UNIVERSIDAD AUTONOMA DEL ESTADO DE HIDALGO

INSTITUTO DE CIENCIAS BASICAS E INGENIERIA

“Implementación de una Red Privada Virtual en Presidencia Municipal de Pachuca de Soto Hidalgo.”

Tesis para obtener el Grado de:
Ingeniero en Electrónica y Telecomunicaciones

Presentan:

P.D.I.E.T. Marcos Aurelio Guzmán Vite
P.D.I.E.T. Raúl Ramírez Arzate

Director de Tesis:
M. en C. Arturo Austria Cornejo

Pachuca de Soto, Hidalgo, Mayo de 2008

AGRADECIMIENTOS

Esta tesis representa un parteaguas entre una etapa muy enriquecedora y el camino que el tiempo obliga. En toda la experiencia universitaria y la conclusión del trabajo de tesis, ha habido personas que merecen las gracias porque sin su valiosa aportación no hubiera sido posible este trabajo y también hay quienes las merecen por haber plasmado su huella en mi camino.

Primero y antes que todo, dar gracias a **Dios**, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.

A mis Padres **Emma y Lorenzo**, a quienes agradezco de todo corazón por su amor, cariño y comprensión. En todo momento los llevo conmigo.

Gracias a mi hermana **Edith** por sus comentarios, sugerencias y opiniones. Además de ser una buena amiga eres la mejor compañía para compartir el mismo techo.

A mi tía **Elfa** por brindarme su apoyo incondicional.

A mis **primos Miguel, Juan, Luis, Sergio y Beto**, por su apoyo y compañía.

A **Lupita, Genaro, Jonatán, Edgar, Eulalio lucio, Ramón, Erika, Memo, Miriam, Rafa, Luis y Pedro** por ser unos amigos increíbles y con quienes he compartido muchos momentos que siempre llevaré en mi corazón. Ustedes han enriquecido mi vida con su cariño y su alegría. Gracias por recordarme que hay personas valiosas en el mundo y gracias por estar en el mío.

Agradezco a mi **país** porque espera lo mejor de mí.

Gracias…Raúl

AGRADECIMIENTOS

Ésta tesis simboliza el ultimo esfuerzo de mi carrera, de un paso mas en mi vida y de una futuro que parte de ella…

Agradezco **a Dios** por permitirme llegar hasta este momento tan importante de mi vida y lograr otra meta más en ella.

Gracias a mis padres **Angelina y Aurelio** por su valioso esfuerzo, cariño, comprensión y apoyo sin condiciones ni medida. Gracias por guiarme sobre el buen camino de la educación y de la vida.

Gracias **a mis hermanos Arturo y Lupita** por sus comentarios, sugerencias y opiniones. Además de ser buenos amigos, son la mejor compañía para compartir el mismo techo.

Gracias **a mi amor Gloria** por su apoyo, compresión y amor que me permite sentir poder lograr lo que me proponga. Gracias por escucharme y por tus consejos. Gracias por ser parte de mi vida.

Gracias **a todos mis amigos** que estuvieron conmigo y compartimos tantas aventuras, experiencias, desvelos. Gracias a cada uno por hacer que mi estancia en la Universidad fuera divertida, Rey y Luís, Octavio(Pared), Pablo (Güera), Manuel (Porro), Demetrio (Mosh), Enrique, César (Pepito), Cristian (Nanny), Edgar (Rojo), Marco (Chuntaro), Juan Carlos (Chente), Homero (Comadreja), Oscar (Sayayin).

Gracias…Marcos

AGRADECIMIENTOS

A la **UAEH** por darnos la oportunidad de ser parte de la comunidad universitaria y disfrutar de todos sus servicios e instalaciones.

A los **catedráticos** que influyeron en nosotros, que participaron en nuestro desarrollo profesional durante la carrera, sin su ayuda y conocimientos no estaríamos en donde nos encontramos ahora.

Al **M. en C. Arturo Austria cornejo**, por tener la disponibilidad para asesorarnos y realizar este proyecto de tesis.

A la **Presidencia de Pachuca de soto Hidalgo** por su disposición y facilidades para poder llevar a cabo esta tesis

Gracias…Marcos y Raúl.

RESUMEN

El punto central del trabajo es la implementación de una Red Privada Virtual (VPN) en la Presidencia de Pachuca de Soto Hidalgo, la cual es una red virtual creada dentro de otra red, generalmente Internet, el intercambio efectivo de paquetes y la calidad del servicio son de alta importancia en el manejo de redes virtuales privadas. En este proyecto se muestra las especificaciones y características para implementar la red virtual privada, siendo un tema de actualidad y de gran futuro. Esto con el fin de proveer la configuración por software de la Red Privada Virtual.

En el primer capítulo se hace una definición de conceptos, además de plantear el problema, la justificación, objetivos particulares y objetivo general, así como el estado del arte que es la base teórica sobre la que se basa el escrito, y la cual se rebate en el desarrollo del escrito y que forma parte introductoria del mismo.

En el segundo capítulo se investigan los antecedentes y fundamentos de las redes privadas virtuales, como lo son los protocolos involucrados, el modelo OSI y las comunicaciones entre sus capas, los tipos de redes que existen entre ellas la que se maneja en este proyecto la red privada y su inclusión en la internet.

El tercer capítulo constituye la idea central de la tesis, ya que es la configuración del servidor, que va desde la instalación de los servicios básicos como lo es el directorio activo hasta dar del alta al usuario con los privilegios de conexión remota por medio del servidor de VPN.

En el cuarto capítulo se muestran las configuraciones del cliente VPN en 2 sistemas operativos como Windows y Linux específicamente en Red Hat, se detalla paso a paso su implementación, en este mismo capítulo se implementa una pequeña red local (LAN) con Windows xp configurado como servidor de una red privada virtual de forma sencilla.

En el capítulo cinco se muestra la red física de la Presidencia de Pachuca de Soto Hidalgo, la red general que une con los distintos departamentos de la presidencia, hasta llegar al site de telecomunicaciones de la presidencia, el cual esta equipado con un Contrafuego (Firewall) físico, un servidor lo suficientemente potente para dar servicio las peticiones de los usuarios, routers para ancaminar y dividir áreas dentro de la Presidencia de Pachuca.

La configuración de una VPN es una tarea complicada y requiere que el administrador de una red tenga un nivel alto de conocimientos. Esta tarea se complica aún más si dentro de la organización existen varias subredes (Intranet) con diferentes políticas de seguridad. En este trabajo de tesis se propone configurar por software el servidor que permita facilitar el acceso de los usuarios con privilegios de una forma remota y/o externa vía Internet. El sistema facilitará el trabajo del administrador de redes, y además podrá mostrar los accesos que se estén y/o se hayan realizado dentro de las redes privadas. Este sistema será desarrollado en un ambiente Web con el fin de acceder al mismo desde cualquier navegador de Internet y desde determinada localización.

ABSTRACT

The central point of the work is the implementation of a Private Virtual (VPN) Net in the presidency of Pachuca de Soto Hidalgo, which is a virtual net created inside another net, Internet, the effective exchange of packages and the quality of the service are generally of high importance in the handling of virtual private nets. In this project it is shown the specifications and characteristics to implement the virtual private net, being a topic of present time and of great future. This with the purpose of providing the configuration for software of the Private Virtual Net.

In the first chapter a definition of concepts is made, besides outlining the problem, the justification, particular objectives and general objective, as well as the state of the art that is the theoretical base on which the writing is based, and which is rebutted in the development of the writing and that it is introductory part of the same one.

In the second chapter surrender the antecedents and basics of the private virtual nets they are investigated, as they are it the involved protocols, the pattern OSI and the communications among their layers, the types of nets that exist among them the one that is managed in this project the private net and their inclusion in Internet.

The third chapter constitutes the central chapter of the thesis, since it is the configuration of the servant that he/she goes from the installation of the basic services as it is it the active directory until giving from the high one to the user with the privileges of remote connection by means of the servant of VPN.

In the fourth chapter the client's configurations VPN is shown specifically in 2 operating systems like Windows and Linux in net hat, it is detailed step-by-step its implementation, in this same one surrenders a local (LAN) small net it is implemented with Windows XP configured as servant of a private virtual net in a simple way.

In I surrender him/her five images of the physical net of the Presidency of Pachuca of noble Soto they are shown, the general net that unites with the different departments of the presidency, until arriving to the site of telecommunications of the presidency, the one which this equipped with a physical firewall, a servant the sufficiently potent thing to give service the petitions of the users, routers for to guide and to divide areas inside the presidency Pachuca.

The configuration of a VPN is a complicated task and it requires the administrator of a net to have a high level of knowledge. This task gets complicated even more if inside the organization several sub nets (Intranet) exists with different politicians of security. In this thesis work he/she intends to configure for software the servant that allows to facilitate the access of the users with privileges in a remote and/or external way Internet. The system will facilitate the network administrator's work, and he/she will also be able to show the accesses that you is and/or have been carried out inside the private nets. This system will be developed in an ambient Web with the purpose of consenting to the same one from any navigator of Internet and from certain localization.

INDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

CAPÍTULO I
INTRODUCCIÓN

1.1 Introducción

En la seguridad de las redes es de suma importancia, los contrafuegos (firewalls). Para la implementación de las Redes Privadas Virtuales es necesario conocer algunos conceptos de los cuales han surgido este tipo de aplicaciones, además de plasmar la problemática presentada, los objetivos y finalmente la sugerencia de la solución propuesta para dicha necesidad.

1.2 Planteamiento del problema

La Presidencia de Pachuca de Soto Hidalgo es un organismo del sector público cuyo fin es brindar servicios a la ciudadanía, de lo que más destacan son trámites de actas de nacimiento, actas de matrimonio, cartillas de servicio militar, licencias de funcionamiento para negocios, licencias de construcción y uso de suelo, reporte de infracciones, impuesto predial, entre otros; todos estos servicios mencionados hace aproximadamente cinco años eran proporcionados en diferentes oficinas pero en el mismo edificio de ubicación, es decir, no existía la necesidad de tener acceso a algún reporte, base de datos o simplemente a los servicios de red desde el exterior porque era suficiente una pequeña red local donde se compartiera la información que algún servidor público necesitara o el inmediato traslado a la oficina donde se encontrara con la información requerida. El rápido crecimiento de la población y la necesidad de brindar a la ciudadanía más y mejores servicios llevó al H. Ayuntamiento a repartir el mismo servicio pero ahora desde diferentes ubicaciones quedando esto divido en Secretarías. Actualmente el edificio principal cuenta con 3 de ellas, Secretaría de Administración, Contraloría y General, cinco más están distribuidas en diferentes

instalaciones, la Secretaría de Desarrollo Económico, Servicios Municipales, Tesorería, Seguridad Pública, Tránsito y Protección Civil, Obras Públicas, Desarrollo Urbano y Ecología, y tres dependencias descentralizadas como Sistema DIF Municipal, Instituto Municipal contra las Adicciones e Instituto Municipal de Investigación y Planeación.

Existe una Intranet en el Edificio Principal y las Secretarías que están comunicadas mediante enlace de microondas y en su caso pueden compartir servicios solo con Obras Públicas y Tesorería, las dependencias restantes no cuentan con algún enlace que permita la centralización de la red y la información, es decir, una interconexión que brinde el acceso a la información de la red interna desde un punto externo.

Si un servidor público saliera a algún municipio o nación incluso y necesitara información confidencial de inmediato y de manera segura de algún equipo de la Intranet, no sería posible ya que lamentablemente el servicio de e-mail, chat o correo han sido maleados y estos ya no son seguros. Es interesante pensar en la posibilidad de llevar a cabo un enlace privado que permita no solo lograr la comunicación y el traspaso de información entre secretarías si no ir más allá y establecer una conexión desde cualquier punto del mundo, para esto es necesario diseñar y marcar un proceso de implantación que bien pueda guiar a la configuración y ejecución de éste proyecto.

1.3 Justificación

Todo tipo de personas y organizaciones requieren de metodologías para transmitir o recibir información de forma rápida y eficiente. Además que esta información sea segura y esto ha llevado a idear tecnologías y actualización de las ya existentes con el propósito de satisfacer las necesidades de cada organización y así llevar a cabo una comunicación con otros equipos aprovechando al máximo su capacidad. La Presidencia de Pachuca Soto Hidalgo necesita también una garantía de seguridad en las transferencias de información para evitar que sus datos sean interceptados por personas ajenas a la Institución. La primera solución para satisfacer esta necesidad de comunicación segura implica conectar redes remotas mediante líneas dedicadas. Sin embargo, como la mayoría de las compañías no pueden conectar dos redes de área local remotas con una línea dedicada, a veces es necesario usar Internet como medio de transmisión. Las redes de área local (LAN) son las redes internas como la de Presidencia de Pachuca, es decir las conexiones entre los equipos de una organización particular. Estas redes se conectan cada vez con más frecuencia a Internet mediante un equipo de interconexión. Muchas veces, necesitan comunicarse por Internet con filiales en este caso con las Secretarias de la Presidencia de Pachuca de Soto, clientes o incluso con el personal que

puede estar alejado geográficamente. Una buena solución consiste en utilizar Internet como medio de transmisión con un protocolo de túnel, que significa que los datos se encapsulan antes de ser enviados de manera cifrada. Las Redes Privadas Virtuales (VPN), constituyen una tecnología a la cual se le está dando cada vez mayor importancia puesto que permiten la transmisión de información a grandes distancias sin necesidad de implantar una compleja y costosa infraestructura de red, y la infraestructura de Presidencia de Pachuca de Soto Hidalgo cuenta con el hardware requerido para ello. Se dice que esta red es virtual porque conecta dos redes "físicas" (redes de área local) a través de una conexión poco fiable (Internet) y privada porque sólo los equipos que pertenecen a una red de área local de uno de los lados de la VPN pueden "ver" los datos. Por lo tanto, el sistema VPN brinda una conexión segura a un muy bajo costo. Sin embargo, no garantiza una calidad de servicio comparable con una línea dedicada, ya que la red física es pública y su buen funcionamiento depende de factores externos. La Presidencia de Pachuca de Soto Hidalgo requiere de la implementación de una VPN porque el crecimiento de la población de Pachuca esta a la par con la exigencia de los tramites de las distintas áreas, dichos documentos e información debe manejarse y estar siempre actual y lo mas a la mano posible , ya que no en un solo edificio se concentran todas las Secretarias pertenecientes a la Presidencia ,existe una conexión básica de ftp, sin embargo no es posible captura datos con software especial el cual solo funciona si se está dentro de la red LAN de la Presidencia, una VPN sería la solución. La aplicabilidad de esta tesis práctica es para todas las secretarias (Secretaría General Municipal, Secretaría de Administración, Secretaría de Contraloría Municipal, Secretaría de Tesorería Municipal, Secretaría de Seguridad Pública, Secretaría de Obras Públicas, Secretaría de Servicios Municipales, Secretaría de Desarrollo Económico) de Presidencia de Pachuca, y directa e indirectamente a toda la ciudadanía del municipio de Pachuca. Los beneficios generados son: mayor rapidez en los tramites, actualización de las bases de datos en tiempo real, información confidencial siempre a disposición desde cualquier parte del mundo para el personal con cualidades y privilegios, se podrá acceder a la información en horas no hábiles de la presidencia como por ejemplo en la madrugadas, el personal de presidencia podrá terminar de capturar datos fuera del horario laboral para así incrementar la velocidad de adquisición de datos al área respectiva. Por lo anterior la utilidad de esta tecnología (VPN) en la Presidencia de Pachuca de soto es grande, conllevando con ello al crecimiento y desarrollo de la entidad.

