UNIVERSIDAD TECNICA DE COTOPAXI

CARRERA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

PROYECTO DE TESIS PREVIO LA OBTENCION DEL TITULO DE INGENIERO EN INFORMATICA Y SISTEMAS COMPUTACIONALES

TEMA: "Desarrollo de un Servidor Proxy Inverso para controlar las seguridades y balance de carga en las redes"

DIRECTOR: ING. MATIUS MENDOZA

POSTULANTES: PACHECO OÑA DARWIN ALONSO
SEMBLANTES SORIA GALO ANIBAL

LATACUNGA – ECUADOR

2008

AUTORIA

Nosotros: Pacheco Oña Darwin Alonso y Semblantes Soria Galo Aníbal, declaramos que la investigación aquí presentada es de nuestra autoría: que no ha sido previamente presentado, y que hemos consultado todo lo que aquí está incluido.

Pacheco Oña Darwin Alonso

C.I. 050239946-2

Semblantes Soria Galo Aníbal

C.I. 050259276-9

CERTIFICACION

HONORABLE CONSEJO ACADEMICO DE LA UNIVERSIDAD TECNICA DE COTOPAXI

De mi consideración.

Cumpliendo con lo estipulado en el capitulo IV, (art. 9 literal f), del reglamento del curso profesional de la Universidad Técnica de Cotopaxi, informo que los postulantes: Pacheco Oña Darwin Alonso y Semblantes Soria Galo Aníbal, han desarrollado su tesis de grado de acuerdo al planeamiento formulado en el plan de tesis con el tema: "Desarrollo de un Servidor Proxy Inverso para controlar las seguridades y balance de carga en las redes", cumpliendo con los objetivos planteados.

En virtud de lo antes expuesto, considero que la presente tesis se encuentra habilitada para presentarse al acto de la defensa de tesis.

Latacunga, 18 de Febrero del 2008

Atentamente,

Ing. Matius Mendoza.

UNIVERSIDAD TECNICA DE COTOPAXI

CARRERA DE CIENCIAS ADMINISTRATIVAS HUMANISTICAS Y DEL HOMBRE

CENTRO DE IDIOMAS

Latacunga- Ecuador

CERTIFICACIÒN

A quien interese.

Por medio de la presente ***CERTIFICO*** *que se realizó el SUMMARY de la tesis de grado para los señores DARWIN ALONSO PACHECO OÑA con cédula N°050239946-2 y GALO ANIBAL SEMBLANTES SORIA con cédula N°050259276-9, estudiantes de esta Institución.*

Latacunga febrero 14, 2008

ATENTAMENTE,·
Lic. M.Sc. Mayra Alpúsig
DOCENTE

UNIVERSIDAD TECNICA DE COTOPAXI
CENTRO DE IDIOMAS
SUPERVISION

Av. Simón Rodríguez s/n –Barrio Elejido -Sector San Felipe Teléfonos: (03) 810-296, 813-157
Fax: 593 (03) 2810-295 Apartado N0.- 05- 01- 491

AGRADECIMENTO

Al concluir una etapa en la larga y permanente trayectoria de la superación intelectual del hombre, este grupo de estudiantes satisface sus anhelos íntimos de superación.

A Dios, artífice de nuestras vidas, refugio y fortaleza en nuestros momentos difíciles.

A nuestros Padres, familiares y amigos por brindarnos su apoyo y haber hecho posible este momento

A la Carrera de Ingeniería en Sistemas y a todos los profesores por transmitirnos sus conocimientos y experiencias.

Al Ingeniero Matius Mendoza, director del proyecto y al Dr. Edwin Vaca por su asesoramiento y confianza brindada en la realización de este trabajo

Darwin, Galo

DEDICATORIA

A mi Padres, Esposa e Hijas, quienes supieron motivarme con cariño y ternura para culminar mi proyecto de tesis y obtener el titulo que lo pondré en practica al servicio del bien en la sociedad.

Porque el fruto de mis años de estudios deben llevarse a la práctica, no solo para satisfacer aspiraciones personales sino, que beneficien en forma directa a nuestros hogares, semejantes y aquellos que necesiten de nuestros conocimientos.

A quien han sido permanentes testigos de nuestras penas y sinsabores, a los que nos has dado una voz de aliento para no truncar nuestras raíces, que con su ternura y abnegación nos impulsaron a entregar todas nuestras capacidades, a aquellos que supieron sembrar en mi el anhelo de superación, que han hecho posible la obtención del presente Título de Ingeniería en Informática y Sistemas Computacionales, lo dedico con mucho amor y comprensión este trabajo fruto de su sacrificio y esfuerzo constante.

Darwin Alonso

DEDICATORIA

A mis Padres, por el apoyo y esfuerzo demostrado no solo durante el desarrollo de este trabajo sino en toda mi vida.

A mis hermanos, por la confianza depositada en mi, por la oportunidad que me dieron para demostrarle que para la superación no importan las condiciones ni obstáculos; hay que aceptarlos con humildad sencillez y solucionar con inteligencia.

A todas las personas que a su debido momento me ayudaron para lograr uno más de mis objetivos.

Galo Aníbal.

INDICE GENERAL

DEL SERVIDOR PROXY INVERSO

INTRODUCCION

La informática y el software en particular como una infraestructura que soporta el desarrollo de una economía más eficiente y más productiva se encuentra actualmente en una situación de monopolio de facto por parte de constructores norteamericanos.

Por su insignificante costo de copia frente al de su desarrollo y las economías de red que se generan en un sector que tiende de forma natural al monopolio. Este hecho facilita a aquellos que alcanzan está posición de preeminencia una elevación artificial de los precios, la imposición de estándares propietarios y/o el pago por productos de dudosa calidad.

De está manera y bajo está premisa hacemos una cordial invitación a que los nuevos egresados y graduados tomen a nuestra carrera como un reto el cual siempre nos va a servir para mejorar y ser buenos en cualquiera de los ámbitos que nos desenvolvemos.

Las seguridades sean estas mediante host o mediante red constituyen una herramienta poderosa y que sabiendo aprovecharlas podemos sacarle mucho provecho, ya que garantizaríamos la información que se genera en las instituciones o empresas, el uso adecuado de herramientas open source o de

código abierto refiere al movimiento que propugna la creación comunitaria o cooperativa de nuevas alternativas que garanticen las seguridades de la información mediante sistemas operativos robustos como el Linux o el mismo Solaris de SUN Microsystems.

En la actualidad tener seguridades ya no resulta una alternativa tecnológica, sino más bien un recurso necesario ya que es precautelar la información de algunos sujetos inescrupulosos que disfrutan alterando información o lo que es peor aun intentado robar.

El objetivo de nuestro trabajo de investigación fue demostrar que mediante un solo servidor podemos brindar un buen servicio de Internet y a la vez garantizar el flujo por toda la red, asegurar que los intrusos no van a poder ingresar en forma de spam o gusanos de Internet ya que mediante reglas de configuración propias del sistema operativo Linux el o los crackers van a notar que las posibles puertas de acceso están bloqueadas.

De las fortalezas de nuestra investigación es el poder contar con suficiente información bibliografica, la misma que va en beneficio de todos los estudiantes de la Universidad en general y de la Carrera de Ciencias de la Ingeniería y Aplicadas en particular.

Nuestro trabajo ha sido diseñado en tres capítulos:

El primero corresponde al conocimiento de algunos aspectos importantes de las Redes de Comunicación y de los Servidores, así como información de los Proxy y sus distintas formas de presentación.

El segundo corresponde al trabajo de campo, el mismo que se baso en entrevistas realizadas a algunos profesionales que son administradores de centros de computo o del área de redes de algunas empresas e instituciones que tuvieron a bien colaborar para que sea posible este trabajo de investigación.

El tercer capitulo consta de las factibilidades de implementación, así como la configuración del servidor Proxy Inverso, con todas las reglas y configuraciones necesarias.

La parte final de nuestra investigación se encuentra las conclusiones que se obtuvieron de nuestro trabajo todas con sus respectivas recomendaciones las mismas que ayudarían a un trabajo adecuado de las personas que utilicen este tipo de servidores.

RESUMEN

El presente trabajo de investigación, tiene que ver con la implementación de seguridades y la optimización de los recursos de compartir recursos mediante un Servidor de Proxy Inverso el mismo que garantiza que los recursos de información lleguen a todos los usuarios de manera optima y con una buena calidad de servicio.

La secuencia de pasos que se han seguido para la implementación de un servidor Proxy Inverso están regidos directamente por estándares y normas internacionales, los mismos que garantizan el normal desenvolvimiento de los servidores con los recursos de un servidor. Es fundamental mencionar la colaboración que tuvimos de parte de los administradores de centros de cómputo de algunas instituciones los mismos que apoyaron a la obtención de datos importante.

La manera como se desarrollo este trabajo, fue mediante configuraciones y reglas que deben tener en un servidor que reparta recursos y provea de seguridades a una red, se utilizo el Linux Red Hat 9, por las facilidades que presta y el bajo costo para su adquisición.

Además el presente trabajo deja un amplio material documental como bibliográfico tanto para docentes como estudiantes que estén interesados en el funcionamiento de un Servidor Proxy Inverso.

SUMMARY

This investigative job has the relation with the performance of securities and taking advantage of the resources through an Inverse Proxy Server this one guarantee that the information resources reach to all the users in excellent way and good quality of service.

The sequence of steps have followed to the performance of an Inverse Proxy Server are guided directly by international standards, these ones guarantee the normal development of the servers with the resources of a server. Its important manifest the computing staff, some institutions collaboration, these ones supported the important data's acquisitions.

The development of this research job through rules and configurations must have a server to distribute resources and give securities to a net, It used the Linux Red Hat 9, by its facilities and the low cost for its acquisitions.

Besides this research job have a documental, and write bibliography material for the teachers and students who are, interested in the Inverse Proxy Server operation.

CAPITULO I

1. FUNDAMENTACIÓN TEÓRICA DE LAS REDES

1.1. HARDWARE DE REDES

Muchas organizaciones tienen una cantidad importante en operación, con frecuencia alejadas entre si, Por ejemplo, una compañía con muchas fabricas pueden tener una computadora en cada localidad para llevar el control de los inventarios, vigilar la productividad y pagar la nomina local. Inicialmente, cada una de estas computadoras puede haber trabajado aislada de las otras, pero en algún momento la gerencia decidió conectarlas para poder extraer y correlacionar información acerca de toda la compañía.

En términos más generales, la cuestión aquí es *compartir los recursos* y la meta es hacer que todos los programas, el equipo y especialmente los datos estén disponibles para cualquiera en la red, sin importar la localización física de los recursos y de los usuarios. En otras palabras el hecho de que un usuario este a 1000 Km. De distancia de sus datos no deberá impedirle usar los datos como si fueran locales. Este objetivo puede resumirse diciendo que es un intento por acabar con la "tiranía de la geografía".

Una segunda meta es lograr una alta confiabilidad al no contar con fuentes alternativas de suministro. Por ejemplo, todos los archivos podrían replicarse en

dos o tres maquinas; así, si una de ellas no esta disponible (debido a una falla del hardware), podrán usarse las otras copias. Además, la existencia de múltiples CPU significa que si una de ellas falla, las otras seran capaces de hacer su trabajo, aunque se reduzca el rendimiento.

Otra meta al establecer redes es la escalabilidad: la capacidad para incrementar el rendimiento del sistema gradualmente cuando la carga de trabajo crece, añadiendo solamente más procesadores. En el caso de mainframes centralizadas, cuando el sistema este lleno hay que reemplazarlo por uno mayor, usualmente más caro, lo que implica largas interrupciones para los usuarios. Con el modelo cliente-servidor se pueden añadir nuevos clientes y nuevos servidores cuando sea necesario.

1.1.1. Redes de Área Personal

Red de área personal o *Personal area network* es una red de computadoras para la comunicación entre distintos dispositivos (tanto computadoras, puntos de acceso a Internet, teléfonos celulares, PDA, dispositivos de audio, impresoras) cercanos al punto de acceso. Estas redes normalmente son de unos pocos metros y para uso personal, así como fuera de ella.

PAN es un Nuevo miembro de la familia GIMCV. El espacio personal abarca toda el área que puede cubrir la voz. Puede tener una capacidad en el rango de los 10 bps hasta los 10 Mbps. Existen soluciones (ejemplo, Bluetooth) que operan en la frecuencia libre para instrumentación, ciencia y medicina de sus siglas en ingles (instrumental, scientific, and medical ISM) en su respectiva banda de frecuencia de 2.4 GHz. Los sistemas PAN podrán operar en las bandas

libres de 5 GHz o quizás mayores a éstas. PAN es un concepto de red dinámico que exigirá las soluciones técnicas apropiadas para esta arquitectura, protocolos, administración, y seguridad.

PAN representa el concepto de redes centradas a las personas, las cuales permite a las personas comunicarse con sus dispositivos personales (ejemplo, PDAs, tableros electrónicos de navegación, agendas electrónicas, computadoras portátiles) y así poder establecer una conexión inalámbrica con el mundo externo.

Las redes para espacios personales continua desarrollándose hacia la tecnología del Bluetooth hacia el concepto de redes dinámicas, el cual nos permite una fácil comunicación con los dispositivos que van adheridos a nuestro cuerpo o a nuestra indumentaria, ya sea que estemos en movimiento o no, dentro del área de cobertura de nuestra red. PAN prevé el acercamiento de un paradigma de redes, la cual atrae el interés a los investigadores, y las industrias que quieren aprender más acerca de las soluciones avanzadas para redes, tecnologías de radio, altas transferencias de bits, nuevos patrones para celulares, y un soporte de software más sofisticado.

El PAN debe proporcionar una conectividad usuario a usuario, comunicaciones seguras, y QoS que garanticen a los usuarios. El sistema tendrá que soportar diferentes aplicaciones y distintos escenarios de operación, y así poder abarcar una gran variedad de dispositivos.

Las diferentes demandas del servicio y los panoramas de uso hacen que PAN acumule distintos acercamientos hacia las funciones y capacidades que pueda tener. Algunos dispositivos, como un simple sensor pito, pueden ser muy baratos, y tener a su vez funciones limitadas. Otros pueden incorporar funciones avanzadas, tanto computacionales como de red, lo cual los harán más costosos. Deben preverse los siguientes puntos como importantes para su fácil escalabilidad:

- Funcionalidad y Complejidad;
- Precio;
- Consumo de energía;
- Tarifas para los datos;
- Garantía;
- Soporte para las interfaces.

Los dispositivos más capaces pueden incorporar funciones multimodo que permiten el acceso a múltiples redes.

Algunos de estos dispositivos pueden estar adheridos o usados como vestimenta para la persona (ejemplo, sensores); otros podrían ser fijos o establecidos temporalmente con el espacio personal (ejemplo, sensores, impresoras, y PDAs).

1.1.2. Redes de Área Local

Generalmente llamadas LAN(local area networks), son redes de propiedad privada dentro de un solo edificio o campus de hasta unos cuantos kilómetros de

extensión. Se usan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de compañías y fabricas con objeto de compartir recursos (por ejemplo, impresoras) e intercambiar información. Las LAN se distinguen de otro tipo de redes por tres características:

- Tamaño
- Tecnología de transmisión
- Topología

1.1.3. Redes de Área Metropolitana

Una **red de área metropolitana** (*Metropolitan Area Network* o *MAN*, en inglés) es una red de alta velocidad (banda ancha) que dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado de cobre a velocidades que van desde los 2 Mbit/s hasta 155 Mbit/s.

El concepto de red de área metropolitana representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas mayores que en algunos casos no se limitan a un entorno metropolitano sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana.

Las redes de área metropolitana tienen muchas y variadas aplicaciones, las principales son:

- Interconexión de redes de área local (LAN)
- Interconexión de centralitas telefónicas digitales (PBX y PABX)
- Interconexión ordenador a ordenador
- Transmisión de vídeo e imágenes
- Transmisión CAD/CAM
- Pasarelas para redes de área extensa (WAN)

Una red de área metropolitana puede ser pública o privada. Un ejemplo de MAN privada sería un gran departamento o administración con edificios distribuidos por la ciudad, transportando todo el tráfico de voz y datos entre edificios por medio de su propia MAN y encaminando la información externa por medio de los operadores públicos. Los datos podrían ser transportados entre los diferentes edificios, bien en forma de paquetes o sobre canales de ancho de banda fijos. Aplicaciones de vídeo pueden enlazar los edificios para reuniones, simulaciones o colaboración de proyectos.

Un ejemplo de MAN pública es la infraestructura que un operador de telecomunicaciones instala en una ciudad con el fin de ofrecer servicios de banda ancha a sus clientes localizados en esta área geográfica

La red MAN abarca desde un grupo de oficinas corporativas cercanas a una ciudad y no contiene elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salidas potenciales.

La principal razón para distinguir una MAN con una categoría especial es que se ha adoptado un estándar para que funcione (se llama DQDB), que equivale a la

norma IEEE. EL DQDB consiste en dos buses (cables) unidireccionales, los cuales se conectan a todas las computadoras.

Teóricamente, una MAN es de mayor velocidad que una LAN, pero diversas tesis señalan que se distinguen por dos tipos de red MAN. La primera de ellas se refiere alas de tipo privado, las cuales son implementadas en zonas de campus o corporaciones con edificios diseminados en un área determinada. Su estructura facilita fa instalación de cableado de fibra óptica.

El segundo tipo de redes MAN se refiere a las redes públicas de baja velocidad, las cuales operan amenos de 2 Megabits por segundo en su tráfico como Frame Relay, ISDN (Integrated Services Digital Network; Red Digital de Servicios Integrados), Tl- E 1, entre otros.

1.1.4. Interredes

Existen muchas redes en el mundo, a veces con diferente hardware y software. La gente conectada a una red a menudo quiere comunicarse con gente conectada a una red distinta. Esto requiere conectar redes diferentes y con frecuencia incompatibles, algunas veces usando maquinas llamadas **pasarelas** para hacer la conexión y realizar la traducción necesaria, ambas en términos de hardware y software. Una colección de redes interconectadas se llama **Interred.**

Una forma común de interred es una colección de LAN conectadas por una WAN. En efecto se remplazamos la etiqueta "subred" por WAN, nada mas tendría que cambiar. En este caso la única distinción real entre una subred y una WAN es si

están o no presentes las HOSTS. Si el sistema dentro de la curva cerrada únicamente enrutadores, es una subred; si contiene tanto enrutadores como hosts con sus propios usuarios, es una WAN.

Para evitar confusión, por favor note que la palabra "interred" siempre se usara en este libro en un sentido genérico. Por su parte, la Internet es una red específica mundial que se usa ampliamente para conectar universidades, oficinas de gobierno, compañías y finalmente individuos. Tendremos mucho que decir acerca de las intercedes y la Internet.

Las subredes, redes e intercedes con frecuencia se confunden. La subred tiene su sentido estándar en el contexto de una red de área amplia, donde se refiere a la colección de enrutadores y líneas de comunicación propiedad del operador de la red; por ejemplo compañías como America Online y CompuServe. Como analogía, el sistema telefónico consiste en centrales telefónicas conectadas unas con otras por líneas de alta velocidad, y a casas y negocios por líneas de baja velocidad. Estas líneas y el equipo, propiedad de la compañía de telefonos y administrado por ella, forman la subred del sistema telefónico. Los teléfonos por si mismos(los nodos de está analogía) no son parte de la subred. La combinación de una subred y sus nodos forma una red. En el caso de una LAN y los nodos forman la red; realmente no hay subred.

Se forma una interred cuando se conectan distintas redes entre si. Desde nuestro punto de vista es decir del grupo investigador, al conectar una LAN y una WAN o a su vez al conectar una MAN con una LAN o simplemente al conectar dos LAN

se estaría formando una Interred, pero no hay mucho consenso en la industria de la terminología en está área.

1.2. UTILIZACION DE LAS REDES DE COMPUTADORES

1.2.1. Aplicación de Negocios

Muchas Organizaciones tienen una cantidad importante de computadoras en operación, con frecuencia alejadas entre si. Por ejemplo una compañía con muchas fábricas o sedes puede tener una computadora en cada localidad para llevar el control ya sea de inventarios o algo que se le asemeje, vigilar la productividad y pagar la nomina local. Inicialmente, cada una de estas computadoras puede haber trabajado aisladas de las otras, pero en algún momento la gerencia decidió conectarlas para poder extraer y correlacionar información acerca de toda la compañía.

En términos generales, la cuestión es compartir recursos y la meta es hacer que todos los programas, el equipo y especialmente los datos estén disponibles para cualquiera en la red, sin importar la localización física de los recursos y de los usuarios. En otras palabras el hecho de que un usuario este a 1000 Km de distancia de sus datos no deberá impedirle usar los datos como si fueran locales. Este objetivo puede resumirse diciendo que es un intento por acabar con la tiranía de la geografía.

Una segunda meta es lograr una alta confiabilidad al contar con fuentes alternativas de suministros. Por ejemplo, todos los archivos podrían replicarse en dos o tres maquinas; así, si una de ellas no están disponibles (debido a una falla de hardware), podrán usarse las otras copias. Además, la existencia de múltiples CPU significa que si una de ellas falta, las otras serán capaces de hacer su trabajo, aunque se reduzca el rendimiento. En aplicaciones militares, bancarias de control de trafico aéreo, seguridad de reactores el rendimiento, seguridad de reactores nucleares y muchas otras, la capacidad para continuar operando pese a problemas de hardware es de suma importancia.

Otro de los objetivos que se persiguen es el establecer la escalabilidad, la capacidad para incrementar el rendimiento del sistema gradualmente cuando la carga de trabajo crece, añadiendo solamente más procesadores, En el caso de mainframes centralizados, cuando el sistema este lleno hay que reemplazarlo por uno mayor, usualmente más caro, lo que implica largas interrupciones para lo usuarios, Con el modelo cliente / servidor lo que se consigue es añadir nuevos clientes y nuevos servidores cuando sea necesario.

Un objetivo más del establecimiento de una red de computadoras tiene poco que ver con la tecnología. Una red de computadoras puede proporcionar un potente medio de comunicación entre empleados que están muy distantes. Al usar una red, es fácil para dos o mas personas que viven lejos escribir un informe juntas, Cuando un trabajador hace un cambio a un documento en línea, los demás pueden ver el cambio inmediatamente, sin tener que esperar varios días la

llegada de una carta. Tal rapidez hace fácil la cooperación entre grupos de gente muy apartada, cosa que previamente era imposible. A largo plazo, el uso de redes para mejorar la comunicación entre las personas probablemente resultara más importante que las metas técnicas tales como la mejora de la confiabilidad.

Los estándares que se aplican a la tecnología inalámbrica permitirá la interoperabilidad y cumplimiento de todas las redes existentes. Como en el caso de las redes cableadas, la IEEE es la principal generadora de estándares para las redes inalámbricas.

El estándar 802.11 se considera como una solución pata la implantación de REDES LAN sin hilos tanto en edificios como en espacios abiertos, con amplia cobertura y rendimiento.

Las tecnologías sobre las que en principio se soportan las redes inalámbricas son:

Espectro ensanchado de secuencia directa DSSS

Espectro ensanchado con salto de frecuencia FHSS

Infrarrojos.

