEBMIN

NOTA.- *Como se va a interactuar con un software que tiene dominio del sistema operativo es muy importante brindar las seguridades necesarias, en nuestro caso todo lo que realicemos va a ser a través de https. También es recomendable cambiar el puerto 10000 al que por defecto se encuentra activado puesto que en firewall implementado cerramos todos los puertos del sistema (desde el puerto 1 al 1024) y se escogió que el puerto a donde se accede a Webmin, esté en el intervalo de puertos del sistema.*

4.1.2.3.4.4. Instalación de SYSSTATS. El ingreso a Webmin debe ser inicialmente como usuario root con su respectiva contraseña. Este software nos entrega múltiples formas de configuración del sistema, en modo gráfico, pero estos cambios al sistema no forman parte de los objetivos del proyecto, por lo que únicamente se detallará la instalación y visualización de los módulos de monitoreo de SYSSTATS (Fig.4.46).

Para la instalación debemos de ingresar a configuración de Webmin y posteriormente al icono de Módulos, este campo nos da múltiples opciones de instalación de paquetes adicionales. En el caso del proyecto de la SBS primero se descargó el archivo en formato TAR y se realiza su búsqueda, una vez encontrado pulsamos OK y posteriormente instalar módulo.

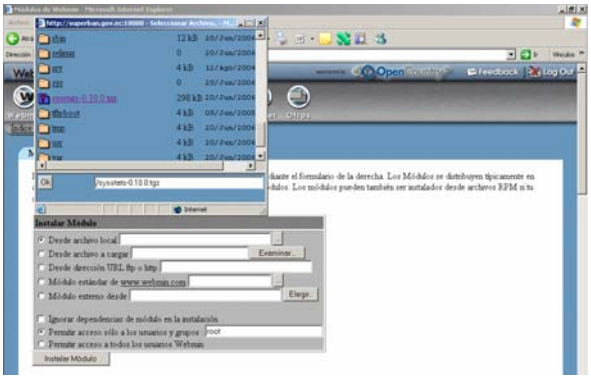

Figura 4.46. Instalación SYSSTATS

Realizada la instalación nos dirigimos a **sistema** y en estadísticas históricas podremos observar las múltiples gráficas entregadas por el software.

Todos estos módulos son susceptibles de cambios, el detalle de los cambios queda en manos de él o los administradores del sistema que deseen implementarlos.

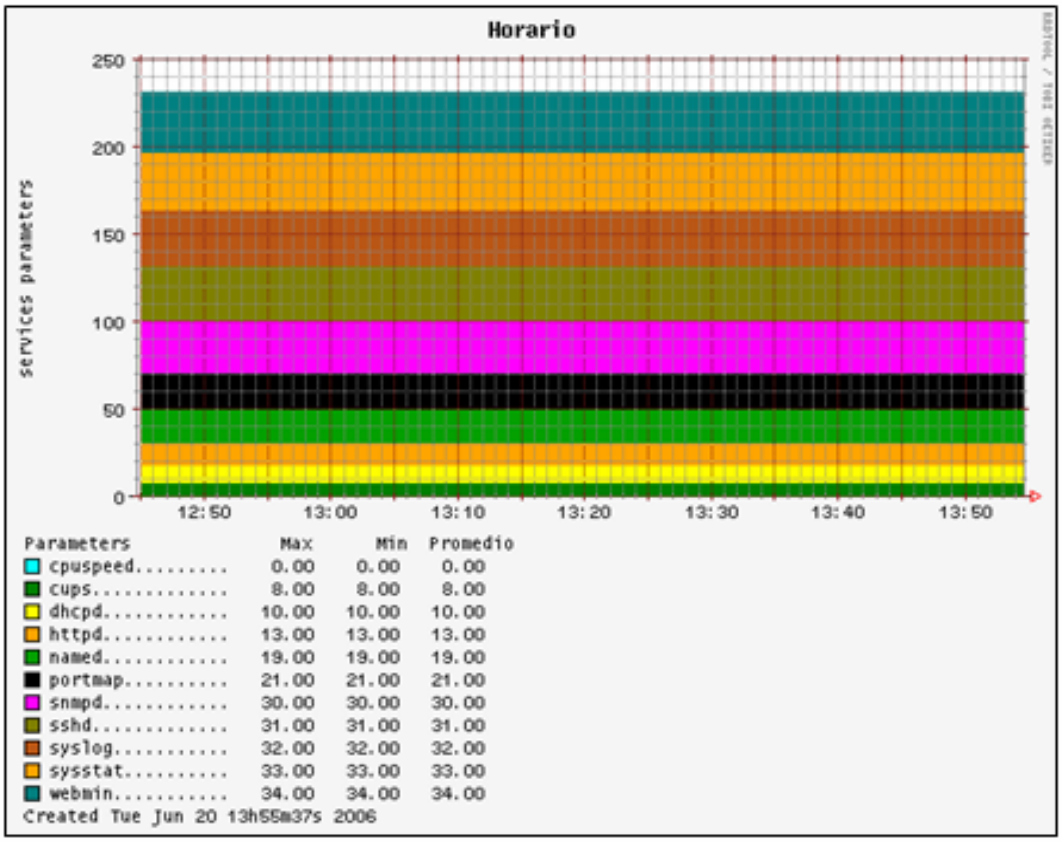

Figura 4.47. Actividad de Servicio Linux

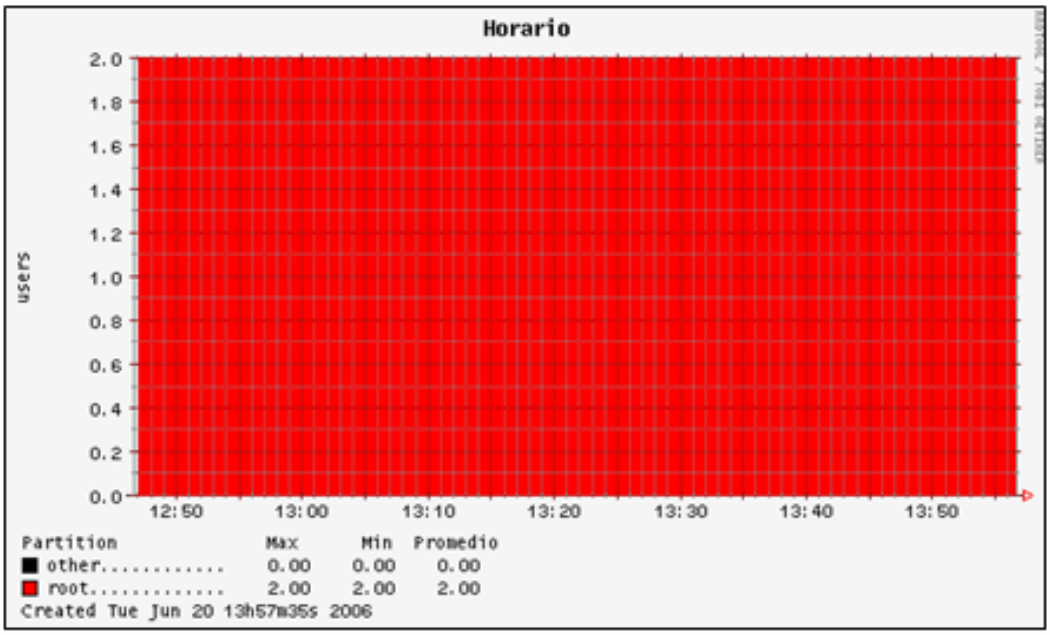

Figura 4.48. Ingresos al Sistema

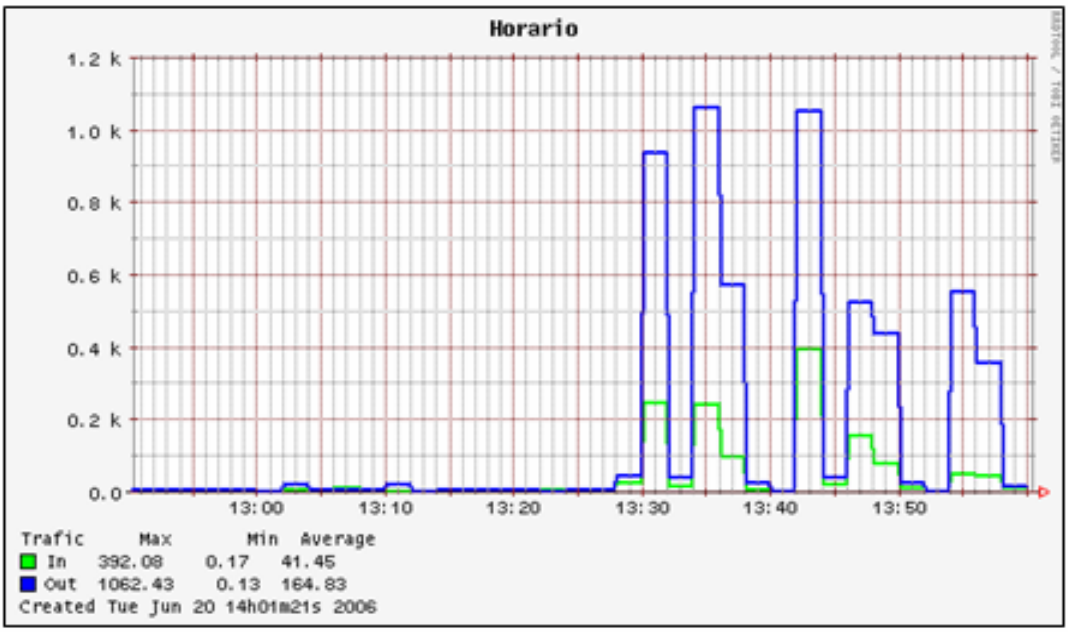

Figura 4.49. Actividad de Interfaz Ethernet

En la figura 4.47 se puede observar la carga de los servicios en funcionamiento . En este campo se editó la gráfica para observar únicamente los servicios del interés del proyecto. En la figura 4.48 muestra que únicamente root ha ingresado al sistema y en caso de que alguno intruso logre vulnerar las seguridades será fácilmente detectado por el monitor. Finalmente la figura 4.49 proporciona la actividad de la interfaz de red.

FIREWALL - IPTABLES SBS

4.1.2.4. Cortafuegos

La seguridad de la información es pensada a menudo como un proceso y no como un producto. Sin embargo, las implementaciones de seguridad estándar usualmente emplean alguna forma de mecanismo dedicado para controlar los privilegios de acceso y restringir los recursos de la red a los usuarios autorizados, identificables y localizables.

Los cortafuegos o firewalls son uno de los componentes principales de la implementación de seguridad. Muchos vendedores de soluciones de cortafuegos dirigidas a todos los niveles del mercado: desde los usuarios del hogar protegiendo un PC hasta las soluciones de Centros de Datos resguardando información vital de la corporación. Los cortafuegos pueden ser soluciones de hardware independiente, tales como aparatos cortafuegos de Cisco, Nokia, y Sonicwall. También existen soluciones de cortafuegos de software propietario desarrolladas para los mercados del hogar y de negocios por vendedores tales como Checkpoint, McAfee y Symantec.