1.4 Objetivo General

Proporcionar a la Presidencia de Pachuca de Soto, Hidalgo, un documento, el cual muestre detalladamente la implementación por software (Windows server 2003) de una Red Privada Virtual, para que el personal

con cualidades y derechos accedan a la red interna de modo alámbrico o inalámbrico vía remota utilizando como medio la internet.

1.5 Objetivos particulares

- Introducir al lector al tema de las Redes Privadas Virtuales mediante reseñas históricas, conceptos y protocolos de comunicación.
- Detallar paso a paso la configuración del un servidor VPN bajo el Sistema Operativo Microsoft Windows 2003 Server.
- Mostrar la configuración de un cliente VPN en distintas versiones del Sistema Operativo Microsoft Windows además del Sistema Operativo Linux.
- Dar a conocer la situación actual de la Presidencia de Pachuca de Soto Hidalgo en cuanto a Red Interna se refiere y equipos existentes en ella.

1.6 Estado del arte

La humanidad ha tenido la necesidad de comunicarse desde tiempos remotos, pero también de hacerlo de manera privada, es decir, que el mensaje sólo le llegue a determinados receptores. En las redes de comunicaciones sucede lo mismo; en especial el Sector Corporativo, donde siempre se ha requerido de la implementación de enlaces privados para transportar de forma segura toda su información confidencial.

No era tan importante conectarse a Internet por motivos laborables hace unos años en México y en gran parte de Latinoamérica, mucho menos pensar en hacerlo en el Estado de Hidalgo, pero a medida que ha pasado el tiempo, las corporaciones alrededor del mundo han requerido que las redes de área local (Local Área Network, LAN) trasciendan más allá del ámbito local para poder incluir personal y centros de información de otros edificios, ciudades, estados e incluso otros países. Lo que pasaba con otras formas de conectar redes a larga distancia, es que era necesario invertir en hardware, software y en servicios de telecomunicaciones costosos para crear redes de servicio amplio (Wide Área Network, WAN). Con el uso de Internet en la actualidad, las corporaciones tienen la posibilidad de dar origen a una red privada virtual (VPN), que requiere de una inversión relativamente baja utilizando Internet como conexión entre diferentes localidades o puntos. Las VPN's utilizan protocolos especiales de seguridad que permiten, únicamente al personal autorizado, obtener acceso a servicios privados de una organización, por ejemplo, cuando un

empleado se conecta a Internet, la configuración VPN le permite conectarse a la red privada de la compañía y navegar en la red como si estuvieran localmente en la oficina.

Una de las necesidades vitales de la empresa moderna, es la de compartir información, esencialmente aquellas empresas que se encuentran dispersas, con sedes en zonas y secciones de negocio que no se encuentran en el mismo entorno físico. Hasta el momento, las grandes corporaciones habían solucionado el problema mediante sistemas de comunicación como líneas punto a punto y sofisticadas instalaciones de interconexión. Aunque efectivas, estas soluciones quedaban fuera del alcance de empresas de menor tamaño y con recursos económicos y técnicos más escasos.

Como ejemplo entre muchas otras empresas que han tenido la necesidad de implementar esta tecnología tenemos al ITESM, mejor conocido como el TEC de Monterrey, que nació en 1943 con aspiración de ser una institución educativa formadora y proveedora de profesionales con un alto desempeño laboral en el ámbito de la tecnología. Con este enfoque, el ITESM inició el desarrollo de una red de cómputo en sus campus que diera acceso a todos sus empleados y alumnos a los servicios internos, además de conectividad entre los diferentes campus.

Tras recorrer una larga brecha del camino, el Tecnológico se enfrentó con el crecimiento constante de sus instalaciones y personal, fenómeno que generó una mayor demanda en materia de servicios tecnológicos, en especial la red datos y comunicación.

Tras la puesta en marcha de la nueva red de información, el equipo de ingenieros en telecomunicaciones del TEC estuvo satisfecho con los resultados, los usuarios podrían intercambiar una cantidad de datos más amplia y variada sin ningún contratiempo, ya que su información es más ágil y está mejor protegida.

En esta Institución, el establecimiento de la VPN para el manejo adicional de voz y videoconferencia es una de las mejores propuestas en materia de informática, tanto en materia administrativa como educativa. Además se logró conectar a las oficinas sucursales y a los usuarios remotos utilizando una red pública o compartida, como Internet, mientras que otorgó la misma seguridad y disponibilidad de una red privada, factor que coadyuvó al Tecnológico de Monterrey a incrementar sustancialmente la interconexión entre los campus y desarrollar programas de comunicación de forma inmediata, lo que permitió iniciar el proceso de consolidación de servidores y servicios, asimismo, el costo de llamadas de larga distancia disminuyó un 75%, en comparación con el uso de conmutadores, siendo uno de los beneficios más palpables a corto plazo [23].

Otro caso relevante surgió en la Universidad Autónoma del Estado de Hidalgo (UAEH), fundada en la ciudad de Pachuca en febrero de 1869, fue la primera institución de enseñanza de la entidad, aunque en ese entonces su nombre era Instituto Literario y Escuela de Artes y Oficios. Desde 1961 a la fecha, la UAEH ha vivido múltiples e importantes cambios caracterizados por su rápido crecimiento y expansión de cada una de sus funciones. Entre los servicios universitarios que ofrece están: biblioteca, centro de cómputo, educación continua, intercambio académico, y videoconferencia.

Desde hace 10 años, la UAEH realizó la implantación de redes digitales para hacer más eficiente sus transmisiones voz, datos y video, que operaban de manera independiente, y eran proveídas y soportadas por diferentes fabricantes y equipos. Hacia el 2001, ésta universidad se dio a la tarea de homologar, unificar y estandarizar sus equipos y cableados estructurado, en cuanto a los protocolos y proveedores. Esto, con la intención de escalar hacia una solución más robusta que permitiera ofrecer aplicaciones de alta calidad y seguridad a sus alumnos, profesores y personal administrativo.

La UAEH se apoyó en la empresa Cisco para la implantación de una red de nueva generación; puesta en marcha de toda una plataforma para la sistematización de los datos y toma de decisiones; la operación del programa de Universidad Virtual y el fortalecimiento de su sistema de telecomunicaciones. Cisco México proporcionó una solución integral basada en diferentes tecnologías como inalámbricas, ópticas, de ruteo, de almacenamiento, seguridad, y de IP (Protocolo de Internet), entre otras. Ante la necesidad de mantener los servicios educativos a la vanguardia, la universidad realiza la actualización tecnológica para lograr la convergencia entre las aplicaciones e información, entre sus 27 puntos de la red, distribuidos en el área metropolitana de Pachuca y del estado de Hidalgo.

La solución implantada por la universidad debía permitir el acceso a todos los recursos, con los más altos niveles de calidad y seguridad, lo que fue posible con la implantación de un Gateway de Voz y el Cisco ACS. El diseño de la infraestructura de telecomunicaciones requirió del despliegue de una red de área metropolitana con enlaces dedicados y VPN's para conectar y dar acceso de alta velocidad a Internet desde cualquiera de los campus de la UAEH (centros de investigación, cuatro preparatorias, nueve dependencias de educación superior, rectoría, edificios de servicio social y otras áreas).

Gracias a la actualización de sus redes, la UAEH ofrece una infraestructura de alta disponibilidad, que da la certeza de que las aplicaciones, como correo electrónico, Internet, videoconferencia o telefonía IP, pueden operar en el momento que sea requerido, sin tener que depender en su totalidad del apoyo de los ingenieros de sistemas o asesores técnicos para acceder a la información.

La actualización tecnológica y los equipos de alto desempeño brindaron la posibilidad de implementar la telefonía IP, videoconferencia y aplicaciones H323 (para transportar multimedia sobre redes de área local –LAN-). Estos servicios ofrecen mayor comunicación e interacción entre el campus y 27 puntos, y los más de 3,000 usuarios

Las tecnologías implantadas para la Actualización tecnológica son:

- 12 switches Cisco power in line 3560 para dar cobertura de telefonía IP a los campus de la Universidad
- 79 Cisco IP Phones, 55 de ellos son modelo 7940 y 24 son modelo 7960
- Migración del gateway de voz, a uno de mayores capacidades
- 1 servidor de Autentificación para el servicio de Internet Inalámbrico
- Call manager para administrar los teléfonos IP
- Migración de los enlaces que se tenían a Enlaces de VPN's. [24]

Las VPN permiten que los servicios puedan ser utilizados por las personas en una empresa en todo lugar y en todo momento, garantizando el correcto traslado de la información.

La tecnología que permite hoy en día la implementación de una VPN por software o hardware surgió con tecnología para conexiones remotas, en 1994 una tecnología usada en NLM llamada iptunnel a tunnel IPX usando las ip atravez de internet (de un servidor Novell a otro servidor Novell). Este unió sitios remotos llamándosele más tarde WAN.

Microsoft Point-To-Point Encryption (MPPE) Protocol, este protocolo surgido en el verano de 1999 un borrador de la IETF el cual se convirtiria en el protocolo PPTP.

En verano de 1.999 Counterpane analizó la revisión del protocolo PPTP que había realizado Microsoft (PPTPv2). Esta revisión soluciona muchos de los problemas de la implementación anterior, pero abre nuevas vías de ataque y adolece de falta de claridad en cuando a los criterios empleados a la hora de diseñar el protocolo.

En el número 53 de la revista electrónica "Phrack" (08/nov/99) se publicó un interesante artículo sobre las vulnerabilidades en la implementación PPTP de Microsoft. Se describen los puntos señalados en el documento de Counterpane, así como un ataque nuevo. Tras un largo proceso como borrador, L2TP (Layer 2 Tunnelling Protocol) pasa a ser una propuesta de estándar en Agosto de 2000.

En el año 2004 IPSec es el nuevo marco de seguridad IP, definido con el advenimiento del IPv6. Aunque IPv6 está muy poco difundido en este momento, la tecnología marco IPSec se está utilizando ya, lo que asegura, entre otras cosas, la interoperatividad de los sistemas de diversos fabricantes. Al menos en teoría. IPSec integra confidencialidad, integridad y autentificación en un mismo marco interoperante.

En general, cualquier VPN de nueva creación debería utilizar tecnología IPSec.

CAPÍTULO II
ANTECEDENTES Y FUNDAMENTOS DE LAS REDES PRIVADAS VIRTUALES

2.1 Introducción

En los últimos años las redes de computadoras se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida las redes transmiten información vital, por tanto es trascendental que cumplan con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Se ha demostrado que en la actualidad las redes de computadoras reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones, sobre todo las que cuentan con oficinas a varios Kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por lo anterior, la seguridad de las redes es de suma importancia.

2.2 Protocolos de red involucrados con las redes privadas virtuales

Los protocolos de VPN's hacen referencia fundamentalmente a los tres niveles OSI inferiores, físico, de enlace y de red. El resto de funciones superiores son asumidas por software de usuario.

Un aspecto resuelto a nivel protocolo, es el encaminamiento de paquetes en la red, y la necesaria identificación de entidades emisoras-receptoras dentro de la misma. Para ello, se concede a cada nodo de la red un código único de identificación que el resto de nodos puede utilizar para transmitirle información. Estos códigos o direcciones no sólo se asignan a todos los nodos de red, sino también a las propias redes a las que pertenecen. La dirección de un nodo suele contener la de su red, de forma que, al emplearla, se pueda identificar ésta.

Cada protocolo emplea su propio esquema de direcciones, distinto al de los demás. Por tanto, dichas direcciones no son fijas, sino que dependen del protocolo empleado. De este modo, como en una red pueden estar funcionando simultáneamente distintos protocolos, un mismo nodo podrá tener varias y diferentes direcciones para cada uno de ellos. Los protocolos que permiten la comunicación entre nodos de distintas redes se denominan "enrutables o encaminables". En caso contrario, o si dicha comunicación está muy limitada, se denominan "no enrutables o no encaminables".

En materia de VPN's, los dos protocolos de red que más comúnmente influyen son TCP/IP, PPTP, IPSec, L2TP. Gracias al manejo de capas del TCP/IP las VPN pueden hacer uso de la capa de red directamente, ya que es la capa que más importancia le torna una VPN, debido al uso de cabeceras que facilitan la comunicación entre redes por medio de Internet.

2.2.1 TCP-IP

Una VPN utiliza TCP/IP (Protocolo de Control de Transmisión / Protocolo Internet, Transmission Control Protocol/Internet Protocol) debido a que se requiere de Internet para su funcionamiento. Se utiliza la parte IP para transferir datos de manera que se encapsula un tipo de paquetes de datos dentro del paquete de datos, no necesariamente diferente al del paquete original (tunneling) y que establece la comunicación segura entre puntos de la VPN. Se describe como trabaja TCP/IP, al ser parecido al trabajo de las VPN; debido al manejo de cabeceras y de direcciones para que viajen paquetes por Internet. El término TCP/IP no es una entidad única que combina dos protocolos, sino un conjunto de programas de software más grande que proporciona servicios de red, como registro de entrada remoto, transferencia de archivos remota y correo electrónico. TCP/IP se ocupa del manejo de errores en la transmisión, de administrar el enrutamiento y entrega de los datos, así como de controlar la transmisión real mediante el uso de señales de estado predeterminadas. TCP/IP se basa en el concepto de clientes y servidores. Esto no tiene nada que ver con un servidor de archivos, que da acceso a una estación de trabajo sin disco o a una PC. En TCP/IP el término cliente/servidor tiene un significado sencillo; cualquier dispositivo que inicia comunicaciones se llama cliente y el dispositivo

.

que responde, servidor. El servidor responde (sirve) a las solicitudes del cliente. Básicamente esto es lo que hace una VPN pero creando un túnel de encriptación. [2]

2.2.1.1 Modelo del Protocolo TCP- IP

El protocolo TCP/IP se compone de las siguientes capas: Capa de Aplicación, Capa de Transporte, Capa de Enrutamiento (Red) y Capa de Interfase. El sistema operativo ejecuta los procesos de la capa de aplicación con privilegio de usuario y los procesos que pertenecen a las capas "transporte, enrutamiento e interfase" son ejecutados con privilegio Kernel.

Capa de aplicación: Su función es proveer servicios de comunicación a las aplicaciones. Un ejemplo es el protocolo HTTP, que provee servicios de recobro y envío de páginas web a las aplicaciones capaces de interpretar el código HTML contenido en dichas páginas.

Capa de transporte: Esta ofrece a la capa de aplicación dos servicios y es la responsable del envío y recepción de los segmentos de datos de la capa de aplicación. Un servicio consiste en el envío y recepción de datos orientado a conexión y el otro del envío y recepción de datos no orientados a conexión. El protocolo TCP de la capa de transporte es un servicio orientado a conexión. La unidad de datos que envía o recibe el protocolo TCP es conocido como segmento TCP. El protocolo UDP de la capa de transporte es un servicio no orientado a conexión. La unidad de datos que envía o recibe el protocolo UDP es conocido como datagrama UDP.

Capa de enrutamiento (capa de red): La capa de red es la responsable de proveer los siguientes servicios a la capa de transporte:

- Establecer el sistema de direccionamiento lógico de la red.
- Enrutamiento de paquetes. Si un paquete que va a ser enrutado excede la máxima unidad de transferencia "Maximum Transfer Unit, MTU" de un enlace, la capa fragmenta el paquete para adaptarse al MTU del enlace y el paquete es ensamblado en la computadora destino.