De las tres la más utilizada es la DSSS, con la que se consigue una alta velocidad y una elevada inmunidad frente a las interferencias.

Las principales ventajas de esta tecnología son la movilidad y flexibilidad de cobertura y ubicación de usuarios, así como un bajo coste en infraestructura al no utilizar un medio guiado, mientras que sus mayores desventajas son una menor fiabilidad que otras soluciones sobre medios guiados y baja velocidad de proceso.

Las WLAN se encuentran dentro de los estándares desarrollados por la IEEE En 1989 en el seno de la IEEE 802 (estándar para redes LAN), se formo el comité IEEE 802.11, que empieza a trabajar para generar normas para las WLAN. Y utiliza la tecnología DSSS. El DSSS se aplica a los dispositivos inalámbricos que operan dentro de un intervalo de 1 a 2 Mbps.

Actualmente son cuatro lo estándares reconocidos dentro de la familia IEEE 802.11. El estándar 802.11. Se aplica a los dispositivos inalámbricos que operan dentro de un intervalo de 1 a 2 Mbps. E un sistema de DSSS puede transmitir hasta 11 Mbps, pero si opera por encima de los 2 Mbps se considera que no cumple con la norma. Luego aparece el Standard 802.11 a que proporciona mejores velocidades. El siguiente estándar aprobado fue el 802.11b, que aumentó las capacidades de transmisión a 11 Mbps. Aunque las WLAN de DSSS podían ínter operar con las WLAN de Espectro de Dispersión por Salto de Frecuencia (FHSS), se presentaron problemas que motivaron a los fabricantes a realizar cambios en el diseño. En este caso, la tarea del IEEE fue simplemente crear un estándar que coincidiera con la solución del fabricante. El 802.11b también recibe el nombre de Wi-Fi™ y finalmente el estándar 802.11g compatible con el pero que proporciona mayores velocidades.

Una red inalámbrica puede constar de tan sólo dos dispositivos. Los nodos pueden ser simples estaciones de trabajo de escritorio o computadores de mano. Equipada con NIC inalámbricas, se puede establecer una red 'ad hoc' comparable a una red cableada de par a par. Ambos dispositivos funcionan como servidores y clientes en este entorno. Aunque brinda conectividad, la seguridad es mínima, al igual que la tasa de transferencia. Otro problema de este tipo de red es la compatibilidad. Muchas veces, las NIC de diferentes fabricantes no son compatibles.

Para resolver el problema de la compatibilidad, se suele instalar un punto de acceso (AP) para que actúe como hub central para el modo de infraestructura de la WLAN. El AP se conecta mediante cableado a la LAN cableada a fin de proporcionar acceso a Internet y conectividad a la red cableada. Los AP están equipados con antenas y brindan conectividad inalámbrica a un área específica que recibe el nombre de celda. Según la composición estructural del lugar donde se instaló el AP y del tamaño y ganancia de las antenas, el tamaño de la celda puede variar enormemente. Por lo general, el alcance es de 91,44 a 152,4 metros (300 a 500 pies). Para brindar servicio a áreas más extensas, es posible instalar múltiples puntos de acceso con cierto grado de superposición. Esta superposición permite pasar de una celda a otra (roaming). Esto es muy parecido a los servicios que brindan las empresas de teléfonos celulares. La superposición, en redes con múltiples puntos de acceso, es fundamental para permitir el movimiento de los dispositivos dentro de la WLAN. Aunque los

estándares del IEEE no determinan nada al respecto, es aconsejable una superposición de un 20-30% . Este índice de superposición permitirá el roaming entre las celdas y así la actividad de desconexión y reconexión no tendrá interrupciones.

Cuando se activa un cliente dentro de la WLAN, la red comenzará a "escuchar" para ver si hay un dispositivo compatible con el cual "asociarse". Esto se conoce como "escaneo" y puede ser activo o pasivo.

El escaneo activo hace que se envíe un pedido de sondeo desde el nodo inalámbrico que busca conectarse a la red. Este pedido de sondeo incluirá el Identificador del Servicio (SSID) de la red a la que se desea conectar. Cuando se encuentra un AP con el mismo SSID, el AP emite una respuesta de sondeo. Se completan los pasos de autenticación y asociación.

Los nodos de escaneo pasivo esperan las tramas de administración de beacons (beacons) que son transmitidas por el AP (modo de infraestructura) o nodos pares (ad hoc). Cuando un nodo recibe un beacon que contiene el SSID de la red a la que se está tratando de conectar, se realiza un intento de conexión a la red. El escaneo pasivo es un proceso continuo y los nodos pueden asociarse o desasociarse de los AP con los cambios en la potencia de la señal.

Una vez establecida la conectividad con la WLAN, un nodo pasará las tramas de igual forma que en cualquier otra red 802.x. Las WLAN no usan una trama estándar 802.3. Por lo tanto, el término "Ethernet inalámbrica" puede resultar

engañoso. Hay tres clases de tramas: de control, de administración y de datos. [1] Sólo la trama de datos es parecida las tramas 802.3. Las tramas inalámbricas y la 802.3 cargan 1500 bytes; sin embargo una trama de Ethernet no puede superar los 1518 bytes mientras que una trama inalámbrica puede alcanzar los 2346 bytes. En general, el tamaño de la trama de WLAN se limita a 1518 bytes ya que se conecta, con mayor frecuencia, a una red cableada de Ethernet.

Debido a que la radiofrecuencia (RF) es un medio compartido, se pueden producir colisiones de la misma manera que se producen en un medio compartido cableado. La principal diferencia es que no existe un método por el que un nodo origen pueda detectar que ha ocurrido una colisión. Por eso, las WLAN utilizan Acceso Múltiple con Detección de Portadora/Carrier y Prevención de Colisiones (CSMA/CA). Es parecido al CSMA/CD de Ethernet.

Cuando un nodo fuente envía una trama, el nodo receptor devuelve un acuse de recibo positivo (ACK). Esto puede consumir un 50% del ancho de banda disponible. Este gasto, al combinarse con el del protocolo de prevención de colisiones reduce la tasa de transferencia real de datos a un máximo de 5,0 a 5,5 Mbps en una LAN inalámbrica 802.11b con una velocidad de 11 Mbps.

El rendimiento de la red también estará afectado por la potencia de la señal y por la degradación de la calidad de la señal debido a la distancia o interferencia. A medida que la señal se debilita, se puede invocar la Selección de Velocidad Adaptable (ARS). La unidad transmisora disminuirá la velocidad de transmisión de datos de 11 Mbps a 5,5 Mbps, de 5,5 Mbps a 2 Mbps o de 2 Mbps a 1 Mbps.

La autenticación de la WLAN se produce en la Capa 2. Es el proceso de autenticar el dispositivo no al usuario. Este es un punto fundamental a tener en cuenta con respecto a la seguridad, detección de fallas y administración general de una WLAN.

La autenticación puede ser un proceso nulo, como en el caso de un nuevo AP y NIC con las configuraciones por defecto en funcionamiento. El cliente envía una trama de petición de autenticación al AP y éste acepta o rechaza la trama. El cliente recibe una respuesta por medio de una trama de respuesta de autenticación. También puede configurarse el AP para derivar la tarea de autenticación a un servidor de autenticación, que realizaría un proceso de credencial más exhaustivo. [1]

La asociación que se realiza después de la autenticación, es el estado que permite que un cliente use los servicios del AP para transferir datos.

Tipos de autenticación y asociación

- No autenticado y no asociado
- El nodo está desconectado de la red y no está asociado a un punto de acceso.
- Autenticado y no asociado
- El nodo ha sido autenticado en la red pero todavía no ha sido asociado al punto de acceso.
- Autenticado y asociado
- El nodo está conectado a la red y puede transmitir y recibir datos a través del punto de acceso.

Métodos de Autenticación

IEEE 802.11 presenta dos tipos de procesos de autenticación.

El primer proceso de autenticación es un sistema abierto. Se trata de un estándar de conectividad abierto en el que sólo debe coincidir el SSID. Puede ser utilizado en un entorno seguro y no seguro aunque existe una alta capacidad de los 'husmeadores' de red de bajo nivel para descubrir el SSID de la LAN.

El segundo proceso es una clave compartida. Este proceso requiere el uso de un cifrado del Protocolo de Equivalencia de Comunicaciones Inalámbricas (WEP). WEP es un algoritmo bastante sencillo que utiliza claves de 64 y 128 bits. El AP está configurado con una clave cifrada y los nodos que buscan acceso a la red a través del AP deben tener una clave que coincida. Las claves del WEP asignadas de forma estática brindan un mayor nivel de seguridad que el sistema abierto pero definitivamente no son invulnerables a la piratería informática.

El problema del ingreso no autorizado a las WLAN actualmente está siendo considerado por un gran número de nuevas tecnologías de soluciones de seguridad.

LOS ESPECTROS DE ONDAS Y RADIO MICROONDAS

Los computadores envían señales de datos electrónicamente. Los transmisores de radio convierten estas señales eléctricas en ondas de radio. Las corrientes eléctricas cambiantes en la antena de un transmisor generan ondas de radio. Estas ondas de radio son irradiadas en líneas rectas desde la antena. Sin embargo, las ondas de radio se atenúan a medida que se alejan de la antena

transmisora. En una WLAN, una señal de radio medida a una distancia de sólo 10 metros (30 pies) de la antena transmisora suele tener sólo 1/100mo de su potencia original. Al igual que lo que sucede con la luz, las ondas de radio pueden ser absorbidas por ciertos materiales y reflejadas por otros. Al pasar de un material, como el aire, a otro material, como una pared de yeso, las ondas de radio se refractan. Las gotas de agua que se encuentran en el aire también dispersan y absorben las ondas de radio.

Es importante recordar estas cualidades de las ondas de radio cuando se está planificando una WLAN para un edificio o en un complejo de edificios. El proceso de evaluar la ubicación donde se instala una WLAN se conoce como inspección del sitio.

Como las señales de radio se debilitan a medida que se alejan del transmisor, el receptor también debe estar equipado con una antena. Cuando las ondas de radio llegan a la antena del receptor, se generan débiles corrientes eléctricas en ella. Estas corrientes eléctricas, producidas por las ondas de radio recibidas, son equivalentes a las corrientes que originalmente generaron las ondas de radio en la antena del transmisor. El receptor amplifica la fuerza de estas señales eléctricas débiles.

1.2.2. Aplicaciones Domesticas

En lo anteriormente citado, para construir redes de computadoras son de naturaleza esencialmente económica y tecnológica. Si mainframes suficientemente

grandes y potentes estuvieran disponibles a precios aceptables, muchas compañías habrían optado por guardar todos sus datos en ellas y proporcionar a sus empleados terminales conectados a estas maquinas.

En la década de 1970 y a principios de la de 1980, casi todas las compañías operaban de esta forma. Las redes de computadoras llegaron a ser populares únicamente cuando los computadoras personales ofrecieron una descomunal ventaja precio / rendimiento sobre los mainframes.

Al iniciar la década de 1990, las redes de computadoras comenzaron a prestar servicios a particulares en su hogar. Estos servicios y la motivación para usarlos son muy diferentes del modelo de eficiencia corporativa descrito anteriormente.

Con las redes hemos estimulado tres aspectos de está evolución:

- Acceso a información remota
- Comunicación de persona a persona
- Entretenimiento interactivo

Dentro del aspecto domestico debemos tener en claro que las redes pueden satisfacer necesidades de comunicación mediante equipos móviles y computadores para descargar información, dentro de los artefactos que se utilizan estarían los celulares PDA, Computadores portátiles

1.2.3. Usuarios Móviles o Inalámbricos

Una de las tecnologías mas prometedoras y discutidas en esta década es la de poder comunicar computadoras y dispositivos móviles mediante tecnología inalámbrica. Las redes inalámbricas facilitan la operación en lugares dónde los

dispositivos móviles no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos.

Pero la realidad es que esta tecnología está todavía en pañales y se deben resolver varios obstáculos técnicos y de regulación antes de que las redes inalámbricas sean utilizadas de una manera general en los sistemas de cómputo de la actualidad.

No se espera que las redes inalámbricas lleguen a reemplazar a las redes cableadas, ya que estas ofrecen velocidades de transmisión mayores que las redes inalámbricas. Mientras que las redes inalámbricas actuales ofrecen velocidades de 2Mbps. Las redes cableadas ofrecen velocidades de 10/100 mbps y se espera que alcancen velocidades de 1000 mbps . Haciendo una analogía y siendo optimistas se espera que con los avances tecnológicos las redes inalámbricas alcancen velocidades de solo 10 mbps.

Sin embargo se pueden mezclar las redes cableadas y las inalámbricas y de esta manera generar una red Híbrida. Y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema de cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o de una oficina.

1.3. TENDENCIA DE LAS TELECOMUNICACIONES

1.3.1 Definición.

La teleinformática es la rama de la informática que trata y estudia las comunicaciones. Mientras que la telemática podría definirse mas técnicamente como la técnica que trata la comunicación remota entre procesos.

El elemento mas importante y fundamental de la telemática son las redes de transmisión.

Dentro de la telemática debemos saber distinguir entre dos conceptos muy diferentes:

La comunicación: Es el proceso telemático por el que se transporta la información de emisor a receptor y a la inversa.

Dicha información ha de ser entendida y significa algo en concreto tanto para el emisor como por el receptor de no ser así no habría una comunicación, pero si una transmisión

La transmisión: Es el proceso telemático por el que se envía la información de un lugar a otro. Esta información no se envía como tal si no como magnitudes físicas, interpretadas.

1.3.2. Importancia de la telemática.

La telemática almacena y procesa datos y los convierte en información significativa a gran velocidad y a bajo costo para ser entregada a quien la necesita, o almacenada para un uso futuro.

El almacén ordenado moderno de datos, se llama base de datos.

El costo de almacenar y procesar datos e información baja todos los años en razón de los avances tecnológicos en la electrónica y en la informática.

Estas características de la telemática permiten, no solo bajar los costos del procesamiento de la información al aumentar la productividad de los que la utilizan, sino además originan un ahorro considerable de recursos en los proyectos y las operaciones, en razón de la rapidez y mejores decisiones que se derivan de su empleo.

La Telemática contribuye al desarrollo del pensamiento y del conocimiento al facilitar la información a bajo costo, que es la base del desarrollo del conocimiento.

En conclusión la Telemática es una potentísima herramienta de reducción de costos, de aumento de la productividad, la eficiencia y la calidad de productos y operaciones. Es pues una gran herramienta indispensable para progresar en un ambiente de competencia. Es el signo de los tiempos del siglo nuevo que se viene, que parece que se adelanta en el campo de la telemática.

1.3.3 Tecnología de las redes de telecomunicaciones

Las redes se dividen hoy en dos grandes categorías en base su medio:

1.3.3.1. Medios inalámbricos

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnologia inalámbrica. La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada. Las Redes Inalámbricas facilitan la operación

en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos.

1.3.3.2. Ondas de radio

Las ondas de Radio son un tipo de ondas electromagnéticas, lo cual confiere tres ventajas importantes:

- No es necesario un medio físico para su propagación, las ondas electromagnéticas pueden propagarse incluso por el vacío.
- La velocidad es la misma que la de la luz, es decir 300.000 Km/seg.
- Objetos que a nuestra vista resultan opacos son transparentes a las ondas electromagnéticas.

No obstante las ondas electromagnéticas se atenúan con la distancia, de igual forma y en la misma proporción que las ondas sonoras. Pero esta desventaja es posible minimizarla empleando una potencia elevada en la generación de la onda, además que tenemos la ventaja de la elevada sensibilidad de los receptores.

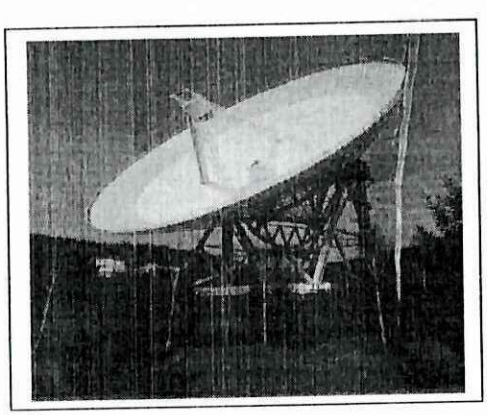


Gráfico 1.15: Ondas de radio
Fuente: Redes de computadoras. Andrew Tanenbaum

Generación y propagación de las ondas

Las ondas de radio son generadas aplicando una corriente alterna de radiofrecuencia a un antena. La antena es un conductor eléctrico de características especiales que debido a la acción de la señal aplicada genera campos magnéticos y eléctricos variables a su alrededor, produciendo la señal de radio en forma de ondas electromagnéticas.

Estas ondas se transmiten desde un punto central (la antena emisora) de forma radial y en todas direcciones, pero podemos diferenciar tres formas de transmisión:

1.3.3.3 Microondas terrestres

Suelen utilizarse antenas parabólicas. Para conexionas a larga distancia , se utilizan conexiones intermedias punto a punto entre antenas parabólicas .
Se suelen utilizar en sustitución del cable coaxial o las fibras ópticas ya que se necesitan menos repetidores y amplificadores. aunque se necesitan antenas alineadas. Se usan para transmisión de televisión y voz.
La principal causa de pérdidas es la atenuación debido a que las pérdidas aumentan con el cuadrado de la distancia (con cable coaxial y par trenzado son logarítmicas) . La atenuación aumenta con las lluvias .Las interferencias es otro inconveniente de las microondas ya que al proliferar estos sistemas , pude haber más solapamientos de señales .

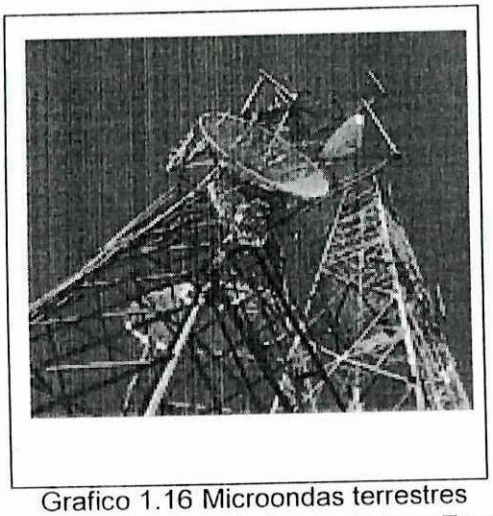


Grafico 1.16 Microondas terrestres
Fuente: Redes de computadoras. Andrew Tanenbaum

1.3.3.4. Fijas o cableadas

Se conoce como fijas o cableadas aquellas que utilizan unos componentes físicos y sólidos para la transmisión de datos. También conocidos como medios de transmisión por cable.

Los medios que se utilizan para transferir en estos sistemas son:

- Cables de 2 hilos (1 par) para telefonía fija.
- Cable coaxial cada ves mas en desuso por su alto costo y difícil manipulación.
- Los cables UTP para acometer a los equipos terminales.
- Cable de fibra Óptica para las conexiones entre equipos de conmutación (Backbone).

1.4. HISTORIA DE LAS REDES

1.4.1. Estándares de calidad de las redes

Como es de conocimiento general la IEEE ha producido varios estándares para las redes tanto LAN, MAN, WAN, WLAN. Estos estándares, conocidos en conjunto como IEEE 802, incluyen CSMA/CD, token bus y token ring. Los diferentes estándares difieren n la capa física y en la subcapa MAC, pero son compatibles en la capa de enlace de datos. Los estándares IEEE 802 han sido adoptados por el ANSI como estándares nacionales en los Estados Unidos de América, por el NIST como estándares internacionales (conocidos como ISO 8802). Estos documentos son sorprendentemente fáciles de entender e implementar como para ser tomados como estándares internacionales.

Los estándares se dividen en dos partes, cada una publicada como libro independiente. El 801.1 es una introducción al grupo de estándares y define las primitivas de la interfaz.

El estándar 802.2 describe la parte superior de la capa de enlace de datos, que usan el protocolo LLC (Logical Link Control, Control de enlace lógico). Las partes 802.3 a 802.5 describen los tres estándares para LAN, CSMA/CD, token bus, token ring, respectivamente. Cada estándar cubre la capa física y el

protocolo de la subcapa MAC. Las tres secciones siguientes cubren estos tres sistemas.

El primer componente del estándar IEEE 802.11 fue ratificado en 1997 y luego en 1999, cuando también se realizaron las primeras extensiones. La estructura de los estándares de la IEEE es tal que las extensiones se elaboran como modificaciones del estándar original y se nombran agregándole una letra al nombre del estándar. En el caso de 802.11, tenemos extensiones 802.11a, 802.11b, etc. En realidad, el estándar 802.11 es sólo una parte de un conjunto más amplio de estándares de IEEE: el 802. La Figura muestra esquemáticamente la estructura del conjunto de estándares 802, dedicado a las capas más bajas de arquitectura de redes.

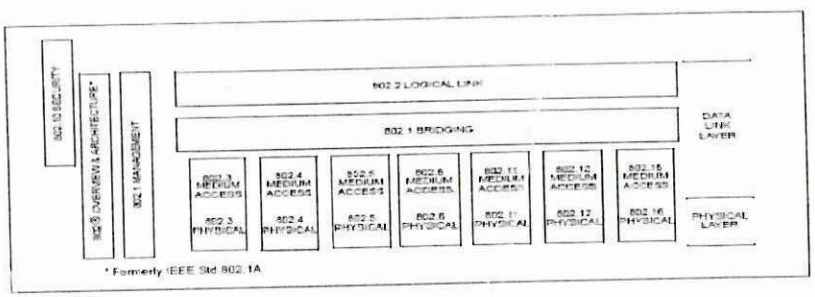


GRAFICO 1.2: FAMILIA DE LOS ESTANDARES DE LA IEEE. 802.11
FUENTE: GRUPO INVESTIGADOR

1.4.2. Seguridades en la Redes de acuerdo a los estándares

La seguridad concierne a todas las organizaciones y a las personas que desean una cierta privacidad en su vida. El estudio de los mecanismos de seguridad, si bien siempre ha sido de importancia en sistemas de ordenadores multiusuarios,

ha tenido una explosión con el uso de Internet, donde millones de equipos están conectados todo el tiempo, y donde personas de pocos escrúpulos realizan ataques, perjuicios o intrusiones de forma diaria tanto a organizaciones, empresas, como a individuales.

Internet nace como una serie de redes que realizan el intercambio de información entre investigadores que colaboran en proyectos conjuntos, o comparten resultados usando los recursos de estar conectados en red. En esta etapa inicial, la información circulaba libremente y no existía una preocupación por la privacidad de los datos ni por ninguna otra problemática de seguridad. Estaba totalmente desaconsejado usarla para el envío de documentos clasificados que pudieran manejar los usuarios, situación muy común, pues hay que recordar que la Internet nace como un contrato del Departamento de Defensa Americano para conectar entre sí tanto las Universidades como los centros de investigación que colaboran de una manera u otra con las Fuerzas Armadas Norteamericanas. La red evolucionó de manera que ahora no sólo sirve para intercambiar información, si no también para investigar, hacer negocios, comprar, vender, etc. Se ha incrementado la variedad y cantidad de usuarios que usan la red para fines tan diversos como el aprendizaje, la docencia, la investigación, la búsqueda de socios o mercados, la cooperación altruista, la práctica política o simplemente el juego. En medio de esta variedad han ido aumentando las acciones poco respetuosas con la privacidad y con la propiedad de recursos y sistemas. Hackers, crackers, virus, gusanos, spam y demás denominaciones han hecho

aparición en el vocabulario ordinario de los usuarios y de los administradores de las redes.