Aparte de las diferencias entre cortafuegos de hardware y software, también existen diferencias en la forma en que los cortafuegos funcionan que los separan unos de los otros. La Tabla 4.4 detalla tres tipos comunes de cortafuegos y como funcionan:

Tabla 4.4 Tipos de cortafuegos

Método	Descripción	Ventajas	Desventajas
NAT	▪ La Traducción de direcciones de red (NAT), coloca las subredes IP internas detrás de una o de un pequeño grupo de direcciones IP, enmascarando todas las peticiones a una fuente en vez de a muchas.	▪ Se puede configurar de forma transparente a las máquinas en una LAN. ▪ Protección de muchas máquinas y servicios detrás de una o más direcciones IP, simplificando las tareas administrativas. ▪ La restricción del acceso de usuarios hacia y desde la LAN se puede configurar abriendo y cerrando puertos en el cortafuegos/puerta de enlace NAT.	▪ No puede prevenir las actividades maliciosas una vez que los usuarios se conectan a un servicio fuera del cortafuego.
Filtrado de paquetes	▪ Un cortafuegos de filtrado de paquetes lee cada paquete de datos que pasa dentro y fuera de una LAN. Puede leer y procesar paquetes de acuerdo a la información de la cabecera y filtra el paquete basado en un conjunto de reglas	▪ Personalizable a través de la utilidad iptables. ▪ No requiere ninguna personalización particular del lado del cliente, pues toda la actividad de la red es filtrada al nivel del enrutador en vez de a nivel de la aplicación. ▪ Puesto que los paquetes no son	▪ No puede filtrar paquetes por contenido como los cortafuegos Proxy. ▪ Procesa los paquetes en la capa del protocolo pero no puede filtrar los paquetes en la capa de la aplicación.

	programables implementadas por el administrador del cortafuego. El kernel de Linux tiene una funcionalidad de filtrado de paquetes embebida a través del subsistema del kernel Netfilter.	transmitidos a través del proxy, el rendimiento de la red es más rápido debido a la conexión directa desde el cliente remoto.	Las arquitecturas de red complejas pueden hacer el establecimiento de reglas de filtrado difíciles, especialmente si están usando enmascaramiento de IP o subredes locales y redes DMZ.
Proxy	Los cortafuegos proxy filtran todas las peticiones de cierto tipo o protocolo desde los clientes LAN a una máquina proxy, la cual luego hace esas peticiones a la Internet en nombre del cliente local. Una máquina proxy actúa como un buffer entre los usuarios remotos maliciosos y las máquinas clientes de la red interna.	Otorga a los administradores el control sobre qué aplicaciones y protocolos funcionan fuera de la LAN. Algunos servidores proxy pueden hacer caché de datos para que los clientes puedan accesar los datos solicitados con frecuencia desde el caché local en vez de tener que utilizar la conexión a Internet para pedirlos, lo cual es conveniente para reducir el consumo innecesario de ancho de banda. Los servicios Proxy se pueden registrar y supervisar de cerca, permitiendo un mayor control sobre el uso de los recursos en la red.	Los proxies a menudo son específicos a las aplicaciones (HTTP, Telnet, etc.) o restringidos al protocolo (la mayoría de los proxies funcionan con servicios conectados a TCP solamente). Los servicios de aplicaciones no se pueden ejecutar detrás del proxy, por lo que sus servidores de aplicaciones deben utilizar una forma de seguridad de la red separada. Los proxies pueden convertirse en un cuello de botella, puesto que todas las peticiones y transmisiones son pasadas a través de una fuente en vez de directamente del cliente a un servicio remoto.

4.1.2.4.1. Tipos de Cortafuegos.

- **Netfilter e Iptables.** El kernel de Linux presenta un subsistema de redes muy poderoso llamado Netfilter. El subsistema netfilter proporciona un filtrado de paquetes con vigilancia continua o sin ella, así como también NAT y servicios de enmascaramiento IP. Netfilter también tiene la habilidad de mutilar la información IP de cabecera para un enrutamiento avanzado y gestión del estado de la conexión. Netfilter es controlado a través de la utilidad iptables.

- **Descripción general de Iptables.** El poder y flexibilidad de Netfilter es implementado a través de la interfaz de iptables. Esta herramienta de línea de comandos es similar en sintaxis a su predecesor, ipchains; sin embargo, iptables utiliza el subsistema Netfilter para mejorar la conexión de la red, inspección y procesamiento; mientras que ipchains usa conjuntos de reglas intrincados para filtrar rutas de fuentes y destino, así como también puertos de conexión o ambos. Iptables presenta funcionalidades como: registro avanzado, acciones previas y posteriores al enrutamiento, traducción de direcciones de red y reenvío de puertos, todo en una interfaz de línea de comandos.

4.1.2.4.2. Uso de Iptables. El primer paso en el uso de Iptables es iniciar el servicio Iptables. Adicionalmente para su funcionamiento es necesario saber que la sintaxis de Iptables está separada en niveles. El nivel principal es la cadena. Una cadena especifica el estado en el cual se puede manipular un paquete. El uso es como se muestra a continuación:

[root@monitor /] # iptables -A chain -j target

La **-A** anexa una regla al final de un conjunto de reglas existente. La chain es el nombre de la cadena para una regla. Las tres cadenas embebidas de iptables (esto es, las cadenas que afectan cada paquete que atraviesa la red) son **INPUT, OUTPUT** y **FORWARD**. Estas cadenas son permanentes y no se pueden borrar.

Las nuevas cadenas (también conocidas como cadenas definidas por el usuario) se pueden crear usando la opción **-N**. Es útil crear una nueva cadena para la personalización granulada o para crear reglas más elaboradas.

4.1.2.4.3. Políticas básicas del cortafuegos. Establecer algunas políticas básicas desde el comienzo puede servir como una base para la construcción de reglas más detalladas definidas por el usuario. Iptables utiliza políticas (**-P**) para crear reglas por defecto. Los administradores orientados a la seguridad usualmente eligen descartar todos los paquetes como una política y solamente permiten paquetes específicos basados en el caso. Las reglas siguientes bloquean todo los paquetes entrantes y salientes en una puerta de enlace de red.

[root@monitor /] # iptables -P INPUT DROP
[root@monitor /] # iptables -P OUTPUT DROP

Adicionalmente, se recomienda que cualquier paquete redirigido (el tráfico de la red que se debe enrutar desde el cortafuegos a su nodo destino) también se niegue, para restringir a los clientes internos de una exposición inadvertida a la Internet. Para hacer esto, se utiliza:

[root@monitor /] # iptables -P FORWARD DROP

Después de configurar las cadenas de políticas, puede crear las nuevas reglas para su red y requerimientos de seguridad particulares. A continuación se resaltan algunas reglas que puede implementar en el curso de la construcción de un cortafuegos iptables.

4.1.2.4.4. Guardar y restaurar reglas Iptables. Las reglas del cortafuegos son válidas únicamente mientras el computador esté encendido. Si se reinicia el sistema, las reglas son vaciadas y reiniciadas automáticamente. Para guardar las reglas para que puedan cargarse más tarde, se utiliza el siguiente comando:

[root@monitor /] # service iptables save

Las reglas son almacenadas en el archivo /etc/sysconfig/iptables y aplicadas cuando el servicio es iniciado o reiniciado, incluyendo cuando la máquina es reiniciada.

4.1.2.4.5. Filtros comunes de Iptables. El mantener a los intrusos fuera de la LAN es un aspecto importante de la seguridad de la red, o quizás el más importante. La integridad de una LAN debería ser protegida de intrusos maliciosos a través del uso de rigurosas reglas del cortafuegos. Sin embargo, con una política por defecto configurada para bloquear todos los paquetes entrantes, salientes y redirigidos, es imposible para el cortafuegos/puerta de enlace y los usuarios internos de la LAN comunicarse entre ellos o con recursos externos. Para permitir a los usuarios realizar funciones relacionadas a la red y utilizar las aplicaciones de la red, los administradores deben abrir ciertos puertos para la comunicación.

Por ejemplo, para permitir el acceso al puerto 80 en el cortafuegos, añada la siguiente regla:

[root@monitor /] # iptables -A INPUT -p tcp -m tcp --sport 80 -j ACCEPT
[root@monitor /] # iptables -A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT

Esto permite la navegación Web normal desde los sitios Web que se comunican a través del puerto 80. Para permitir el acceso a sitios Web seguros (tales como https://www.sbs.com/), debe abrir el puerto **443** también.

Cuando se crea un conjunto de reglas iptables, es crítico recordar que el orden es importante. Por ejemplo, una cadena que especifica que cualquier paquete desde la subred local 192.168.100.0/24 sea descartado y luego se agrega una cadena (**-A**) para permitir paquetes desde 192.168.100.13 (la cual está dentro de la subred restringida descartada), entonces la regla anexada es ignorada. Primero debe configurar una regla para permitir 192.168.100.13 y luego configurar una regla de rechazo en la subred.

Para insertar una regla de forma arbitraria en una cadena de reglas existente, utilice **-I**, seguido por la cadena en la cual desea insertar la regla y un número de regla (1,2,3,...,n) donde desea que resida la regla. Por ejemplo:

[root@monitor /] # iptables -I INPUT 1 -i lo -p all -j ACCEPT

La regla es insertada como la primera regla en la cadena INPUT para permitir el tráfico en loopback local del dispositivo.

Hay muchas veces en que se requiere el acceso remoto a la LAN desde fuera de la LAN. Se puede utilizar un servicio seguro, tal como SSH, para encriptar conexiones remotas a los servicios LAN. Para aquellos administradores con recursos basados en PPP (tales como bancos de módem o cuentas ISP en cantidades), el acceso de marcado se puede utilizar para burlar las barreras del cortafuegos de forma segura, pues las conexiones de módem están típicamente detrás de un cortafuegos/puerta de enlace ya que son conexiones directas. Sin embargo, para los usuarios remotos con conexiones de banda ancha, se pueden hacer casos especiales. Puede configurar iptables para aceptar conexiones desde clientes SSH remotos. Por ejemplo, para permitir acceso SSH, se deben utilizar las reglas siguientes:

[root@monitor /] # iptables -A INPUT -p tcp --dport 22 -j ACCEPT

[root@monitor /] # iptables -A OUTPUT -p udp --sport 22 -j ACCEPT

Hay otros servicios para los cuales puede necesitar definir reglas.

Estas reglas permiten el acceso a servicios regulares y seguros en el cortafuegos; sin embargo, no permiten a nodos detrás del cortafuegos acceder a estos servicios. Para permitir el acceso a la LAN de estos servicios, puede utilizar NAT con reglas de filtrado iptables.

4.1.2.4.6. Reglas FORWARD Y NAT. La mayoría de las organizaciones se les asigna un número limitado de direcciones IP públicas enrutables desde sus ISP. Debido a esta limitación en la asignación, los administradores deben buscar formas creativas de compartir el acceso a los servicios de Internet sin otorgar las limitadas direcciones IP públicas a todos los nodos en la LAN. El uso de direcciones IP privadas es la forma común de permitir a todos los nodos en una LAN acceder apropiadamente a los servicios de redes internos y externos. Los enrutadores en las puntas de la red (tales como cortafuegos), pueden recibir las transmisiones entrantes desde la Internet y enrutar los paquetes al nodo objetivo en la LAN; al mismo tiempo los cortafuegos/puertas de enlace pueden enrutar peticiones salientes desde un nodo LAN al servicio Internet remoto. Este reenvío del tráfico de la red se puede volver peligroso a veces, especialmente con la disponibilidad de herramientas modernas para violar redes que pueden engañar direcciones IP internas y hacer que la máquina remota del atacante actúe como un nodo en su propia LAN. Para prevenir esto, iptables proporciona políticas de enrutamiento y reenvío que se pueden implementar para prevenir el uso inadecuado de los recursos de la red.

La política FORWARD permite al administrador controlar donde se enviaran los paquetes dentro de una LAN. Por ejemplo, para permitir el reenvío a la LAN completa (asumiendo que el cortafuegos/puerta de enlace tiene una dirección IP interna en eth1), se pueden configurar las reglas siguientes:

[root@monitor /] # iptables -A FORWARD -i eth1 -j ACCEPT
[root@monitor /] # iptables -A FORWARD -o eth1 -j ACCEPT

Esta regla da a los sistemas detrás del cortafuegos/puerta de enlace acceso a la red interna. La puerta de enlace enruta los paquetes desde un nodo de la LAN hasta su nodo destino, pasando todos los paquetes a través del dispositivo eth1.