Durante el proceso de enrutamiento se usa un servicio de conexión no orientado para el envío y recepción de paquetes. Esta capa está compuesta por los protocolos IP, ARP, ICMP. El protocolo IP ofrece el servicio de direccionamiento lógico de la red TCP/IP y el de enrutamiento de paquetes, es por eso que una

.

VPN usa este protocolo. El protocolo ARP ofrece el servicio de resolución de direcciones IP con su respectiva dirección física y el protocolo ICMP ofrece el servicio de reporte de errores que pueden ocurrir durante el enrutamiento de paquetes. La unidad de datos que envía o recibe el protocolo IP se conoce con el nombre de datagrama IP.

Capa de interfase: Esta capa es importante para una VPN, aunque no tanto como la capa de red. Está compuesta por dos capas: capa de enlace (capa de acceso a la red) y capa física. La capa de enlace es responsable de proveer los siguientes servicios a la capa de red:

- Delimita el principio y fin de los frames a ser enviados.
- Establece el sistema de direccionamiento físico de la red.
- Detecta los errores de envío o recepción de información entre dos o más computadoras.

La **capa de enlace** puede ofrecer un servicio de conexión orientado o un servicio de conexión no orientado. Los protocolos DIC, PPP, LLC son protocolos de la capa de enlace. La función la **capa física** es la de hacer uso de la línea de transmisión para el envío y la recepción de los bits contenidos en un frame. Los protocolos Ethemet y Token Ring son protocolos de la capa física. La unidad de envío o recepción de datos de la capa física se conoce con el nombre de frame. [4]

2.2.1.2 Comunicación entre capas

El envío y recepción de datos entre dos aplicaciones, es un proceso de intercambio de datos entre capas iguales basado en un modelo cliente - servidor. La aplicación de la computadora 1 es una aplicación cliente "Browser / Navegador" que hace uso del protocolo HTTP de la capa de aplicación y la aplicación de la computadora 2 es una aplicación de servicios de páginas web que hace uso del demonio HTTPD.

Cuando la aplicación cliente requiere de los servicios de la aplicación servidor HTTPD, dicha aplicación solicita los servicios de red al sistema operativo a través de una interfaz de programación de servicios TCP-IP "API socket BSD". Un socket es un descriptor que un proceso cliente utiliza para establecer una conexión e intercambiar datos con el proceso servidor. Este descriptor sirve para identificar el protocolo, el proceso-cliente, la dirección-cliente, el proceso- servidor y la dirección-servidor. Establecida la conexión virtual entre el proceso cliente Navegador - HTTP y el proceso servidor HTTPD pueden comenzar con el intercambio de datos.

.

Las aplicaciones cliente - servidor dependen de los servicios de las capas de aplicación, transporte, enrutamiento y enlace. Cuando una aplicación usa los servicios de la capa de aplicación para el envío de datos, cada capa debe incluir los parámetros del protocolo de comunicación entre capas adyacentes y los parámetros del protocolo de comunicación entre capas iguales. Cuando cada capa haya incluido los parámetros antes mencionados, los datos de la aplicación estarán encapsulados. Y cuando los datos encapsulados llegan a la computadora destino un proceso de desencapsulamiento ocurre en cada capa estableciendo de esta manera la comunicación virtual entre capas iguales [4]. En las tecnologías VPN adoptan un sistema parecido y para ello utilizan TCP/IP y OSI para lograrlo pero adicionando sus propias cabeceras, aunque podrían de cierto modo utilizar otros protocolos pero no con los mismos resultados.

En la figura 2.1 se observa que los servicios que ofrecen cada una de las capas determinan la manera como los datos de la aplicación son enviados y recibidos entre capas iguales.

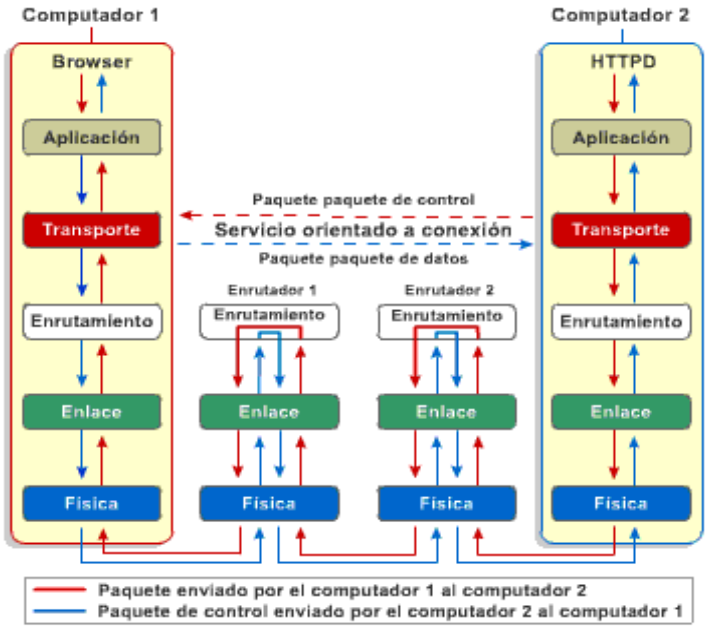

Figura 2.1 *Servicios que ofrece una capa.*

El servicio que ofrece una capa puede ser de cuatro tipos:

- **Servicio orientado a conexión:** Un servicio de conexión orientado se caracteriza por la iniciación de la conexión previa al envío y/o a la recepción de información entre capas iguales. Una vez iniciada la conexión ambas capas pueden comenzar a enviar y/o recibir los datos de la aplicación.

.

Un servicio de conexión orientado es diseñado para corregir errores que pueden ocurrir durante el envío y/o recepción de datos, como también es diseñado para controlar el flujo de envío y recepción de datos.

- **Servicio no orientado a conexión:** Un servicio de conexión no orientado se caracteriza por el envío y recepción de datos sin la previa iniciación de la conexión entre capas iguales. Es un servicio que no está diseñado para corregir errores que puedan ocurrir durante el envío y/o recepción de datos ya que este tipo de servicio es utilizado cuando la probabilidad de error durante el envío y/o recepción de datos es prácticamente nula. Tampoco está diseñado para controlar el flujo de envío y recepción de datos.

- **Servicio de conexión punto a punto:** Consiste en no modificar lo parámetros de control de una capa durante el proceso de enrutamiento de los datos. Por ejemplo el protocolo TCP de la capa de transporte es un servicio de conexión orientado a conexión y es un servicio de conexión punto a punto ya que los parámetros de control generados por esta capa no son modificados durante el proceso de enrutamiento.

- **Servicio de conexión de salto en salto:** Consiste en que los parámetros de control de una capa son modificados durante el proceso de enrutamiento de los datos. Por ejemplo el protocolo IP de la capa de enrutamiento es un servicio de conexión no orientado a conexión y es un servicio de conexión de salto en salto ya que los parámetros de control generados por esta capa son modificados durante el proceso de enrutamiento. [4]

2.2.2 PPTP

Point-to-Point Tunneling Protocol fue desarrollado por ingenieros de Ascend Communications, U.S. Robotics, 3Com Corporation, Microsoft, y ECI Telematics para proveer entre usuarios de acceso remoto y servidores de red una red privada virtual.

Como protocolo de túnel, PPTP encapsula datagramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser ruteado a través de una red IP, como Internet.

.

PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si discaran directamente al servidor. En vez de discar a un modem conectado al servidor RAS, los usuarios se conectan a su proveedor y luego "llaman" al servidor RAS a través de Internet utilizando PPTP.

Existen dos escenarios comunes para este tipo de VPN:

- El usuario remoto se conecta a un ISP que provee el servicio de PPTP hacia el servidor RAS.
- El usuario remoto se conecta a un ISP que no provee el servicio de PPTP hacia el servidor RAS y, por lo tanto, debe iniciar la conexión PPTP desde su propia máquina cliente.

Para el primero de los escenarios, el usuario remoto estable una conexión PPP con el ISP, que luego establece la conexión PPTP con el servidor RAS. Para el segundo escenario, el usuario remoto se conecta al ISP mediante PPP y luego "llama" al servidor RAS mediante PPTP. Luego de establecida la conexión PPTP, para cualquiera de los dos casos, el usuario remoto tendrá acceso a la red corporativa como si estuviera conectado directamente a la misma.

La técnica de encapsulamiento de PPTP se basa en el protocolo Generic Routing Encapsulation (GRE), que puede ser usado para realizar túneles para protocolos a través de Internet. La versión PPTP, denominada GREv2, añade extensiones para temas específicos como Call Id y velocidad de conexión.

El paquete PPTP está compuesto por un header de envío, un header Ip, un header GREv2 y el paquete de carga. El header de envío es el protocolo enmarcador para cualquiera de los medios a través de los cuales el paquete viaja, ya sea Ethernet, frame relay, PPP. El header IP contiene información relativa al paquete IP, como ser, direcciones de origen y destino, longitud del datagrama enviado, etc. El header GREv2 contiene información sobre el tipo de paquete encapsulado y datos específicos de PPTP concernientes a la conexión entre el cliente y servidor.

Por último, el paquete de carga es el paquete encapsulado, que, en el caso de PPP, el datagrama es el original de la sesión PPP que viaja del cliente al servidor y que puede ser un paquete IP, IPX, NetBEUI, entre otros. En la figura 2.2 se ilustra las capas del encapsulamiento PPTP.

.

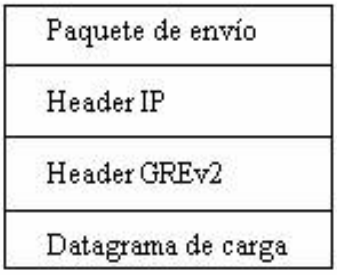

Figura 2.2 *Capas de encapsulamiento PPTP.*

Para la autenticación, PPTP tiene tres opciones de uso: CHAP, MS-CHAP y aceptar cualquier tipo, inclusive texto plano. Si se utiliza CHAP, standard en el que se intercambia un "secreto" y se comprueba ambos extremos de la conexión coincidan en el mismo, se utiliza la contraseña de Windows NT, en el caso de usar este sistema operativo, como secreto. MS-CHAP es un standard propietario de Microsoft y resulta ser una ampliación de CHAP. Para la tercer opción, el servidor RAS aceptará CHAP, MS-CHAP o PAP (Password Autenthication Protocol), que no encripta las contraseñas.
Para la encriptación, PPTP utiliza el sistema RC4 de RSA, con una clave de sesión de 40 bits; en el caso de los puerto para éste protocolo se tendrá que abrir el puerto TCP 1723 y abrir tambien el protocolo con el Id. 47 (GRE) [36].

2.2.3 IPSec

IPSec trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.
IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Protocolo de Autenticación (Authentication Protocol AH) y Encapsulated Security Payload (ESP).

Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión. Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación.

Por autenticidad se entiende por la validación de remitente de los datos. Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

.

AH provee autenticación, integridad y protección a repeticiones pero no así confidencialidad. La diferencia más importante con ESP es que AH protege partes del header IP, como las direcciones de origen y destino. ESP provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al header.

AH sigue al header IP y contiene diseminaciones criptográficas tanto en los datos como en la información de identificación. Las diseminaciones pueden también cubrir las partes invariantes del header IP.

El header de ESP permite rescribir la carga en una forma encriptada. Como no considera los campos del header IP, no garantiza nada sobre el mismo, sólo la carga.
Una división de la funcionalidad de IPSec es aplicada dependiendo de dónde se realiza la encapsulación de los datos, si es la fuente original o un gateway:

- El modo de transporte es utilizado por el host que genera los paquetes. En este modo, los headers de seguridad son antepuestos a los de la capa de transporte, antes de que el header IP sea incorporado al paquete. En otras palabras, AH cubre el header TCP y algunos campos IP, mientras que ESP cubre la encriptación del header TCP y los datos, pero no incluye ningún campo del header IP.

- El modo de túnel es usado cuando el header IP entre extremos está ya incluido en el paquete, y uno de los extremos de la conexión segura es un gateway. En este modo, tanto AH como ESP cubren el paquete entero, incluyendo el header IP entre los extremos, agregando al paquete un header IP que cubre solamente el salto al otro extremo de la conexión segura, que, por supuesto, puede estar a varios saltos del gateway.

Los enlaces seguros de IPSec son definidos en función de Security Associations (SA). Cada SA está definido para un flujo unidireccional de datos y generalmente de un punto único a otro, cubriendo tráfico distinguible por un selector único. Todo el tráfico que fluye a través de un SA es tratado de la misma manera. Partes del tráfico puede estar sujeto a varios SA, cada uno de los cuales aplica cierta transformación. Grupos de SA son denominados SA Bundles. Paquetes entrantes pueden ser asignados a un SA específico por los tres campos definitorios: la dirección IP de destino, el índice del parámetro de seguridad y el protocolo de seguridad. El SPI puede ser considerado una cookie que es repartido por el receptor del SA cuando los parámetros de la conexión son negociados. El protocolo de seguridad debe ser AH o ESP. Como la dirección IP de destino es parte de la tripleta antes mencionada, se garantiza que este valor sea único.

.

Un ejemplo de paquete AH en modo túnel se muestra en la figura 2.3:

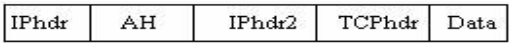

Figura 2.3 *Paquete AH en modo túnel.*

Un ejemplo de paquete AH en modo transporte se muestra en la figura 2.4:

Figura 2.4 *Paquete AH en modo transporte.*

Como ESP no puede autentificar el header IP más exterior, es muy útil combinar un header AH y ESP para obtener un Transport Adjacency, mostrado en la figura 2.5:

Figura 2.5 *Transport Adjacency.*

La versión de entunelamiento sería lo mostrado en la figura 2.6

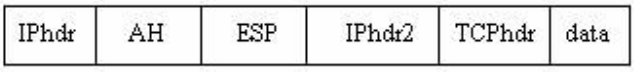

Figura 2.6 *Transport Adjacency versión entunelamiento.*

Sin embargo, no es mencionado en las RFC que definen estos protocolos. Como en Transport Adjacency, esto autenticaría el paquete completo salvo algunos pocos campos del header IP y también encriptaría la carga. Cuando un header AH y ESP son directamente aplicados como en esta manera, el orden de los header debe ser el indicado. Es posible, en el modo de túnel, hacer una encapsulación arbitrariamente recursiva para que el orden no sea el especificado.

Cabe hacer mención que para el uso de éste protocolo se tendrá que hacer uso y abrir el puerto UDP 500 y los protocolos de Id. 50 (IPSec ESP) y 51 (IPSec AH) [36].

.

2.2.4 L2TP

Layer-2 Tunneling Protocol (L2TP) facilita el entunelamiento de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos corran.