También podemos recorrer el ciberespacio, dejando o recibiendo mensajes aquí o allá, aunque difícilmente podamos saber con precisión quien es la persona con la que nos estamos interactuando, no sabemos donde vive, si es hombre o mujer, viejo o joven. Al ser interesante lugar para conservar el anonimato, es allí donde pueden generarse problemas.

Debido a todo esto, nuevos mecanismos de ataques y de prevención se han desarrollado, de forma que se puedan asegurar los privilegios de intimidad de cada usuario. De todos modos, no existe mecanismo de protección perfecto, y diariamente escuchamos noticias sobre sitios atacados, e-mails revisados sin autorización, o recibimos una gran cantidad de e-mail basura.

Es importante hacer una distinción entre seguridad y protección. El problema de la seguridad consiste en lograr que los recursos de un sistema sean, bajo toda circunstancia, utilizados para los fines previstos. Para eso se utilizan mecanismos de protección.

Los sistemas operativos proveen algunos mecanismos de protección para poder implementar políticas de seguridad. Las políticas definen qué hay que hacer, y los mecanismos determinan cómo hay que hacerlo. Esta separación es importante en términos de flexibilidad, puesto que las políticas pueden variar en el tiempo y de una organización a otra. Los mismos mecanismos, si son flexibles, pueden usarse para implementar distintas políticas.

Los mecanismos que ofrece el sistema operativo necesariamente deben complementarse con otros de carácter externo. Por ejemplo, impedir el acceso físico de personas no autorizadas a los sistemas es un mecanismo de protección cuya implementación no tiene nada que ver con el sistema operativo.

Un aspecto importante de la seguridad es el de impedir la pérdida de información, la cual puede producirse por diversas causas: fenómenos naturales, guerras, errores de hardware o de software, o errores humanos. La solución es una sola: mantener la información respaldada, de preferencia en un lugar lejano.

Otro aspecto importante de la seguridad, es el que tiene que ver con el uso no autorizado de los recursos:

- • Lectura de datos.
- • Modificación de datos.
- • Destrucción de datos.
- • Uso de recursos: ciclos de CPU, impresora, almacenamiento.

Mucho sobre el tema de seguridad y criptografía se trata en el curso de redes, por lo que aquí se hará una recorrida rápida y general a los temas de seguridad.

Recomendaciones para mantener la privacidad y seguridad en Internet.

A pesar de la gran cantidad de consejos que se pudieran brindar sobre el tema, hay uno sólo que es realmente valioso: **utilizar el sentido común**. Todos los

demás consejos se basan en la pauta de que usted entiende lo que está haciendo y que se dará cuenta del actuar extraño de sitios, correos o programas.

- Debe tenerse una gran precaución al revelar información personal (dirección, nº de teléfono, etc.) a personas que se conocen en el "ciberespacio", aunque fuera en un foro local, puesto que es imposible saber quien en realidad está del otro lado y cuales son sus intenciones.
- Los correos gratuitos vía web ofrecen supuestas garantías de privacidad, pero la verdad es que no podemos saber lo que ocurre con la información que enviamos y recibimos mientras se encuentre en su servidor.
- Las sesiones en terminales públicas deben cerrarse, para evitar que otro usuario posterior pueda ingresar a su información personal.
- Para hacer compras que involucren tarjetas de crédito, asegúrese de ser un sitio serio, y que brinde servidores seguros para realizar las transacciones.
- Cuando se realizan compras, es importante tener claro que se está comprando, cuales son los precios, impuestos y gastos de envíos, a fin de evitar recibir ítems que no eran lo deseado, o que los costos superen grandemente lo que se creía. También es importante tener claras las garantías que se dan y las formas de devolución o reclamo ante objetos que llegaran dañados o que se perdieran en el envío.
- Es interesante tener las versiones de los programas que se utilizan en Internet (navegadores, manejadores de e-mail, chat, mensajeros, FTP, etc.), ya que las nuevas versiones suelen corregir errores y evitar diferentes tipos de intrusiones que aparecieron hasta ese momento para las versiones anteriores.

- Con claves de 7 caracteres tomados al azar de entre los 95 caracteres ASCII que se pueden digitar con cualquier teclado, entonces las 957 posibles claves deberían desincentivar cualquier intento por adivinarla. Sin embargo, una proporción demasiado grande de las claves escogidas por los usuarios son fáciles de adivinar, pues la idea es que sean también fáciles de recordar. Para las contraseñas convienen utilizarse palabras de varias letras, en especial con combinación de números y caracteres especiales. Muchas personas utilizan palabras demasiado comunes (amor, dios, el nombre de familiares, fechas importantes etc.) que permite que ataques de fuerza bruta mediante diccionarios o ataques por gente conocida sean más fáciles de encontrar la palabra clave. Además estas deberían cambiarse a menudo, de forma que si uno fue descubierto, el atacante tenga poco tiempo acceso a los recursos. Un grave error que comenten los usuarios es utilizar la misma contraseña en varios servicios (password del equipo, del correo, del FTP, de su alarma, del sistema de base de datos de la empresa, etc.), y si uno de estos es descubierto, el intruso puede acceder a todos los demás servicios a partir de ese momento. Evidentemente no se debe compartir la contraseña con otras personas aunque sean compañeros de trabajo o amigos. Muchos sistemas de bases de datos registran el actuar de cada persona logueada al sistema, y otra persona puede utilizar su cuenta para realizar actividades que finalmente serán achacadas a usted.
    - Los antivirus actuales tienen capacidades de revisión de páginas Web, correos electrónicos y montaje de firewalls para chequear toda la información que entra y sale de la máquina. Éstas son herramientas

tremendamente importantes en la actualidad para mantener sanos los equipos.

- Hay que tener mucho cuidado al bajar programas de sitios web cuyo origen desconocemos, lo mismo para servidores FTP y para adjunto de mensajes en mensajeros como ICQ, Messenger, etc. Muchos sitios de "warez" o de hackers tienen programas infectados que traen consigo virus o que instalan programas como el "Back Orifice", que permiten el acceso y control total de la máquina a desconocidos.
- No se deben abrir correos electrónicos con mensajes adjuntos de personas desconocidas, en otros idiomas, o con información no solicitada. Muchos virus ingresan de esa manera por culpa del propio usuario que abre el mensaje debido a la curiosidad. En todo caso, puede revisarse el código fuente del mensaje primero, para revisar su contenido y verificar si realmente es algo malicioso o no.
- En cuanto a la administración de servidores, siempre deben instalarse los parches de seguridad que aparecen periódicamente, puesto que al descubrirse debilidades en estos, inmediatamente gran cantidad de hackers se dedican a entrar a los sistemas o a escribir aplicaciones para aprovecharse de los problemas en esos sistemas. En Linux el problema cada vez se hace más grave en ese sentido, puesto que al ser de código abierto, cualquiera puede revisar el mismo buscando mecanismos de ataque.

Si bien los sistemas de Microsoft se han demostrado débiles también ante los ataques, la incapacidad de no poder revisar su código fuente hace que este tipo de ataque sea más difícil de realizar.

Mecanismos de seguridad.

Dependiendo del uso que un equipo o sistema de seguridad, existen diferentes métodos de protección ante el acceso o uso del mismo por personas no autorizadas. Algunos restringen el acceso a través de la red, otros el acceso físico, etc. Muchas veces un único mecanismo no es suficiente seguridad, por lo que se tienen que aplicar varios en conjuntos para dar una mayor seguridad. La Protección absoluta contra uso malicioso de los sistemas es imposible, pero si los costos de violar un sistema son superiores a los potenciales beneficios que se pueden obtener, entonces el sistema puede considerarse seguro. Además, por lo general, la seguridad se rompe en el eslabón más débil de la cadena, que suele ser el factor humano.

- **Restricción física de acceso:** Ciertos equipos o procesos requieren una presencia física del usuario, por lo que si se restringe el acceso físico al lugar únicamente a las personas autorizadas, el problema se soluciona.
- **Control de acceso al servicio:** Esfuerzo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red, con mecanismos de autenticación. Este mecanismo puede ser la posesión de un ítem (llave o tarjeta), un conocimiento (una clave) o un atributo propio del usuario (controles biométricos: dactilar, ocular, voz).

- **Intercambio de autenticación:** Corrobora que una entidad, ya sea origen o destino de la información, es la deseada, por ejemplo, A envía un número aleatorio cifrado con la clave pública de B, B lo descifra con su clave privada y se lo reenvía a A, demostrando así que es quien pretende ser. Por supuesto, hay que ser cuidadoso a la hora de diseñar estos protocolos, ya que existen ataques para desbaratarlos.
- **Cifrado:** Garantiza que la información no es inteligible para individuos, entidades o procesos no autorizados (confidencialidad). Consiste en transformar un texto en claro mediante un proceso de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado. Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el sistema es simétrico. Estos sistemas son mucho más rápidos que los de clave pública, resultando apropiados para funciones de cifrado de grandes volúmenes de datos.
- **Tráfico de relleno:** Consiste en enviar tráfico espurio junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo. Esto evita el método de ataque en donde se conocen el tamaño de los datos y paquetes, y a partir de ellos se puede reconstruir la información parcialmente y luego descubrir el resto.
- **Control de encaminamiento:** Permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras rutas, en caso que se detecten persistentes violaciones de integridad en una ruta determinada.

- **El firewall:** Es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada e Internet. El firewall determina cual de los servicios de red pueden poseer accesos dentro de ésta por los que están fuera, o viceversa, es decir, quien puede entrar para utilizar los recursos de red pertenecientes a la organización o que usuarios o programas tienen derechos a salir a Internet. Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través de él mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración, desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa. Un firewall es vulnerable: él no protege de la gente que esta dentro de la red interna, éste trabaja mejor si se complementa con una defensa interna.
- **Filtros para Internet.** (se trata de manera especial en la siguiente sección, por ser un caso más complejo)
- **Seguridad de los módems de acceso telefónico:** La primera línea de defensa es mantener el número de teléfono fuera del alcance de personas no autorizadas, es decir, no publicarlo, no listarlo en los sistemas, etc. También se puede añadir una contraseña de módem válida que sea independiente y distinta de la de inicio de sesión del sistema para que mantenga alejado a todo aquel que no la conozca
- **Inmunice su equipo (antivirus):** Hay muchos programas antivirus disponibles en el mercado y en la propia Internet, que funcionan como vacunas virtuales contra virus conocidos. Asegúrese de tener un programa

antivirus actualizado en su equipo y utilícelo. Tenga en cuenta que constantemente se están desarrollando nuevos virus, de modo que debe actualizar su programa antivirus frecuentemente. Por lo general, los proveedores de estos programas recomiendan actualizarlos como mínimo cada 30 días.

El problema es que esa protección no obstaculice el uso del sistema por parte de usuarios autorizados. Demasiada seguridad podría ser contraproducente si es muy engorrosa para los usuarios, pues estos tenderán a eludir los procedimientos para facilitarse la vida. Por lo tanto se debe tener un punto de equilibrio entre los mecanismos de seguridad y la comodidad según el caso que se tenga.

Tipos de ataques o molestias.

Al ir evolucionando los mecanismos de defensa ante las intrusiones, también se han ido perfeccionando sus mecanismos de ataque, y actualmente se combinan mecanismos tradicionales con otros nuevos para acceder a información restricta o utilizar recursos no permitidos.

Backdoors (trampillas)

Un backdoor es un punto de entrada secreto a un programa que permite a alguien que lo conozca conseguir el acceso sin pasar por los procedimientos usuales de seguridad de acceso. Las trampillas las han usado los programadores de una forma legítima durante muchos años para depurar y probar los programas. La

posibles de letras una tras otra) o por métodos de diccionarios de palabras conocidas y comúnmente utilizadas. De todos modos, estos ataques, en especial los de fuerza bruta, al tener una complejidad exponencial respecto a la cantidad de letras utilizadas, pueden tardar días o semanas en romper una clave según la cantidad de caracteres que ésta tenga.

También existen versiones semejantes de estos programas que intentan romper claves de usuarios de servicios on-line. Por ejemplo, si se conoce la cuenta de un usuario en un sistema, se puede dejar al programa probando combinaciones de este id de usuario con los métodos anteriormente citados. Una protección ante este tipo de ataques sería configurar al servidor para que luego de una cantidad de intentos de accesos infructuosos con un usuario, éste quede bloqueado hasta que el administrador verifique lo que estuviera ocurriendo.

1.4.3. Vulnerabilidades

Con un poco de tiempo, los recursos y la motivación, un intruso puede violar casi cualquier sistema, todos los procedimientos de seguridad y la tecnología disponible en la actualidad no pueden garantizar que sus sistemas estén seguros de un ataque. Los enruteadores (Routers) pueden ayudar a asegurar sus puertas de enlace (gateways) a la Internet. Los firewalls Ike permiten asegurar el borde de su red. Las redes privadas virtuales pueden pasar con seguridad sus datos en un flujo que se encuentre encriptado. Los IDS o sistemas de detección de intrusos pueden advertir de actividades maliciosas, todo esto depende de algunas variables que incluyen las siguientes:

- La experiencia que tenga el equipo de trabajo responsable de la configuración, supervisión y mantenimiento de las tecnologías.
- La habilidad de remendar y actualizar servicios y el Kernel(Código fuente de los Sistemas Open Source) rápida y eficientemente.
- La habilidad de aquellos responsables de mantener vigilancia constante sobre la red.

Dado el estado dinamico de los sistemas de datos y tecnologías, asegurar sus recursos corporativos pueden ser bien complejo. Debido a está complejidad, puede ser difícil encontrar recursos expertos para todos sus sistemas. Mientras que es posible tener personal con conocimientos en muchas áreas de seguridad de la información a un nivel alto, es difícil mantener personal que sea experto en más de unas pocas áreas particulares. Este se debe principalmente a que cada área en particular de seguridad de la informaciór requiere constante atención y foco. La seguridad de la información es algo que no se puede estar estancado, es decir no podemos dejarla quieta ya que siempre van a existir personas con conocimientos frescos y con nuevas ideas e intenciones de alterar o borrar información de cualquier institución o empresa.

depuración y las pruebas se suelen hacer cuando el programador esta desarrollando una aplicación que dispone de un procedimiento de autenticación o una preparación muy larga, que requiere del usuario introducir muchos valores diferentes para ejecutar la aplicación. Para depurar el programa, el desarrollador puede querer disponer de privilegios especiales o evitar toda la preparación y autenticación necesarias. El programador también puede querer asegurarse que hay un método para activar el programa en el caso de que algo vaya mal en el procedimiento de autenticación que se está construyendo en la aplicación. La trampilla es un código que reconoce alguna secuencia de entrada especial o que es lanzado al ser ejecutado por un cierto ID de usuario o mediante una secuencia improbable de sucesos.

Caballos de Troya

Se estudian mejor en el apartado de Virus, pero de todos modos cabe mencionar que son programas que realizan una supuesta tarea cuando en realidad hacen otras cosas, como podría ser liberar un virus, activar un mecanismo de envío de información fuera de la máquina, copiar archivos, robar información, o causar daños. Programas como el "Back Orifice" muchas veces vienen ocultos como caballos de Troya en otras aplicaciones que se bajan de sitios poco fiables de Internet.

Rompedores de claves

Son programas preparados para atacar ciertos tipos de archivos intentando descubrir la clave que los protege, de manera a poder acceder a su información. Pueden utilizar métodos de fuerza bruta (probando todas las combinaciones

CAPITULO II

TRABAJO DE CAMPO

2. ELEMENTOS NECESARIOS PARA LA CONFIGURACIÓN Y FUNCIONAMIENTO DE UN SERVIDOR PROXY INVERSO

2.1. Estándares de calidad para el aseguramiento de la calidad en el flujo de información bajo estándares internacionales

Las propiedades de gran valor necesitan ser protegidas de robo o destrucción potencial. Algunos hogares equipados con sistemas de alarmas que pueden detectar ladrones, notificar a las autoridades cuando curre una entrada ilegal y hasta advertir a los dueños cuando sus hogares están bajo fuego.

Tales medidas son necesarias para asegurar la integridad de los hogares y la seguridad de sus dueños.

La Internet ha facilitado el flujo de la información, desde personal hasta financiera. Al mismo tiempo, también ha promovido muchos peligros. Los usuarios maliciosos y crackers buscan objetivos variables buscan objetivos vulnerables tales como sistemas no actualizados, sistemas infectados con troyanos

y redes ejecutando servicios inseguros. Las alarmas son necesarias para notificar a los administradores y a los miembros del equipo de seguridad que ha ocurrido una entrada ilegal para que así estos puedan responder en tiempo real a la amenaza. Se han diseñado los *sistemas de detección de intrusos* tales como sistemas de notificación.

En la Universidad Técnica de Cotopaxi, los administradores nos supieron manifestar que se encuentra implementado un IPS (*Sistema de Prevención de Intrusos*), el mismo que precautela la información que se genera en el centro educativo.

2.1.1. Sistema de Detección de Intrusos (IDS)

Un sistema de detección de intrusos (IDS) es un proceso o dispositivo activo que analiza la actividad del sistema y de la red por entradas no autorizadas y/o actividades maliciosas. La forma en que un IDS detecta las anomalías pueden variar ampliamente; sin embargo, el objetivo final de cualquier IDS es el de atrapar a los perpetradores en el acto antes de que hagan algún daño a sus recursos.

Un IDS protege a un sistema contra ataques, malos usos y compromisos. Puede también monitorear la actividad de la red, auditar las configuraciones de la red y sistemas por vulnerabilidades, analizar la integridad de los datos y más. Dependiendo de los métodos de detección

que seleccione utilizar, existen numerosos beneficios directos e incidentales de usar un IDS.

2.1.2. Sistemas de Detección de Intrusos basados en HOST

Un IDS basado en host analiza diferentes áreas para determinar el uso incorrecto (actividades maliciosas o abusivas dentro de la red) o alguna intrusión (violaciones desde afuera). Los IDSes basados en host consultan diferentes tipos de registros de archivos (kernel, sistema, servidores, red, cortafuegos, y más) y comparan los registros contra una base de datos interna de peculiaridades comunes sobre ataques conocidos. Los IDSes basados en host de Linux y Unix hacen uso extensivo de syslog y de su habilidad para separar los eventos registrados por severidad (por ejemplo, mensajes menores de impresión versus advertencias importantes del kernel). El comando syslog está disponible cuando se instala el paquete sysklogd, incluido con Red Hat Enterprise Linux. Este paquete proporciona el registro de mensajes del sistema y del kernel. Los IDSes basados en hosts filtran los registros (lo cual, en el caso de algunas redes y registros de eventos del kernel pueden ser bastante detallados), los analizan, vuelven a etiquetar los mensajes anómalos con su propia clasificación de severidad y los reúne en su propio registro para que sean analizados por el administrador.

Los IDSes basados en host también pueden verificar la integridad de los datos de archivos y ejecutables importantes. Funciona verificando una base de datos de archivos confidenciales (y cualquier archivo añadido por el administrador) y crea una *suma de verificación* de cada archivo con una utilidad de resumen de archivos de mensajes tal como md5sum (algoritmo de 128-bit) o sha1sum (algoritmo de 160-bit). El IDS basado en host luego almacena las sumas en un archivo de texto plano y periódicamente compara las sumas de verificación contra los valores en el archivo de texto. Si cualquiera de estas sumas no coinciden, el IDS alertará al administrador a través de un correo electrónico o a un mensaje al celular.

2.1.3. Sistema de Detección de Intrusos basados en Red

Los sistemas de detección de intrusos basados en la red operan de una forma diferente que aquellos IDSes basados en host. La filosofía de diseño de un IDS basado en la red es escanear los paquetes de red al nivel del enrutador o host, auditar la información de los paquetes y registrar cualquier paquete sospechoso en un archivo de registros especial con información extendida. Basándose en estos paquetes sospechosos, un IDS basado en la red puede escanear su propia base de datos de firmas de ataques a la red y asignarles un nivel de severidad para cada paquete. Si los niveles de severidad son lo suficientemente altos, se enviará un correo electrónico o un mensaje de pager de advertencia a los miembros del

equipo de seguridad para que ellos puedan investigar la naturaleza de la anomalía.

Los IDSes basados en la red se han vuelto muy populares a medida en que la Internet ha crecido en tamaño y tráfico. Los IDSes que son capaces de escanear grandes volúmenes de actividad en la red y exitosamente etiquetar transmisiones sospechosas, son bien recibidos dentro de la industria de seguridad. Debido a la inseguridad inherente de los protocolos TCP/IP, se ha vuelto imperativo desarrollar escaners, huzmeadores y otras herramientas de auditoria y detección para así prevenir violaciones de seguridad por actividades maliciosas en la red, tales como:

- Engaño de direcciones IP (IP Spoofing)
- Ataques de rechazo de servicio (DoS)
- Envenenamiento de caché arp
- Corrupción de nombres DNS
- Ataques de hombre en el medio

La mayoría de los IDSes basados en la red requieren que el dispositivo de red del sistema host sea configurado a modo *promiscuo*, lo cual permite al dispositivo capturar *todos* los paquetes que pasan por la red. El modo promiscuo puede ser configurado a través del comando ifconfig, tal como sigue:

ifconfig eth0 promisc

Al ejecutar ifconfig sin ninguna opción revela que eth0 está ahora en modo promiscuo(PROMISC).

Una vez digitados estos comandos en Linux obtenemos la siguiente ventana:

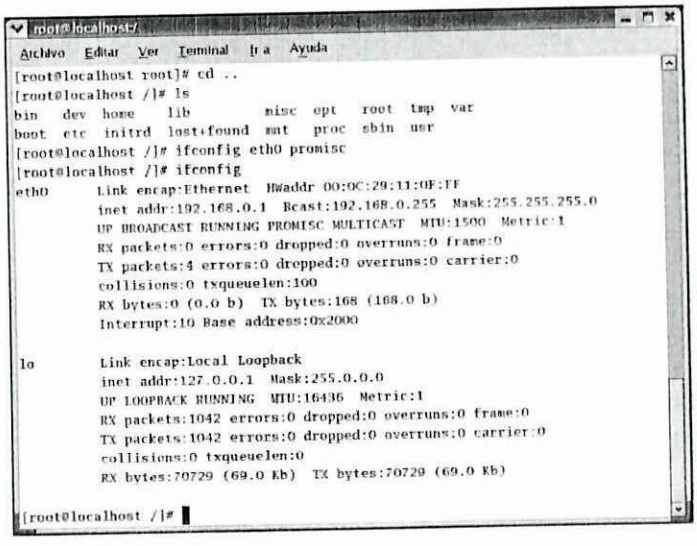


Gráfico 2.1: Salida del test hacia una tarjeta de red en Linux
Fuente: Grupo Investigador

2.2. Metodologías a ser aplicadas para el aseguramiento del sistema de red

La metodología a seguir en el estudio del caso del Servidor Proxy Inverso, está basado en el documento de la Norma ISO IEC 17799, del Código de Practica para la Administración de la seguridad de la Información. TECNOLOGIA INFORMATICA.