NOTA.- *Por defecto, la política IPv4 en los kernels Red Hat Enterprise Linux desactivan el soporte para el reenvío IP, lo cual previene que las cajas ejecutando Red Hat Enterprise Linux funcionen como enrutadores de bordes de la red dedicados. Para activar el reenvío IP, ejecute el comando siguiente:*

[root@monitor /] # sysctl -w net.ipv4.ip_forward=1

Si este comando se ejecuta a través del indicador de comandos, entonces el valor no se recuerda luego de un reinicio. Puede configurar el reenvío de forma permanente modificando el archivo **/etc/sysctl.conf**. Busque y modifique la línea siguiente, reemplazando 0 con 1:

net.ipv4.ip_forward = 0

Ejecute el comando siguiente para activar el cambio al archivo **sysctl.conf:**

[root@monitor /] # sysctl -p /etc/sysctl.conf

El aceptar paquetes reenviados a través del dispositivo interno IP interno del cortafuegos permite a los nodos LAN comunicarse entre ellos; sin embargo, no se les permite comunicarse externamente (por ejemplo, a la Internet). Para permitir a los nodos de la LAN que tengan una dirección IP privada comunicarse con redes públicas externas, configure el cortafuegos para el enmascaramiento IP, lo cual coloca máscaras en las peticiones desde los nodos LAN con la dirección IP del dispositivo externo del cortafuegos (caso - SBS, eth0):

[root@monitor /] # iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

La regla utiliza la tabla de coincidencias de paquetes NAT (**-t nat**) y especifica la cadena incorporada de **POSTROUTING** para NAT (**-A POSTROUTING**) en el dispositivo de red externo del cortafuegos (**-o eth0**). **POSTROUTING** permite la alteración de los paquetes a medida que dejan el dispositivo externo del cortafuegos. Se especifica el objetivo de **-j MASQUERADE** para enmascarar la dirección IP privada de un nodo con la dirección IP del cortafuegos/puerta de enlace.

Si tiene un servidor en su red interna que desea colocar disponible de forma externa, puede utilizar el objetivo **-j** DNAT de la cadena **PREROUTING** en NAT para especificar una dirección IP destino y un puerto donde se pueden reenviar los paquetes entrantes solicitando una conexión a su servicio interno. Por ejemplo, si desea reenviar las peticiones HTTP entrantes a su sistema Servidor Apache, HTTP dedicado en 172.31.0.23, ejecute el comando siguiente:

[root@monitor /] # iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT \ --to 172.31.0.23:80

Esta regla especifica que la tabla NAT utiliza la cadena incorporada PREROUTING para reenviar las peticiones HTTP entrantes exclusivamente a la dirección IP listada 172.31.0.23.

NOTA.- *Si tiene una política por defecto de DROP en su cadena FORWARD, debe anexar una regla para permitir el reenvío de peticiones HTTP entrantes para que sea posible el enrutamiento NAT. Para lograr esto, ejecute el comando siguiente:*

[root@monitor /] # iptables -A FORWARD -i eth0 -p tcp --dport 80 -d 172.31.0.23 -j ACCEPT

Esta regla permite el reenvío de peticiones HTTP entrantes desde el cortafuegos a su Servidor Apache HTTP destino detrás del cortafuegos.

DMZs e iptables. Se puede establecer reglas iptables para enrutar el tráfico a ciertas máquinas, tales como a un servidor HTTP o FTP dedicado, en una zona demilitarizada (DMZ), una subred local especial dedicada a proporcionar servicios en un transportador público como la Internet. Por ejemplo, para configurar una regla para el enrutamiento de todas las peticiones HTTP entrantes a un servidor HTTP dedicado en la dirección 10.0.4.2 (fuera del intervalo 192.168.1.0/24 de la LAN), la traducción de direcciones de red (NAT) llama una tabla PREROUTING para reenviar los paquetes al destino correcto:

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT \ --to-destination 10.0.4.2:80

Con este comando, todas las conexiones HTTP al puerto 80 desde afuera de la LAN son enrutadas al servidor HTTP en una red separada del resto de la red interna. Esta forma de segmentación de la red es más segura que permitir conexiones HTTP a una máquina en la red. Si el servidor HTTP es configurado para aceptar conexiones seguras, entonces se debe también redirigir el puerto 443.

4.1.2.4.7. Iptables y Seguimiento de Conexiones. Iptables incluye un módulo que permite a los administradores inspeccionar y restringir conexiones a servicios disponibles en una red interna conocido como seguimiento de conexiones. El seguimiento de conexiones almacena las conexiones en una tabla, lo que permite a los administradores otorgar o negar acceso basado en los siguientes estados de conexiones:

- **NEW.-** Un paquete solicitando una nueva conexión, tal como una petición HTTP.
- **ESTABLISHED.-** Un paquete que es parte de una conexión existente.
- **RELATED.-** Un paquete que está solicitando una nueva conexión pero que es parte de una conexión existente, tal como las conexiones FTP pasivas donde el puerto de conexión es 20, pero el puerto de transferencia puede ser cualquiera desocupado más allá del puerto 1024.

- **INVALID.-** Un paquete que no forma parte de ninguna conexión en la tabla de seguimiento de conexiones.

Puede utilizar la funcionalidad de vigilancia continua de seguimiento de conexiones de iptables con un protocolo de red, aún si el protocolo mismo es sin supervisión (tal como UDP). El ejemplo siguiente muestra una regla que utiliza el seguimiento de conexiones para reenviar solamente paquetes que estén asociados con una conexión establecida:

[root@monitor /] # iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ALLOW

DISEÑO DEL SERVICIO VPN - SBS

4.2. SERVICIO DE REDES PRIVADAS VIRTUALES (VPN)

4.2.1. Diseño de la red VPN de la SBS. Como se mencionó en el Capítulo II, la propuesta tecnológica de Backup (Fig. 4.50) busca respaldar las vías de comunicación ya existentes en la Entidad (bajo plataforma Linux) mas no reemplazarlas. Toda esta propuesta tecnológica se desenvuelve en los siguientes escenarios:

- LAN-to-LAN
- SERVICIO DE ACCESO REMOTO VPN - RAS
- SERVICIO DE ACCESO REMOTO VPN – INTERNET

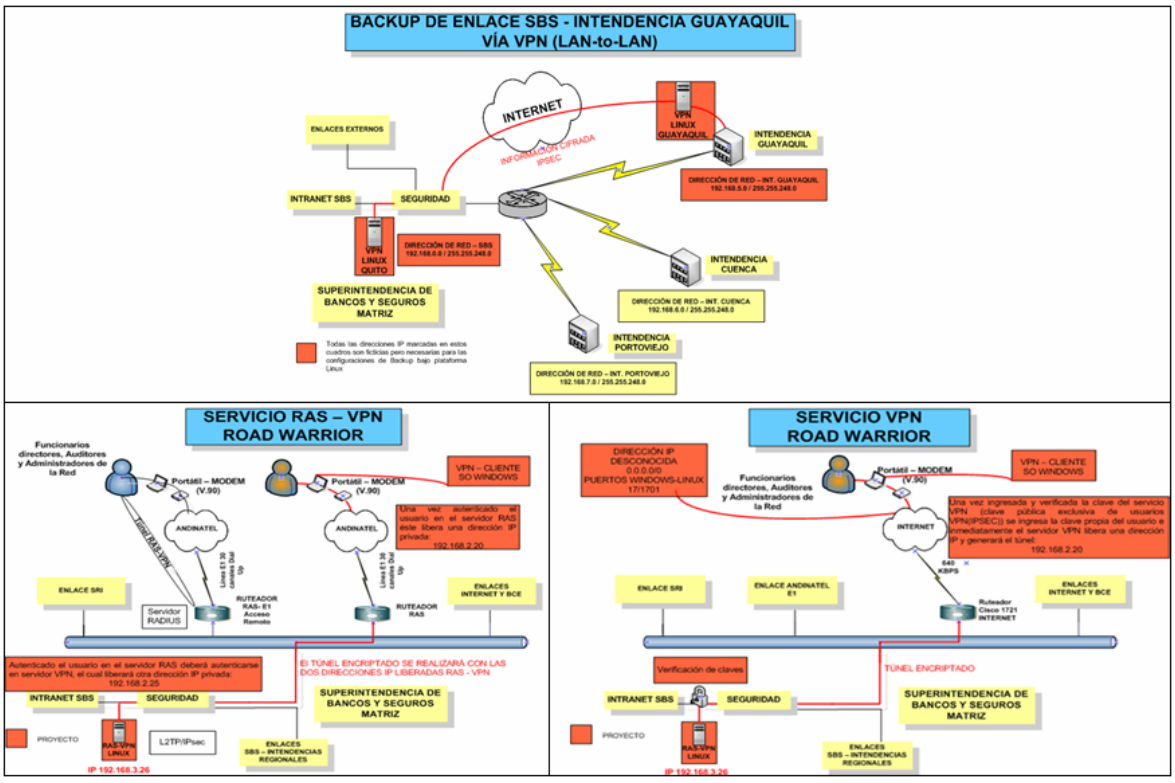

Figura 4.50. Escenarios BACKUP - VPN

4.2.2. Características Técnicas de Hardware y Software. Las características técnicas de Hardware, del servidor DELL, que brindará los servicios DHCP, DNS y VPNs son:

Tabla 4.5 Características Técnicas del Servidor SBS

Placa base:	
Tipo de procesador	Dual Intel Pentium IIIE, 860 MHz (6.5 x 132)
Nombre de la Placa Base	Dell Computer Corporation PowerEdge 2400
Memoria del Sistema	1024 MB
Tipo de BIOS	Phoenix (10/10/00)
Monitor:	
Tarjeta gráfica	ATI Technologies Inc. 3D RAGE IIC PCI (4 MB)
Acelerador 3D	ATI 3D-Rage IIC
Monitor	Compaq V55 (844BF23AJ100)
Almacenamiento:	
Disquetera de 3 1/2	Unidad de disquete
Disco duro	FUJITSU MAN3367MC SCSI Disk Device (36 GB, 10000 RPM, Ultra160 SCSI)
Disco duro	FUJITSU MAN3367MC SCSI Disk Device (36 GB, 10000 RPM, Ultra160 SCSI)
Disco duro	SEAGATE ST318404LC SCSI Disk Device (18 GB, 10000 RPM, Ultra160 SCSI)
Disco duro	SEAGATE ST318404LC SCSI Disk Device (18 GB, 10000 RPM, Ultra160 SCSI)
Lector óptico	NEC CD-ROM DRIVE:466 SCSI CdRom Device
Red:	
Tarjeta de Red	Adaptador Ethernet PCI basado en Intel 8255x (10/100)
Propiedades del Sistema:	
Fabricante	Dell Computer Corporation
Producto	PowerEdge 2400
Tipo de arranque	Botón marcha/parada
Propiedades del chasis:	
Fabricante	Dell Computer Corporation
Número de serie	82DT701
Tipo de chasis	Main Server Chasis
Propiedades del procesador 1 y 2:	
Fabricante	Intel
Reloj externo	133 MHz
Velocidad de reloj máxima	1066 MHz
Velocidad de reloj actual	866 MHz
Tipo	Central Processor
Voltaje	1.7 V
Identificación del socket	Processor 1 – 2
Propiedades del caché 1 y 3:	
Tipo	Interna
Estado	Activado
Tamaño máximo	32 KB
Tamaño instalado	32 KB
Corrección de errores	Multi-bit ECC
Propiedades del caché 2 y 4:	
Tipo	Interna
Estado	Activado
Modo de operación	Write-Back

Tamaño máximo	512 KB
Tamaño instalado	256 KB
Tipo de SRAM	ActualPipeline Bursa
Corrección de errores	Multi-bit ECC
Propiedades del dispositivo de memoria DIMM_A_B_C_D:	
Forma	DIMM
Tipo	SDRAM
Tipo detallado	Synchronous
Tamaño	256 MB
Velocidad	100 MHz
Tamaño total	72 bits
Ancho de datos	64 bits
Emplazamiento del dispositivo	DIMM_A_B_C_D

4.2.2.1. Características Técnicas del Software. El kernel 2.6 de Red Hat Enterprise Linux 4 posee soporte para implementaciones VPN (ver Tabla 3..3 Requerimientos de seguridad de la distribución Linux SBS). Es necesario confirmar estas bases por medio del siguiente procedimiento:

Primero.- Para realizar esta verificación ingresamos a la carpeta que contenga el kernel Linux de la siguiente manera:

[root@monitor /] # cd /usr/src/kernels/2.6.x.x

Segundo.- El método manifestado generalmente se utiliza para compilar nuevos kernels, sin embargo, se recurrirá al mismo para realizar las verificaciones pertinentes al soporte que proporciona el kernel 2.6 de RHEL4.