El escenario típico L2TP, cuyo objetivo es la creación de entunelar marcos PPP entre el sistema remoto o cliente LAC y un LNS ubicado en una LAN local, es el que se muestra en la figura 2.7:

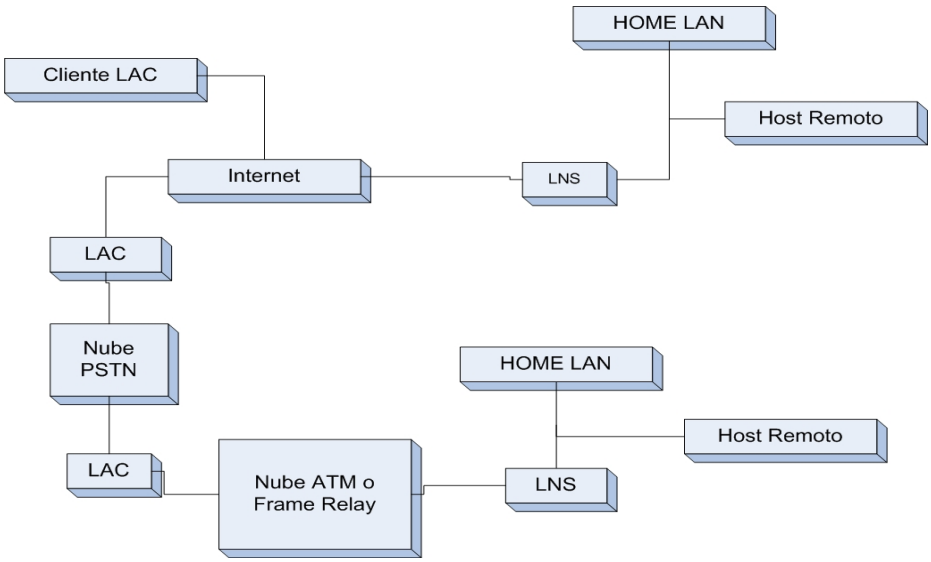

Figura 2.7 *Escenario típico L2TP.*

Un L2TP Access Concentrator (LAC) es un nodo que actúa como un extremo de un túnel L2TP y es el par de un LNS. Un LAC se sitúa entre un LNS y un sistema remoto y manda paquetes entre ambos. Los paquetes entre el LAC y el LNS son enviados a través del túnel L2TP y los paquetes entre el LAC y el sistema remoto es local o es una conexión PPP.

Un L2TP Network Server (LNS) actúa como el otro extremo de la conexión L2TP y es el otro par del LAC. El LNS es la terminación lógica de una sesión PPP que está siendo puesta en un túnel desde el sistema remoto por el LAC.

.

Un cliente LAC, una máquina que corre nativamente L2TP, puede participar también en el túnel, sin usar un LAC separado. En este caso, estará conectado directamente a Internet.
El direccionamiento, la autenticación, la autorización y el servicio de cuentas son proveídos por el Home LAN's Management Domain.

L2TP utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los túneles y las llamadas. Utilizan un canal de control confiable dentro de L2TP para garantizar el envío. Los mensajes de datos encapsulan los marcos PPP y son enviados a través del túnel.
La siguiente figura 2.8 muestra la relación entre los marcos PPP y los mensajes de control a través de los canales de control y datos de L2TP.

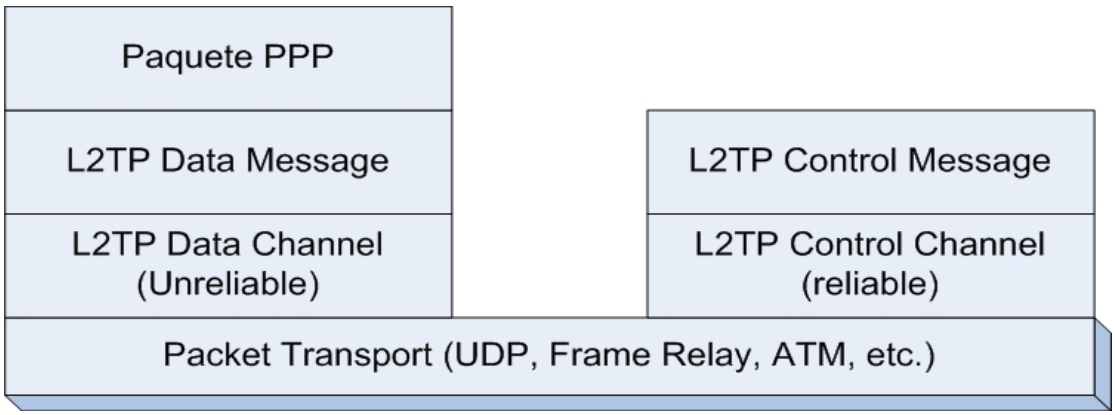

Figura 2.8 *Relación entre marcos PPP y mensajes de control.*

Los marcos PPP son enviados a través de un canal de datos no confiable, encapsulado primero por un encabezado L2TP y luego por un transporte de paquetes como UDP, Frame Relay o ATM. Los mensajes de control son enviados a través de un canal de control L2TP confiable que transmite los paquetes sobre el mismo transporte de paquete.

Se requiere que haya números de secuencia en los paquetes de control, que son usados para proveer el envío confiable en el canal de control. Los mensajes de datos pueden usar los números de secuencia para reordenar paquetes y detectar paquetes perdidos.

Al correr sobre UDP/IP, L2TP utiliza el puerto 1701. El paquete entero de L2TP, incluyendo la parte de datos y el encabezado, viaja en un datagrama UDP. El que inicia un túnel L2TP toma un puerto UDP de origen que esté disponible, pudiendo ser o no el 1701 y envía a la dirección de destino sobre el puerto 1701. Este extremo toma un puerto libre, que puede ser o no el 1701, y envía la respuesta a la dirección de

.

origen, sobre el mismo puerto iniciador. Luego de establecida la conexión, los puertos quedan estáticos por el resto de la vida del túnel.

En la autenticación de L2TP, tanto el LAC como el LNS comparten un secreto único. Cada extremo usa este mismo secreto al actuar tanto como autenticado como autenticador.

Sobre la seguridad del paquete L2TP, se requiere que el protocolo de transporte de L2TP tenga la posibilidad de brindar servicios de encriptación, autenticación e integridad para el paquete L2TP en su totalidad. Como tal, L2TP sólo se preocupa por la confidencialidad, autenticidad e integridad de los paquetes L2TP entre los puntos extremos del túnel, no entre los extremos físicos de la conexión.
El uso de éste protocolo requiere de la apertura del puerto TCP 170.1. [36]

2.3 Modelo OSI

OSI (Open Systems Interconection/ Interconexión de sistemas abiertos) es otro protocolo utilizado por las VPN y se usa para describir el uso de datos entre la conexión física de la red y la aplicación del usuario final. Este modelo es el más conocido y el más usado para describir los entornos de red [6]. Una de las necesidades más deseables de un sistema de comunicaciones es el establecimiento de estándares, sin ellos sólo podrían comunicarse equipos del mismo fabricante que usen la misma tecnología. La ISO (lntemational Organisation for Standarisation) ha generado una gran variedad de estándares, donde la norma ISO- 7494 define el modelo OSI, este modelo ayuda a comprender mejor el funcionamiento de las redes de computadoras. OSI no garantiza la comunicación entre equipos pero pone las bases para una mejor estructuración de los protocolos de comunicación. No existe ningún sistema de comunicaciones que los siga estrictamente, siendo la familia de protocolos TCP/IP la que más se acerca. El modelo OSI describe siete niveles para facilitar las interfaces de conexión entre sistemas abierto, en la tabla 2.1 se puede ver con más detalle. [5]

Nivel	Nombre	Función	Dispositivos y protocolo
1	Físico	Se ocupa de la transmisión del flujo de bits a través Cables, tarjetas y el medio	Cables, tarjetas y repetidores (hub) RS-232, X.21

.

2	Enlace	Divide el flujo de bits en unidades con formato (tramas) intercambiando estas unidades mediante el empleo de protocolos.	Puentes (bridges). HDLC y LLC
3	Red	Establece las comunicaciones y determina el camino que tomarán los datos en la red. Aquí se adicionan cabeceras extras VPN o son modificadas.	Encaminador (router). IP, IPX.
4	Transporte	La función de este nivel es asegurar que el receptor reciba exactamente la misma información que ha querido enviar el emisor, y a veces asegura al emisor que el receptor ha recibido la información que le ha sido enviada. Envía de nuevo lo que no haya llegado correctamente.	Pasarela (gateway). UDP, TCP, SPX.
5	Sesión	Establece la comunicación entre las aplicaciones, la mantiene y la finaliza en el momento adecuado. Proporciona los pasos necesarios para entrar en un sistema utilizando otro. Permite a un mismo usuario, realizar y mantener diferentes conexiones a la vez (sesiones).	Pasarela.
6	Presentación	Conversión entre distintas representaciones de datos y entre terminales y organizaciones de sistemas de ficheros con características diferentes.	Pasarela.
7	Aplicación	Este nivel proporciona unos servicios estandarizados para poder realizar unas funciones específicas en la red. Las personas que utilizan las aplicaciones hacen una petición de un servicio (por ejemplo el envío de un archivo). Esta aplicación utiliza un servicio que le ofrece el nivel de aplicación para poder realizar el trabajo que se le ha encomendado (enviar el archivo).	X.400

Tabla 2.1 *Función, dispositivos y protocolos del modelo OSI.*

.

La comunicación según el modelo OSI siempre se realizará entre dos sistemas tal cual se desea según el funcionamiento de una VPN, y más si es a muy larga distancia, sino, no tendría sentido una VPN. Supongamos que la información se genera en el nivel 7 de uno de ellos, y desciende por el resto de los niveles hasta llegar al nivel 1, que es el correspondiente al medio de transmisión (por ejemplo el cable de red) y llega hasta el nivel 1 del otro sistema, donde va ascendiendo hasta alcanzar el nivel 7. En este proceso, cada uno de los niveles va añadiendo a los datos a transmitir la información de control relativa a su nivel, de forma que los datos originales van siendo recubiertos por capas de datos de control. De forma análoga, al ser recibido dicho paquete en el otro sistema, según va ascendiendo del nivel 1 al 7, va dejando en cada nivel los datos añadidos por el nivel equivalente del otro sistema, hasta quedar únicamente los datos a transmitir. La forma de enviar información en el modelo OSI tiene una cierta similitud con enviar un paquete de regalo a una persona, donde se ponen una serie de papeles de envoltorio, una o más cajas, hasta llegar al regalo en sí. [5]

Emisor	Paquete	Receptor
Aplicación	C7 Datos	Aplicación
Presentación	C6C7 Datos	Presentación
Sesión	C5C6C7 Datos	Sesión
Transporte	C4C5C6C7 Datos	Transporte
Red	C3C4C5C6C7 Datos	Red
Enlace	C2C3C4C5C6C7 Datos	Enlace
Físico	C2C3C4C5C6C7 Datos	Físico

Tabla 2.2 *Comunicación entre capas del modelo OSI.*

Los niveles OSI se entienden entre ellos, es decir, el nivel 5 enviará información al nivel 5 del otro sistema (lógicamente, para alcanzar el nivel 5 del otro sistema debe recorrer los niveles 4 al 1 de su propio sistema y el 1 al 4 del otro), de manera que la comunicación siempre se establece entre niveles iguales, a las normas de comunicación entre niveles iguales es a lo que llamaremos protocolos. Este mecanismo asegura la modularidad del conjunto, ya que cada nivel es independiente de las funciones del resto, lo cual garantiza que a la hora de modificar las funciones de un determinado nivel no sea necesario reescribir todo el conjunto. [5]

.

2.4 Enlaces Privados antes de la aparición de las Redes Privadas Virtuales

Los enlaces privados brindan seguridad en la transmisión de datos de extremo a extremo, siendo esta su principal característica. Se valen siempre de una red de transmisión para conectar sus partes (en algunos casos existe una red de conmutación). Estos enlaces pueden ir desde los 9600bps (en el caso de una conexión conmutada usando un modem análogo de 9600bps) hasta el orden de los Gigabps (usando redes ópticas, con equipos de transporte de última generación).

2.4.1 Tipos de Enlaces Privados

Las redes de computadoras se han valido de los enlaces privados para interconectarse a través de grandes distancias geográficas. Antes de la aparición de las VPN habían existido solo dos tecnologías de enlaces WAN, los enlaces dedicados, y los enlaces conmutados. Dentro de los enlaces dedicados caben topologías tales como Clear Channel, Frame Relay y ATM. Aunque se sabe que Frame Relay usa conmutación de paquetes y ATM usa conmutación de celdas, en este trabajo se clasifican como enlaces dedicados, dado que para el usuario la conmutación es transparente. Dentro de los enlaces conmutados están los análogos que van desde 2400bps hasta los 56 kbps y los digitales RDSI de 64 kbps y 128 kbps.

2.4.1.1 Enlaces Dedicados

Los enlaces dedicados, como su nombre lo indica, son conexiones permanentes punto-punto, o punto-multipunto, que se valen de una infraestructura de transporte (Capa 1) o de transporte y conmutación (Capa 1 y 2) del modelo TCP/IP o del modelo OSI. Los primeros son comúnmente llamados enlaces Clear Channel y los segundos son enlaces Frame Relay o ATM. [3]

Clear Channel: Clear Channel es un enlace donde solo interviene la red de transporte del proveedor de servicios. Para el mercado corporativo comúnmente van desde los 64 kbps hasta los 2048 kbps, en pasos nx64. Para el mercado de proveedores de servicio van desde alcances "E1" hasta "OC-3" y superiores. En la tabla 2.3 se observan los alcances de transmisión desde OC-1 hasta OC-768 así como su correspondencia entre redes SONET y SDH. [3]

.

SONET	SDH	Mbps
OC-1	---	51.84
OC-3	STM-1	155.52
OC-12	STM-4	622.08
OC-48	STM-16	2455.32 (≈ 2.5 Gbps)
OC-192	STM-64	9953.28 (≈ 10 Gbps)
OC-768	STM-256	39813.12 (≈ 40 Gbps)

Tabla 2.3 *Equivalencia entre sistemas SONET y SDH.*

Los enlaces Clear Channel ofrecen un throughput efectivo casi del 100% ya que no usan ningún tipo de encapsulación de nivel 2, es decir, no hay cabeceras de ningún tipo. Estos enlaces son entregados en interfaz "E1" balanceada o desbalanceada con trama G.703, o en interfaz serial de datos V.35. La compañía (o cliente) debe tener un puerto disponible DTE que cumpla con las especificaciones técnicas del equipo de comunicaciones entregado por el proveedor. La mayoría de los equipos que se usan para recibir los enlaces Clear Channel por parte del cliente son routers o switches de nivel 3, que se encargan de manejar los niveles 2 y 3(2). Las topologías de los enlaces Clear Channel son robustas pero a su vez estáticas. Esto significa que para aumentar o disminuir el alcance del enlace es necesario cambiar equipos o manipularlos localmente. El enlace Clear Channel fue la primera tecnología WAN que se adoptó usando la infraestructura de voz PCM de los operadores de telefonía locales, nacionales e internacionales. Por venir de una tecnología que no había sido pensada para transmitir datos fue superada rápidamente por otros tipos de tecnologías como Frame Relay y ATM. La figura 2.9 muestra un esquema básico, donde se observa la transparencia para una organización del enlace contratado. [3]

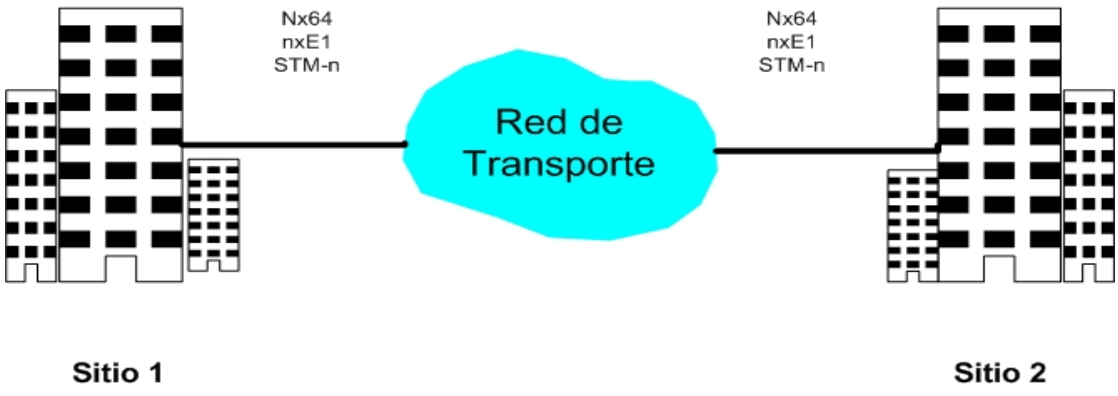

Figura 2.9 *Enlace típico Clear Channel. Esquema Básico.*

.