La ISO para la infraestructura de la Seguridad de la información manifiesta:

Administrar la seguridad de la información dentro de la organización. Debe establecerse un marco gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización

Deben establecerse adecuados foros de gestión liderados por niveles gerenciales, a fin de aprobar la política de seguridad de la información, asignar funciones de seguridad y coordinar la implementación de la seguridad en toda la organización. Si resulta necesario se debe establecer y hacer accesible dentro de la organización, una fuente de asesoramiento especializado en materia de seguridad de la información. Deben desarrollarse contactos con especialistas externos en materia de seguridad para estar al corriente de las tendencias de la industria, monitorear estándares y métodos de evaluación y proveer puntos de enlace adecuados al afrontar incidentes de seguridad. Se debe alentar la aplicación de un enfoque multidisciplinario de la seguridad de la información, por ej., comprometiendo la cooperación y colaboración de gerentes, usuarios, administradores, diseñadores de aplicaciones, auditores y personal de seguridad, y expertos en áreas como seguros y administración de riesgos.

Conclusión:

De acuerdo a las entrevistas realizadas con las personas encargadas de la administración de las redes en los distintos departamentos de sistemas pudimos concluir que en ningún caso existe una persona que se encargue de la seguridad de la información sino que más bien el administrador de los servidores se encarga tanto de las bases de Datos como de la seguridad de los DMZ en

general, causando de está manera que la información pueda ser alterada tanto interna como externamente.

En la Dirección de Servicios Informáticos de la Universidad Técnica de Cotopaxi se pudo observar que la red principal no cuenta con ninguna seguridad física como servidor de firewall local aunque lo destacable era la implementación de un IDS el mismo que hacia las veces de servidor Proxy para la distribución de Internet y a la vez de Firewall externo el mismo que precautela la información como los DMZ y el escolástico de la Universidad.

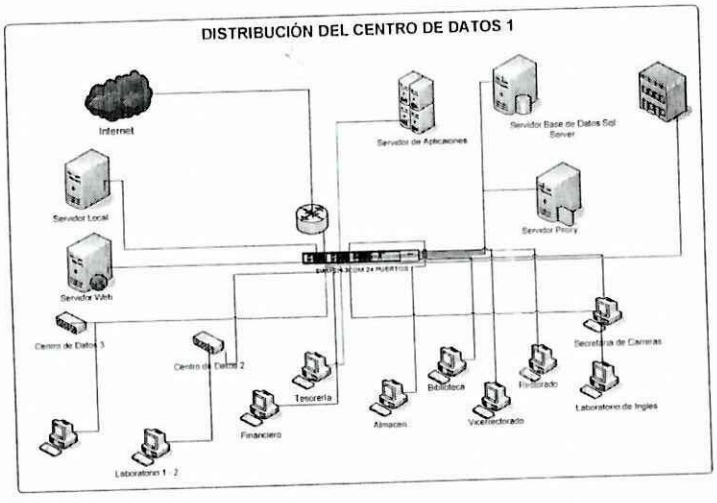


Gráfico 2.2: Distribución del Centro de Datos UTC - 2007
Fuente: Grupo Investigador

Como muestra la grafica todo se encuentra centralizado de manera que la administración se lo puede hacer desde un servidor de dominios el cual comparte recursos y provee servicios a todos los usuarios de la red.

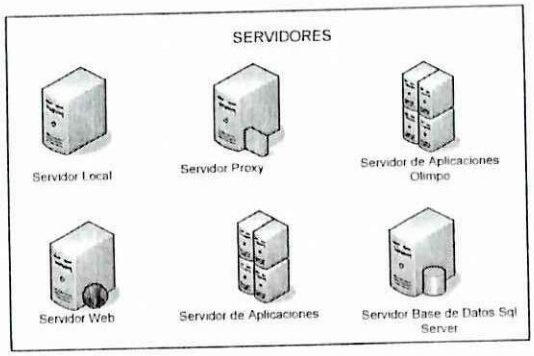


Gráfico 2.3: Especificación de Servidores del Centro de Datos UTC - 2007
Fuente: Grupo Investigador

De igual manera en nuestra investigación realizada al Departamento de Tecnologías de la Información y las Comunicaciones de la Escuela Politécnica del Ejercito sede Latacunga, se pudo observar que cuenta con algunas seguridades tanto físicas como lógicas las cuales precautelan la información de posibles amenazas tanto internas como externas.

Adicionalmente nos facilitaron algunos de sus esquemas de red los mismos que dejan ver el grado de seguridad con el que cuenta está institución.

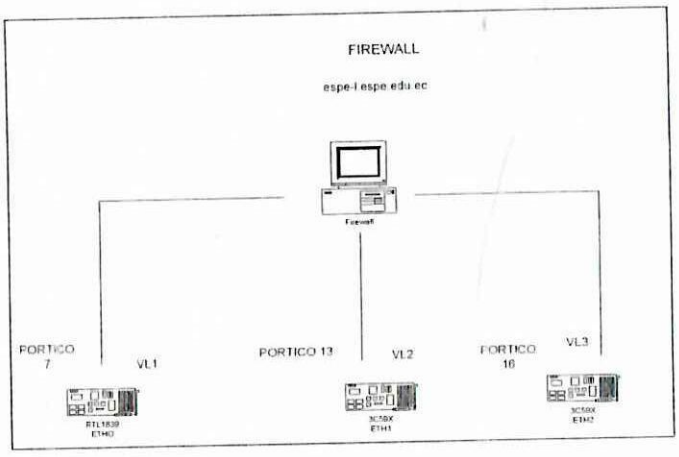


Gráfico 2.4: Diseño del esquema de Firewall ESPEL - 2007
Fuente: Grupo Investigador

La intranet de igual manera se encarga de brindar servicios a distintos estamentos de está institución

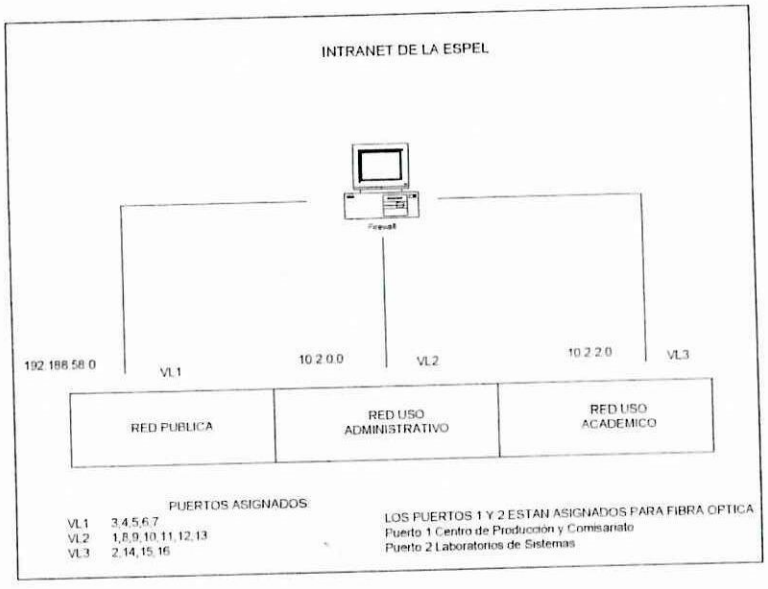


Gráfico 2.5: Diseño del esquema de Intranet de la ESPEL - 2007
Fuente: Grupo Investigador

Como se pudio observar en las diferentes graficas la realidad es distinta en los dos casos tanto en la UTC como en la ESPE, los dos cuentan con seguridades fisicas y lógicas pero en ningún caso han invertido su tiempo y dinero en comprar un servidor que pueda hacer de Proxy inverso el cual vendría a facilitar el trabajo de las dos instituciones ya que garantizaría el flujo de la información y brindaría las seguridades a todos los usuarios de red.

2.3. Logros e Insuficiencias observadas en el sistema actual

De los resultados obtenidos en las entrevistas realizadas a los administradores de las redes hemos podido notar que los esquemas tentativos de redes no soportarían la inclusión de nuevas reglas de configuración de servidores, adoptando de está manera

nuevo hardware para proporcionar seguridades en sus respectivas redes, esto es valido pero la inversión es bastante alta y requiere de una constante capacitación y sobre todo soporte de parte de las empresas suministradoras de este tipo de hardware.

Es importante manifestar que en un sistema podríamos clasificarlo de dos modos, activa preventiva. La seguridad activa de un sistema consiste en protegerlo todo lo posible ante potenciales intentos de abuso del mismo. Un firewall es un buen ejemplo de seguridad activa, trata de filtrar el acceso a ciertos servicios en determinadas conexiones para evitar el intento de forzamiento desde alguno de ellos.

Por otro lado, la seguridad preventiva es aquella que implantamos en nuestro sistema para que nos informe si en el está teniendo lugar una incidencia de seguridad. No pretende proteger el sistema, pretende alertarnos de que algo extraño esta sucediendo en el. Un buen ejemplo de seguridad preventiva es un sistema de detección de intrusos.

Un sistema de detección de intrusos es aquel que nos permite recabar información de distintas fuentes del sistema en el que se implanta para alertar de un posible intrusión en nuestras redes o máquinas. La alerta puede ser del hecho de que existe un intento de intrusión, como del modo en el que este se está realizando y en algunos casos por parte de quén esta siendo efectuado. Podemos considerar un sistema de detección de intrusos como un *control de auditoría* que nos permitirá tomar decisiones a la hora de realizar una auditoría de seguridad de nuestro sistema.

Un sistema de detección de intrusos surge como una medida preventiva, nunca como una medida para asegurar nuestros sistemas, ayudan al administrador de dicho sistema a permanecer al tanto de cualquier intención aviesa contra el sistema que administra

Este es el caso de la Universidad Técnica de Cotopaxi el cual adquirió el IDS para precautelar su información de potenciales ataques externos, pero internamente no lo protege, para este caso el Administrador de la Red nos manifiesta que se repartieron en VLAN (Virtual Local Area Network), y de está manera cada una de las secciones de la Universidad se encuentran asignadas en distintas redes.

2.4. Análisis de los resultados obtenidos de las fuentes de información primaria, criterios de los docentes y estudiantes

Para nuestro trabajo de investigación se tomo el criterio de 2 señores docentes de la Carrera de Ciencias de la Ingeniería y Aplicadas de la Universidad Técnica de Cotopaxi así como de un estudiante de la misma carrera y que cursaba el último nivel, las preguntas en los 3 casos fueron las mismas y sus respuestas están detalladas a continuación, para lo cual se les abrevio de la siguiente manera:

Docente 1	D1	Ing. Patricio Navas
Docente 2	D2	Ing. Juan Rodríguez
Estudiante 1	E1	Sr. Vinicio López

¿A escuchado hablar de un Proxy Inverso?

D1: Si, son servidores que permiten distribuir información, así como recursos de Internet pero con la particularidad de que se lo realiza de manera segura ya que actúa como un firewall, también consta de un cache el mismo que ayuda para que las páginas web que ya han sido previsitadas solamente con llamarlas se carguen inmediatamente.

D2: Un Proxy es un servidor que sirve para compartir recursos en una red, tales como el Internet, un Proxy inverso tiene la misma capacidad pero no conozco del funcionamiento de un Proxy inverso a ciencia cierta.

E1: Es un programa que comparte recursos de Internet ya que este comparte el ancho de banda en la misma proporción a la red, y a todos los usuarios.

¿Qué tipos de seguridades conoce a nivel de servidores?

D1: A nivel de servidores se puede configurar un servidor Firewall, ahora ya tanto en Linux como en Windows incluso Windows ya viene preinstalado un firewall el cual brinda seguridades para que otros usuarios de la red no puedan acceder a un equipo personal, en Linux el firewall viene como parte del sistema operativo pero hay que ponerle algunas reglas propias de una empresa o institución, de igual manera se puede configurar unos IDS o IPS para evitar el acceso de hackers a nuestra red, pero la tendencia ha sido ir buscando seguridades mediante hardware ya que por estabilidad como que resulta mucho más cómodo para todos los administradores.

D2: Existen Firewalls en los dos sistemas operativos los cuales son administrables, ahora ya están como parte de la instalación.

E1: He tenido la oportunidad de observar la configuración del firewall a nivel de sistemas operativos Microsoft, he visto que en Linux en la instalación pregunta si desea instalar un firewall, es lo único que podría manifestar.

¿Qué servidores WEB conoce y que le parece su funcionamiento?

D1: El de Microsoft el Internet Information Server, que se configura mediante asistentes y las seguridades son propios del Sistema Operativo, y que mejorar las seguridades hay que recurrir al ISA Server que tiene un costo adicional que resulta bastante caro.

El Apache de Linux que al igual que cualquier servicio de Linux hay que configurar las reglas las mismas que pueden ofrecer seguridades para filtrar algunas páginas y otras no ya que pueden ser spam o algún tipo de virus informático.

D2: Son dos el Internet Information Server de la Compañía Microsoft y el Apche de Linux los mismos que brindan el recurso de subir páginas WEB, existen en Internet otros tipos pero los mas famosos son los dos.

E1: En Internet existen muchos pero los que he podido ver son el apache y el IIS, que

son de Microsoft y Linux.

¿Qué seguridades existen para prevenir ataques de Internet a través de Paginas Web?

D1: Hoy en día podemos encontrar medios de prevención de ataques a los sitios Web tanto en hardware como en software, en software conozco que existe unas configuraciones que hay que hacerle al Linux tanto al apache como al firewall para que trabaje como un IDS y de igual manera en Windows tendría que instalar el ISA Server que es un paquete que está destinado a prevenir ataques en hardware cada marca está preparada para prevenir los ataques con IPS o IDS o firewall en forma de hardware.

D2: Se lo realiza mediante configuraciones a los servidores tanto en el IIS de Microsoft y al apache en Linux claro que también hay firewalls que impiden el acceso de hackers.

E1: La verdad, pienso que se lo debe poner reglas a los servidores Web, y también los que venden el hosting se encargan de proveer un antivirus y un firewall

CAPITULO III

3. PROPUESTA PARA LA REALIZACIÓN DEL DESARROLLO Y PRUEBAS DEL SERVIDOR PROXY INVERSO

3.1. Diseño y factibilidad de Servidores Proxy

Un **Servidor Intermediario** (Proxy) se define como una computadora o dispositivo que ofrece un servicio de red que consiste en permitir a los clientes realizar conexiones de red indirectas hacia otros servicios de red. Durante el proceso ocurre lo siguiente:

- Cliente se conecta hacia un **Servidor Intermediario** (Proxy).
- Cliente solicita una conexión, fichero u otro recurso disponible en un servidor distinto
- **Servidor Intermediario** (Proxy) proporciona el recurso ya sea conectándose hacia el servidor especificado o sirviendo éste desde un caché.
- En algunos casos el **Servidor Intermediario** (Proxy) puede alterar la solicitud del cliente o bien la respuesta del servidor para diversos propósitos.

Los **Servidores Intermediarios** (Proxies) generalmente se hacen trabajar simultáneamente como muro cortafuegos operando en el **Nivel de Red**, actuando como filtro de paquetes, como en el caso de **iptables**, o bien operando en el

Nivel de Aplicación, controlando diversos servicios, como es el caso de **TCP Wrapper**. Dependiendo del contexto, el muro cortafuegos también se conoce como **BPD** o Border Protection Device o simplemente **filtro de paquetes**.

Una aplicación común de los **Servidores Intermediarios** (Proxies) es funcionar como caché de contenido de Red (principalmente HTTP), proporcionando en la proximidad de los clientes un caché de páginas y ficheros disponibles a través de la Red en servidores HTTP remotos, permitiendo a los clientes de la red local acceder hacia éstos de forma más rápida y confiable.

Cuando se recibe una petición para un recurso de Red especificado en un **URL** (Uniform Resource Locator) el **Servidor Intermediario** busca el resultado del **URL** dentro del caché. Si éste es encontrado, el **Servidor Intermediario** responde al cliente proporcionado inmediatamente el contenido solicitado. Si el contenido solicitado no estuviera disponible en el caché, el **Servidor Intermediario** lo traerá desde servidor remoto, entregándolo al cliente que lo solicitó y guardando una copia en el caché. El contenido en el caché es eliminado luego a través de un algoritmo de expiración de acuerdo a la antigüedad, tamaño e historial de **respuestas a solicitudes** (hits) (ejemplos: **LRU**, **LFUDA** y **GDSF**).

Los **Servidores Intermediarios** para contenido de Red (Web Proxies) también pueden actuar como filtros del contenido servido, aplicando políticas de censura de acuerdo a criterios arbitrarios.

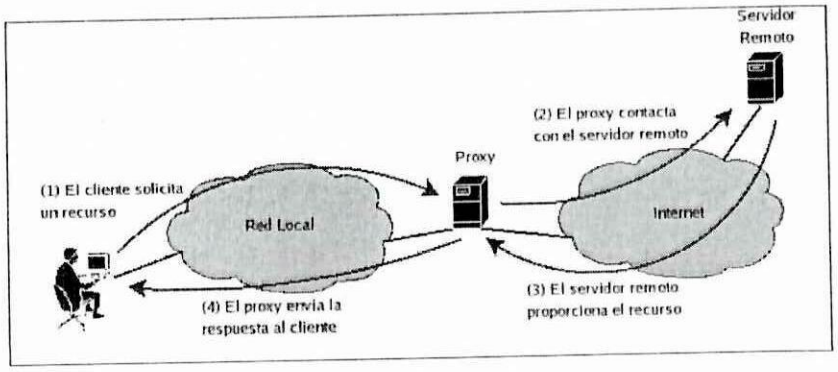


Figura 3.1: Diseño de un Proxy
Fuente: www.linuxparatodos.com

3.1.1. Tipos de Proxy

Dentro de los Proxy tenemos claramente identificados 3 tipos de servidores que son:

WEB PROXY CACHE

Se dice que un servidor esta actuado como Web Proxy cache cuando almacena en su disco duro las páginas Web descargadas de forma que, en próximas consultas, pueda acceder a ellas de forma muy rápida. De está forma estamos optimizando el canal de acceso a Internet de la organización del usuario en momentos de ocupación importante de la línea.

Este tipo de Proxy se suele usar en alguno de estos entornos:

- Cuando por motivos de seguridad, no deseas permitir acceso libre a Internet a los usuarios pero se desea proporcionarles acceso a la Web, se les proporciona a través del Proxy.

- Cunado se desea optimizar el ancho de banda y acelerar la navegación para los usuarios por ejemplo, una oficina con muchos trabajadores que sueles visitar frecuentemente las mismas páginas.

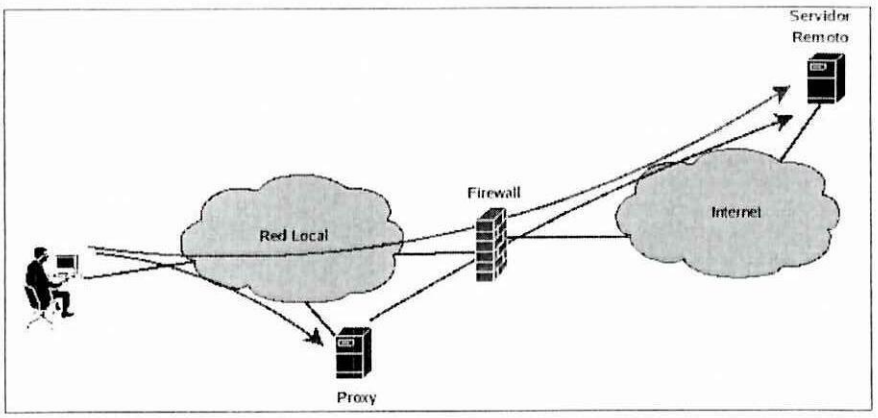


Figura 3.2: Diseño de un Web Proxy Cache
Fuente: www.linuxparatodos.com

Proxy Inverso

Un Proxy inverso (o *reverse proxy*) es aquel que se sitúa cerca de uno o mas servidores Web, de forma que es el Proxy quien recibe las peticiones y las reenvía a los servidores Web. Este tipo de Proxy se suele usar en algunos de estos entornos:

- Para añadir seguridad a los servidores web, en nungun momento se accede directamente a ellos sino al Proxy
- Para balancear la carga de los servidores: el servidor Proxy es el encargado de enviar las peticiones a aquellos a servidores que esdten más descargados
- Para descargar a los servidores webs de contenido estático como imágenes o documentos

- En caso de sitios webs seguros se puede dejar al Proxy que haga el encriptado de los datos y descargar así a los servidores Web

PROXY TRANSPARENTE

Tal como hemos visto es posible usar un Proxy para aplicar politicas de control de acceso a Internet. Normalmente esa configuración no es transparente: es necesario modificar el cliente para que use el Proxy al acceder a Internet, de forma que es posible que un usuario modifique esa configuración.

Una configuración de Proxy transparente hace que no sea necesaria modificación alguna en las maquinas clientes, eliminando el riesgo de que un usuario modifique dicha configuración a su antojo. El uso de un Proxy transparente combina un servidor Proxy con NAT, de forma que todas las conexiones son encaminadas a través del Proxy sin la intervención de la maquina cliente.

3.1.2. Factibilidad Técnica

El desarrollo de un proyecto en el cual se va a reforzar las seguridades de un departamento de sistemas, es principalmente influenciado por 3 grandes objetivos los mismos que deben ser cumplidos para poder alcanzar la factibilidad técnica:

- Resolver un problema: Esto es cuando ya existe un servidor implementado ya sea para Proxy o firewall y este tiene procesos que ya no satisfacen el desempeño para lo cual fue creado y es necesario hacerles ciertas modificaciones.

- Dar respuesta a directivos: Cuando se hacen modificaciones de tecnología de la información y las comunicaciones y forzosamente es necesario cambiar el sistema de información o hacerle modificaciones que mejore luego aprovechar esta oportunidad ya que, si de por si se va a hacer un cambio de sistema de información se puede hacer el cambio con las nuevas disposiciones legales y con esto seguir siendo competitivo.

- Aprovechar una oportunidad: Un cambio ya sea para ampliar o mejorar el rendimiento económico de la empresa y su competitividad.

Para alcanzar estos objetivos, las empresas emprenden proyectos por una o más de las siguientes razones: capacidad, control, costo, comunicación y competitividad como se lo menciona dentro del Análisis y diseño de Sistemas de Comunicación y Datos.

Capacidad: Las actividades de la empresa están influenciadas por la capacidad de ésta para procesar transacciones con rapidez y eficiencia. Los sistemas de información mejoran esta capacidad en tres formas estas son:

- Aumento de la velocidad de procesamiento.
- Permiten el manejo de un volumen creciente de transacciones.
- Recuperan con rapidez la información.

Control: La falta de comunicación es una fuente común de dificultades que afectan a todos los que laboran en una empresa. Sin embargo, los sistemas de comunicación bien desarrollados tratan de ampliar la comunicación y facilitan la integración de funciones individuales.