[root@monitor 2.6.x.x] # make menuconfig

NOTA.- *Existen dos maneras recomendadas tanto para verificar como para hacer cambios al kernel, estas son menuconfig y xconfig.*

Ingresando a **Drivers --->Networking Support --->Networking Options,** se puede observar detalladamente todos y cada uno de los módulos necesarios para las implementaciones VPN (Fig. 4.51).

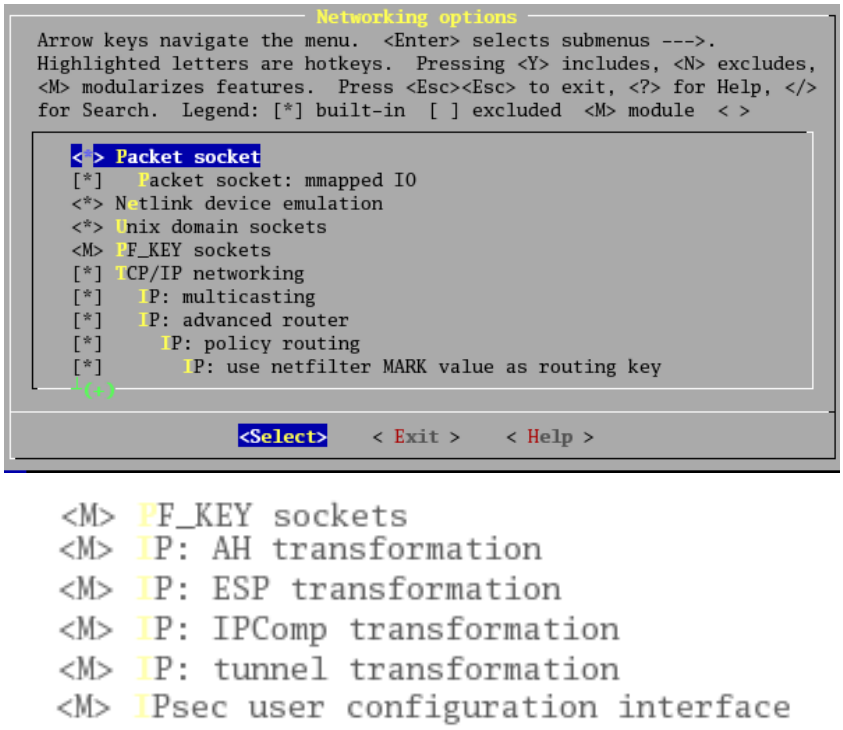

Figura 4.51. Soporte del Kernel Linux para levantar VPNs

4.2.3. Autenticación de Usuarios internos y externos. Por políticas de seguridad solo los usuarios internos tienen claves para ingresar a los servicios Institucionales sean estos RAS, VPN, y demás servicios de comunicación que posee.

A pesar que la SBS es un organismo de Control de Entidades Bancarias no está exenta de supervisión. Dicho control se ejecuta dentro de las instalaciones (Ej. Cuando la Contraloría desea realizar algún tipo de control acuden personalmente a las instalaciones de la SBS), sin necesidad de interactuar con entes externos. En caso, no contemplado, se requiera algún acceso a la Red Institucional se deberá brindar un servicio VPN para el ingreso a la misma. Este ingreso obligadamente deberá cumplir con una serie de requisitos ante las autoridades de la SBS.

4.2.4. Selección del Método de Autenticación. En las configuraciones realizadas en el servidor VPN de la SBS se utilizaron tres modos de autenticación, detallados a continuación:

4.2.4.1. Backup VPN de enlaces Clear Channel. Para esta propuesta tecnológica se procedió a configurar **claves RSA** (Rivest- Shamir- Adleman) que es un sistema de cifrado de llaves públicas que se usa tanto para cifrado de datos como para autenticación de dichas llaves. Fue inventado por Ronald Rivest, Adi Shamir y Leonard Adleman en 1977. De las iniciales del apellido de sus creadores RSA tomó su nombre.

En el caso de interacción entre las Regionales y la Superintendencia de Bancos y Seguros se estableció este tipo de autenticación, puesto que, por razones de seguridad permite generar claves con nbits generados aleatoriamente (dentro de los límites 1536 y 4096) y además dichas claves serán manejadas únicamente por los administradores de la Red.

4.2.4.2. Acceso Remoto VPN - Internet y Acceso Remoto VPN - Ras. Las conexiones L2TP/IPSec necesitan una autenticación más segura porque requieren dos niveles de autenticación: autenticación en el equipo (SERVIDOR) por medio de certificados o claves previamente compartidas para la sesión IPSec y autenticación de usuario mediante un protocolo de autenticación PPP para establecer el túnel L2TP.

4.2.4.2.1. PSK (PRE SHARED KEY). Una llave pre-compartida es una cadena de caracteres (unicode) usada para autenticar conexiones de L2TP/IPSec. Esta clave es gestionada únicamente por el administrador del servicio.

4.2.4.2.2. PPP. Para autenticar enlaces PPP existen 2 métodos PAP y CHAP. CHAP es un protocolo de tres vías y al igual que PAP, puede ser usado al comienzo de un enlace PPP y ser repetido cuando el enlace ya se haya establecido. CHAP incorpora tres pasos para la autenticación de un enlace, que son:

- El autenticador envía un mensaje al nodo remoto.
- El nodo calcula un valor usando una función HASH y lo envía de regreso al autenticador.

- El autenticador avala la conexión si la respuesta concuerda con el valor esperado.

El proceso puede repetirse en cualquier momento del enlace PPP para asegurarse que la conexión no ha sido tomada por otro nodo. A diferencia de PAP, en CHAP el servidor controla la reautenticación. PAP y CHAP tienen algunas desventajas, en ninguno de los dos se pueden asignar diferentes privilegios para acceder a la red a diferentes usuarios remotos que usan el mismo computador.

CONFIGURACIÓN DEL SERVICIO VPN – SBS

ARQUITECTURA LAN-TO-LAN

4.2.5. Configuración VPN LAN-to-LAN. Red Hat Enterprise proporciona soporte VPN bajo su herramienta propietaria RACOON, pero ésta no cubre todos los campos que abarca la propuesta tecnológica de BACKUP, motivo por el cual se procedió a descargar los siguientes paquetes:

- **openswan-2.4.0-1.src.rpm**. Software libre que se encarga de implementar los protocolos IPSec (IP Security) bajo Linux, brindando cifrado y autenticación a nivel IP.

- **l2tpd-0.69-13.src.rpm**. L2tpd al igual que Openswan es un software libre que habilita el levantamiento de túneles con sesión PPP.

4.2.5.1. Conexión LAN-to-LAN. Una vez verificado el kernel procedemos a descomprimir el paquete OPENSWAN (descargado en formato src.rpm).

[root@monitor /] # rpmbuild –rebuild –clean openswan2.x.src.rpm

Una vez finalizada la descompresión y construcción de los paquetes OPENSWAN en formato RPM se procede a instalarlos desde: **/usr/src/redhat/RPMS/xxx (xxx es la representación de la arquitectura en la cual se instaló Linux)**.

NOTA.- *Los paquetes descargados en formato SRPM tienen la ventaja de construir paquetes compilados de forma especial para el sistema Linux instalado (SBS – RHEL4).*

4.2.5.2. Configuración OPENSWAN. Para evitar exponer las comunicaciones a ataques del tipo men in the middle (hombre en el medio), OPENSWAN maneja dos tipos de autenticación para sus túneles:

- **Manual Keying**.- Donde las dos partes comparten una llave secreta para encriptar sus mensajes. OPENSWAN almacena estas llaves en el archivo /etc/ipsec.conf. Es claro que si alguien obtiene acceso a este archivo la comunicación será vulnerable.

- **Automatic keying**.- Aquí los dos sistemas se autentican el uno con el otro por medio de sus propias llaves secretas. Estas llaves son cambiadas automáticamente de una manera periódica. Obviamente, este método de autenticación es mucho mas seguro, ya que si un intruso obtiene la llave, solo los mensajes entre la renegociación anterior y la siguiente serán expuestos.

NOTA.- *Por razones de maniobrabilidad y facilidad de implementación de las claves en los equipos de los Funcionarios remotos, se estableció generar llaves manuales (Manual Keying).*

4.2.5.3. Generación de Claves y verificación del funcionamiento de OPENSWAN.

Primero.- Se requiere generar una clave, esto se consigue con el siguiente comando:

```
[root@monitor /] # ipsec newhostkey -output /etc/ipsec.secrets --bits 2048
```

Segundo.- Se requiere que los paquetes del cliente lleguen a red interna, motivo por el cual se deberá habilitar el ruteo en el concentrador de túneles. Para activarlo inmediatamente se utilizará: **echo 1 > /proc/sys/net/ipv4/ip_forward.** Para que el ruteo siga activado después de un rebooteo, se recomienda editar la siguiente línea en el archivo **/etc/ sysctl.conf:**

ip_forward=y.

Tercero.- Una vez generadas las claves en los extremos de la VPN (LAN-to-LAN) y activación del ruteo en las mismas, se debe comprobar la correcta instalación de OPENSWAN (Fig. 4.52), con los comandos:

 # service ipsec start e # ipsec verify.

```
[root@monitor RPMS]# ipsec verify
Checking your system to see if IPsec got installed and started correctly:
Version check and ipsec on-path                                 [OK]
Linux Openswan U2.4.0/K2.6.9-5.EL (netkey)
Checking for IPsec support in kernel                            [OK]
Checking for RSA private key (/etc/ipsec.secrets)               [OK]
Checking that pluto is running                                  [OK]
Two or more interfaces found, checking IP forwarding            [OK]
Checking NAT and MASQUERADEing                                  [N/A]
Checking for 'ip' command                                       [OK]
Checking for 'iptables' command                                 [OK]
Checking for 'setkey' command for NETKEY IPsec stack support    [OK]

Opportunistic Encryption DNS checks:
   Looking for TXT in forward dns zone: monitor.superban.gov.ec [MISSING]
   Does the machine have at least one non-private address?      [FAILED]
```

Figura 4.52. Inicialización OPENSWAN

NOTA.- *Los errores presentados no involucran falta de soporte del kernel sino configuraciones adicionales del servidor.*

4.2.5.4. Archivos de configuración OPENSWAN. Antes de realizar los cambios en el archivo de configuración es necesario definir las direcciones de RED que se van a implementar. Como se observa en la figura 4.53, tenemos la dirección de red de la SBS Quito 192.168.0.0 (dirección ficticia) y la dirección de red de la Intendencia de Guayaquil 192.168.5.0 (dirección ficticia) con sus correspondientes direcciones IP públicas. 200.2.3.4 y 200.5.6.7 (direcciones ficticias) respectivamente.