Frame Relay: Frame Relay es un protocolo WAN de alto rendimiento que trabaja en la capa física y de enlace de datos del modelo OSI. Frame Relay fue diseñado originalmente para trabajar con redes ISDN. Frame Relay es una tecnología de conmutación de paquetes, que permite compartir dinámicamente el medio y el ancho de banda disponible. La longitud de los paquetes es variable para hacer más eficiente y flexible las transferencias de datos. Estos paquetes son conmutados por varios segmentos de la red hasta que llegan hasta el destino final. Todo el acceso al medio en una red de conmutación de paquetes es controlado usando técnicas de multiplexación estadística, por medio de las cuales se minimiza la cantidad de demoras y/o colisiones para acceder al medio. Frame Relay es una evolución de las redes X.25, no hace retransmisión de paquetes perdidos, características que si ofrecía su antecesor ya que en los años 70 (época en la que aparece X.25) los medios físicos no eran tan confiables como los de hoy día, y por tanto se necesitaba mayor robustez. Todas las ventajas que ofrecen los medios actualmente, han posibilitado a Frame Relay ofrecer un alto desempeño y una gran eficiencia de transmisión. [3]

Dispositivos Frame Relay: Los equipos usados en una red Frame Relay se dividen en dos categorías: Equipos Terminales de Datos (DTE's) y Equipos Terminales de Circuitos de Datos (DCE's).

- **DTE:** Son considerados equipos terminales de una red específica, son routers, computadoras personales, terminales o bridges. Estos equipos se localizan en las premisas del cliente y en la mayoría de los casos son propiedad de los mismos

- **DCE:** Normalmente son dispositivos propiedad del carrier. El propósito de los equipos DCE's es proveer o generar señales de reloj y conmutar los paquetes de la red. Son llamados packet switchs o conmutadores de paquetes.

En la conexión entre los dispositivos DCE y DTE intervienen dos componentes, uno de nivel físico y otro de nivel de enlace de datos. En el nivel físico se definen todas las características físicas, eléctricas y mecánicas entre los dos, y el nivel de enlace de datos define todas las especificaciones Frame Relay o Frame Relay LMI según sea el caso. [3]

Circuitos Virtuales Frame Relay: Frame Relay es una tecnología WAN que usa enlaces orientados a conexión, significa que una comunicación se define entre un par de dispositivos y que cada conexión existente en la red tiene un identificador asociado particular. Este servicio es implementado usando circuitos virtuales bidireccionales, que son conexiones lógicas creadas entre dos dispositivos DTE a través

.

de la red conmutada de paquetes Frame Relay. Los circuitos virtuales Frame Relay se dividen en dos categorías: circuitos virtual es conmutados (SVC's) y circuitos virtuales permanentes (PVC's).

Circuitos Virtuales Conmutados (SVC's): Los SVC's son conexiones temporales que se usan cuando la transferencia de datos entre un par de dispositivos DTE, es esporádica a través de la red Frame Relay. Los SVC's tienen 4 estados operacionales:

- Call Setup: Cuando se realiza la negociación y el establecimiento de un circuito virtual entre dos DTE's.
- Data Transter: Cuando los datos entre los dos DTE's son transmitidos sobre el circuito virtual.
- Idle: Cuando la conexión entre los dos DTE's está todavía activa, pero no hay tráfico de datos. Si por cierto periodo de tiempo el circuito se encuentra en este estado, se procede a terminar la conexión.
- Call Termination: Cuando el circuito virtual entre los dos DTE's es terminado.

Si después de terminado el circuito los dispositivos DTE's necesitan transmitir más datos, se deberá establecer un nuevo SVC, y así sucesivamente.

Circuitos Virtuales Permanentes (PVC's): Los PVC's son conexiones establecidas permanentemente, que se usan donde la transferencia de datos es continua entre dos dispositivos DTE. Este tipo de conexiones no requieren hacer una llamada de configuración ni de terminación como en los SVC's. De hecho los PVC's siempre operan en uno de los siguientes dos estados:

- Data transfer: Cuando los DTE's están intercambiando tráfico.
- Idle: Cuando no hay transferencia de datos, pero la conexión sigue activa. A diferencia de los SVC's, un PVC puede estar indefinidamente en este estado y el enlace no es terminado.

Identificadores de Conexión de enlace de datos (DLCI)

Los circuitos virtuales Frame Relay son identificados por DLCI's. Los valores de los DLCI's son asignados por el proveedor de servicio y tienen solo significado a nivel local, esto quiere decir que en una red Frame Relay pueden existir varios DLCI's con el mismo valor, pero no puede haber varios DTE's con un mismo DLCI conectados al mismo Packet Switch.

.

ATM (Asynchronous Transfer Mode)

El Modo de Transferencia Asíncrono es un estándar que desarrollo la Unión Internacional de Telecomunicaciones (ITU-T) para transmitir múltiples tipos de servicios, como voz, video y datos usando técnicas de conmutación de celdas pequeñas, de tamaño fijo sobre redes públicas. Las redes ATM son, al igual que las redes Frame Relay, orientadas a conexión.

Funcionamiento de las Redes A TM

ATM es una tecnología de multiplexación y conmutación de celdas que combina los beneficios de una red de conmutación de circuitos (capacidad garantizada, retardos constantes) y de una red de conmutación de paquetes (flexibilidad y eficiencia para tráfico intermitente). Permite transmisiones desde unos pocos Mbps hasta cientos de Gbps. Su naturaleza asíncrona, la hace una tecnología más eficiente que las síncronas como TDM. En TDM a los usuarios se les asigna un timeslot, y ningún otro cliente puede transmitir en ese timeslot aunque el propietario no transmita, por lo que no es muy eficiente. En ATM los timeslots siempre están disponibles y se asignan por demanda basándose en la información que contienen las cabeceras de las celdas.

Formato de una celda ATM

ATM transmite información en celdas donde cada una contiene 53 octetos o bytes. Los primeros 5 bytes conforman la cabecera y los 48 restantes contienen la información del usuario o payload, tal como se ve en la figura 2.10; las celdas son unidades de tamaño fijo. El tamaño pequeño de cada celda hace que la transmisión de voz y la de video sean de calidad, dado que el tráfico no tolera retardos producidos por esperar paquetes de gran tamaño. [3]

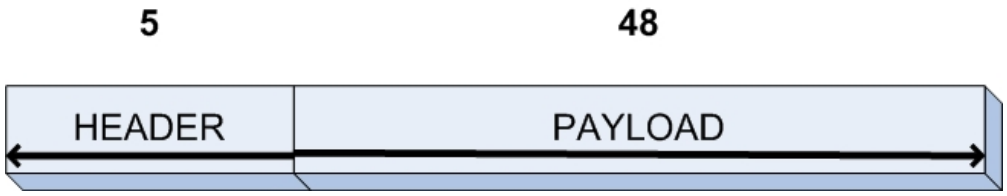

Figura 2.10 *Formato básico de una celda ATM.*

.

Dispositivos ATM

Una red ATM se compone de dos tipos de dispositivos: switches ATM y terminadores ATM. Un switch ATM se encarga de recibir las celdas entrantes provenientes de otro switch ATM, leer y actualizar las cabeceras de cada celda y de direccionar la celda hasta llegar a su destino final. Los terminadores ATM (sistemas finales) son dispositivos que proveen un adaptador de interfaz de red ATM, por lo general están en las premisas del cliente.

En ATM hay dos tipos de interfaces: la UNI (user-network interface) que conecta un terminador con un switch ATM y la NNI (network-node interface) que conecta dos switches ATM. [3]

Conexiones Virtuales ATM

Las redes ATM son redes orientadas a conexión, por lo que se tienen que configurar canales virtuales (VC's, Virtual Channels) a través de la red para una transferencia de datos adecuada. Haciendo la analogía con Frame Relay, un canal virtual equivale a un circuito virtual.

En ATM existen dos tipos de conexiones: los caminos virtuales (Virtual Paths, VP's), los cuales son identificados por medio de VPI's (Virtual Path Identifiers), y los canales virtuales, los cuales son identificados con una combinación de VPl's y de VCl's (Virtual Channel Identifier). Un camino virtual es una suma de canales virtuales, donde cada uno de los cuales es conmutado transparentemente sobre la red ATM. La figura 2.11 muestra la relación entre VC's y VP's. [3]

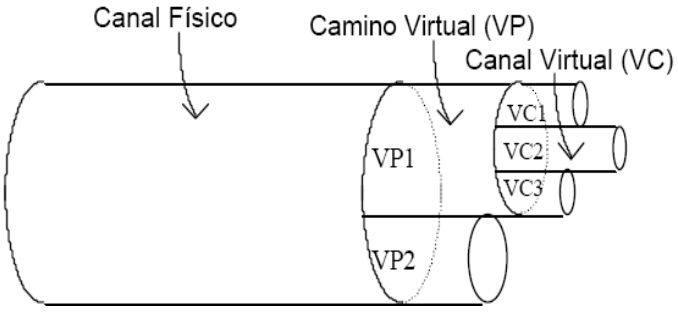

Figura 2.11 *Canales Virtuales (VC) dentro de Caminos Virtuales (VP).*

.

2.5 Tipos de Red de Computadoras

Como en casi todos los ámbitos de la computación, hay varios tipos de redes de computadoras que son definidas por tamaño, espacio, utilidad, cobertura, conexión y propiedad. Es por eso que en la figura 2.12 se ilustran algunos de estos tipos de redes.

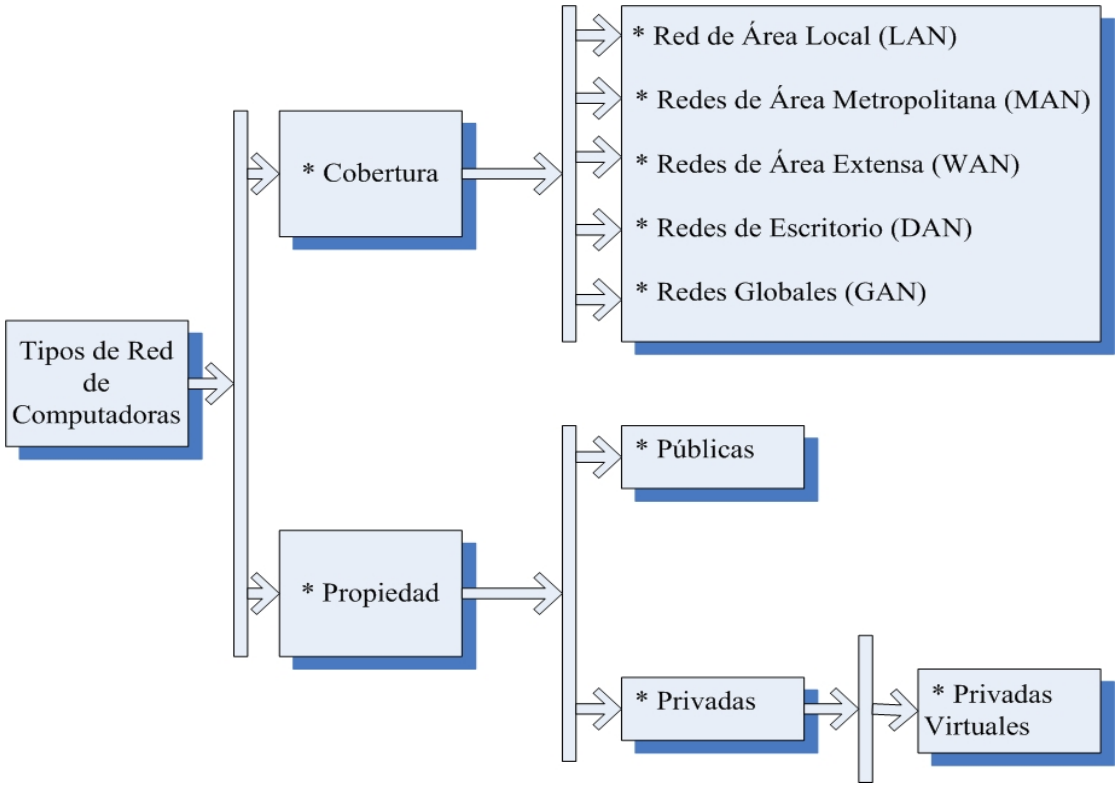

Figura 2.12 *Tipos de Redes.*

2.6 Definición de Red Privada Virtual

Una Red Privada Virtual (VPN, Virtual Private Network) es un proceso de comunicación cifrada o encapsulada que transfiere datos de un punto a otro de manera segura; la seguridad de los datos se logra gracias a una tecnología robusta de cifrado, y los datos que se transfieren pasan a través de una red abierta, insegura y enrutada. Las redes privadas virtuales "son una estructura donde el cifrado, la autenticación y la confidencialidad pueden coexistir y operar". Desde un punto de vista más simple, una VPN es un método para conectar redes, utilizando Internet para transportar datos; lo que quiere decir que enlaza computadoras y redes entre si. Es virtual, debido a que toda la información que viaja a través de la red se realiza mediante

.

Internet; y es privada, porque los datos se encriptan por medio de un protocolo de túnel. Éste último asegura la transferencia de información a través de la VPN de una compañía. [9]

Los ingenieros de Enterasys Network dicen que, la VPN utiliza técnicas de cifrado y criptografía y está considerada como una solución punto a punto que es adecuada para un amplio margen de aplicaciones, tales como:

- Road warrior: Usuario móvil que puede conectarse desde cualquier lugar a su red corporativa.
- Horne Office: Permite a cualquier empleado trabajar desde su casa.
- Branch Office: Posibilita a un grupo de empleados trabajar desde oficinas remotas.
- Business to Business Partners: Establece e interconecta recursos de información con los principales socios comerciales de una empresa. [9]

De cualquier forma, el sistema de Red Privada Virtual es la mejor opción para conectar sucursales y oficinas entre ellas. Así se pueden intercambiar archivos, facturas, contratos y todo tipo de datos sin tener que pedirlos, y directamente de la máquina que hace de servidor. En algunos casos los requisitos mínimos para que funcione correctamente, son que la máquina "Usuario VPN" tenga una conexión a Internet, igualmente que la máquina "Servidor VPN"; esta conexión debe tener un ancho de banda considerable para que los problemas a la hora de pasar datos sean nulos; las conexiones más recomendadas son el ADSL o el cable, pero si no se tiene acceso a este tipo de conectividad, se pueden utilizar de velocidades inferiores como por ejemplo una línea RDSI. Como último requisito el cliente y el servidor deberán de tener una IP fija. En la Figura 2.13 se muestra un sistema de Red Privada Virtual entre una intranet de usuarios que se conectan al "Servidor VPN", es decir, una conexión simple entre Usuario -Servidor. [10]

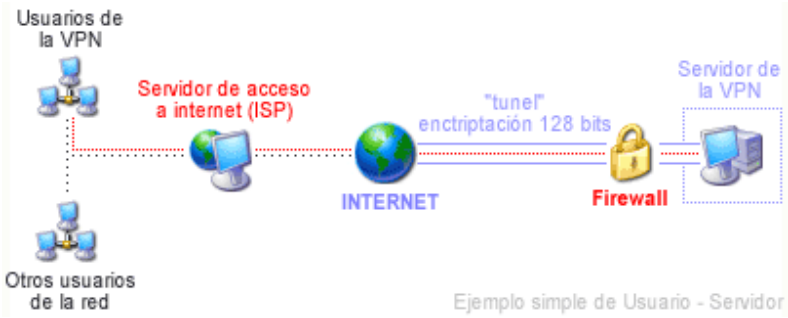

Figura 2.13 *Sistema de Conexión simple Usuario - Servidor.*

.