Aumento de la comunicación: Muchas empresas aumentan sus vías de comunicación por medios de redes.

Costo: Muchas empresas han desaparecido y muchas otras imposibilitadas para alcanzar el éxito debido al poco control sobre los costos o por el total desconocimiento para el control de estos. Los sistemas de información juegan un papel importante tanto con el control como en la reducción de los costos de operación.

Ventaja competitiva: Los sistemas de información y las comunicaciones son un arma estratégica que puede cambiar la forma en como compite la empresa en el mercado. Los sistemas de información y las comunicaciones mejoran la organización y ayudan a la empresa a ser más competitiva. Por lo contrario si los competidores de la empresa tienen sistemas de información más avanzados, entonces los sistemas de información y comunicación pueden convertirse en una

desventaja competitiva. Por lo tanto las capacidades de los sistemas de información son una consideración importante al formular la estrategia de la empresa.

Una empresa puede ganar ventaja competitiva a través de su sistema de información y comunicación en cuatro formas diferentes que garantizan la competitividad en el mercado estos son: clientes, competidores, proveedores y servicios.

Todo proyecto de sistemas de comunicación debe ser desarrollado bajo las actividades de un grupo de trabajo que se haga responsable del inicio y culminación del sistema de información.

El grupo de trabajo va a depender de tamaño de acuerdo al proyecto que va a desarrollarse.

La seguridad, es un aspecto clave para generar en las empresas y en los consumidores la confianza necesaria para que el comercio electrónico se desarrolle. La necesidad de generar confianza, es especialmente importante debido al hecho de que Internet es una red abierta y a la sensación de inseguridad (quizá a veces excesiva) que este hecho genera en los usuarios.

Sin embargo, la seguridad de la red, en este caso Internet, es solo uno de los factores que intervienen en la seguridad del comercio electrónico en conjunto.

3.1.3. Factibilidad Económica

Cuando escuchamos hablar de seguridades y de compartir recursos como lo es el Internet siempre puede sonar a gastos extremadamente fuertes, pero al tener las empresas e instituciones instalado equipos de ultima generación y en algunos casos configurables como son los casos de las computadores personales que pueden trabajar como servidores, muchas ocasiones pensamos si uno de estos equipos podemos destinar a la utilización de un caso de investigación y estudio como lo es la implementación de servidores Proxy Inverso

Al contar con todo implementado nuestro trabajo y el de los administradores de los departamentos de Sistemas fue de otorgar un servidor de Proxy inverso y de está manera se puede asignar puertos y protocolos que va a servir de enlace entre los servidores y los usuarios de la red, cabe recalcar que siempre es bueno tener más de una tarjeta de red la misma que pueden ser asignadas para cada uno de los recursos.

Lo que se desea llegar es a proporcionar a las empresas una alternativa de Intranet a bajos costos utilizando normas y protocolos de Internet, para permitir a los miembros de una organización comunicarse y colaborar entre si con mayor eficiencia, aumentando la productividad.

La factibilidad económica esta dada por la implementación de un servidor de Proxy inverso que viene a suplantar a los dos corta fuegos(firewall) y un servidor Proxy los mismos que regulan el acceso a la Intranet y el servidor de firewall, con el Proxy Inverso ahorramos en recursos y solamente uno haria este trabajo, como podemos observar en la grafica.

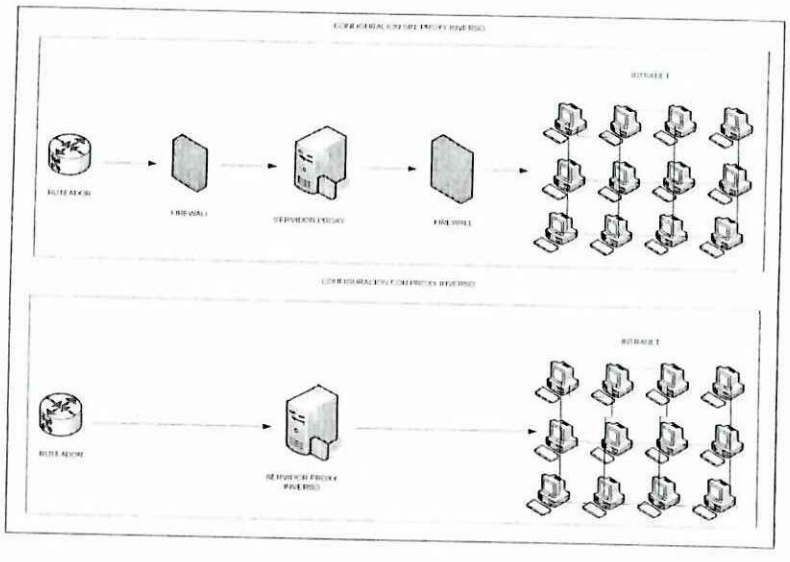


Figura 3.3: Representación Grafica de Factibilidad Económica
Fuente: Grupo Investigador.

3.1.4. Factibilidad Operacional

Un servidor Proxy hace de un portero entre la intranet y el Internet o entre ciertos servidores de archivos y la intranet. Cuando una maquina cliente tiene prohibido solicitar directamente a los servidores en nombre de la maquina cliente. Los servidores Proxy pueden también comprobar el tráfico de entrada. Al igual que en un encaminador, un servidor Proxy verifica las reglas que el administrador ha listado (para ver si el contacto esta autorizado) antes de permitir el paso de trafico.

Los servidores Proxy Inverso tiene su funcionamiento especifico el mismo que está dado por las seguridades tanto de paginas Web, como de Correo Electrónico, cuando se desea realizar un FTP, de igual manera presta las facilidades para la realización de navegación segura mediante las reglas del servidor Apache para las paginas Web, incluye además algunas reglas de Firewall para precautelar la

información que ingresa y sale de las instituciones así como también de la información que es interna de la Intranet.

Los servidores Proxy Inverso también pueden inspeccionar el contenido de un paquete y aceptarlo o rechazarlo, según las reglas del administrador. Así, si un servidor Proxy Inverso para cualquier servicio contiene una regla de negación, este simplemente niega la acción, así de forma general este diga que se lo debe realizar.

Los servidores Proxy Inverso pueden examinar, más cosas que la dirección.

Los intrusos extremos del tipo humano van desde el curioso al maligno y a los individuos motivados por el beneficio económico. En su mayoría, los piratas solían ser estudiosos y experimentados benignos. Los primeros piratas veían el ciberespacio como un lugar público gigantesco de juegos electrónicos y en realidad, más bien como un puzzle absorbente y desafiante. El intento de entrar en un sistema (y salir sin que los atrapasen) era un deporte de competición.
Un intruso puede inyectar un virus o piratear e interceptar, cambiar o robar datos. Y lo hacen. El espionaje industrial es uno de los crímenes informáticos en auge y una vía de ataque.

Todavía hay muchos piratas que pretenden asustar, que se cuelan y miran pero no hacen daño real. Aunque su intrusión es fastidiosa, su principal motivación es la sensación de logro y poder. A su manera, su atención hacia nuestra red puede ser

positiva y puede servir para recordarnos que siempre somos vulnerables y para poner de relieve algunas deficiencias especificas en nuestra protección.

3.2. Distribución de equipos en una Red de acuerdo a puertos y protocolos

La distribución de los distintos equipos en una red estaría dada de acuerdo al tipo de información que manejen los usuarios, de igual manera como se encuentren armados los backbones institucionales o empresariales, ya que esto tiene mucho que ver las comunicaciones entre concentradores y equipos de oficina.

Debemos también mencionar que es muy importante la conexión a Internet ya que a estos recursos todos los usuarios de computador desea ingresar y navegar por este el amplio mundo de la información.

Hoy en día la gente se encuentra inundada de información y a menudo recibía más de la que podría manejar. El diluvio de información, con más revistas que leer, más publicaciones comerciales a mantener, más anuncios, más llamadas telefónicas y más reuniones, se convirtió en la corriente interminable de los bits de información.

Una de las ventajas es la navegación a altas velocidades sin restricción alguna, pero la seguridad en cambio se ve limitada y puede la empresa ser presa fácil de los piratas electrónicos que podrían incluso desde alterar información hasta perjudicar económicamente a una empresa.

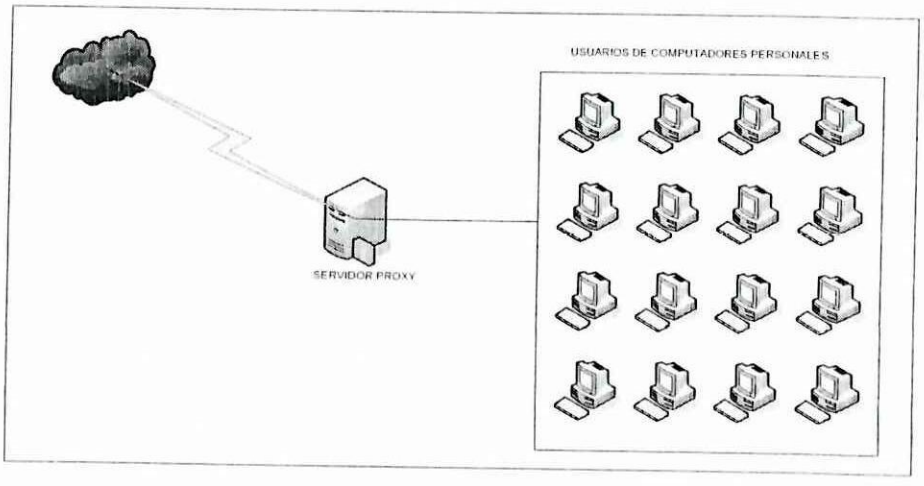


Figura 3.4: Representación Grafica del Acceso Ilimitado a Internet
Fuente: Grupo Investigador

Como se puede observar en la figura 3.3. las conexiones deben permitir al menos un puerto por donde ingresaría el servicio del Internet, a parte de que se necesita de una dirección IP publica para la interconexión con el ISP(Internet Service Provider, Proveedor de Servicios de Internet).

Los puertos a los que se hace referencia serian el *3128*, para el puerto que maneja el Proxy en Linux denominado *SQUID*

El puerto que se le configura en Windows es el *80* o en su defecto *el 8080*.

Las direcciones IP Públicas que también se hace referencia es aquella que provee el ISP, y que tiene que estar en el rango del grupo de direcciones con la que ellos cuentan, ya que estos siempre tienen que verse entre equipos. No tomamos en cuenta las direcciones de la Intranet ya que están dadas de acuerdo a políticas

propias de las empresas o instituciones y mas que todo por el numero de usuarios de redes y hosts.

3.2.1. Switch

SWITCH

En lo que tiene que ver a los concentradores debemos agradecer a la Dirección de Servicios Informáticos de la UTC quien nos facilito la información de los equipos que cuenta:

Switch 3COM OfficeConnect Dual Speed de 16 Puertos

Información del Producto:

Clave de Artículo:	55015	Garantía:	1 año
Modelo del Fabricante:	3C16792A		

Este switch básico y económico acelera las aplicaciones de base de datos, contabilidad y multimedia, así como el intercambio de archivos. Idóneo para servidores de alta velocidad, troncales o estaciones de trabajo de usuarios que requieren un alto rendimiento. O utilice este switch para incrementar más hubs Fast Ethernet a un grupo de trabajo. El Auto MDI-MDIX en cada puerto

simplifica la expansión de red al eliminar los errores de cableado más comunes, tanto si el puerto está conectado a un servidor, a un PC o a otro switch o hub.

Especificaciones

- Con instalación plug-and-play y sin necesidad de configuración, el switch encaja fácilmente en su red sin administración
- El Auto MDI/MDIX en cada puerto simplifica la expansión de red al eliminar los errores de cableado más comunes
- Dieciséis puertos con auto-detección identifican automáticamente la velocidad del dispositivo conectado para maximizar el rendimiento de la red
- Con instalación plug-and-play y sin necesidad de configuración, encaja fácilmente en su red sin administración
- La función full-duplex soporta la transferencia de datos en los dos sentidos, duplicando así el ancho de banda efectivo de la red
- El diseño compacto, sin ventiladores, garantiza un funcionamiento silencioso en espacios de pequeñas oficinas
- Los conectores en la parte trasera ayudan a reducir la acumulación de cables enredados

Especificaciones de producto Puertos totales:

- 16 puertos 10/100 Ethernet con detección automática
- Interfaces con los medios: 10/100BASE-TX/RJ-45

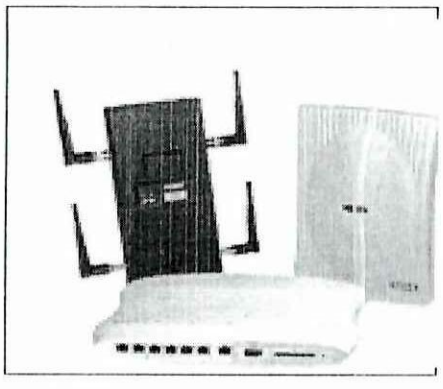
Características de switching Ethernet:

Store-and-forward; autonegociación full/half dúplex

Altura:	54,6 mm
Anchura:	228 mm
Fondo:	185,4 mm

3.2.2. Switch Inalámbrico, Antenas y Access Point

El Switch inalámbrico WS2000 es una poderosa solución integrada que simplifica y reduce los costos de la gestión de redes cableadas e inalámbricas (802.11a/b/g) en sucursales. El dispositivo integra router, puerta de enlace, servidor de seguridad, Power-over-Ethernet (PoE) y otras funciones, se elimina la necesidad de adquirir varios dispositivos y la complejidad de su gestión. La compatibilidad con extensiones Wi-Fi Multimedia (WMM) permite al WS2000 ofrecer el mejor rendimiento incluso en las aplicaciones más complejas con voz y vídeo.



Access Point

Un **punto de acceso inalámbrico** (**WAP** o **AP** por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cableada y los dispositivos inalámbricos. Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming". (Por otro lado, una red donde los dispositivos cliente se administran a sí mismos - sin la necesidad de un punto de acceso - se convierte en una red **ad-hoc**)."Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada".[1]

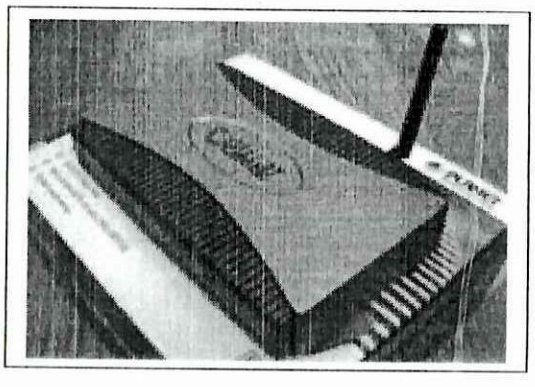


GRAFICO 3.6: ACCES POINT.
FUENTE: HTTP://ES.WIKIPEDIA.ORG/WIKI/PUNTO_DE_ACCESO.

[1] http://www.pucelawireless.net/index.php?pagename=AccessPoint

Características de las tarjetas inalámbricas más utilizadas en la auditoria wireless.

Basándome en la experiencia y los informes presentados por muchos de las personas integrantes del foro gírcles presento esta tabla que recoge algunas de las características que deben ser tenidas en cuenta a la hora de la elección de las mismas para la auditoria wireless. No se pondrá bajo ningún concepto ningún precio ni ninguna dirección donde poder adquirirlas ya que estos datos cambian constantemente y será estudio particular de cada persona en función de sus necesidades y de su economía.

Modelo	Chipset	Win	Lin	Inyección	Antena	Cobertura	Observaciones
AirisV257 mini-pci 11g	Ralink RT2500	No	Si	Lx (??)	No	Buena	Mini PCI
Belkin F5D7050	Ralink RT2570	No	Si	Lx (b/g)	No	Normal	Barata. USB, R. V3
CiscoAironet PCM352	Aironet	airo	Si	No+??	No	Buena	Necesario act. firmware
D-link DWL-510	RTL8180L	airo	Si	Lx (b/g)	Si	Normal	PCI. R A1. RTL = Realtek
Edimax EW-7128g	Ralink RT2500	No	Si	Lx (b/g)	Si	Normal	PCI
Gygabyte GN_WMAG	Atheros	airo	Si	Lx+??	No	**Muy sorda**	PCMCIA -108M
Intellinet 54 Wireless	Ralink RT2500	No	Si	Lx (b/g)	Si	**Sorda**	PCI
IPW 2100 (Portatiles)	Intel Centrino	com	Si	No	No	Muy buena	Mini PCI. Cobertura OK
Linksys WMP54G v2	Broadcom	Si	??	No	No	**Sorda**	Dificil linux-drivers V2
Netgear WG311T (FS)	Atheros A2	??	Si	Lx(b/g)	Si	**Sorda**	Sicodelica
Orinco Gold 8470WD	Atheros	airo/com	Si	Lx(b/g)+CV	Si	Normal	Pcmcia. Pigtail MC-Card
Senao2511cdplusext2	Prism 2.5	No	Si	Lx (b)	No	**Sorda**	Pcmcia. Pigtail MMCX
SMC SMCWPCIT-G	Atheros	airo/com	Si	Lx(b/g)+CV	Si	Buena	PCI. Barata
Zcom XI-32HP+300W	Prism 2.5	No	Si	Lx (b)	Si	Normal	Pcmcia. Pigtail MMCX.

TABLA 3.1: TABLA DE TARJETAS INALÁMBRICAS (ACTUALIZADO A (3-10-06)
FUENTE: HTTP://WWW.SYMBOL.COM.MX/INFO8.HTML

3.2.3. Host

Muchas son hoy en día las personas que se conectan, de una manera u otra, a Internet. Desde empresas que operan en la red con un host hasta personas en sus casas que pasan un rato divertido navegando por sus páginas preferidas, a través de un host o computador personal, los mismos que pueden tener características variadas de acuerdo al gusto y necesidad de los usuarios.

Pero pocas de estas personas entienden realmente las consecuencias que tiene el *abrir* sus sistemas informáticos a Internet, unas consecuencias que no sólo son de carácter benigno e incluso beneficioso. El bien que obtenemos de Internet tiene un precio: **Internet no es un lugar seguro.**

Al igual que en cualquier sociedad, en Internet existen buenas intenciones, ayudas, compañerismo... pero también existen mentes perversas y llenas de maldad. En Internet existen personas decididas a hacer daño, pocas, pero es un hecho que existen, y debemos protegernos de sus acciones, por insignificantes que pensemos que somos.

Es común entre los *navegantes* más o menos habituales de Internet, que nunca han tenido, o mejor dicho, *creen* que nunca han tenido un problema de seguridad en sus sistemas, el pensar que no es probable que lleguen jamás a recibir uno de

estos ataques por el simple hecho de no poseer nada de interés, de no ser nadie importante. Esto es, claramente, **falso**. Cualquiera puede ser presa de un ataque en la Red, cualquiera, por insignificante que se pueda pensar que uno es.

Es precisamente esa sensación de sentirse a salvo la que hace que sea este tipo de gente el que tome, por lo general, las menores precauciones, y por ello, al mismo tiempo, que se conviertan en la presa más apetecible para aquéllos que simplemente desean hacer daño, por el placer de hacerlo.

3.3. Configuración de servidores de acuerdo al Sistema Operativo

A manera de introducción a los sistemas operativos hemos tomado de una lectura realizada en la revista de tecnología el cual manifiesta lo siguiente, valgan los sorprendentes datos recogidos por mí mismo como usuario de un proveedor de servicios Internet (ISP) común en España, detectando los intentos de atacar el puerto TCP 80 (servidor web) de mi ordenador mientras estaba conectado a Internet, puerto que había dejado abierto intencionadamente (aunque, naturalmente, protegiendo mi servidor web) para guardar un log de los ataques que se intentaban llevar a cabo. Los datos son los siguientes:

Fechas: del 19 de Septiembre al 21 de Noviembre de 2001

Promedio de horas de conexión diarias: 1,5 horas.

Intentos de ataque al puerto 80/tcp: **87**[2]

[2] Tomado de la revista peworld, Noviembre del 2007

Lo cual nos da una idea del peligro que corre un usuario cualquiera de Internet que no tome las precauciones mínimas, teniendo en cuenta que soy alguien tan *insignificante* como cualquier otro en la Red y que, de no ser porque deseaba hacer ese estudio, posiblemente no hubiese podido detectar dichos ataques, y por ello seguiría considerándome *seguro*.

Como dato, el 100% de los 87 ataques eran destinados a servidores Microsoft Internet Information Server o Microsoft Personal Web Server sean estos servidores Windows 2003 o Windows XP, aquí es cuando nosotros pensamos en voz alta y manifestamos (afortunadamente yo tengo Apache, el servidor WEB de Linux), y se trataba de intentos de ejecución de *scripts malignos*, de intentos de ejecución de cgi's peligrosos y de explotar algún tipo de *buffer overflow* en parámetros de algunos scripts de estos servidores.

Por tanto, una vez visto que el peligro existe, es la hora de hablar de que siempre es bueno tener a Linux de nuestro lado y todas las bondades que este nos puede brindar, claro siempre es bueno conocer que son Windows y Linux, a continuación detallamos un tanto cada uno de los dos sistemas operativos con sus características más sobresalientes.

Por lo anteriormente expuesto nuestro trabajo es la puesta en práctica de la configuración de Apache con sus respectivas reglas las mismas que son:

Para poder configurar el Apache como servidor Web de Linux ponemos el comando:

Ntsysv

Procedemos a Habilitar la opción del Apache que en este caso es el httpd, así como el named quien es el que va a resolver el nombre del dominio como paso fundamental.

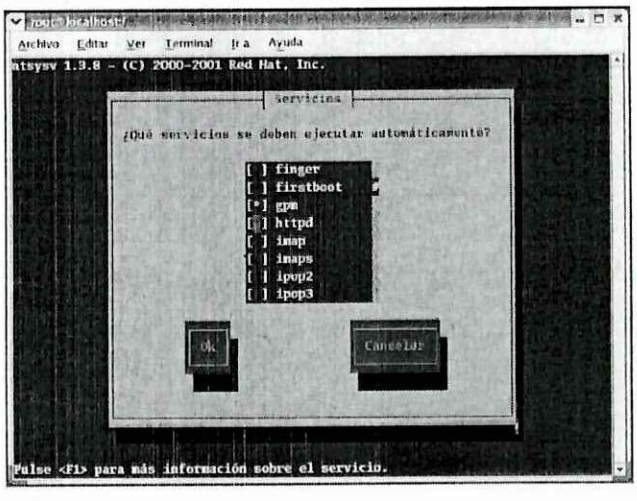


GRAFICO 3.7: configuración del Servidor WEB Apache
FUENTE: Grupo Investigador.

Reiniciamos el servicio del Apache para que aparezca en las configuraciones del sistema de Linux, esto lo realizamos mediante:

Service httpd restart

```
[root@localhost root]#  cd ..
[root@localhost /]# ntsysv
[root@localhost /]# service httpd restart
Parando httpd:                                             [  OK  ]
Iniciando httpd:                                           [  OK  ]
[root@localhost /]# rpm -q httpd
httpd-2.0.40-21
[root@localhost /]#
```

GRAFICO 3.8: Activar el Servidor WEB Apache
FUENTE: Grupo Investigador

Una vez configurado el Apache en el ntsysv procedemos a ver en la red que refleje las tarjetas de red para la asignación de puertos y protocolos.