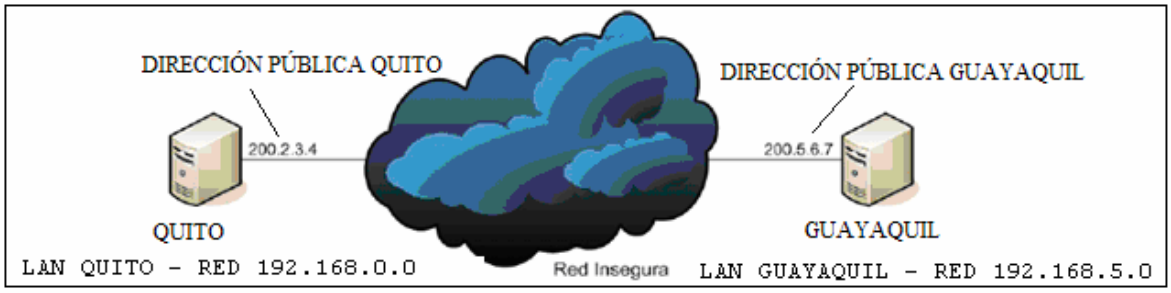

Figura 4.53. VPN LAN-to-LAN

Descripción IPSec.conf. El archivo /etc/ipsec.conf se puede dividir en dos secciones: la primera donde se configuran las opciones generales de IPSec, llamada config setup; y la segunda donde se define cada pareja IPSec llamada conn <nombre que identifica el túnel>

La parte más importante del archivo /etc/ipsec.conf es la que define cada conexión IPSec, de hecho todas las opciones en la sección config setup son opcionales. Los campos básicos que define cada pareja IPSec son:

left=
leftsubnet=
leftnexthop=
leftrsasigkey=
right=
rightsubnet=
rightnexthop=
rightrsasigkey=
auto=

- Los campos left y right son las direcciones IP públicas de cada gateway.
- Los campos leftsubnet y rightsubnet son las subredes que se encuentran detrás de cada gateway (la red privada SBS).
- Los campos leftnexthop y rightnexthop son las direcciones IP del equipo que recibe la conexión en el ISP. Es la puerta de enlace de cada máquina Linux.
- Los campos leftrsasigkey y rigthrsasigkey son las llaves públicas de cada gateway IPSec, y se obtienen con los comandos:

ipsec showhostkey --left e ipsec showhostkey --right

En caso de no contar con estas llaves, se puede generar cada una de ellas con el comando:

ipsec newhostkey --output /etc/ipsec.secrets –hostname <hostname>

4.2.5.5. IPSec.conf SBS. A cada gateway, sea éste la SBS o la Intendencia Regional de Guayaquil, se le debe asignar por nomenclatura como right o left, indistintamente cual se escoja para cada nombre. En el caso SBS el gateway IPSec con IP público 200.2.3.4 es el left y el gateway (Intendencia Regional) IPSec con IP público 200.5.6.7 es el right. Lo

importante es ser congruente con esta nomenclatura a lo largo del proceso de configuración del archivo /etc/ipsec.conf (Fig. 4.54).

```
version 2.0     # conforms to second version of ipsec.conf specification
config setup
        klipsdebug=all
        plutodebug=dns

conn %default
        keyingtries=0
        spi=0x200
        esp=3des-md5-96
        espenckey=0x01234567_89abcdef_02468ace_13579bdf_12345678_9abcdef0
        espauthkey=0x12345678_9abcdef0_2468ace0_13579bdf
        keylife=8h

conn vpnsbs
        left=200.2.3.4
        leftsubnet=192.168.0.0/255.255.248.0
        leftrsasigkey=0sAQPEdAJ04xuayPZ2jl2idlmFtlk1jwCOM+bGLznTgBTbFw4Sy
CRWWvXKygMJ/luCXPaLXTVHbYb8/l65aCF6U16mF1vavxngAo9z1sgjLyMynnrVHVQ8Th8uLC
yJtClH4I+4IQLIEMkcFRD6417DK+YEwi+kDQjhsuC3tPNzFTN71BMbVX8QaeNeVAL29wQtN+Q
387zxAoQuYzhEvhrbBel06iy2tKfL281T3loDJesD99uq1NBASA+fUhwRbvgYWEj+lRktf5zS
7znroDi3qtPUrATnAHjRQKXKIVDAPhmaD+3ggLJNKaekRsS3
        right=200.5.6.7
        rightsubnet=192.168.5.0/255.255.248.0
        rightrsasigkey=0sAQPEdAJ04xuayPZ2jl2idlmFtlk1jwCOM+bGLznTgBTbFw4S
dCRWWvXKygMJ/luCXPaLXTVHbYb8/l65aCF6U16mF1vavxngAo9z1sgjLyMynnrVHVQ8Th8uL
ayJtClH4I+4IQLIEMkcFRD6417DK+YEwi+kDQjhsuC3tPNzFTN71BMbVX8QaeNeVAL29wQtN+
B387zxAoQuYzhEvhrbBel06iy2tKfL281T3loDJesD99uq1NBASA+fUhwRbvgYWEj+lRktf5z
A7znroDi3qtPUrATnAHjRQKXKIVDAPhmaD+3ggLJNKaekRsS3
        rightnexthop=%defaultroute
        auto=start
```

Figura 4.54. OPENSWAN ipsec.conf (SBS)

Adicionalmente todos estos cambios pueden realizarse fuera del archivo de configuración por medio de la directiva include /<<**ubicación**>>/<<**conexión**>> (nombre del archivo).

Realizada la configuración en ambos extremos VPN LINUX se debe iniciar la conexión:

[root@monitor /] # ipsec auto --up vpnsbs

4.2.5.6. Pruebas del Servicio VPN LAN-to-LAN – SBS

Para realizar las pruebas que certifiquen una transmisión encriptada con IPSEC, basta usar un sniffer (SBS – tcpdump) en un equipo perteneciente a la Red 192.168.0.0 (192.168.0.23 caso SBS), por ejemplo, y realizamos ping desde el equipo perteneciente a la Red 192.168.5.0 (192.168.5.23 caso SBS), obteniendo los siguientes resultados:

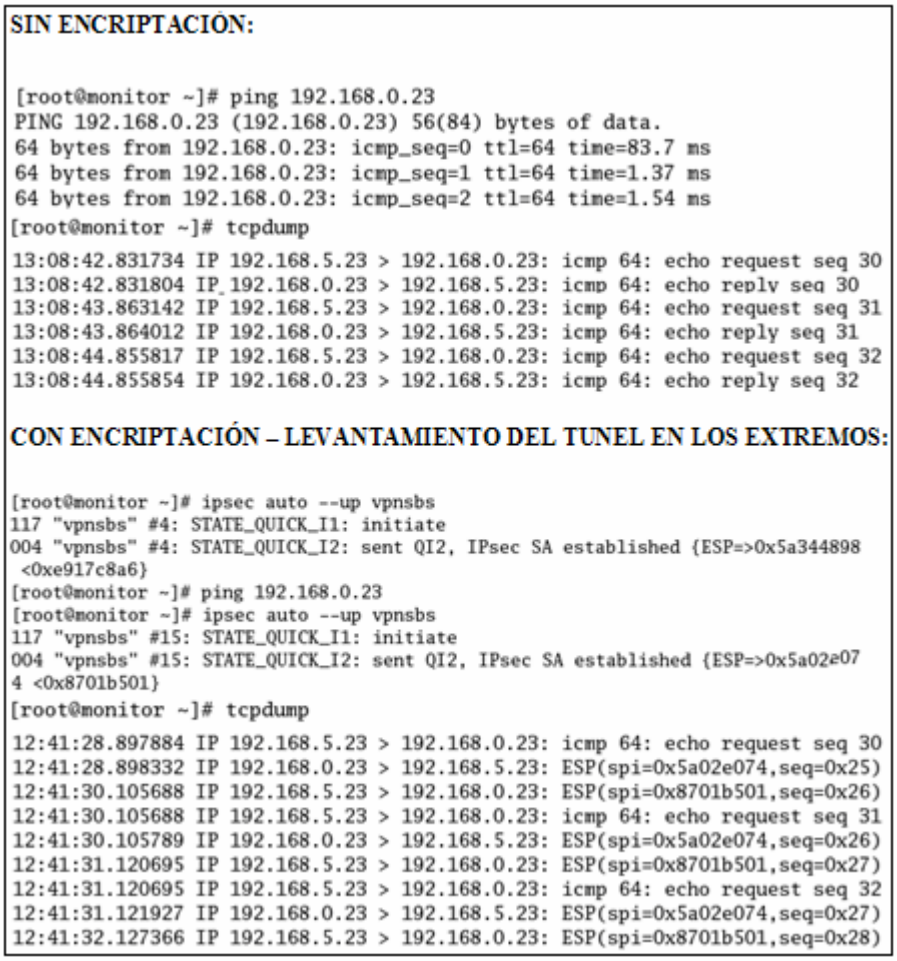

Figura 4.55. Pruebas enlace VPN

Aquí se puede observar la diferencia entre la conexión con IPSEC y sin ella, básicamente cifra todo el contenido de los paquetes IP (**ESP**).

DISEÑO DEL SERVICIO VPN – SBS

ARQUITECTURA ACCESO REMOTO VPN

4.3. DISEÑO DEL SERVICIO DE ACCESO REMOTO VPN - RAS

4.3.1. Arquitectura del Servicio. El acceso remoto VPN es una arquitectura en la cual un host remoto (Funcionario) crea un túnel para conectarse a la Intranet SBS. El dispositivo remoto es un computador personal con un software cliente (VPN- Windows XP) para crear una VPN usando una conexión conmutada (RAS Fig. 4.56) o una conexión de banda ancha permanente (Fig. 4.57).

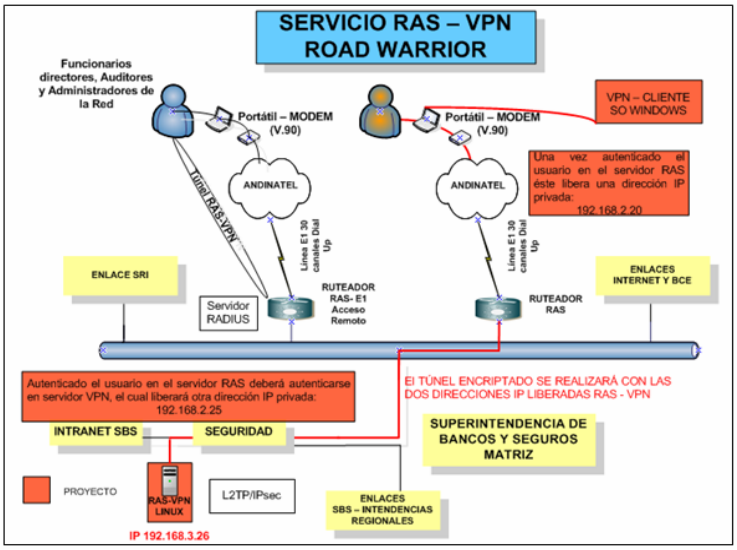

Figura 4.56. Arquitectura Acceso Remoto VPN -RAS

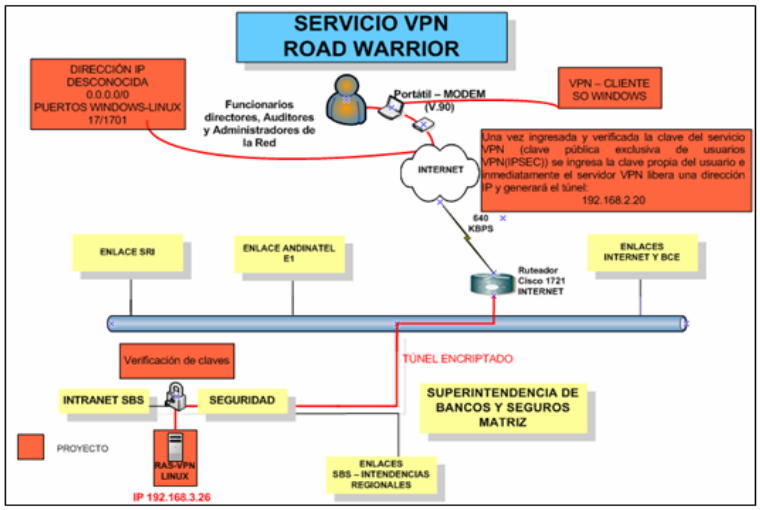

Figura 4.57. Arquitectura Acceso Remoto VPN - Internet

La solución Acceso Remoto VPN – RAS nació a partir de la necesidad de acceso a la red Institucional desde cualquier ubicación. Con el uso de una conexión conmutada (Andinatel Enlace E1, línea telefónica), consiste en usar cualquier RAS que brinde el servicio de comunicación, como punto de acceso a la misma.

4.3.2. Características técnicas del servicio RAS - SBS. La Superintendencia de Bancos y Seguros como Institución de supervisión, posee funcionarios auditores que se movilizan a todas las Instituciones Controladas obteniendo información y enviándola a la misma para su procesamiento.

Todo este intercambio de información requiere un medio de comunicación como es el caso de Internet, pero no todas las Instituciones Controladas poseen el servicio para brindar a los auditores, en caso de ser necesario, motivo por el cual los funcionarios ingresan a la Red Institucional vía RAS (servicio de acceso remoto).

Actualmente la reducción de los costos del servicio de Internet de banda ancha (Cablemódem, Fastboy, etc.) está abriendo un nuevo camino, a los funcionarios remotos, para acceder a la Red Institucional, por este medio. El presente proyecto Linux cubre este escenario, facilitando el acceso vía VPNs.