En este caso específico, el sistema VPN cuenta con un "**Túnel**" de encriptación de 128 bits y un "**Firewall**"; el primero aísla a los otros usuarios de la red y el segundo protege al servidor de la entrada de IP's que no son de la misma VPN. De esta manera solo tienen acceso los usuarios que el "Servidor VPN" tiene añadidos como clientes con su correspondiente IP. Este sistema de conectividad privada es la forma más económica y fiable del mercado para mantener conectados diversos puntos (computadoras) de cualquier parte del mundo. [10]

Una VPN es una red corporativa implantada sobre una red de recursos de transmisión y conmutación públicas, que utiliza la misma gestión y políticas de acceso que se utilizan en las redes privadas. En la mayoría de los casos la red pública es Internet, pero también puede ser una red ATM o Frame Relay. Puede definirse como una red privada que se extiende, mediante procesos de encapsulación y cifrado (encriptación) de los paquetes de datos a distintos puntos remotos, mediante el uso de unas infraestructuras públicas de transporte, como la Internet. [8]

Red Privada Virtual, es una red privada (red con acceso restringido) construida sobre la infraestructura de una red pública (recurso público, sin control sobre el acceso a los datos), normalmente Internet. Así que, en vez de utilizar enlaces dedicados o redes de paquetes (como X.25 y Frame Relay) para conectar redes remotas, se utiliza la infraestructura de Internet. Para los usuarios la forma como están conectadas es transparente. [7]

Una Red Privada Virtual es un servicio que transforma la Internet en una red global segura para dirigir negocios y comercios, ya que hace posible conectar los recursos y componentes de una red a otra en lugares distantes, con el fin de compartir y transmitir la información de forma segura y confidencial entre la empresa y sus sucursales, socios, proveedores, distribuidores, empleados y clientes utilizando una red pública como canal para comunicar los datos privados.
Una Red Privada Virtual en IP, es una conexión privada entre dos o más computadoras que intercambian tráfico privado a través de una red pública compartida como Internet. Esta tecnología permite a las organizaciones extender sus servicios de red, a través de Internet, hacia sus sucursales y usuarios remotos creando una WAN (Wide Area Network) privada vía Internet. [13]

2.7 Requerimientos básicos de las VPN

Por lo general, al implementar una solución de red remota, una compañía desea facilitar un acceso controlado a los recursos y a la información de la misma. La solución deberá permitir la libertad para que

.

los clientes roaming o remotos autorizados se conecten con facilidad a los recursos corporativos de la red de área local (LAN) así como las oficinas remotas se conecten entre si para compartir recursos e información (conexiones de N). Por último, la solución debe garantizar la privacidad y la integridad de los datos al viajar a través de Internet público. Lo mismo se aplica en el caso de datos sensibles que viajan a través de una red corporativa. Por lo tanto, como mínimo, una solución de VPN debe proporcionar lo siguiente:

Autenticación de usuario. La solución deberá verificar la identidad de un usuario y restringir el acceso de la VPN a usuarios autorizados. Además, deberá proporcionar registros de auditoría y contables para mostrar quién accedió a qué información y cuándo.

Administración de dirección. La solución deberá asignar una dirección al cliente en la red privada, y asegurarse de que las direcciones privadas se mantengan así.
Encriptación de datos. Los datos que viajan en una red pública no podrán ser leídos por clientes no autorizados en la red.

Administración de llaves. La solución deberá generar y renovar las llaves de encriptación para el cliente y para el servidor.

Soporte de protocolo múltiple. La solución deberá manejar protocolos comunes utilizados en las redes públicas; éstos incluyen Protocolo de Internet. Una solución de VPN de Internet basada en un Protocolo de túnel de punto a punto (PPTP) o un Protocolo de túnel de nivel 2 (L2TP) cumple con todos estos requerimientos básicos, y aprovecha la amplia disponibilidad de Internet a nivel mundial. [12]

2.8 VPN de acceso remoto.

(Remote Access VPNs). Provee acceso remoto a la intranet o extranet corporativa a través de una infraestructura pública, conservando las mismas políticas, como seguridad y calidad de servicio, que en la red privada. Permite el uso de múltiples tecnologías como discado, ISDN, xDSL, cable, o IP para la conexión segura de usuarios móviles, telecommuters o sucursales remotas a los recursos corporativos.

Características:

- Outsourcing de acceso remoto
  - llamadas locales o gratuitas (n° 900)

.

  - ubicuidad del acceso
- Instalación y soporte del PS (Proveedor de servicio)
- Acceso único al nodo central (elimina la competencia por puertos)
- Tecnologías de acceso RTC, ISDN, xDSL
- Movilidad IP
- Seguridad reforzada por el cliente
  - AAA en el ISP proporciona 1° y posiblemente 2° nivel de seguridad.

2.9 VPN de intranet.

Vincula la oficina remota o sucursal a la red corporativa, a través de una red pública, mediante enlace dedicado al proveedor de servicio. La VPN goza de las mismas cualidades que la red privada: seguridad, calidad de servicio y disponibilidad, entre otras.
Característica:

- Extiende el modelo IP a través de la WAN compartida.

2.10 VPN de extranet.

Permite la conexión de clientes, proveedores, distribuidores o demás comunidades de interés a la intranet corporativa a través de una red pública (ver figura 2.14 "Extranet VPN"). [12]

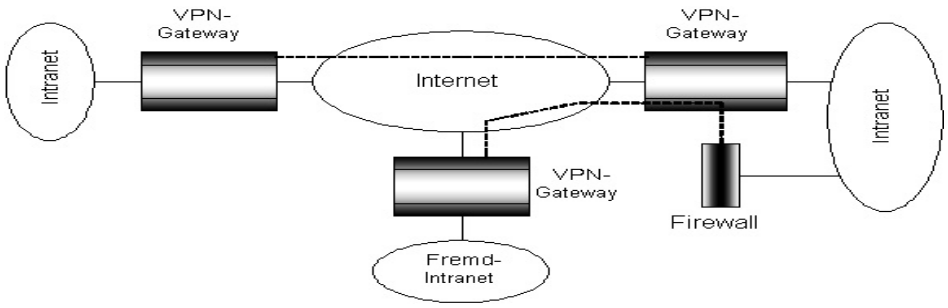

Figura 2.14 *"Extranet VPN"*.

Características:

- Extiende la conectividad a proveedores y clientes
  - sobre una infraestructura compartida
  - usando conexiones virtuales dedicadas

.

- Los pharters tienen diferentes niveles de autorización
  - access control lists, firewalls, filtros, según decida la empresa.

2.11 VPN Solución por Software

Estos sistemas son ideales para las situaciones donde los dos puntos de conexión de la VPN no están controlados por la misma organización, o cuando los diferentes cortafuegos o routers no son implementados por la misma organización. Este tipo de VPN's ofrecen el método mas flexible en cuanto a el manejo de tráfico. Con este tipo, el tráfico puede ser enviado a través de un túnel, en función de las direcciones o protocolos, en cambio en los VPN por hardware, todo el tráfico es enrutado por el túnel. Podemos hacer un enrutamiento inteligente de una manera mucho más fácil.

El Protocolo de Túnel Punto-a-Punto (Point to Point Tunneling Protocol) es un protocolo que Permite establecer conexiones con túneles PPP, a través de una red IP, creando una VPN. La Compañía Microsoft, ha implementado sus propios algoritmos y protocolos con soporte PPTP, el Microsoft PPTP, y este es uno de los mas ampliamente extendidos, por la popularidad de los Productos Microsoft (Windows 98/ME, NT4, 2000, XP, vista, 2000 Server, 2003 Server, ISA Server 2004 y 2006, 2008 Server) los cuales llevan incluidos de serie estos protocolos.

Tenemos por ejemplo a las soluciones nativas de Linux (Debian, Fedora and Red Hat Enterprise Linux (RHEL), Gentoo, Mandriva, Slackware, SUSE Linux Enterprise / OpenSUSE, Ubuntu y los Unix en general. Todos ellos ocupan código abierto como OpenSSH (es un conjunto de aplicaciones que permiten realizar comunicaciones cifradas a través de una red, usando el protocolo SSH), OpenVPN(es una solución de conectividad basada en software: SSL (Secure Sockets Layer)) y FreeS/Wan(utiliza una implementación estandarizada de IPSec (o Protocolo de Internet de Seguridad)). En tanto que para los clientes GNU/Linux, el programa a usar es el pptp-linux, que sirve para acceder a servidores VPN corriendo GNU/Linux, o distribuciones Windows.

Además de Apple - Mac OS X Server y algunas de las herramientas que nos proporciona cisco para la configuración del cliente, “Cisco VPN Client” para Windows, Mac y Linux.
Es importante señalar, que además requieren otro conjunto de componentes. Estos componentes son simples requisitos que garantizan que la red sea segura, esté disponible y sea fácil de mantener.

.

Luego de realizar análisis comparativos entre las soluciones para configurar VPNs basadas en software y hardware se decidió que este proyecto se base en los tipos de soluciones basados en software ya que mediante la combinación de ciertos factores, brinda mayores beneficios tanto en seguridad y desempeño como en costos a los usuarios de presidencia de pachuca de soto hidalgo.
Algunas de las herramientas que nos proporciona cisco para la configuración del cliente son "Cisco VPN Client" para Windows, Mac y Linux.

Microsoft proporciona desde Windows NT, 2000 server, 2003 server y versión beta de prueba el server 2008, ISA Server 2006 de Microsoft como servidor VPN.

2.12 VPN Solución por Hardware

Como ya se sabe, los dispositivos de red Cisco cuentan para su administración con un software de sistema operativo llamado IOS (Sistema operativo de internerworking) mediante el cual es posible realizar las configuraciones necesarias de los dispositivos. Como por ejemplo el router Cisco 3640, Cisco 2620

El algoritmo de encripción a utilizar es el DES o Estándar de Encripción de Datos, por sus siglas en inglés. Es un esquema de encripción de llave secreta basado en el algoritmo Lucifer de IBM. Los dispositivos Cisco usan el algoritmo DES para encriptación clásica, encriptación de IPSEC y para los cortafuegos (Firewalls) PIX.

2.12.1 Equipos para Redes privadas virtuales

VPN Gateway: Dispositivos con un software y hardware especial para proveer capacidad a la VPN. Varias funciones son optimizadas sobre varios componentes de software y hardware. Algunos ejemplos de esto tenemos Alcatel 7130,Altiga C10, VPN−1 Gateway, Lucent VPN Gateway, Intel Shiva Lan Rover VPN Gateway Plus, TimeStep Permit/Gate 4620 y VPNet VPNware VSU−1010, las cuales incluyen el software y hardware necesario para realizar y administra VPN. Acatel 7130 Gateways de VPN

Sólo Software: El software está sobre una plataforma PC o Workstation, el software desempeña todas las funciones de la VPN. Algunos ejemplos de esto el Sistema Operativo Windows 9x, ME, NT, 2000 y XP

.

Basado en Firewall: Funciones adicionales son agregadas al firewall para habilitar capacidades de VPN. Algunos ejemplos de esto son los modelos PIX de Cisco como 506, 515, 525 y 535. Cisco 535 Secure PIX Firewall 535

Basado en Router: Funciones adicionales son agregadas al router para habilitar capacidades de VPN, las cuales se encuentran en el IOS de los router de Cisco como los modelos 804, 806, 827, 905, 1710, 1720, 1750, 2611, 2621, 2651, 3620, 3640, 3660, 7120, 7140 y 7200. Aunque los router son mejores que los concentradores, existen algunos capaces de realizar VPN como los modelos 3005, 3015, 3030, 3060 y 3080.

2.13 Conexión de las redes sobre Internet

Existen dos métodos para utilizar VPN a fin de conectar redes de área local a sitios remotos:
Uso de líneas dedicadas para conectar una sucursal a una LAN corporativa. En lugar de utilizar un circuito dedicado de arrastre extenso entre la sucursal y el hub corporativo, tanto los ruteadores del hub de la sucursal corno el corporativo pueden emplear un circuito dedicado local e ISP local para conectarse a Internet. El software VPN utiliza las conexiones ISP locales y el Internet público, con el propósito de crear una red privada virtual entre el ruteador de la sucursal y el del hub corporativo.

Uso de una línea de marcación para conectar una sucursal a una LAN corporativa. A cambio de que el ruteador en la sucursal realice una llamada de larga distancia (0 1800) a un NAS corporativo o externo, el ruteador en la sucursal puede llamar al ISP local. El software VPN utiliza la conexión al ISP local para crear una red privada virtual entre el ruteador de la sucursal y el del hub corporativo, a través de Internet.

Note que en ambos casos las facilidades que conectan la sucursal y la oficina corporativa a Internet son locales; se recomienda que el ruteador del hub corporativo que actúa como un servidor VPN se conecte a un ISP local con una línea dedicada. Este servidor VPN puede estar listo 24 horas al día para tráfico VPN entrante. [12]

2.14 Conexión de computadoras sobre una intranet

En algunas redes corporativas los datos departamentales son tan sensibles, que la LAN está físicamente desconectada del resto de la intranet corporativa. Aunque esto protege la información confidencial del

.

departamento, crea problemas de acceso a la información para otros usuarios que no están conectados en forma física a la LAN separada.

Las VPN permiten que la LAN del departamento esté físicamente conectada a la intranet corporativa, pero separada por un servidor. Nótese que el servidor VPN no está actuando como un ruteador entre la intranet corporativa y la LAN del departamento.

Un ruteador interconectaría las dos redes, lo que permitiría que todos tuvieran acceso a la LAN sensible. Pero al utilizar una VPN el administrador de sólo los la red puede asegurar que solo los usuarios en la intranet corporativa, que tienen el nivel adecuado (basado en una política de lo que necesiten saber dentro de la compañía), pueden establecer una VPN con el servidor VPN y tener acceso a los recursos protegidos del departamento. Además, todas las comunicaciones a través de la red efectos VPN pueden encriptarse hay que de confidencialidad de datos. Tomar en cuenta que los usuarios que no tienen el nivel adecuado no podrán ver la LAN del departamento. [12]

2.15 Conclusiones

La realidad es que las VPN aseguran el envío de información en todos los caminos y en cualquier circunstancia en que sea requerida la seguridad de la misma, como ya vimos en este capítulo las VPN se hacen de diferentes artificios para lograr lo que en la actualidad es, una red con los beneficios que la información en una organización requiere para ser transmitida.

.