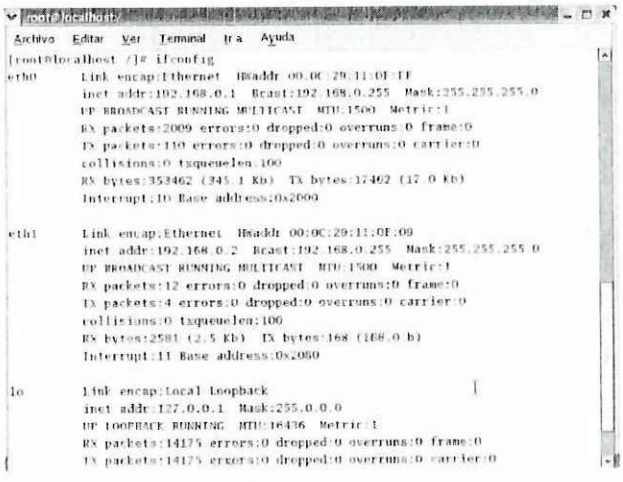


GRAFICO 3.9: Asignación de Ip a las dos tarjetas de red
FUENTE: Grupo Investigador

Los puertos abiertos hasta el momento serian los siguientes:

```
[root@localhost /]# nmap localhost

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1590 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
23/tcp     open        telnet
53/tcp     open        domain
80/tcp     open        http
111/tcp    open        sunrpc
139/tcp    open        netbios-ssn
443/tcp    open        https
631/tcp    open        ipp
953/tcp    open        rndc
3128/tcp   open        squid-http
6000/tcp   open        X11

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
```

GRAFICO 3.10: Asignación de puertos
FUENTE: Grupo Investigador

Como se puede observar en el grafico 3.10 tenemos muchas puertas abiertas lo que genera es que nuestro servidor este totalmente desprotegido, también podemos observar que está habilitado el puerto del Apache que para el Linux es el 80, así también se encuentra habilitado el puerto 443 para el https o paginas que cuentan con certificado digital o SSL (Security Socket Layer).

```
#
#Listen 12.34.56.78:80
# Ponemos estas reglas para que puedan ver paginas WEB nrormales y seguras

Listen 80
Listen 443
#
# Load config files from the config directory "/etc/httpd/conf.d".
#
Include conf.d/*.conf


ServerAdmin root@localhost

#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If this is not set to valid DNS name for your host, server-generated
# redirections will not work.  See also the UseCanonicalName directive.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
# You will have to access it by its address anyway, and this will make
# redirections work in a sensible way.
#
# Ubicamos el nombre del Servidor WEB

ServerName 192.168.0.1
```

GRAFICO 3.11: Asignación de reglas para configuración del Apache
FUENTE: Grupo Investigador

Las reglas arriba declaradas forzan a que se permita observar paginas web normales y las paginas web que tienen algún contenido encriptado.

Una vez configurado el httpd. Conf, mandamos a reiniciar el servicio y por consiguiente si existe un error debería darnos, en caso de no existir nos daría todo Ok. El comando es:

service httpd restart

```
[root@localhost conf]# service httpd restart
Parando httpd:                                             [  OK  ]
Iniciando httpd:                                           [  OK  ]
```

Otra de las comprobaciones es subir una página web la misma que va a llevar un éxito sencillo y todo configurado bajo LINUX.

Las configuraciones de las páginas web se encuentran en una carpeta la misma que va a dar la cara al exterior.

```
[root@localhost /]# ls
bin   dev  home    lib         misc  opt   root  tftpboot  usr
boot  etc  initrd  lost+found  mnt   proc  sbin  tmp       var
[root@localhost /]# cd var
[root@localhost var]# cd www
[root@localhost www]# ls
cgi-bin  error  html  icons  manual
[root@localhost www]# cd html
[root@localhost html]# ls
index.html  index.html~  usage
[root@localhost html]#
```

GRAFICO 3.12: Donde subir una pagina WEB
FUENTE: Grupo Investigador

Con la comprobación de que el servidor Apache se encuentra arriba, debemos probar subir una página Web la misma que se la diseña en HTML para poder mirar todos los datos de un sitio.

GRAFICO 3.13: Página WEB de Prueba
FUENTE: Grupo Investigador

Con está practica estamos subiendo un sitio web que bien se lo podría realizar desde cualquier institución o empresa con la adquisición de una dirección IP publica en lugar de adquirir un hosting, y de esa manera la administración del sitio Web se lo tendría que hacer la empresa que sea la contratista lo que no garantiza nada la información que se pueda publicar.

3.4. Asignación de IP de acuerdo a disponibilidad de equipos con distinta tecnología

La asignación de direcciones IP se lo debe realizar, por medio de un análisis de perfiles los mismos que nos van a dar las actividades que realizan los usuarios de la red. Debemos notar que en una institución de educación por ejemplo lo que mas se quiere es tener un acceso a Internet ilimitado, se tiene comandos propios de linux los mismos que nos ayudan a la administración de todos los recursos de la red, no es recomendable tener activado por ejemplo el DHCP en una red cableada ya que se corre importantes riesgos de alteración de información o intrusiones.

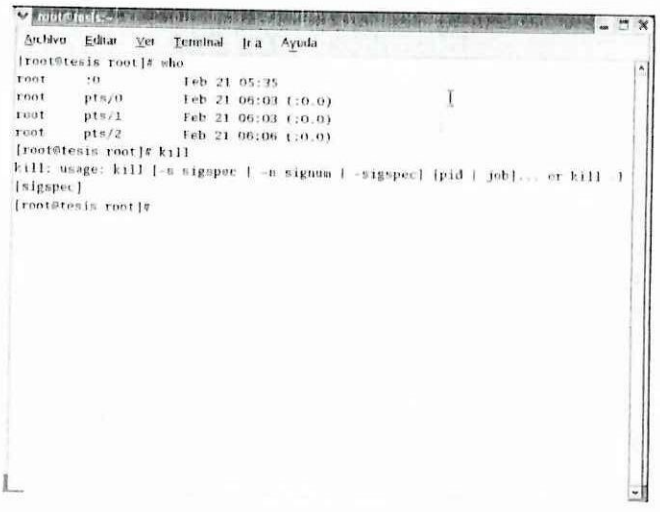


GRAFICO 3.14: Comando de muestra de usuarios de red.
FUENTE: Grupo Investigador

Para compartir recursos con computadores de distintas tecnologías pero que se encuentran en una misma red lo que tenemos que hacer es compartir algunas carpetas mediante el demonio denominado *samba*.

La activación es mediante pasos sencillos que anteriormente ya lo habiamos tenido la oportunidad de observar, como en todo servicio se lo realiza en el ntsysv, como se puede observar:

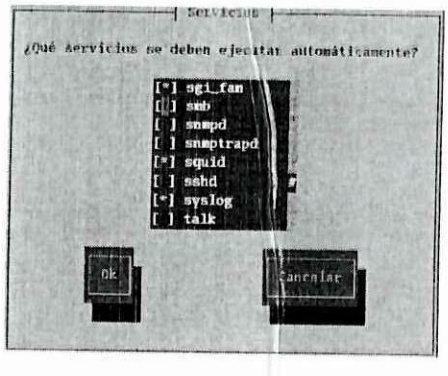


GRAFICO 3.15: Activación del servicio samba (smb).
FUENTE: Grupo Investigador

Una vez iniciado el servicio restauramos el mismo para que entre en funcionamiento, caso contrario debería estar apagado, ya que no ha sido habilitado nunca antes.

```
[root@tesis root]# service smb restart
Apagando los servicios SMB:                                [FALLÓ]
Apagando los servicios NMB:                                [FALLÓ]
Iniciando servicios SMB:                                   [  OK  ]
Iniciando servicios NMB:                                   [  OK  ]
[root@tesis root]#
```

GRAFICO 3.16: Restauración del servicio samba (smb).
FUENTE: Grupo Investigador

Una vez reiniciado el servicio el resto es modo grafico parecido a cualquier sistema operativo de Microsoft por lo que se ha venido haciendo amigable al ojo del usuario.

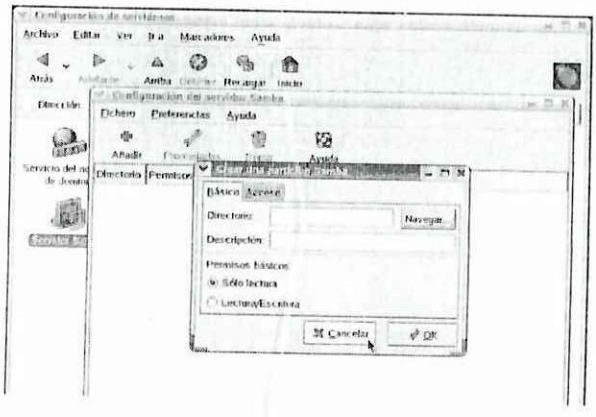


GRAFICO 3.17: Asistente del servicio samba (smb).
FUENTE: Grupo Investigador

3.5. Asignación de flujo de trafico en Internet de acuerdo a perfiles

Las opciones para limitar y acelerar el flujo de tráfico en Internet desde la intranet están dados por las reglas de configuración del firewall y del squid los mismos que están configurados de forma tal que puedan filtrar solamente la información que se desea sea vista por los usuarios de la red.

Hay que tomar en cuenta que los dos procesos tanto el firewall y el squid en Linux conforman una forma de embudo el mismo que forma un Servidor Proxy Inverso.

Las configuraciones del firewall en primer lugar se encuentra igual que todo en el *ntsysv*, donde se habilita las opciones de *iptables*, las mismas que son las reglas que se van a configurar para poder tener acceso a las actividades que se mencionan a lo largo de este trabajo investigativo.

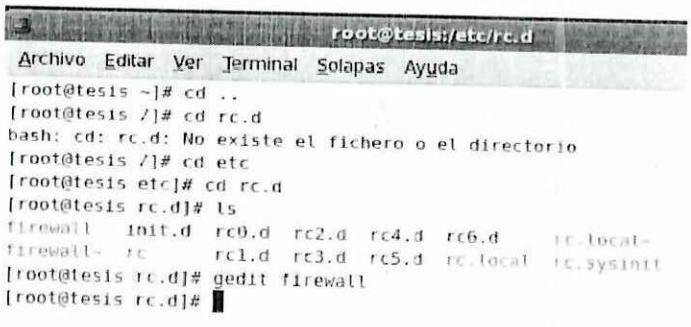


GRAFICO 3.18: Configuración de los Iptables del Firewall.
FUENTE: Grupo Investigador

Una vez realizada esta actividad detallamos el script que tenemos en el archivo firewall el mismo que no consta de extensión alguna ya que solamente es un archivo para levantar las reglas del iptable.

```
#!/bin/sh

## SCRIPT

## Firewall entre red-local e internet con DMZ pero con IPs públicas.

## Grupo Investigador

## Grupo de Tesis Galo Semblantes - Darwin Pacheco



echo -n Aplicando Reglas de Firewall...


## FLUSH de reglas

iptables -F

iptables -X

iptables -Z

iptables -t nat -F


## Establecemos politica por defecto

iptables -P INPUT ACCEPT

iptables -P OUTPUT ACCEPT

iptables -P FORWARD ACCEPT

iptables -t nat -P PREROUTING ACCEPT

iptables -t nat -P POSTROUTING ACCEPT


## Empezamos a filtrar


## Nota: eth0 es el interfaz conectado hacia afuera y eth1 a la LAN
```

```
# El localhost se deja (por ejemplo conexiones locales a mysql)
/sbin/iptables -A INPUT -i lo -j ACCEPT

# Al firewall tenemos acceso desde la red local
iptables -A INPUT -s 192.168.0.0/24 -i eth1 -j ACCEPT

# Ahora hacemos enmascaramiento de la red local
# para que puedan salir hacia fuera y activamos el BIT DE FORWARDING
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE

# Con esto permitimos hacer forward de paquetes en el firewall, o sea
# que otras máquinas puedan salir a traves del firewall.
echo 1 > /proc/sys/net/ipv4/ip_forward

## Permitimos el acceso desde el exterior a los puertos 80 y 443 de DMZ
iptables -A FORWARD -d 192.168.0.2/248 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -d 192.168.0.2/248 -p tcp --dport 443 -j ACCEPT

# El resto, cerrar
iptables -A FORWARD -d 192.168.0.2/248 -j DROP

# El resto, cerrar
iptables -A FORWARD -d 192.168.0.2/248 -j DROP

# Cerramos el acceso de la DMZ a la LAN
iptables -A FORWARD -s 192.168.0.2 -d 192.168.0.0/24 -j DROP

## Y ahora cerramos los accesos indeseados del exterior:
```

```
# Nota: 0.0.0.0/0 significa: cualquier red

# Cerramos el rango de puerto bien conocido
iptables -A INPUT -s 0.0.0.0/0 -p tcp -dport 1:1024 -j DROP
iptables -A INPUT -s 0.0.0.0/0 -p udp -dport 1:1024 -j DROP

# Cerramos un puerto de gestión: webmin
iptables -A INPUT -s 0.0.0.0/0 -p tcp -dport 10000 -j DROP
echo " OK . Verifique que lo que se aplica con: iptables -L -n"

# CERRAMOS EL ACCESO ALGUNOS SITIOS QUE VUELVEN LENTO AL INTERNET

# Red de Audio Galaxy
/sbin/iptables -A FORWARD -d 64.245.58.0/23 -j REJECT

# GNUtella, Bearshare y ToadNode
'sbin/iptables -A FORWARD -p TCP --dport 6346 -j REJECT

# eDonkey
/sbin/iptables -A FORWARD -p tcp --dport 4661:4662 -j REJECT
/sbin/iptables -A FORWARD -p udp --dport 4665 -j REJECT

# Puertos y redes de Kazaa y Morpheus
/sbin/iptables -A FORWARD --dport 1214 -j REJECT
/sbin/iptables -A FORWARD -d 213.248.112.0/24 -j REJECT
/sbin/iptables -A FORWARD -d 206.142.53.0/24 -j REJECT
```

```
# Red de Napigator
/sbin/iptables -A FORWARD -d 209.25.178.0/24 -j REJECT

# Red de Napster
/sbin/iptables -A FORWARD -d 64.124.41.0/24 -j REJECT

# Redes de WinMX
/sbin/iptables -A FORWARD -d 209.61.186.0/24 -j REJECT
/sbin/iptables -A FORWARD -d 64.49.201.0/24 -j REJECT

# Red de IMesh
/sbin/iptables -A FORWARD -d 216.35.208.0/24 -j REJECT

# AIM e ICQ
/sbin/iptables -A FORWARD --dport 9898 -j REJECT
/sbin/iptables -A FORWARD --dport 5190:5193 -j REJECT
/sbin/iptables -A FORWARD -d login.oscar.aol.com -j REJECT
/sbin/iptables -A FORWARD -d login.icq.com -j REJECT

# Jabber
/sbin/iptables -A FORWARD --dport 5222:5223 -j REJECT

# MSN Messenger
/sbin/iptables -A FORWARD -p TCP --dport 1863 -j REJECT
/sbin/iptables -A FORWARD -d 64.4.13.0/24 -j REJECT

# Yahoo! Messenger
/sbin/iptables -A FORWARD -p TCP --dport 5000:5010 -j REJECT
```

```
/sbin/iptables -A FORWARD -d cs.yahoo.com -j REJECT
/sbin/iptables -A FORWARD -b scsa.yahoo.com -j REJECT


# Fin del script
```

Como se puede notar en el script del firewall tenemos algunas reglas que impiden el acceso a algunas páginas que tiene aplicaciones que pueden realizar escaneo de puertos, o a los programas de Chat que son los que limitan el ancho de banda del Internet.

De igual manera el servidor Proxy llamado squid en linux se lo configura mediante reglas las mimas que ayudan a que se ejecuten o limiten algunas páginas de navegación tales como pornografía, entre otras que afectan en alto grado al conocimiento y puede acarrear un virus informático.

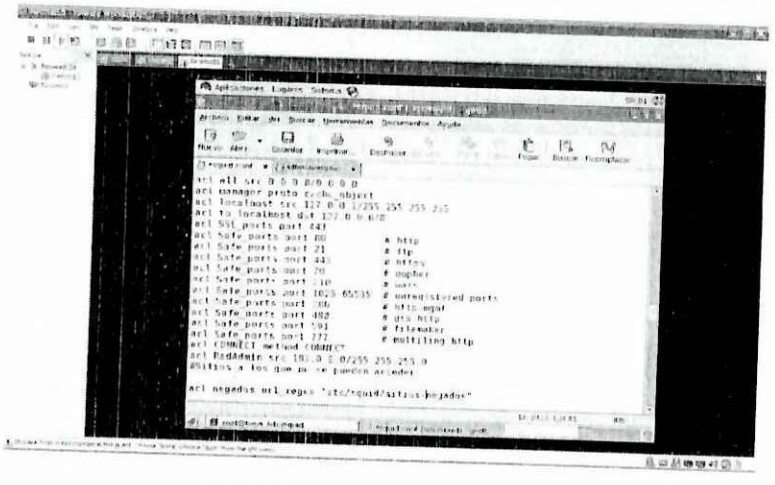


GRAFICO 3.19: Configuración del squid.
FUENTE: Grupo Investigador

Las configuraciones del squid.conf están encaminadas a proveer servicio de Internet a un segmento de red que esta dada por la dirección 192.0.0.0, otra regla manifiesta que todas las direcciones que no son permitidas van al archivo sitios negados, como se puede observar en el grafico 3.20.

GRAFICO 3.20: Configuración del squid.
FUENTE: Grupo Investigador

Una vez concluida las configuraciones de estos 3 servicios importantes del linux podemos manifestar que mediante este servidor de Proxy inverso tenemos garantizada la seguridad de la información.

3.6. Asignación de Ancho de Banda de acuerdo al número de usuarios

Mediante este servidor y con las reglas planteadas tanto en el firewall como en el Proxy podemos concluir que el ancho de banda esta garantizado para todos los usuarios ya que está restringido el acceso a páginas que requieren de mucho ancho de banda.

El servidor de Proxy Inverso a parte de garantizar la seguridad, permite distribuir de manera ordenada la información tanto de subida como de bajada, una de las reglas manifestaba que tengan acceso interno como externo así como permitir hacer una distribución interna, esta regla está dada en el firewall, como se puede observar en el Proxy.

3.7. Controlar de manera eficiente el acceso a la red de parte de los usuarios

Para el acceso de manera eficiente debemos realizar una conexión que bien podría ser Windows hacia linux una vez que determinemos las direcciones del servidor de Linux como se puede observar en el grafico siguiente:

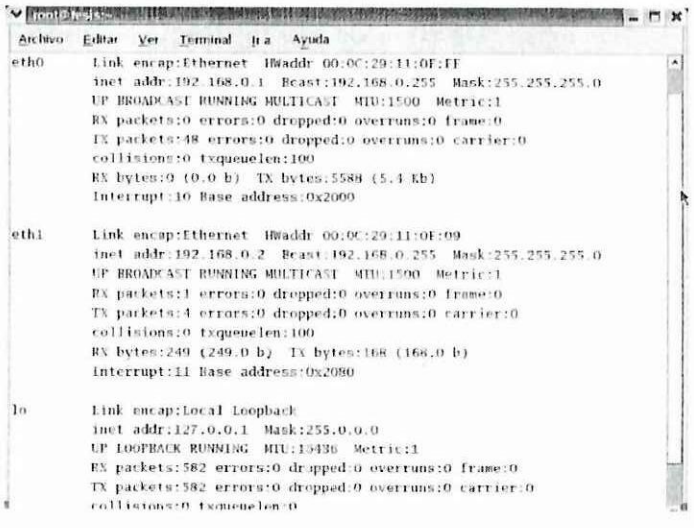


GRAFICO 3.21: Configuración del Acceso a la Red.
FUENTE: Grupo Investigador

Bajo estas configuraciones lo único que queda es configurar en los clientes la red que este dentro de ese rango de direcciones es decir 192.168.0.3 hasta la

dirección 192.168.0.254, ya que como se puede observar la dirección 192.168.0.2 se encuentra reservada en la eth0 y la 192.168.0.2 está reservada en la eth1 para Proxy y para firewall.

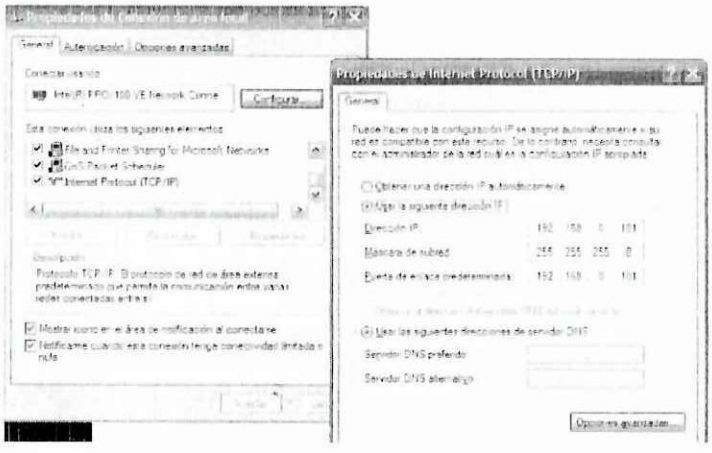


GRAFICO 3.22: Configuración del Acceso a la Red.
FUENTE: Grupo Investigador

Podemos concluir que el acceso a la red está garantizado una vez que se encuentran dentro de la misma clase de red.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Un servidor de Proxy Inverso nos brindan la oportunidad de sacarle el mayor provecho posible a nuestras redes de computadores personales ya que podemos interactuar con otros sistemas operativos, es decir Linux y Windows.

2. Al distribuir de manera ordenada los servidores en uno solo a través de un servidor de Proxy inverso se consiguió mejorar el rendimiento y balancear las cargas del ancho de banda de una red, y con esto hemos conseguido ganar en calidad de servicio.

3. Linux Red Hat 9 es un sistema operativo que nos permite administrar de mejor manera los servicios de una red, permitiendo que los puertos físicos puedan ser abiertos para ciertas actividades.

4. Se debe tomar siempre en cuenta los estándares y normas internacionales para la configuración y administración de ciertos servicios con que cuentan los servidores, ya que de está manera estaremos precautelando la información que se genera en los distintos departamentos.

5. El continuo avance de las tecnologías a influenciado notablemente en la reestructuración de los estándares de la IEEE y de las normas ISO y dentro de estos se ha implementado el Código de Practica para la Administración de la Seguridad de la Información.

6. La norma ISO IEC 17799 manifiesta que la información al igual que el resto de activos de una empresa necesita de todas las seguridades posibles, razón por la cual invita a seguir algunos pasos para cuidar de ésta.