4.3.2.1. Escenario Actual de la Institución. La Superintendencia de Bancos y Seguros provee el Servicio de Acceso Remoto a 60 Funcionarios entre los cuales se encuentran: Auditores, Directores y Subdirectores de los diferentes departamentos de la Entidad, El Superintendente de Bancos y Seguros y Administradores de la Red Institucional

El servidor RAS que interactúa con el enlace E1 permite transportar datos a una tasa de 2 Mbps (32 canales de 64 Kbps). De estos 32 canales 31 son canales activos simultáneos para voz o datos en SS7 (Sistema de Señalización Número 7) en R2 el canal 16 se usa para señalización por lo que están disponibles 30 canales para voz o datos.

Velocidades de Conexión. Los equipos que poseen permisos y acceso al Servicio RAS son computadores portátiles exclusivamente. Estos equipos son de MARCA HP

(MODEM - V.90) última generación y algunos de marca DELL, THINKPAD y COMPAQ que serán remplazados con las últimas adquisiciones que realizará la entidad. Todos estos equipos poseen MODEMS internos que trabajan con normas V.90 y V.34. Permitiendo una velocidad máxima de 56 Kbps (en casos donde la infraestructura de cobre de Andinatel presente buen estado, caso contrario, la velocidad será inferior). La norma V.90 se caracteriza por un funcionamiento asimétrico, puesto que la mayor velocidad sólo es alcanzable "en bajada", ya que en el envío de datos está limitada a 33,6 Kbps.

4.3.2.2. Recomendación Técnica en la adquisición de Equipos portátiles. Los costos de una migración del enlace conmutado analógico (actual) al digital involucrarían costos superiores a los manejados por la Entidad y costos asociados en la adquisición de equipos que permitan este tipo de enlaces, para los equipos remotos de los funcionarios, lo que no representaría una solución inmediata.

En las nuevas adquisiciones de equipos portátiles, de poder hacerlo, sería importante solicitar a las empresas concursantes MODEMS internos que trabajen bajo la norma V.92 puesto que al compararla con la norma V.90 se determina que:

- La velocidad de transmisión que brinda es de hasta 48Kbps, frente a la velocidad máxima de transmisión de la norma V.90 de hasta 33.6 Kbps (Velocidad de Rx 56 Kbps).

- Conexión más rápida puesto que los módem actuales tardan unos 20 segundos en efectuar una conexión. Los nuevos módem V.92 se conectan en apenas 10 segundos.

- Posibilidad de atender o realizar una llamada telefónica mientras se mantiene una conexión de datos. El nuevo servidor RAS debe tener la posibilidad de brindar este tipo de conexiones.

NOTA.- *La nueva norma V.92 utiliza en la transmisión de datos del usuario al proveedor un sistema PCM (Pulse Code Modulation o modulación por impulsos codificados). En otras palabras, no modula sobre una portadora analógica, sino que directamente transmite los bits sobre la línea.*

4.3.2.3. Características Técnicas del Hardware del Servidor RAS.

- Permite la conexión de usuarios remotos dial up a través de la red telefónica pública.
- 30 módems digitales internos, accesibles a través del enlace E1.
- Puerto de red Ethernet 10/100 BaseT.
- Accesorios de conexión a los módems de enlace E1.
- Permitir llamadas de los siguientes tipos: V.92, V.90, K56Flex, V.34, ISDN.
- Fuente de poder 110 V.

4.3.2.4. Formas de conexión del Servidor RAS.

- 1 puerto digital MFC-R2 que permite la conexión de la troncal al proveedor de acceso telefónico Andinatel.
- Cuatro puertos con módems incorporados, que operan con las normas V.92, V.90, K56Flex, V.34, que permiten conectarlos a las líneas convencionales de Andinatel, como respaldo de la línea E1.
- Puerto alterno para administración por consola.

4.3.2.5. Características técnicas del software de Administración del RAS.

- Filtrado de paquetes.
- Usuarios estáticos configurables.
- Administración del servidor gráfica.
- Permite configurar opciones de seguridades y encriptación de datos.

CONFIGURACIÓN DEL SERVICIO VPN – SBS

ARQUITECTURA ACCESO REMOTO VPN

4.3.3. Configuración del Acceso Remoto VPN sobre Linux. Como se mencionó con anterioridad, las configuraciones de los accesos remotos VPN abarcan los dos escenarios que pueden presentarse vía enlace conmutado (RAS) e Internet. Cada conexión remota (road warrior) a la red privada, realizará un "Túnel" con el servidor Linux. Este equipo remoto aprovechará el software VPN de Windows XP.

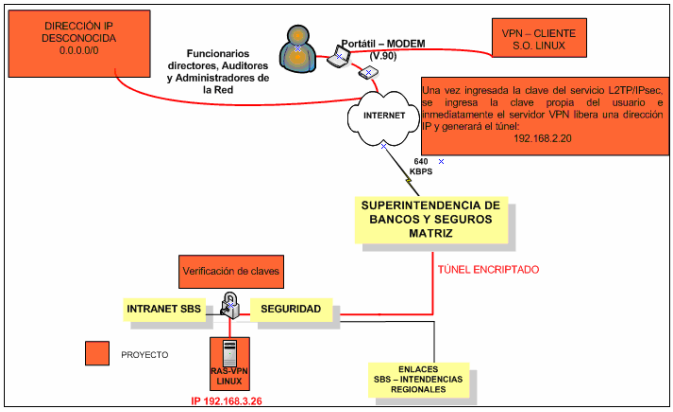

Figura 4.58. Accesos Funcionarios SBS

4.3.3.1. Configuración IPSec. Dentro de Ipsec.conf se puede detallar diferentes tipos de conexiones, en el caso SBS **(**OPENSWAN Fig. 4.59), siete son las secciones.

En la primera (config setup) se describe las opciones generales de IPSec para del servicio RAS-VPN. Conn %default, define los valores que por defecto tendrán las conexiones IPSEC y las cinco restantes conexiones, conn <nombre de la conexión>, que cubren todos y cada uno de los accesos que permitirá el servidor remoto VPN.

Como breve descripción de algunos valores de ipsec.conf, se detallan las 3 clases de RED privadas existentes (vitual_private). Adicionalmente se observa que las todas las conexiones serán tipo túnel y se especifican todos los modos de acceso a la Red Institucional (192.168.0.0), que puedan darse, ya sea el acceso desde el puerto 17/1701 o una dirección de RED desconocida (0.0.0.0/0, clientes que no accedan vía RAS). Sea cual fuere el modo de acceso del cliente remoto (Fig. 4.58), sino digita correctamente las claves no podrá ingresar al servicio VPN y consecuentemente a la Red Institucional.

```
version 2.0
config setup
       interfaces=%defaultroute
       klipsdebug=none
       plutodebug=none
       overridemtu=1410
       nat_traversal=yes
       virtual_private=%v4:10.0.0.0/8,%v4:172.16.0.0/12,%v4:192.168.0.0/16

conn %default
       keyingtries=3
       compress=yes
       disablearrivalcheck=no
       authby=secret
       type=tunnel
       keyexchange=ike
       ikelifetime=240m
       keylife=60m

conn roadwarrior-net
       leftsubnet=192.168.0.0/24
       also=roadwarrior

conn roadwarrior-all
       leftsubnet=0.0.0.0/0
       also=roadwarrior

conn roadwarrior-l2tp
       leftprotoport=17/0
       rightprotoport=17/1701
       also=roadwarrior

conn roadwarrior-l2tp-updatedwin
       leftprotoport=17/1701
       rightprotoport=17/1701
       also=roadwarrior

conn roadwarrior
       pfs=no
       left=192.168.3.26
       leftnexthop=192.168.3.10
       right=%any
       rightsubnet=vhost:%no,%priv
       auto=add

#Disable Opportunistic Encryption
include /etc/ipsec.d/examples/no_oe.conf
```

Figura 4.59. Archivo de configuración del Servidor Linux para conexiones remotas ipsec.conf

NOTA.- *En una configuración real se debe sustituir "150.150.150.150" por una dirección IP pública y "150.150.150.1" con la puerta de enlace o gateway.*

El siguiente paso es añadir la siguiente línea a **ipsec.secrets** en el directorio **etc**.

150.150.150.150 %any: PSK "clave no mayor a 256 caracteres"

NOTA.- *Cada cliente que intente establecer una conexión de VPN tendrá que proporcionar esta llave pre-compartida.*

4.3.3.2. Instalación L2TPD. Este paquete (l2tpd-0.69-13.src.rpm) es descargado en formato RPM y su instalación se realiza bajo modo comando o en forma grafica como se explicó en instalaciones anteriores.

4.3.3.3. Archivos de configuración L2TP. En el directorio **/etc/l2tpd,** se encuentra el archivo de configuración **l2tpd.conf (Fig. 4.60)** en el cual se define el puerto donde escuchará el servidor L2TP, el rango de direcciones IP que serán asignadas a los clientes remotos, y la dirección IP correspondiente al extremo del túnel residente en el concentrador (192.168.3.26).

```
[global]
port = 1701

[lns default]
ip range = 192.168.3.30-192.168.3.40
local ip = 192.168.3.26
require chap = yes
refuse pap = yes
require authentication = yes
name = LinuxVPN
ppp debug = yes
pppoptfile = /etc/ppp/options.l2tpd
length bit = yes
```

Figura 4.60. Archivo de configuración l2tpd.conf

4.3.3.4. Configuración del protocolo PPP. Como requerimiento básico es recomendable saber si está instalado PPP en el kernel. En la conexión L2TP/IPsec, quien se encarga de cifrar toda la información, es OPENSWAN, pero en el acceso es necesaria una autenticación adicional (CHAP - PPP), puesto que, en el caso del acceso a la Red vía Internet, la única forma de saber si el usuario tiene privilegios es por medio de una clave, por que su IP es desconocida por el servidor. Esta autenticación se realiza por medio del protocolo CHAP (Fig. 4.61) del protocolo PPP, el cual se especifica en "/etc/ppp/options.l2tpd".

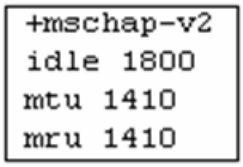

Figura 4.61. Archivo de configuración options.l2tpd

Continuando con la autenticación PPP en el directorio **"/etc/ppp/**" y en **chap-secrets** se almacenan los nombres y las respectivas claves de los usuarios que tendrán acceso al servidor VPN (Fig. 4.62).

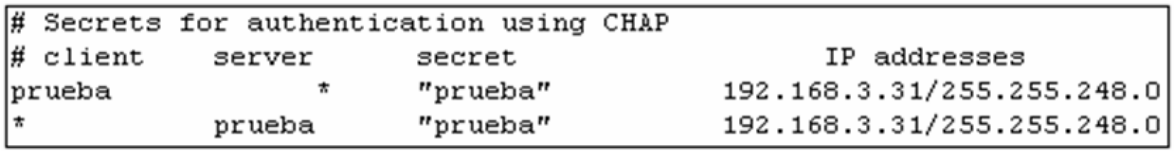

Figura 4.62. Archivo de configuración chap-secrets

Son necesarias las dos líneas, como se observa en el modelo anterior, para cada usuario porque es una autenticación doble, una del cliente al servidor y la otra del servidor al cliente. La contraseña y la dirección IP deben ser iguales en ambas líneas. La dirección que se especifique será la que se le asigne al usuario.

NOTA.- *En la configuración del cortafuegos se debe tener en cuenta que los puertos UDP 500 Y 4500, TCP 4500 deben estar abiertos caso contrario el VPN no trabajará.*

4.3.3.5. Configuración del cliente VPN en Windows. El procedimiento para instalar y configurar un cliente remoto L2TP/IPSec es:

Para crear una nueva conexión, se abre la ventana donde aparecen las conexiones de red establecidas, para esto se sigue la ruta:

Inicio | Conectar a | Mostrar todas las conexiones

Figura 4.63. Nueva conexión cliente VPN WinXP

En la ventana de diálogo que se despliega, damos doble click en el asistente para conexión nueva:

Figura 4.64. Asistente de nueva conexión cliente VPN WinXP

Luego se despliega el cuadro de diálogo para iniciar el Wizard que crea la nueva conexión de tipo VPN:

Se da click en Siguiente, y a continuación se despliega una ventana donde se escoge el tipo de conexión nueva que se quiere crear, en el caso de los funcionarios remotos, Conectarse a la red de mi lugar de trabajo (que hace alusión a una red privada virtual).