CAPITULO III
IMPLEMENTACIÓN DEL SERVIDOR VPN

3.1 Introducción

Ahora se procederá a la implementación de la configuración de la Red Privada Virtual en el servidor de Presidencia de Pachuca de Soto, para ello se aplicará todo lo relacionado con los capítulos anteriores, se instalará el servicio de VPN paso a paso basado en un Windows Server 2003 ya que es el sistema operativo que se tiene instalado en el servidor de la Presidencia, sobre dicho servidor tiene instalado 2 tarjetas de red y un soporte de hardware suficiente para las demandas de los usuarios en presidencia que van desde una base de datos como por ejemplo el sistema de administración "Tonalli" entre otros servicios de red, impresoras, archivos, y algunos otros.

Es importante hacer mención que para la implementación de este proyecto se debe tener acceso total al servidor, además de que la configuración de algunos componentes requerirán del reinicio de este y, considerando que todo el personal debe estar comunicado no se realizará en horas laborales del H. Ayuntamiento.

3.2 Configuración de las tarjetas de red del servidor VPN

Figura 3.1 *Conexiones de red.*

Dentro del menú inicio se da clic en la opción conexiones de red y ahí se encontrarán las dos tarjetas de red, para la aplicación estas se renombrarán a conexión externa; la que permitirá acceso a Internet y que usa una IP WAN, la segunda tarjeta red será denominada conexión local que es de donde se toma la salida para distribuir los servicios internos de presidencia entre ellos el Internet, figura 3.1.

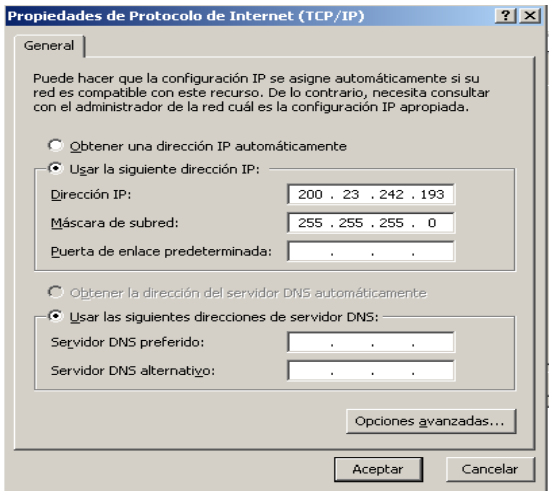

Figura 3.2 *Propiedades TCP/IP, conexión externa.*

Dar clic derecho a la conexión externa, entrar a las propiedades del protocolo TCP/IP de lo cual se supondrá la siguiente dirección IP 200.23.242.193 y un mascara 255.255.255.0 ya que por seguridad y reglamento interno de presidencia no se mostraran los reales, figura 3.2

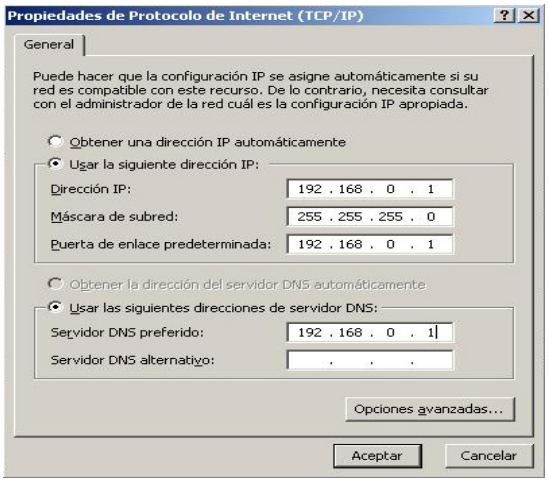

Figura 3.3 *Propiedades TCP/IP, conexión interna.*

En seguida accesar a las propiedades del protocolo TCP/IP de conexión local con lo cual se supondrá la siguiente dirección IP 192.168.0.1, mascara 255.255.255.0, puerta de enlace 192.168.0.1 y en DNS se asignará como preferido 192.168.0.1, figura 3.3.

3.3 Asistente para configurar funciones típicas del Server 2003

Figura 3.4 *Administrador del servidor*.

En el menú inicio se deberá buscar la opción Administre su servidor, ya accesado a esta opción en seguida se da clic en la flecha verde que indica agregar o quitar función. (Figura 3.4), en seguida la figura 3.5 se nos dará un aviso de los procedimientos que tuvimos que haber realizado antes de comenzar con la configuración, instalar módems, conexión de cables, acceso a Internet, etc.

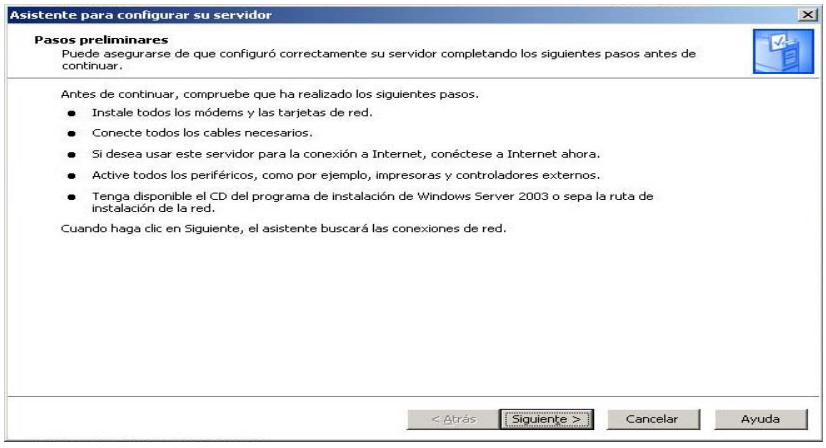

Figura 3.5 *Asistente de configuración.*

Figura 3.6 *Detección de red.*

El asistente comenzará a detectar las conexiones de red como se muestra en la figura 3.6.

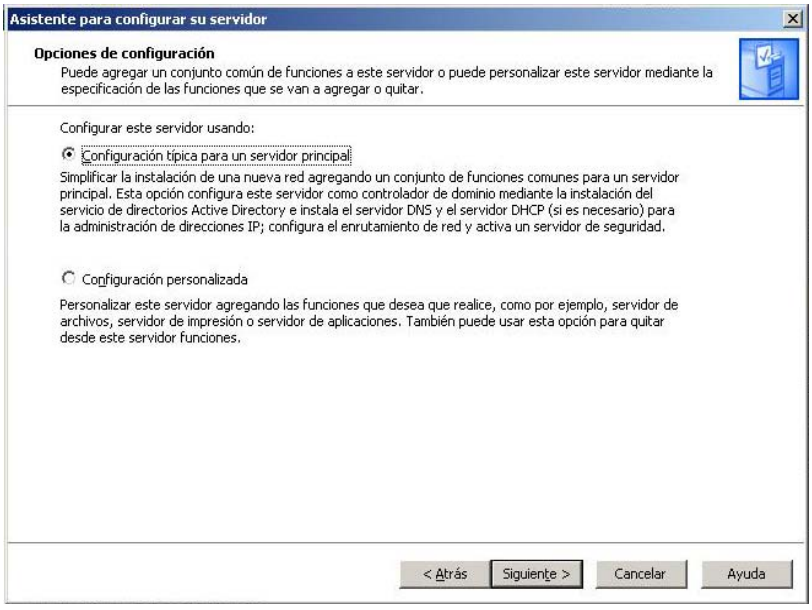

Figura 3.7 *Configuración típica.*

En la figura 3.7 Dejar seleccionada la opción configuración típica para un servidor principal.

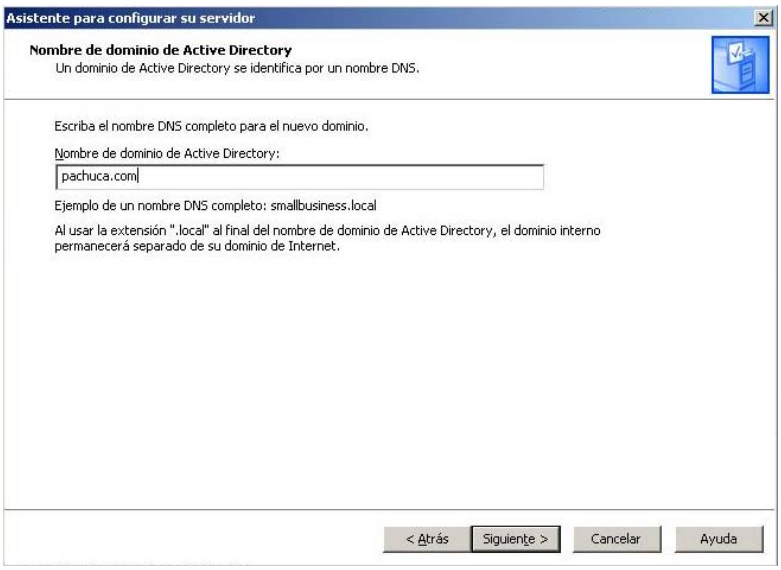

Figura 3.8 *Nombre de dominio.*

Se solicitará un nombre para directorio activo (Active Directory), en este teclear "pachuca.com" o el nombre que desee el administrador, también puede iniciar el asistente directamente ejecutando el archivo ejecutable Dcpromo.exe desde el cuadro de dialogo Ejecutar, figura 3.8

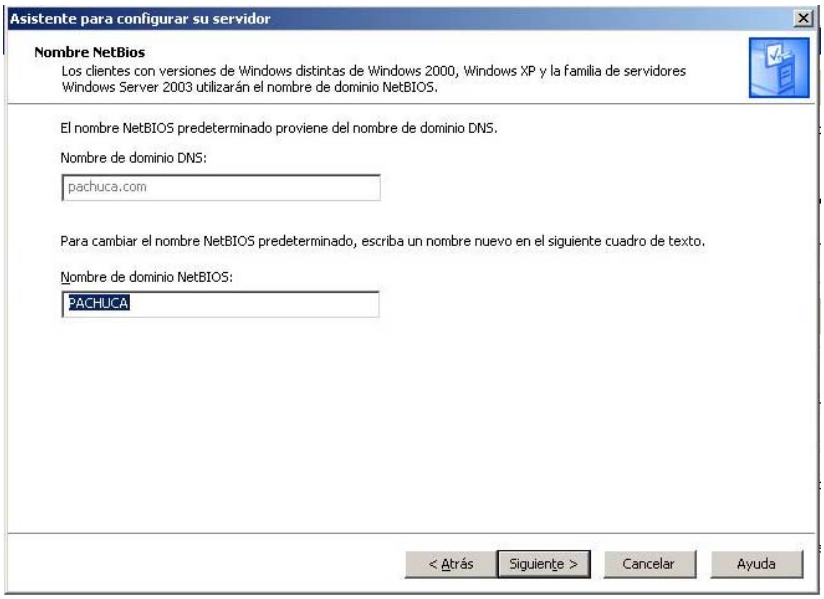

Figura 3.9 *NetBios.*

Posteriormente en nombre de dominio NetBios (Sistema Básico de Entrada/Salida de red) teclear PACHUCA, figura 3.9.

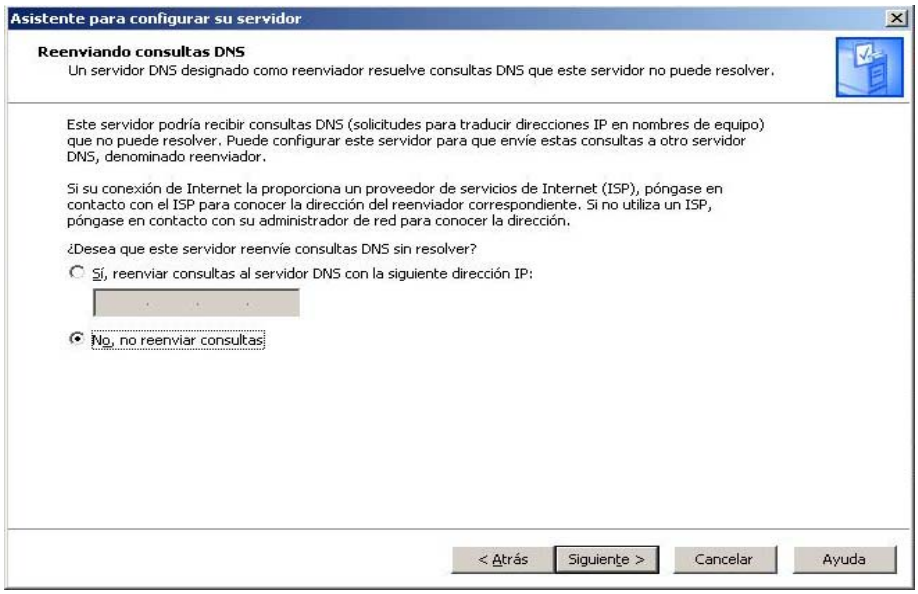

Figura 3.10 *Reenviar consultas DNS.*

Como se muestra en la figura 3.10 se deberá elegir no reenviar consulta de DNS.

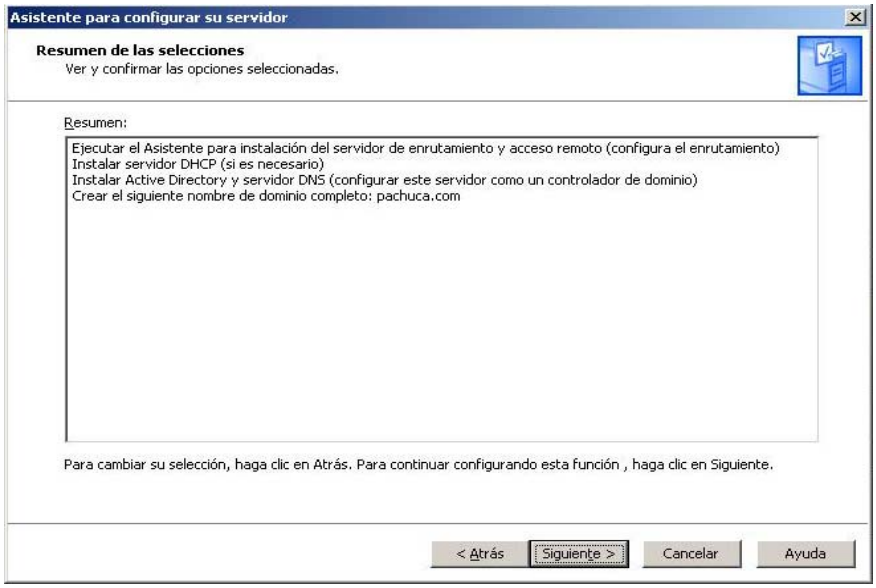

Figura 3.11 *Resumen, servicios adicionados.*

Al dar siguiente en la figura anterior se muestra un resumen de los servicios seleccionados, figura 3.11.

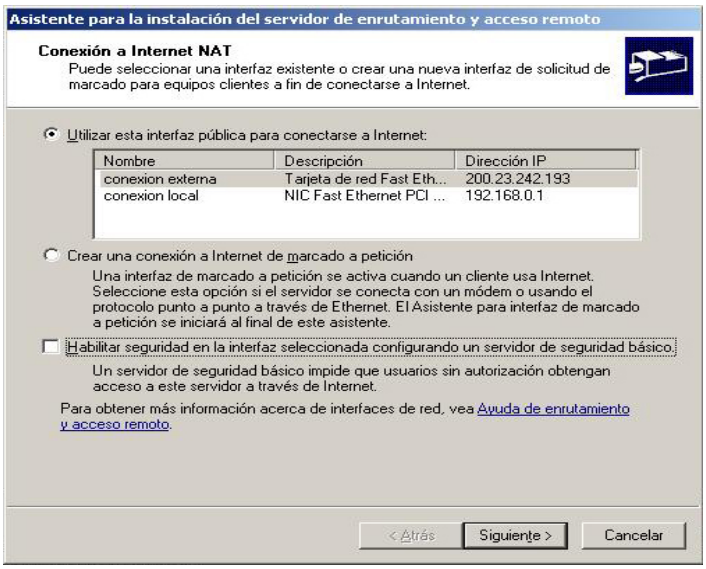

Figura 3.12 *Internet NAT.*

El asistente cuestiona cual es la tarjeta de red que se conectara a internet, se deberá elegir la tarjeta de conexión externa, también se puede elegir crear una conexión a internet de marcado a petición o elegir habilitar el servidor básico de seguridad si es que lo tiene previamente configurado, figura 3.12.