7. Los servidores deben contar con la mayor cantidad de memoria posible, capaz de garantizar un optimo rendimiento de los sistemas operativos que se ejecuten en las maquinas virtuales, así como un espacio en disco que pueda brindar un trabajo holgado al sistema operativo invitado.

8. Mediante la implementación de este proyecto de grado se ha podido brindar una alternativa para evitar la utilización de muchos equipos para solamente brindar seguridades y distribuir el ancho de banda del Internet en una red corporativa.

9. Este trabajo investigativo va a brindar una alternativa de consulta tabto a estudiantes como docentes de la Universidad ya que el contenido a sido un minucioso trabajo de aplicación.

RECOMENDACIONES

1. Un servidor de estas características hay que manejarlo con mucha prudencia, ya que son herramientas que ayudan a la configuración de un solo equipo, tomando las características de muchos servidores en uno solo ya que hemos optimizado tres servidores en uno solo.

2. La adquisición de equipos sean estos servidores o equipos personales se lo debe realizar buscando cumplir con las expectativas de la empresa o institución donde se vaya a implementar el servidor.

3. Los servidores establecidos en toda empresa son los necesarios en la actualidad pero para un futuro se recomienda la investigación de la nueva tecnología ya que trabajos como este ahorran en recursos físicos y económicos.

4. Los estándares aplicados en este proyecto de tesis están siempre en actualización por lo cual no se debe dejar de revisar dichas actualizaciones y aplicar a la institución donde se lo implemente para poder dar un mejor servicio a los usuarios y para mantener un mejor control sobre estos.

5. Para evitar conflictos de incompatibilidad de equipos de red y otros problemas se recomienda se tome como política de equipos con recursos suficientes a fin de evitarnos contratiempos en las configuraciones.

6. Se debe pensar ya en la adquisición de nuevos equipos con al menos tres tarjetas de red para suplir las necesidades existentes en toda institución, así como tener abundante memoria RAM para que el servidor trabaje sin tener que asignar memoria a cada instante para otros recursos.

GLOSARIO DE TÉRMINOS Y SIGLAS

Amplitud de banda

La amplitud de banda especifica la cantidad de datos que pueden transmitirse en una cantidad de tiempo fija. En el caso de los dispositivos digitales, la amplitud de banda se define en bits por segundo (bps) o bytes por segundo.

ASIC

Circuito integrado específico de una aplicación. Chip personalizado diseñado para una aplicación específica.
Asignaciones de amplitud de banda
La cantidad de amplitud de banda asignada a una aplicación, usuario o interfaz específicos.

Capa 2

Capa de vínculo de datos o capa MAC. Contiene la dirección física de un cliente o estación de servidor. El proceso de la capa 2 es más rápido que el de la capa 3 porque hay menos información que deba procesarse.

Capa 4

Establece una conexión y garantiza que todos los datos lleguen a su destino. Los paquetes inspeccionados en el nivel de la capa 4 se analizan y las decisiones se reenvían en función de sus aplicaciones.

Capa MAC

Subcapa de la capa de control de vínculo de datos (DTL).

Class of Service (Clase de servicio)

La clase de servicio es el esquema de prioridad 802.1p. La CoS proporciona un método para asignar etiquetas a los paquetes con información sobre la prioridad. Un valor de CoS situado entre 0 y 7 se agrega al encabezado de la capa 2 de los paquetes, donde cero es la prioridad más baja y siete es la más alta.
Transmisión de superposición de dos o más paquetes que colisionan. Los datos transmitidos no pueden utilizarse, y la sesión se reinicia.

Dirección IP

Dirección del protocolo de Internet. Dirección exclusiva asignada a un dispositivo de red con dos o más LAN o WAN interconectadas.

Dirección MAC

Dirección Media Access Control. La dirección MAC es una dirección específica del hardware que identifica cada nodo de red.

DSCP

DiffServe Code Point (DSCP). DSCP proporciona un método de asignación de etiquetas de paquetes IP con información de prioridad QoS.

Router

Dispositivo que conecta redes separadas. Los routers reenvían paquetes entre dos o más redes. Los routers funcionan al nivel de la Capa 3.

Ethernet

Ethernet se estandariza como IEEE 802.3. Ethernet es el estándar de LAN implementado más común. Admite velocidades de transferencia de datos de Mpbs, compatibles con velocidades de 10, 100 ó 1000 Mbps.

FIFO

Primeras entradas, primeras salidas. Proceso de colocación en cola en el que el primer paquete de la cola es el primer paquete que sale del paquete.
Fragmento
Paquetes Ethernet de tamaño inferior a los 576 bits.

GARP

Protocolo de registro de atributos general. Registra estaciones cliente en un dominio multidifusión.

Gigabit Ethernet

Gigabit Ethernet transmite a 1000 Mbps y es compatible con los estándares Ethernet 10/100 Mbps existentes.

GVRP

Protocolo de registro VLAN GARP. Registra estaciones cliente en una VLAN.

HACKER

Experto informático especialista en entrar en sistemas ajenos sin permiso, generalmente para mostrar la baja seguridad de los mismos o simplemente para demostrar que es capaz de hacerlo.

ICMP

Protocolo de mensajes de control de Internet. Permite a la puerta de enlace o al sistema principal de destino comunicarse con un sistema principal de origen; por ejemplo, para informar sobre un error de proceso.

IEEE

Institute of Electrical and Electronics Engineers. Organización de ingeniería que desarrolla estándares de comunicación y redes.

IEEE 802.1d

Utilizado en el protocolo de árbol extensible, el estándar IEEE 802.1d es compatible con el puente de MAC para evitar bucles de red.

IEEE 802.1p

Prioriza el tráfico de red en la subcapa de vínculo de datos/MAC.

IEEE 802.1Q

Define el funcionamiento de los puentes VLAN que permite definir, hacer funcionar y administrar VLAN dentro de las infraestructuras de LAN con puente.

Mejor esfuerzo

El tráfico se asigna a la cola de prioridad más baja, y no se garantiza la entrega de los paquetes.

Multicast

Transmite copias de un único paquete a varios puertos.

Paquetes

Bloques de información para la transmisión en sistemas de conmutación de paquetes.

Proxy Server

Un Server que se sitúa entre la aplicación cliente, como por ejemplo un web browser, y un Server real. Intercepta todos los requerimientos al Server real para ver si las puede resolver él. Si no, envía el requerimiento al Server real. Los Proxy Server tienen dos propósitos principales.

QoS

Calidad de servicio. QoS permite a los administradores de red decidir qué tráfico de red se reenvía y cómo se reenvía en función de las prioridades, tipos de aplicación y direcciones de origen y destino.

Switch

Filtra y reenvía paquetes entre segmentos de LAN. Los conmutadores admiten cualquier tipo de protocolo de paquetes.

TFTP

Protocolo trivial de transferencia de archivos. Utiliza el protocolo de datos de usuario (UDP) sin características de seguridad para transferir archivos.

Trama

Los paquetes que contienen el encabezado y la información de cola que requiere el medio físico.

Tramas gigantes

Permiten transportar datos idénticos en menos tramas. Las tramas gigantes reducen el coste, necesitan un tiempo de procesamiento inferior y garantizan menos interrupciones.

Velocidad de puerto

Indica la velocidad del puerto. La velocidad de los puertos incluye:

Ethernet 10 Mbps
Fast Ethernet 100 Mbps
Gigabit Ethernet 1000 Mbps

BIBLIOGRAFÍA

- **Andrew Tanenbaum,** Redes de Computadores, Cuarta Edición 2004
- **VLADIMIROV ANDREW A.(2005).** Seguridad de redes Inalámbricas, EDICIONES AMAYA MULTIMEDIA, Madrid, España.
- **ANSI/IEEE Std 802.11, 1999** Edition."Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications"
- **Hills. "Large-Scale Wireless LAN Design"**. IEEE Communications Magazine, vol. 39, nº 11, noviembre 2001.
- **Tyson Creer,** Así son las Intranets, Segunda Edición. 2002
- Building Cisco Multilayer Switched Networks; Cisco System, Cisco Press, 2000.
- Cisco CCNA Exam #640-607; Cisco System, Cisco Press, 2002.
- Implementing Cisco Quality of Service v 2.0; Cisco System, Cisco Press, 2003.

WEB BIBLIOGRAFÍA

- http://informatica.uv.es/doctorado/SST/docto-2-qos.ppt#389,2,Sumario
- http://www.3com.es/news/reportajes/pdfs/switching_comunicaciones_world.pdf
- http://dmi.uib.es/~loren/docencia/webxtel/bibliografia/tutorial%20VLAN.pdf
- http://net21.ucdavis.edu/newvlan.htm
- http://www.itlp.edu.mx/publica/revistas/revista_isc/anteriores/jun99/vlan.html
- http://iie.fing.edu.uy/~rgaglian/Docs/VPLS.pdf
- http://lauca.usach.cl/~lsanchez/Vlan/
- http://www.eduangi.com/documentos/3_CCNA2.pdf
- http://www.avantel.net/~rcruz/Cap3qosrba.pdf
- http://www.lavioleta.net/Capitulo1.htm
- http://www.commlogik.com.ar/cisco.html
- http://www.emagister.com/frame.cfm?id_user=889302005026967485067487070455&id_centro=57953030052957564866666952674548&id_curso=6542504005016

7555457685550674555&url_frame=http://www.emagister.com/public/pdf/comunidad_emagister/01793120043168694849677065484567-config-ciscos.pdf

- http://www.it.iitb.ac.in/~it605/resources/Local/Docs/VLAN/VLANIntro.pdf
- http://www.isa.uniovi.es/docencia/redes/tema4.pdf
- http://www.mythdragon.com/QoS/documents/QoS%20routing%20for%20support%20MM%20apps.pdf
- http://www.alcatel.ch/com/en/appcontent/apl/A0506-Broadband_QoS-ES_tcm172-287901635.pdf
- http://www.adictosaltrabajo.com/linux/proxy.htm
- http://www.adictosaltrabajo.com/linux/proxyinverso.htm
- http://www.adictosaltrabajo.com/linux/firewall.htm
- http://www.adictosaltrabajo.com/linux/cortafuegos.htm
- http://www.monografias.com/proxy.htm
- http://www.monografias.com/firewall.htm
- http://www.cudi.edu.mx/primavera_2005/presentaciones/felipe_alvarez.pdf
- http://www.si.uji.es/bin/ponencies/ipp.pdf
- http://www.idg.es/comunicaciones/especial-avether160/Pag08.pdf
- http://www.iec.uia.mx/proy/titulacion/proy14/vpnprin.htm

ANEXOS

1.- SELECCIÓN Y DELIMITACIÓN DEL TEMA

En la actualidad podemos observar el continuo avance de la tecnología a nivel local y mundial, nos damos cuenta que uno de los recursos más importantes dentro de las redes de telecomunicaciones es la implementación de seguridades bajo estándares, ya que este es el medio por donde va a circular el recurso más importante de las organizaciones como es la información, permitiendo obtener mejoras significativas para el buen desempeño de las instituciones tanto publicas como privadas; ya que gracias a la implementación de seguridades se han logrado optimizar recursos técnicos, humanos y financieros de esta manera proporcionan a los usuarios tener acceso a la información en tiempo real y en forma segura en cualquier lugar dentro de la organización.

En cuanto al desarrollo tecnológico del país éste recurso se ha visto diezmado ya que a pesar nuestro, tenemos un insipiente avance y se encuentra en la lista de las naciones tercermundistas, sin embargo con la tecnología con la que cuenta no a permitido realizar nuevas aplicaciones de redes que sean de gran utilidad para el buen desenvolvimiento de las instituciones que se encuentran en nuestro alrededor y así como empresas en particular, por lo que existe la necesidad de integrar algunos estándares para mejorar la calidad de servicio para satisfacer un número mayor de usuarios en la red

Las instituciones de la localidad consideran que una implementación de seguridades en la red es de gran importancia tanto para precautelar el bien más preciado de toda empresa o institución que es la información o también para la enseñanza de los futuros profesionales; es por ello que mediante la implementación de un servidor Proxy de forma inversa podemos brindar una alternativa a las seguridades a la red de la instituciones de nuestra ciudad y provincia, se podrá optimizar de mejor manera un servicio de calidad hacia la comunidad en general de una manera óptima y eficiente.

A lo expuesto anteriormente y ante la necesidad existente de mejorar la funcionalidad de las redes de comunicación de las instituciones nuestro grupo se plantea un tema nuevo como lo es **DESARROLLO DE UN SERVIDOR PROXY INVERSO** mismo que será de gran utilidad para el buen desempeño y la buena administración de la información mediante la utilización de "NORMAS Y ESTANDARES" que garantizara el flujo de la información que circula a través de la red.

2.- PLANTEAMIENTO DEL PROBLEMA

Muchas empresas de la provincia y del país, siempre está buscando el bienestar y satisfacción de las personas que en ella laboran, es por eso que conjuntamente con las personas que imparten cátedra universitaria en el área de sistemas hemos visto la oportunidad de realizar el desarrollo de un servidor Proxy inverso; ya que al no contar con la misma, no garantiza a los usuarios acceder a la información y recursos de la red en tiempo real

de manera segura, causando las denominadas interferencias, falta de confiabilidad en la información, falta de control en la integridad que ocasionan el malestar generalizado de los usuarios de la red.

Las instituciones al no contar con las seguridades en las red a llevado a que exista pérdida y alteración de la información, que no exista libertad de movimientos, espacio suficiente causando graves inconvenientes, como la reubicación de las estaciones de trabajo y por ende bloqueo de servidores, cambio de direcciones IP de las maquinas causando conflictos en las redes permitiendo de esa manera la fácil manipulación de los datos provocando daños irreversibles a los administradores de la red inalámbrica en la Institución.

En la gran mayoría de instituciones lo que se acostumbra es a situar al Proxy directamente con el acceso al web, lo que ocasiona es estar más cerca de los crackers, del código malicioso y de los spam o correos no deseados, todo esto podemos resumir con que no contamos con las seguridades ya que no podemos balancear la carga de los servidores, bloquear lo indeseado y cuando se trata de sitios seguros el Proxy inverso se haga cargo del encriptado de los datos.

3.- ENUNCIADO DEL PROBLEMA

Nuestra investigación se basará en un meticuloso proceso de diagnóstico en la que presumimos detectar el problema que surge en la red de muchas dependencias por lo que hemos llegado a determinar lo siguiente:

¿Cómo el servidor Proxy inverso permitirá el control de tráfico y calidad de servicio de la red de las instituciones para mejorar el flujo, manejo y seguridad de la información?

¿Con el desarrollo de un servidor de Proxy inverso, se permitirá balancear la carga de ancho de banda, brindar optimas seguridades en las redes de comunicaciones en las empresas de la localidad y ser un aporte investigativo para la Universidad Técnica de Cotopaxi?

4. JUSTIFICACIÓN

En la actualidad podemos observar como la alteración y el robo de la información de muchas empresas o instituciones hace que aparezcan nuevas y modernas tecnologías y claro esto acompañado de una alta inversión en el área tecnológica.

El desarrollar seguridades principalmente en las redes de datos, es y será lo más importante en un ambiente que sea capaz de brindar un servicio de calidad a los usuarios ya que sin tener implementado hardware o software que precautelen la información o el recurso informático estaríamos a expensas a que usuarios ajenos a las instituciones puedan acceder y alterar de alguna manera el bien más preciado que es la información.

El presente grupo de investigación consiente de que en nuestra universidad y en instituciones de la ciudad y provincia existen deficiencias en el área de aseguramiento de calidad de la información planteamos este tema el mismo que va a ser desarrollado mediante la utilización de

Maquinas Virtuales las mismas que pueden ser instaladas en cualquier equipo de computo, llamasen estos servidores o computadores de escritorio o móviles, nuestro trabajo utilizara la plataforma de Linux la misma que brinda muchas ventajas por lo que ha sido adoptado en muchas partes del mundo, cabe mencionar que el Linux es un Sistema Operativo de Código Abierto por lo que cualquier institución incluyendo la universidad podría adoptar nuestro tema de investigación.

Para este trabajo se cuenta con el apoyo de docentes técnicos en el área de Ingeniería en Sistemas de la Universidad Técnica de Cotopaxi, los mismos que pueden aportar con su experiencia en la implementación de seguridades en las redes informáticas, se extraerá información a los administradores del área de redes de algunas instituciones, con el fin de conocer sus posibles falencias en lo que tiene que ver a las seguridades y como balancean sus cargas de ancho de banda en las redes.

Por lo expuesto anteriormente podemos manifestar que nuestro tema es viable, ya que contamos con los conocimientos adquiridos a lo largo de nuestra vida estudiantil en la universidad, en el medio existen algunas instituciones de las cuales podemos obtener mucha información, de igual manera contamos con el recurso tecnológico adecuado para el desarrollo y posteriores pruebas de un Proxy Inverso utilizando a un Sistema Operativo como Linux que es de Código Abierto y es muy accesible para cualquier institución.

5. OBJETIVOS

5.1 OBJETIVO GENERAL

Desarrollar un Servidor Proxy Inverso para controlar las seguridades y balance de carga en las redes, lo que evitará el mal uso de información y mejorara de una manera eficaz y confiable el flujo de información en la red.

5.2 OBJETIVOS ESPECÍFICOS

- Realizar un monitoreo para medir la calidad de servicio en las redes de Área local, que permitan detectar falencias en la red
- Diseñar un sistema proxy que brinde seguridades necesarias a base de estándares en las redes institucionales, para mejorar la calidad de servicio de la información.
- Demostrar que se puede administrar de mejor manera el balance de carga de una red que disponga del servicio de Internet mediante un sistema operativo de Código Abierto

6. MARCO TEÓRICO

6.1 ANTECEDENTES

Las empresas en la actualidad ya no invierten grandes cantidades de dinero en actualizar o mejorar sus procesos, sino que buscan en herramientas de software una alternativa viable para garantizar su bien más preciado que es la información, partiendo de está premisa nuestro tema se hace más importante al momento de ofrecer está alternativa al mercado local, ya que con el desarrollo de un servidor Proxy inverso vamos a garantizar que las empresas ahorren grandes cantidades de dinero y optimizar el espacio físico de las mismas.

BASES TEÓRICAS

Considerando que nuestro objeto de estudió es el desarrollo de seguridades en las redes y la administración de la carga del ancho de banda mediante un servidor Proxy Inverso, fundamentaremos científicamente nuestra investigación citando conceptos y categorías de varios autores.

Según la dirección, http://www.monografias.com/trabajos/redesinalam/proxy.shtml, define **PROXY INVERSO** como: "Un Proxy inverso (o *reverse Proxy*) es aquel que se sitúa cerca de uno o mas servidores web, de forma que es el Proxy quien recibe las peticiones y las reenvía a los servidores web. Este tipo de Proxy se suele usar en algunos de estos entornos:

- Para añadir seguridad a los servidores web: en ningún momento se accede directamente a ellos sino al Proxy.

- Para balancear la carga de los servidores: el servidor Proxy es el encargado de enviar las peticiones a aquellos servidores que estén mas descargados.
- Para descargar a los servidores webs de contenido estático como imágenes o Documentos.
- En caso de sitios webs seguros se puede dejar al Proxy que haga el encriptado de los datos y descargar así a los servidores web. "

De acuerdo a lo expuesto consideramos que, **PROXY INVERSO** es un servidor muy completo y de compleja administración el mismo que nos va a servir para brindar seguridades tanto con usuarios externos como internos.

En cambio la dirección, http://es.wikipedia.org/wiki/Red_inal%C3%AAmbrica, dice que **PROXY INVERSO** es: "Un servidor Proxy se sitúa entre la estación cliente (el usuario) y el acceso a Internet (ADSL, cable, Frame Relay...). El cliente se conecta al servidor Proxy, solicita un recurso de Internet (una conexión, un fichero o cualquier otro recurso) y es el servidor Proxy el encargado de solicitar ese recurso a Internet para proporcionárselo al cliente. La traducción de la palabra inglesa "Proxy" viene a ser "*por poderes*", es decir dejaremos que sea el servidor Proxy el que se conecte a Internet por nosotros.

En algunos casos es posible que el Proxy no se conecte a Internet para obtener el recurso solicitado sino que lo obtenga de una cache. El término *cache* es utilizado en el ámbito informático para designar un conjunto de datos replicando a los originales, residentes en un Almacenamiento remoto: Cuando se accede por primera vez a un dato, se hace una copia en el caché, los accesos siguientes se realizan a dicha copia, haciendo que el tiempo de acceso aparente al dato sea menor."

De acuerdo a esta dirección, **PROXY INVERSO** es un sistema que permite compartir recursos principalmente el Internet con un numero determinado de usuarios que necesitan

de este recurso, Siempre este recurso va a ser adquirido a un ISP sin importar cual sea la conexión

Para la dirección, http://www.netmotionwireless.com/resource/whitepapers/security.aspl **SEGURIDADES EN LAS REDES** son: "Aquella norma IEEE 802.11 que fue diseñada para sustituir a la capa física y MAC de la norma 802.3 (Ethernet), así, la única diferencia entre ambas es la manera en la que los dispositivos acceden a la red, por lo que ambas normas son perfectamente compatibles."

De acuerdo a esta dirección, **SEGURIDADES** son normas que permite corregir errores en el flujo de la información que circula a través de la red permitiendo de esta manera encontrar los errores y corregirlos; por lo tanto se hace necesario la implementación de seguridades en la redes.

En cambio la dirección, http://www.dric.com.mx/seguridad/monitoreo/monitoreo1.php?cat=10 define **SEGURIDADES EN LAS REDES** como: "las tres cuestiones que definen la seguridad resueltas de manera robusta las cuales son: la autentificación, la privacidad, la integridad; es decir más que hablar de la gran regla de la seguridad podemos hablar de una serie de estrategias que, aunque no definidas de forma individual, en su conjunto pueden mantener nuestra red oculta o protegida de ojos ajenos."

Según esta dirección, **SEGURIDADES EN LAS REDES INALAMBRICAS** es aquella en donde se puede plantear una serie de estrategias que aunque no vienen definidas sirven para mantener la red oculta o protegida de ojos ajenos permitiendo a los administradores mantener una seguridad en la red.

Para la dirección, http://www.saulo.net/pub/inv/SegWiFi-art.htm **SEGURIDADES EN LAS REDES INALAMBRICAS** es: "Un aspecto crítico que no se puede descuidar. Debido a que las transmisiones viajan por un medio no seguro, se requieren mecanismos que aseguren la confidencialidad de los datos así como su integridad y autenticidad. El sistema WEP, incluido en la norma IEEE 802.11 para proporcionar seguridad, tiene distintas debilidades que lo hacen no seguro, por lo que deben buscarse alternativas."

De acuerdo a esta dirección, **SEGURIDADES EN LAS REDES INALAMBRICAS** son aquellos aspectos que no se puede descuidar ya que el flujo de la información viaja por medios no confiables, razón por las que hay que buscar nuevas alternativas de seguridad para prestar un mejor servicio de calidad de red inalámbrica a la comunidad Universitaria.

En consecuencia la implementación de seguridades en la red inalámbrica de la Universidad Técnica de Cotopaxi, será de gran importancia ya que el mismo ayudara a solucionar los distintos problemas e inconvenientes por los que ha venido atravesando la Institución y a su vez beneficiara a la comunidad universitaria y a los administradores obteniendo una mejor optimización de recursos, control, manejo y seguridad en el flujo de la información de la red que facilitara a la toma de decisiones.