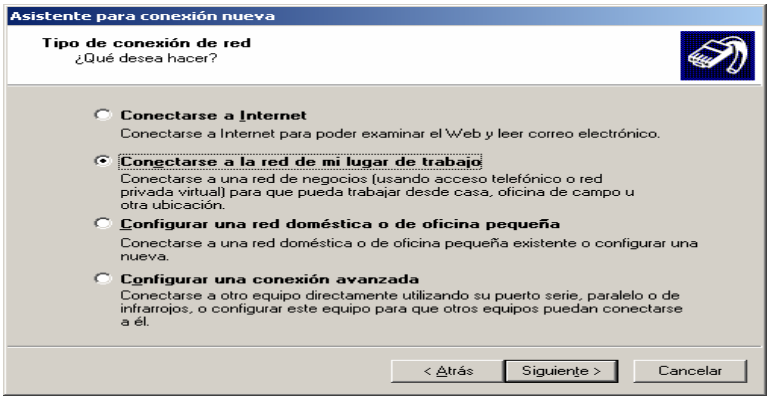

Figura 4.65. Tipo de nueva conexión

Se da click en Siguiente y aparece una ventana donde se selecciona, Conexión de red privada virtual, y se da click en Siguiente:

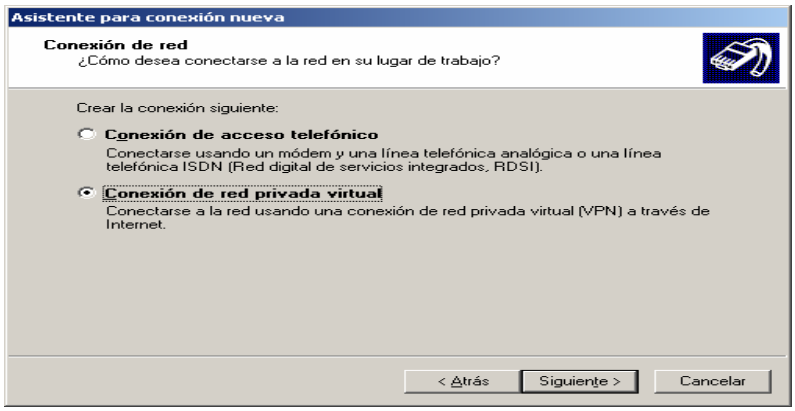

Figura 4.66. Conexión de red privada virtual

Aparece una ventana donde se escribe un nombre que identifica la conexión de red (tesis VPN - SBS) a la que se quiere acceder por medio la VPN y se da click en siguiente.

A continuación aparece un cuadro donde Windows pregunta al usuario si quiere ejecutar una conexión telefónica antes de lanzar la conexión L2TP/IPSec. Es aquí prácticamente donde radica la diferencia de los escenarios del acceso RAS VPN y Road Warrior, pero para casos prácticos se escogió, No usar la conexión inicial.

Luego aparece un cuadro donde se digita el nombre o el IP del servidor L2TP/IPSec de la SBS (por fines prácticos se utilizó la IP 192.168.3.26).

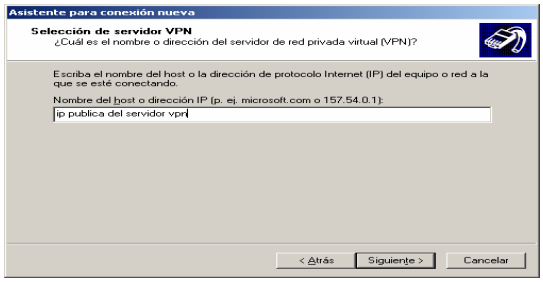

Figura 4.67 Puerta de enlace de conexión VPN

Para terminar el Wizard, se da click en Siguiente y en la ventana de finalización Finalizar.

Antes de lanzar la conexión L2TP/IPSec, se tienen que configurar ciertos parámetros que el Wizard deja por defecto, tales como la asignación del gateway, el servidor WINS y clave del servicio IPSEC. Para que el PC que se va a conectar a la VPN no pierda su conexión a Internet es necesario especificar en las propiedades TCP/IP que no use la puerta de enlace predeterminada en la red remota, esto es necesario para que no se creen dos rutas por defecto distintas, la de la conexión PPP y la de la conexión L2TP/IPSec.

Continuando con los detalles propios de la conexión L2TP/IPSec recién creada, se selecciona Propiedades, la cual permite visualizar varias de ellas:

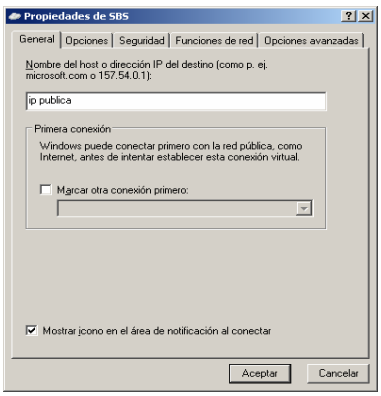

Figura 4.68 Propiedades cliente-VPN

Como se mencionó el enlace RAS-VPN utiliza doble autenticación. La clave pública del servidor debe se escrita por los encargados de la instalación del servicio en:

Seguridad | Configuración IPSec:

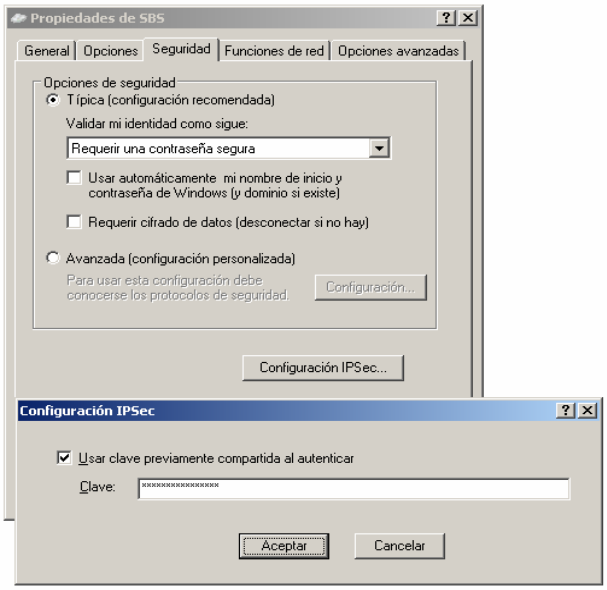

Figura 4.69 Ingreso de la clave IPSec

Luego se selecciona la pestaña Funciones de red y aparecen los siguientes cuadros:

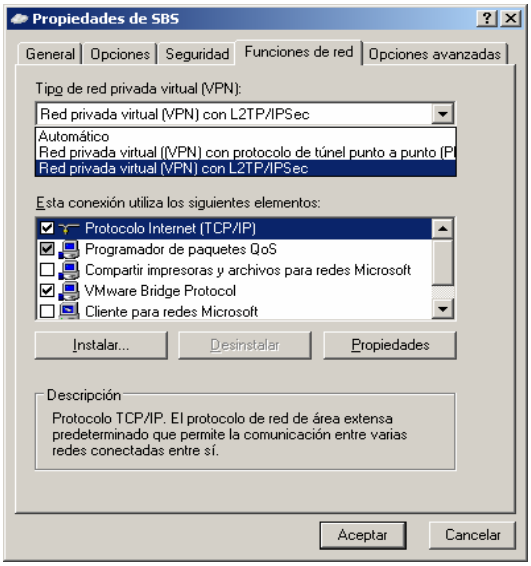

Figura 4.70 Propiedades TCP/IP

El siguiente paso es seleccionar Protocolo Internet (TCP/IP) y dar click en Propiedades. Aparece un cuadro de dialogo que se deja con la configuración por defecto, es decir que la dirección IP y los servidores DNS sean asignados dinámicamente. Se da click en Opciones Avanzadas, y aparece una ventana con tres pestañas:

General, DNS y WINS.

En General se desactiva la opción Usar la puerta de enlace predeterminada en la red remota:

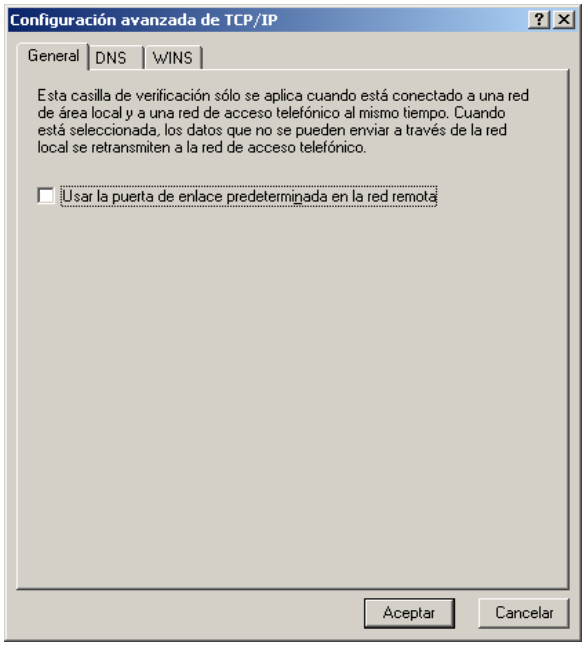

Figura 4.71. Desactivación de la puerta de enlace predeterminada

Por ultimo se da click en Aceptar en todas las ventanas abiertas hasta llegar a la ventana de Conexiones de Red.

4.3.3.5.1. Pruebas del Servicio VPN: Acceso remoto VPN

Una vez conectados a Internet, bien sea por acceso telefónico o estando en una LAN, se da doble click en el icono **tesis vpn**, y a continuación aparece un cuadro de diálogo con el nombre de usuario y la contraseña con el cual el usuario se va a autenticar en el servidor L2TP/IPSec. Se da click en Conectar.

Figura 4.72.Conexión al servicio VPN

Dando doble click en el icono VPN, podemos ver el estado de la conexión (Fig. 4.73):

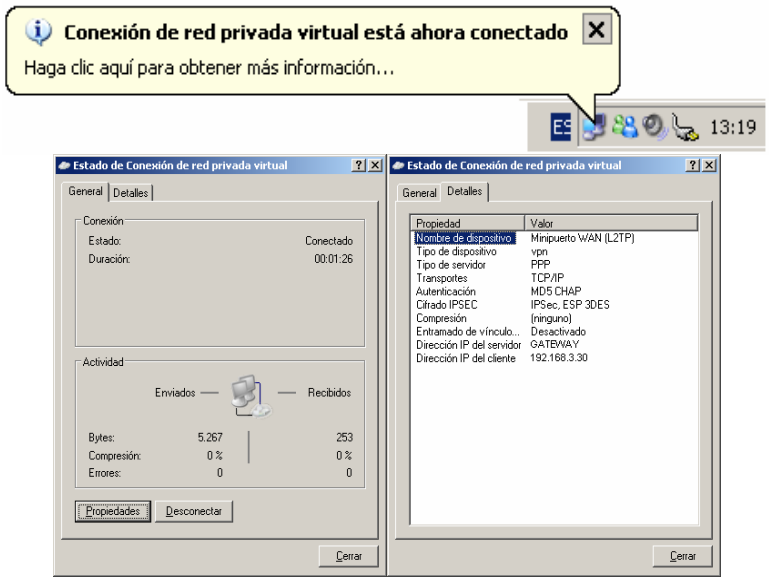

Figura 4.73. Pruebas del acceso remoto VPN

Finalizando, para verificar la conectividad a la red remota abrimos un ping al IP del servidor L2TP/IPSec.

4.4. CONSIDERACIONES DE SEGURIDAD

En las implementaciones realizadas, los aspectos de seguridad fueron un factor predominante, puesto que no solo aseguran el servidor como tal, sino crean un entorno de seguridad en enlaces públicos como el Internet (propuestas de Backup). A continuación se detallará cada una de las seguridades implementadas en el servidor de la Superintendencia de Bancos y seguros.