DEFINICIÓN DE TÉRMINOS BÁSICOS

HOST: Computadora con funciones centralizadas que hace disponibles programas a otras computadoras.

Redes: Las redes en general, consisten en "compartir recursos", y uno de sus objetivo es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a 1000 Km. de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente.

Protocolo: Es un estándar que define el método de comunicación entre computadoras. Esto es el lenguaje y las reglas gramaticales que las computadoras acuerdan usar para entenderse. El protocolo para Internet es conocido como TCP/IP (Transmisión Control Protocol/Internet Protocol).

Redes Inalámbricas: Una red de área local inalámbrica (WLAN) es un sistema de comunicación de datos flexible que puede reemplazar o extender una red de área local cableada (LAN) para ofrecer funcionalidad adicional. Una red de área local cableada tradicional (LAN) envía paquetes de datos desde un equipo a otro a través de cables. Una red de área local inalámbrica (WLAN), por el contrario, depende de ondas de radio para transferir datos. Estos datos son sobrepuestos en una onda de radio por medio de un proceso

denominado modulación, y esta onda portadora, actúa entonces como el medio de transmisión, ocupando el lugar del cable.

Estándares de la Red de área local inalámbrica (WLAN): La promoción de normas que regula la operación de la red de área local inalámbrica se iniciaron con el estándar 802.11, desarrollado en 1997 por el Instituto de Instituto de Ingeniería Eléctrica y Electrónica (IEEE)2. Este estándar base permitió la transmisión de datos hasta 2 Mbps. Con el pasar del tiempo, dicho estándar fue ampliado, a través de extensiones las cuales son reconocidas por la incorporación de una carta al estándar 802.11 original, incluyendo el 802.11a y el 802.11b. A continuación de detallan los diferentes estándares que se relacionan con el 802.11.

Red de infraestructura: En una red de infraestructura, los clientes WLAN se conectan a una red corporativa a través de un punto de acceso inalámbrico y luego operan tal como lo haría un cliente con cableado. La mayoría de las redes de área local inalámbricas corporativas opera en modo de infraestructura y acceden la red cableada para conectarse a las impresoras y servidores de archivos.

Hot Spots: Un Hot Spot ofrece servicio LAN inalámbrico, sin costo o cancelando una tarifa, desde una amplia variedad de sitios públicos de reunión, incluyendo cafeterías y salones en aeropuertos. Existen en la actualidad miles de Hot Spots alrededor del Boletín: Redes de Área Local Inalámbricas mundo y se están incorporando diariamente nuevos puntos de acceso. La utilización de "Hot Spots" exige que su computadora portátil esté

configurada con la tecnología certificada Wi-Fi, de este modo usted puede conectarse con otros productos. Las computadoras con certificación Wi-Fi pueden enviar y recibir datos a cualquier parte dentro del rango de una estación base LAN inalámbrica.

Alianza Wi-Fi: La Alianza Wi-Fi es una asociación internacional sin fines de lucro formada en 1999 para certificar la interoperabilidad de los productos de la red de área local inalámbrica basados en la especificación 802.11 del IEEE.

WEP (*Wired Equivalent Privacy*)**:** Es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11. WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes.

WPA (*Wi-Fi Protected Access*, acceso protegido Wi-Fi)**:** Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

WPA2 (*Wi-Fi Protected Access*, acceso protegido Wi-Fi): es el nuevo estándar del IEEE para proporcionar seguridad en redes WLAN. Se espera que esté concluido todo el proceso de estandarización para mejorar este servicio. Wi-Fi [4] está haciendo una implementación completa del estándar en la especificación WPA2.

Ancho de banda: En conexiones a Internet el ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bites por segundo (BPS), kilobites por segundo (kbps), o megabites por segundo (mps). En general, una conexión con ancho de banda alto es aquella que puede llevar la suficiente información como para sostener la sucesión de imágenes en una presentación de video.

Access Point: Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dan servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada.

Switch Inalámbrico: Redefine los estándares de las redes de clase empresarial, aumentando funcionalidad, seguridad, escalabilidad y administración a un costo total menor. Esta segunda generación inalámbrica contiene un incomparable nivel de control, calidad y manejo en redes inalámbricas. El WS 5000 lo logra gracias a la centralización de la inteligencia, la cual está previamente distribuida a través de las redes inalámbricas vía Access Points. La arquitectura Wireless Switch de esta segunda generación nos entrega un nivel incomparable del control Wireless LAN y la simplicidad de la administración.

Nodo: Generalmente ordenador o punto de una red en el que se producen operaciones de conmutación o similares. Tratándose en este aspecto, cada nodo precisa una conexión, que es

un adaptador, este proporciona un número (en hexadecimal) único en la red para poder distinguir de forma inequívoca el terminal.

Puente: Si se tienen dos Redes de Área Local utilizando los mismos protocolos, éstas pueden ser conectadas entre si por medio de estos dispositivos, de manera que a efectos de los usuarios funcionen como si de una sola se tratase. Lo que utilizan es la dirección MAC de los paquetes que circulan, y si corresponden a otro segmento de red lo envían a él. Pueden dividir grandes redes en subredes de forma que armonicen el tráfico.

Puerto: Nombre genérico de los puntos de conexión en un ordenador. Son típicos los denominados puertos serie y los puertos paralelo, indicando por su nombre que pueden recibir o enviar información bajo una modalidad u otra (en serie o en paralelo). También se utiliza esta terminología para referirse a los puntos en que se conecta la placa base.

RJ_45: Registered Jack _45 Un conectar de 8 alambres utilizado mayormente para conectar computadoras a una red local, especialmente Ethernet. Su apariencia física es muy similar a los utilizados para la conexión de teléfonos de los tipos actuales, que denominan familiarmente como "pinza".

Servidor: Se denomina así al ordenador que se encarga de suministrar lo necesario a una red, dependiendo de cual sea la finalidad de ésta.

TCP-IP: Transmisión Control Protocol-Internet Protocol. Protocolo en el que se basa Internet y que en realidad consiste en dos. El TCP, especializado en fragmentar y recomponer paquetes, e IP para diseccionarlos hasta su destino.

WLAN (*Wireless Local Area Network*): Es un sistema de comunicación de datos inalámbrico flexible muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Las WLAN van adquiriendo importancia en muchos campos, como almacenes o para manufactura, en los que se transmite la información en tiempo real a una Terminal central. También son muy populares en los hogares para compartir el acceso a Internet entre varias computadoras.

Estándar 802.11b: Estándar WLAN para banda de 2.4 Ghz. Soporta 11 Mbps.

Estándar 802.11g: Establece una técnica de modulación adicional para banda de 2.4 Ghz. Propuesta para ofrecer velocidades hasta 54 Mbps.

SWITCH: Es la tecnología más sencilla y económica para mejorar el desempeño de una red muy ocupada.

INTERNET.- Conjunto de millones de computadores conectadas entre si a nivel mundial.

Ondas Electromagnéticas: Son ondas producidas por la oscilación o la aceleración de una carga eléctrica. Las ondas electromagnéticas tienen componentes eléctricos y magnéticos.

La radiación electromagnética se puede ordenar en un espectro que se extiende desde ondas de frecuencias muy elevadas (longitudes de onda pequeñas) hasta frecuencias muy bajas (longitudes de onda altas). La luz visible es sólo una pequeña parte del espectro electromagnético. Por orden creciente de longitudes de onda (orden decreciente de frecuencias), se ha confeccionado una escala denominada espectro electromagnético.

Ondas de Radio: Son el resultado de la aceleración de cargas a través de alambres conductores. Son generados por dispositivos electrónicos.

Microondas: Son ondas de radio de longitud corta también generadas por dispositivos electrónicos, se utilizan en sistemas de radar y para hornos a microondas.

Ondas Infrarrojas: Llamadas también térmicas, llegan hasta la luz visible (el rojo del espectro), se producen por la vibración de los electrones de las capas superiores de ciertos elementos, estas ondas son absorbidas fácilmente por la mayoría de los materiales. La energía infrarroja que absorbe una sustancia aparece como calor, ya que la energía agita los átomos del cuerpo, e incrementa su movimiento de vibración o translación, lo cual da por resultado un aumento de la temperatura.

Ondas Visibles: Son la parte del espectro electro-magnético que puede percibir el ojo humano. La luz se produce por la disposición que guardan los electrones en los átomos y moléculas. Las diferentes longitudes de onda se clasifican en colores que varían desde el violeta el de menor longitud de onda hasta el rojo el de mayor longitud de onda (de 4 a

$7x10^{-7}$). La máxima percepción del ojo humano se produce en la longitud de onda del amarillo-verdoso.

Ondas Ultravioletas: Son aquellas que se producen por vibraciones de mayor frecuencia, producidas por ejemplo en el sol.

Rayos X: Son aquellas cuya fuente más común es la desaceleración de electrones que viajan a altas velocidades (alta energía) al chocar en un bombardeo de un blanco metálico.

Telecomunicaciones: Las aplicaciones de telecomunicaciones contemplan el intercambio de información, tanto entre personas, entre éstas y equipos domésticos y entre equipos y equipos, ya sea dentro de la propia vivienda como desde ésta con el exterior. En este grupo se incluyen todas las infraestructuras necesarias para la comunicación de voz y de datos que nos permiten disfrutar de los servicios de telefonía o de las funciones de distribución de ficheros de texto o multimedia, compartir recursos entre dispositivos, acceder a Internet varios usuarios simultáneamente, etc.

Frecuencia: Repetición de un suceso o acto. fis. En lo movimientos vibratorios y oscilatorios, número de vibraciones oscilaciones que se producen en una unidad de tiempo. El movimiento ondulatorio, número de ondas que pasan por un punto durante una unidad de tiempo. Numero de ciclos por unidad de tiempo de una onda sonora. Se mide en Hz (Herzios). Un Herzio es un ciclo por segundo). La respuesta en frecuencia en las personas suele ir de 20 a 20.000 Hz.

7. HIPÓTESIS

¿El desarrollo de seguridades y la administración del equilibrio de la carga en la red mediante un servidor Proxy inverso desarrollado mediante Linux Red Hat, mejorará las seguridades y la calidad de servicio de las instituciones que dispongan de red en su infraestructura tecnológica?

8. VARIABLES E INDICADORES

8.1 VARIABLE INDEPENDIENTE

El desarrollo de seguridades y la administración del equilibrio de la carga en la red mediante un servidor Proxy inverso desarrollado mediante Linux Red Hat

INDICADORES

_ Pérdida de recursos al momento de brindar los servicios de Internet por falta de equilibrio en la carga en la red

_ Falta de conocimiento por parte de los Administradores del ancho de banda para los distintos usuarios de Internet

_ Existencia de inseguridades en la comunicación de las redes institucionales

8.2 VARIABLE DEPENDIENTE

Mejorar las seguridades y la calidad de servicio de las instituciones que dispongan de red en su infraestructura tecnológica.

.INDICADORES

_ Aplicar protocolos de seguridades adecuados para evitar invasiones de intrusos en la información confidencial.

_ Reconocimiento del ancho de banda por parte de los Administradores para garantizar el flujo de la información

_ Obtención de un mejor control en la administración de la información en las redes

.

9. ESQUEMA DE CONTENIDOS

- Portada
- Pagina de responsabilidad de Autoria
- Certificación del Director de Tesis
- Certificación de la Institución Objeto de investigación.
- Agradecimiento
- Dedicatoria

- índice General
- índice de Cuadros
- índice de Tablas
- Resumen
- Abstrae
- Introducción

Esta tesis comprende de tres capítulos los mismos que fundamentan lo siguiente:

CAPITULO I

FUNDAMENTACIÓN TEÓRICA DE LAS REDES

1.1 HARDWARE DE REDES

1.1.1 Redes de Área Personal

1.1.2 Redes de Área Local

1.1.3 Redes de Área Metropolitana

1.1.4 Interredes

1.2 UTLIZACION DE LAS REDES DE COMPUTADORES

1.2.1 Aplicación de negocios

1.2.2 Aplicaciones Domesticas

1.2.3 Usuarios Móviles

1.3. Tendencia de telecomunicaciones

1.3.1. Definiciones

1.3.2. Unificación de los sistemas

1.3.3. La razón y su importancia

1.3.4. Tecnología de redes de telecomunicaciones

1.3.4.1. Inalámbricas

1.3.4.2. Fijas o alambicas

1.4. Historia de las Redes

1.4.1. Estándares de Calidad de las Redes

1.4.2. Seguridades en la Red Inalámbrica de acuerdo a los estándares

1.4.3. Vulnerabilidades

CAPITULO II

TRABAJO DE CAMPO

ELEMENTOS NECESARIOS PARA LA CONFIGURACIÓN Y FUNCIONAMIENTO DE UN SERVIDOR DE PROXY INVERSO

2.1. Estándares de calidad para el aseguramiento de la calidad en el flujo de información bajo estándares internacionales

2.2 Metodologías a ser aplicada para el aseguramiento del sistema de red.

2.3 Logros o insuficiencias observadas en el sistema actual.

2.4 Análisis de los resultados obtenidos de las fuentes de información primaria, criterios de los docentes y estudiantes.

CAPITULO III

3. PROPUESTA

EJECUCIÓN Y DESARROLLO DE UN SERVIDOR PROXY INVERSO PARA CONTROLAR LAS SEGURIDADES Y BALANCE DE CARGA EN LAS REDES, REALIZANDO EL SEGUIMIENTO, MONITOREO, EVALUACION Y REPARACION.

3.1. Factibilidades y Diseño de Servidores Proxy

3.1.1. Factibilidad Técnica.

3.1.2. Factibilidad Económica.

3.1.3. Factibilidad Operacional.

3.2. Distribución de Equipos en una Red de acuerdo a puertos y Protocolos

3.2.1. Switch

3.2.2. Switch Inalámbricos, Antenas y Access Point.

3.2.3. Host

3.3. Configuración de Servidores de acuerdo al Sistema Operativo.

3.4. Asignación de IP de acuerdo a disponibilidad de equipos con distinta tecnología

3.5. Asignación de flujo de tráfico en Internet de acuerdo a perfiles.

3.6. Asignación de Ancho de Banda de acuerdo al número de usuarios

3.7. Controlar de manera eficiente el acceso a la red de parte de los usuarios

10. POBLACIÓN Y MUESTRA

10.1.- POBLACIÓN

La investigación propuesta se realizará en la Universidad Técnica de Cotopaxi, las encuestas estarán enfocadas a los docentes y estudiantes de la Carrera de Ciencias de la ingeniería y Aplicadas especialidad de Ingeniería en informática y Sistemas Computacionales.

INVOLUCRADOS	CANTIDAD
DOCENTES DE SISTEMAS	15
ESTUDIANTES DE SISTEMAS	550
PROFESIONALES DEL ÁREA DE SISTEMAS	50
PERSONAS EXTERNAS	50

10.2.- MUESTRA

Para obtener una muestra representativa de la población investigada se opto por la muestra no probabilística para los administradores de la red, docentes y probabilística para los estudiantes, de la siguiente manera.

Con relación a los administradores de la red se considero conveniente seleccionar un universo del (100 %).

En el caso de los docentes se aplico a un 100 % para obtener información sobre las dificultades en el rendimiento de las conexiones par la búsqueda de información y la necesidad de elaborar una propuesta que ayude a obtener máximo rendimiento en el sistema.

En relación a los estudiantes de la especialidad de sistemas, se tomo una muestra probabilística estratificada para llegar a establecer el numero de la muestra.

FORMULA:

$$n = \frac{NO^2 Z^2}{(N-1)E^2 + 0^2 Z^2}$$

DONDE:

n = Tamaño de la muestra

N = numero de población

O = 0,5 de varianza

Z = 1,96 Nivel de Confianza

E = 0,06 Error Máximo Admisible

Reemplazando los valores en la formula tenemos:

$$n = \frac{550 * 0.5^2 * 1.96^2}{(550-1)0,06^2+0,5^2*1,96^2}$$

$$n = \frac{550 * 0,25 * 3,8416}{(549)\ 0,0036 + 0,25 * 3,84\ 16}$$

$$n = \frac{528,22}{1,9764 + 0,9604}$$

$$n = \frac{528,22}{2,9368}$$

n= 179,86

CUADRO DE RESUMEN INVOLUCRADOS	POBLACIÓN	MUESTRA
1. ESTUDIANTES	550	179
2. DOCENTES	15	15
3. PROFESIONALES DEL ÁREA DE SISTEMAS	50	50
4. PERSONAS EXTERNAS	50	50
TOTAL	665	294

11. PROCEDIMIENTO METODOLÓGICO.

11.1 TIPO DE INVESTIGACIÓN

Para la realización del estudio de este trabajo se utilizara la investigación descriptiva cuasiexperimental ya que se trata de una Investigación que nos permitirá tener un contacto con la realidad y las fuentes directas que guarden relación con el flujo de la información para el desarrollo de un servidor de Proxy inverso, en la especialidad de Ingeniaria en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi; este análisis nos permitirá desarrollar y presentar nuevos puntos de vista, que nos van a servir como referencia para interpretar los diferentes procesos que se encuentren en la elaboración del proyecto, y para un mejor soporte nos apoyaremos en la investigación bibliográfica.

11.2 MÉTODOS, TÉCNICAS E INSTRUMENTOS

Para la presente investigación se utilizaran los siguientes métodos:

EL Método Científico Hipotético Deductivo para alcanzar los objetivos propuestos; a la vez comprobar la hipótesis planteada, en segundo lugar el método dialéctico permitirá explicar las causalidades y procesos lógicos del problema y de ésta manera conocer su rol significativo y por último para una correcta formulación de la investigación se aplicarán los métodos empíricos que llevara a una correcta formulación de las encuestas, entrevistas y

análisis documental con los cuales se describirán las propiedades permitiendo establecer criterios que nos lleven a un entendimiento claro de las variables y a formular las vías de evolución que faciliten mejorar los procesos para dotar de mayor agilidad al sistema.

11.3 TECNICAS

LECTURA CIENTÍFICA

Está técnica es muy útil para la recopilación de información ya que son datos sustentados por autores que poseen gran experiencia en su ámbito.

LA PERCEPCIÓN

Esta técnica nos permitirá utilizar nuestros órganos sensoriales y receptivos, de manera que podamos percibir actitudes y así tener con claridad el contenido de la información

LA ENTREVISTA

Es una técnica para obtener datos que consisten en un dialogo entre dos personas el entrevistador y el entrevistado, se realizará con el fin de obtener información de parte de éste para la consecución de la investigación

LA ENCUESTA

Para poder aplicar esta técnica se hace uso de cuestionarios adecuados con el fin de recopilar información, nos basaremos en un banco de preguntas que se le entregara a las personas a quienes se les vaya a realizar las encuestas.

NSTRUMENTOS

Para realizar la investigación, utilizaremos varios métodos y técnicas que nos ayudaran a recabar toda la información necesaria para nuestro trabajo.

- Formularios, preguntas semiestructuradas
- Cuestionarios

12. DISEÑO ESTADÍSTICO

En nuestra investigación se tomara como base a los diferentes sectores como estudiantes y docentes de la carrera de ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi.

Para el procesamiento de la información se utilizara la Estadística Descriptiva por cada variable, para la tabulación de las respuestas enmarcados en los cuestionarios, organizados en una matriz de datos, para obtener cuadros de distribución de frecuencias en histogramas

13. RECURSOS

13.1 Humanos.

Director:

Ing. Matius Mendoza

Asesor:

Dr. Edwin Vaca.

Postulantes:

Pacheco Oña Darwin Alonso

Semblantes Soria Galo Anibal.

13.2 Materiales.

Hojas de papel bond

Carpetas

Esferos

Cuadernos

Lápices

Copias de documentos

Tecnológicos.

Uso de maquina

Disketts

CD's

Internet.

Impresora.

Cartuchos de tinta

Escáner.

Flash Memory 1GB

14. PRESUPUESTO

14.1 COSTOS DIRECTOS.

Nomina	Cantidad	Valor/unit	Total
Hojas de papel bond	1200	0.02	24.00
Carpetas	5	0.15	0.75
Esferos	9	0.25	2.25
Cuadernos	2	3.00	6.00
Portaminas	3	1.50	4.50
Uso de maquina	500	0.08	300.00
Disketts	15	0.35	5.25
CD's	3	1.30	3.90.00
Internet.	250	0.70	175.00

Impresiones	1200	0.15	180.00
Cartuchos de tinta	4	25	100.00
Escáner.	20	0.25	5

COSTOS INDIRECTOS.

Nomina	Total
Viáticos.	200.00
Trasporte	100.00
Comidas	150.00

SUB-TOTAL	1642.75
(+) 10% IMPREVISTOS	197.13
COSTO TOTAL DEL PROYECTO	1839.88

16. BIBLIOGRAFÍA

16.1 BÁSICA

http://www.virtual.unal.edu.com

http://manuales.dgsca.unam.mx/webdina/arQuitectura.htm

http://ar.geocities.eom/r niella/Document/t marco.htm

http://www.monografias.com/trabajosll/admicomp/admicomp.shtml

http://www.ual.mx/servicios/ccomputo.html

16.2 CONSULTADAS

DYSON, PETER (1999); Diccionario de Redes; Editorial McGraw-Hffl; Bogotá

RODRÍGUEZ, JORGE (1999); Introducción a las Redes de Área Local; Editorial McGraw-Hill; México.

TENEMBAUM ANDREW S. (1999); Sistemas Operativos Distribuidos; Editorial Prentice Hall; México.

16.3 CITADA

http://www.google.com

http://www.monografias.com/

http://www.maxitrucos.CQm/

http://www.abcdatos.com/

http://www.tutorialesgratis.coni/

16.4 VIRTUAL

PROTOCOLOS Y TECNOLOGÍAS DE RED.

DIRECCIÓN:

http://www.microsoft.ccaiVwindows2000es/advenced/networkingies.htm

http://infase.es/FORMACION/INTERNET/tcpip.html

http://www.redes.upv.es/re 1/transp/t I intro.pdf

http://usuarios.lycos.es/redesyprotocolos/modules.php?name=http

http://usuarios.lycos.es/redes

http://www.geocities.com/Silicon valley/8195/noscs.htm

REDES Y TECNOLOGÍAS

DIRECCIÓN:

http://www. aquioaxaca. com/acerca/rafael. htm

hitp://www. infonomics.net/comella/tmarim. htm

http://wmv. ucm. es/info/multidoc/ multidoc/revista/num9/general/olava. htm

http://www.mec.es http://www.mec.es/redinet2/htm I/

SISTEMAS OPERATIVOS PARA REDES CLIENTE/SERVIDOR

DIRECCIÓN:

http://www.ucpr.edu.com

http://www.mx/publica/tutoriales/redes/lema35.htm

http://www.itlp.edu.com

http://www.geocities.com

CALIDAD DE SERVICIO (QoS)

http://www.Calidad de servicio\Spanish-QOS.htm

http://www.Calidad de servicio\RedIRIS - Modelo de evaluación de QoS para una red de Campus.htm