- Inicio del servidor en modo texto.
- Desactivación de las teclas **Control-Alt-Supr.**
- Asignación de permisos exclusivos a ROOT a todos y cada uno de los archivos de configuración puesto que es el administrador del sistema.
- Control de RNDC al demonio named exclusivamente desde la dirección IP del servidor (192.168.3.26).
- Desde el servicio DCHP se asigna una dirección IP fija al administrador, puesto que es la única IP que tiene acceso al servidor y a su monitoreo.
- Configuraciones named bajo entorno CHROOT.
- Configuración de un servidor Web seguro (HTTPS).
- Monitoreo del servidor y de los servicios que provee vía WEB.
- Configuración de un contafuegos exclusivamente como filtro, en donde solo a una dirección IP se le permite monitorear el servidor y tener acceso SSH a Linux y se permite acceder al servidor DNS y DHCP.
- Implementación del protocolo IPSEC para levantar Túneles Encriptados para usuarios remotos y Entidades Regionales.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Este proyecto permite ampliar los conocimientos del Sistema Operativo Linux y fomentar su migración dentro de la Superintendencia de Bancos y Seguros. Adicionalmente demuestra que es una alternativa que intenta cubrir el campo de las comunicaciones con protocolos seguros sin vulnerabilidades como IPSec, que es fácilmente configurable y su administración puede personalizarse a los requerimientos de la empresa.

2. Se concluye que la migración de la plataforma Windows, actual de la SBS hacia Linux es totalmente factible, pues se ha podido observar con el presente desarrollo que todos y cada uno de los servicios de comunicación son compatibles con el entorno en que se desenvuelven las comunicaciones actualmente.

3. La propuesta tecnológica planteada en el presente trabajo puede ser utilizada como un Backup para los servicios de comunicación que posee actualmente la SBS a costos relativamente bajos y con características de alta seguridad, pues se ha utilizado una plataforma (Linux) con código abierto y protocolos seguros.

4. Desde el punto de vista de las seguridades se ha demostrado, por medio del proyecto, que Red Hat Enterprise Linux 4 es totalmente competitivo con tecnologías de comunicaciones y seguridades presentadas en la actualidad. Esta plataforma sin ser invulnerable demuestra estabilidad es sus procesos y permite personalizar su administración.

5. La propuesta de Backup VPN LAN-to-LAN, bajo el protocolo IPSEC, es una solución económica a los requerimientos de comunicaciones de hoy en día, puesto que, es más factible poseer una conexión a Internet que tener un enlace dedicado, como Backup, que demandaría la compra o alquiler de equipos electrónicos para este fin.

6. Los servidores RAS con el pasar de los años perderán campo en las comunicaciones, por los altos costos que demanda y bajas velocidades (enlace conmutado analógico) que provee. Este inconveniente ya comienza a sentirse en los funcionarios remotos de

la Entidad, pero el auge que tiene el Internet a nivel doméstico comienza a crecer y por ende los usuarios comienzan a inclinarse por esta alternativa y es aquí donde se enfocó la solución VPN Linux, provista de protocolos de encriptación y entunelamiento.

7. Las soluciones Linux son muy amplias, como se ha demostrado en el proyecto, pero no significa que se dejará de utilizar soluciones comerciales VPNs, Firewalls, Ruteadores, etc. Ya que su fuerte es levantar esos servicios en sistemas operativos privados los cuales no poseen tantas vulnerabilidades como se ha venido observando los últimos años en Linux o Windows.

8. Checkpoint es una solución VPN comercial que inicialmente se quiso proponer en el proyecto. Este software trabaja con el protocolo IPSEC y adicionalmente viene con un FIREWALL administrable, pero su costo comercial es muy elevado y no amerita su compra puesto que la SBS no tiene una gran demanda del servicio por parte de los Funcionarios. Al realizar la respectiva investigación en Linux, se determinó que esta plataforma puede ofrecer dicho servicio bajo el mismo protocolo que Checkpoint y se puede levantar un FIREWALL que satisfaga las normas de Seguridad que demanda la Institución

9. Los Ingenieros en Telecomunicaciones deben indagar y brindar soluciones acordes a las demandas actuales de seguridad en las comunicaciones. Como se pudo demostrar en el desarrollo del Proyecto SBS, la implementación VPN está provista de altos niveles de seguridad ya que de ellos dependerá la confidencialidad y solidez de la Información.

10. Ha sido sorprendente los innumerables privilegios para el software libre y en particular para los sistemas operativos GNU/Linux, ocurridos durante los últimos años. El crecimiento del sistema operativo GNU/Linux ha sido tan significativo que compañías tan importantes como Intel, IBM, Sun, Apple, Corel, Netscape, Oracle, Informix, SyBase, Dell, Compaq, Hewlett Packard, Silicon Graphics, Toshiba, Novell y otras, lo han acogido en mayor o menor grado y lo están apoyando con fines netamente de negocios. Todo esto se explica porque el software libre representa un nuevo modelo de desarrollo de software, un verdadero paradigma. El sistema operativo GNU/Linux representa un terreno inexplorado que ha conseguido captar la atención de una tras otra

de las empresas mencionadas, lo que se está traduciendo en rentabilidad para ellas y en beneficio para los usuarios. Hace unos años GNU/Linux era un sistema sólo para universitarios e investigadores, ahora ya está ocupando un lugar a nivel empresarial.

RECOMENDACIONES

1. Es importante que todo software adicional que se desee descargar para su instalación e implementación se lo realice bajo formato **src.rpm**, puesto que construye paquetes RPM adecuados al entorno Linux donde se esté trabajando

2. Como se demostró en las configuraciones VPN, el sistema Red Hat Enterprise Linux 4 sí posee el soporte necesario para levantar VPNs sin ningún inconveniente, pero es importante recalcar, que este software es comercial y que existen otras alternativas entre ellas clones y proyectos abiertos como FEDORA que también permiten realizar soluciones VPNs.

3. Como procedimiento de respaldo y reinstalación de los servicios de comunicación, es recomendable almacenar todos y cada uno de los archivos que contengan claves y configuraciones esenciales del servidor en unidades externas, para que en una próxima configuración solo se anexe estos archivos en los directorios respectivos, con permisos de administrador ROOT.

4. Es conveniente incrementar el número de serie en el servidor DNS, cuando éste haya sido modificado, puesto que, si no se incrementa el número de “serial” en los archivos de configuración de named, el servidor de nombres maestro no se refrescará con los nuevos cambios realizados.

5. Se debe hacer hincapié en la utilización correcta de las llaves, puntos, puntos y comas y tabulaciones en el archivo /etc/named.conf, como en el resto de archivos de configuración del sistema, ya que un solo error no permitirá el correcto levantamiento de los servicios.

6. Si el firewall está bloqueando las conexiones con el programa named a otros servidores de nombres se debe modificar su archivo de configuración permitiendo la entrada y salida por el puerto 53 de todas las conexiones. Por defecto, la versión 9 de BIND usa los puertos aleatorios por encima de 1024 para consultar otros servidores de nombres. Algunos cortafuegos, sin embargo, esperan que todos los servidores de nombres se comuniquen usando solamente el puerto 53. Se puede forzar a named que use el puerto 53 añadiendo la línea siguiente a la declaración options de /etc/named.conf: query-source address * port 53;

7. Es aconsejable realizar una instalación personalizada, escogiendo todos y cada uno de los paquetes necesarios para las configuraciones, previamente establecidas, evitando así nuevas instalaciones.

8. No se deben realizar cambios en los archivos que permitan visualizar procesos del sistema, como el archivo *MESSANGES*, puesto que si se lo hace dejarán de entregar la información del mismo.

9. Por razones de seguridad, se debe revisar los permisos a cada uno de los archivos de configuración, puesto que, son de uso exclusivo de ROOT y si le otorgan mayores privilegios estos podrían ser causa de vulnerabilidad a futuro.

10. Como se puede observar en los servicios realizados para la Superintendencia de Bancos y Seguros existe redundancia de seguridad, motivo por el cual, se recomienda tomar las medidas pertinentes para que no existan conflictos con otras seguridades de los sistemas una vez puesta en producción la propuesta Tecnológica de Backup.

REFERENCIAS BIBLIOGRÁFICAS

- FELIX, Rolando, *Manual avanzado de servidores Linux*,Tomo 1, Quito 2005
- SCHENK, Thomas, *Administración de Red Hat Linux*, Tomo 1, España 2001
- Documentación brindada por los Funcionarios del área de Comunicaciones de la Superintendencia de Bancos y Seguros.
- MRTG, http://mrtg.hdl.com/mrtg.html

2005-12-12 09:45 AM

- MRTG, http://www.cyberciti.biz/nixcraft/linux/docs/uniqlinuxfeatures/mrtg/mrtg_ config_ step_4.php

2005-12-12 10:45 AM

- Tecnologías de la Información, (TI) http://www.microsoft.com,

2005-12-15 12:15 PM

- http://www.linuxparatodos.net/geeklog/staticpages/index.php?page=06-manejo-software&mode=print

2006-02-15 08:52 AM

- http://www.zonasiete.org/manual/ch09s05.html

2006-03-17 10:35 AM

- Introducción Linux, ttp://intercentres.cult.gva.es/cefire/12400551/asesorias/informat /manual-knoppix/c40.html,

2006-03-30 03:15 PM

- Introducción SBS, https://www.superban.gov.ec/pages/1_generalidades1.htm

2006-03-30 03:31 PM

- Introducción SBS http://www.dlh.lahora.com.ec/paginas/judicial/PAGINAS/Ley. Inst.Finacieras.htm

2006-03-30 03:38 PM

- Servicio VPN, http://www.olotwireless.net/catala/PRACT2.pdf,

2006-04-06 09:14 PM

- Servicio DHCP, http://www.wikilearning.com/introduccion-wkccp-275-1.html

2006-04-11 14:56 PM

- Servicio VPN, http://www.ipsec-howto.org/spanish/x257.html,

2006-04-27 11:10 AM

- Servicio DNS, http://dns.bdat.net/documentos/cursos/ar01s619.html

2006-05-02 12:20 AM

- Servicio de comunicación bajo Linux, http://www.europe.redhat.com/documentation/rhl7.3/rhl-rg-es-7.3/ch-ext3.php3

2006-05-17 11:01 AM

- Kernel Linux, http://www.linux-es.org/kernel.php#que_es

2006-05-17 11:02 AM

- Distribuciones Linux, http://es.wikipedia.org/wiki/Distribuci%C3%B3n_Linux

2006-05-17 11:06 AM

- Servicio DHCP, http://es.wikipedia.org/wiki/DHCP#DHCP_Discover

2006-05-17 15:17 AM

- Freeswan, http://www.freeswan.org/freeswan_trees/CURRENT-TREE/doc/manpage.d/ipsec_rsasigkey.8.html

2006-07-04 10:13 AM

- Openswan, http://gentoo-wiki.com/HOWTO_OpenSwan_2.6_kernel#Introduction

2006-06-06 13:45 AM

- Manuales Red Hat Enterprise Linux 4, http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/es/ref-guide/

2006-07-03 10:12 AM

- Servicio VPN, http://www.ecualug.org/?q=2006/03/08/forums/vpn

2006-07-04 10:45 AM

- Servidor Linux – servicio Acceso Remoto VPN, http://megaz.arbuz.com/2005/01/28/linux-vpn-guide/

2006-07-05 11:30 AM

- Mrtg-SYS, http://guias.ovh.com/InstalarMRTGSys/contenu.html

2006-07-06 10:00 PM

- Ipsec, http://www.slackbasics.org/html/ipsec.html

2006-07-07 12:00 PM

- MRTG-SNMP, http://gentoo-wiki.com/HOWTO_SNMP_and_MRTG_Made_Easy#Required_.26_Optional_Packages

2006-07-07 12:01 PM

ACTA DE ENTREGA

El proyecto fue entregado en el Departamento de Eléctrica y Electrónica y reposa en la Escuela Politécnica del Ejército desde:

Sangolquí, a _____

_____

Sr. Patricio Xavier Zambrano Rodríguez

AUTORIDADES:

_____

Sr. Ing. Gonzalo Olmedo

COORDINADOR DE CARRERA

_____

Sr. Dr. Jorge Carvajal

SECRETARIO ACADÉMICO