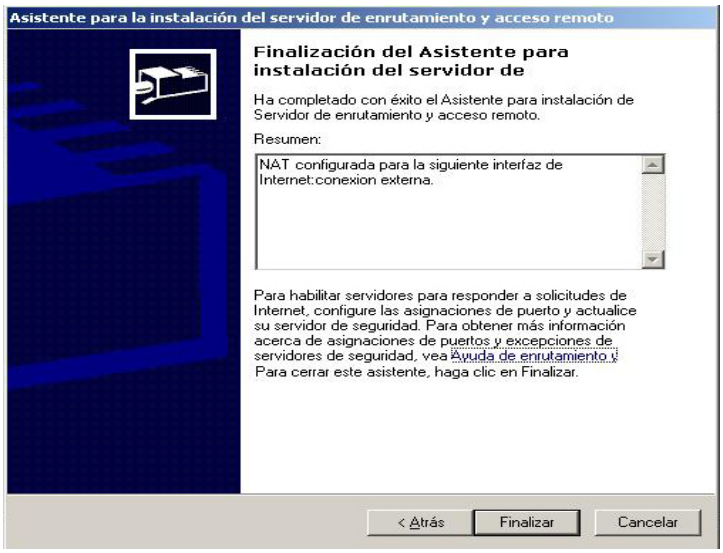

Figura 3.13 *Finalización del asistente.*

Por último hacer clic en Finalizar, figura 3.13.

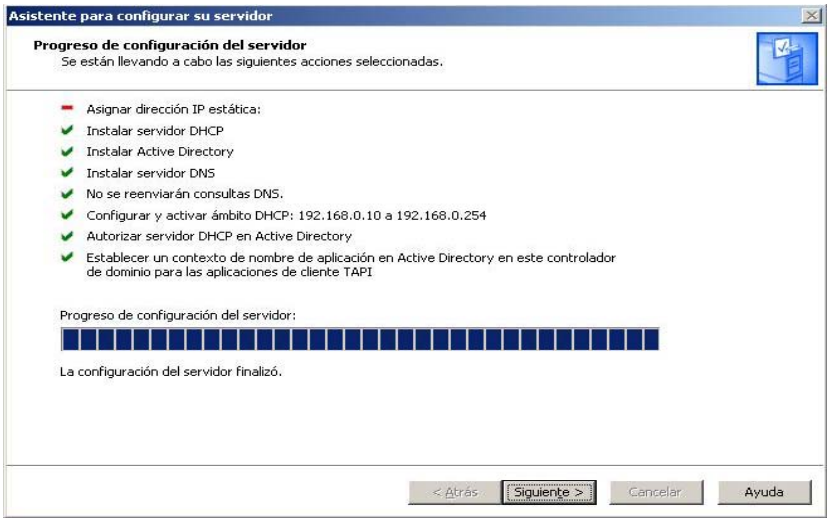

Figura 3.14 *Resumen, servicios adicionados.*

Al finalizar el asistente y después del proceso de instalación de las funciones se muestra un resumen de los servicios instalados aunque falte aun configurar algunas opciones manualmente, figura 3.14.

Figura 3.15 *Indicación de termino de configuración.*

Finamente se indica que el servidor esta configurado. Figura 3.15.

3.4 Configuración DNS

La configuración del DNS indicará el acceso al servidor mediante una página o dirección IP, para ello se seguirá la siguiente ruta inicio/herramientas administrativas/DNS y dar clic para accesar, figura 3.16

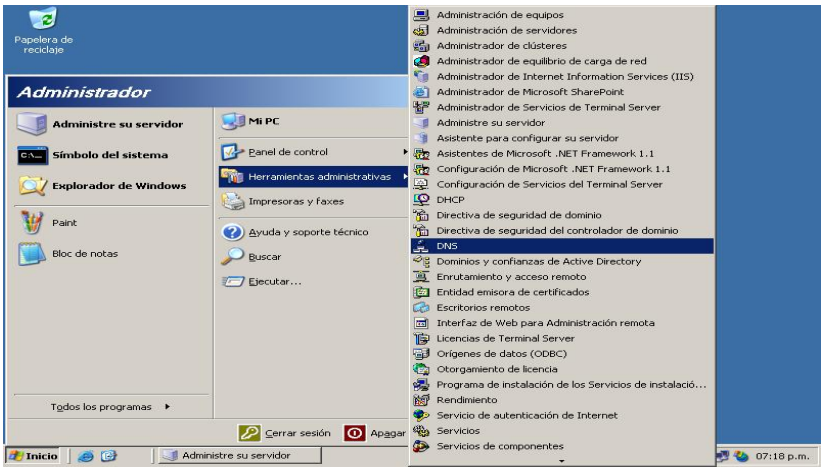

Figura 3.16 *Configuración DNS.*

El DNS se tiene que configurar antes o después de instalar el DA en el servidor. En el caso de instalarlo después de la instalación del directorio activo en el servidor, una de las preguntas que nos hará al promocionar el servidor es si queremos que el asistente nos instale el DNS y pondrá que es la opción recomendada, en esta opción le diremos que lo configuraremos nosotros manualmente. En la consola de DNS crearemos una zona directa nueva.En el árbol que se despliega elegir zona de búsqueda directa/pachuca.com, figura 3.17.

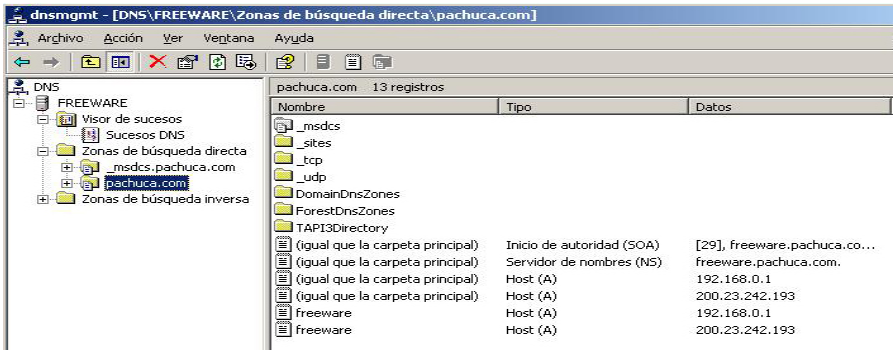

Figura 3.17 *Búsqueda directa (A).*

Dar clic derecho sobre pachuca.com y se deberá elegir Host nuevo (A), figura 3.18

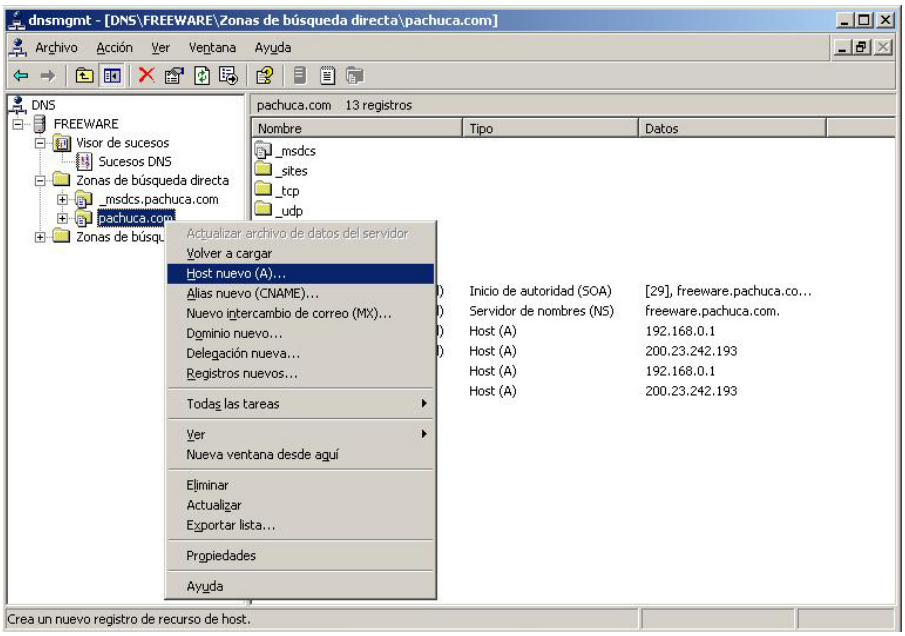

Figura 3.18 *Búsqueda directa (B).*

En el nombre del nombre de dominio FQDN (nombre de dominio totalmente calificado) se escribirá www y en la dirección ip, colocar la ip homologada 200.23.242.193. Una dirección FQDN se caracterizará por una dirección completa y única de tipo www.domaine.com , figura 3.19.

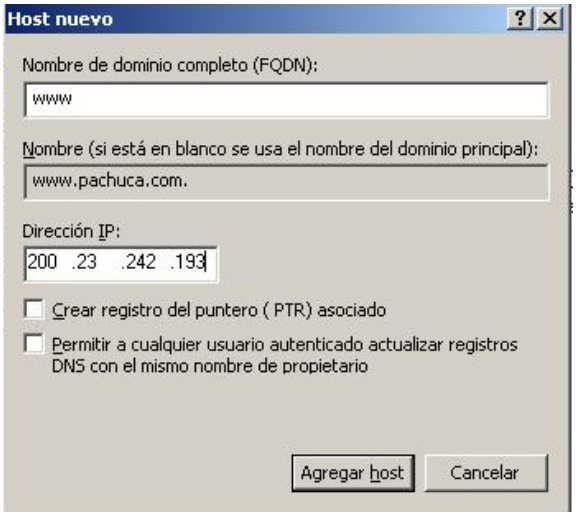

Figura 3.19 *Nuevo Host.*

En el siguiente cuadro se indica que el host fue creado satisfactoriamente, figura 3.20.

Figura 3.20 *Registro exitoso del Host.*

Ahora se prosigue a configurar la zona de búsqueda inversa, la zona inversa lo que nos hace es traducir las direcciones IP en nombres de maquinas, para lo cual se dará clic derecho y en el submenú se elegirá zona nueva, figura 3.21.

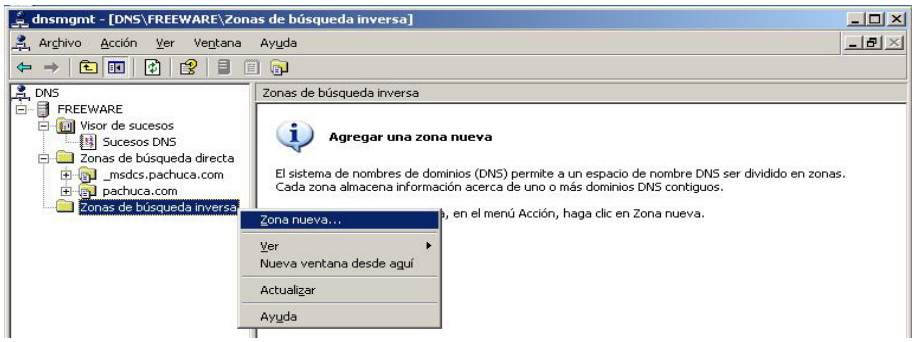

Figura 3.21 *Búsqueda inversa.*

En el cuadro de dialogo desplegado se deberá seleccionar la opción de zona principal y en seguida dar clic en siguiente, figura 3.22.

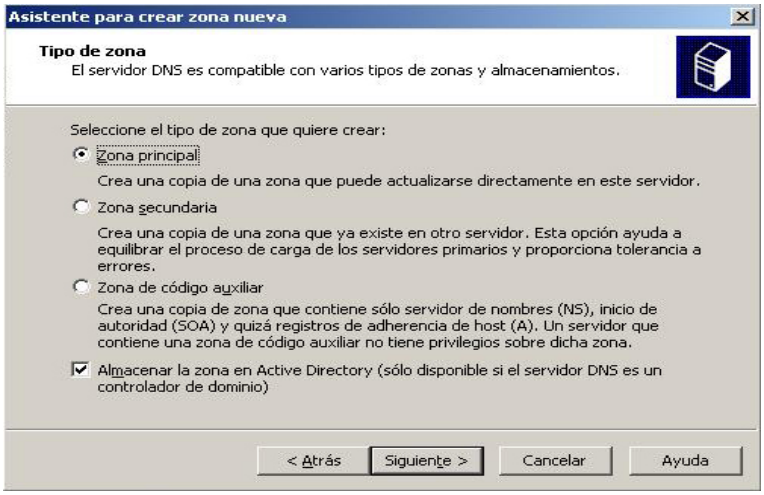

Figura 3.22 *Nueva zona.*

En la figura 3.23 muestra el ámbito de replicación de zona de Active Directory, en la primera opción, todos los servidores DNS del bosque de Active Directory Replica datos de zona en todos los servidores DNS que se ejecutan en controladores de dominio del bosque de Active Directory. Todos los servidores DNS del dominio de Active Directory: Replica datos de zona en todos los servidores DNS que se ejecutan en controladores de dominio del dominio de Active Directory. Esta opción es la configuración predeterminada para la replicación de zonas DNS integradas en Active Directory de la familia Windows Server 2003. Todos los controladores de dominio del dominio de Active Directory: Reproduce datos de zona en todos los controladores de dominio del dominio de Active Directory. Si desea que los servidores DNS de Windows 2000 carguen una zona de Active Directory, deberá seleccionar esta opción para esa zona. Todos los controladores de dominio de una partición de directorio de aplicaciones especificada: Reproduce datos de zona de acuerdo con el ámbito de replicación de la partición de directorio de aplicaciones especificada. Para que una zona se pueda almacenar en la partición de directorio de aplicaciones especificada, el servidor DNS que alberga la zona debe estar inscrito en dicha partición. Para obtener más información, vea Crear una partición de directorio de aplicaciones DNS y Incluir un servidor DNS en una partición de directorio de aplicaciones DNS.

Cuando vaya a decidir la opción de replicación que se debe elegir, tenga en cuenta que cuanto más amplio sea el ámbito de replicación, mayor será el tráfico de red originado por la replicación. Por ejemplo, si elige la replicación de datos de zona DNS integrada en Active Directory en todos los servidores DNS del bosque, se producirá mucho más tráfico de red que si se replican los datos de zona DNS en todos los servidores DNS de un solo dominio de Active Directory de ese bosque. Se elegirá la tercera opción de arriba hacia abajo, y consecuente dar clic en siguiente, figura 3.23.

Figura 3.23 *Ámbito de replicación.*

El dato critico, y el que va a hacer que esto funcione correctamente es el siguiente. Nos pedirá que le introduzcamos el nombre de la zona de búsqueda inversa. Aquí deberemos introducir el rango de ip que maneja nuestro escenario. A continuación debemos especificar la zona de búsqueda inversa que deberá resolver nuestro servidor DNS; indicamos el identificativo de red "200.23.242", para que nuestro servidor DNS haga resolución inversa de cualquier dirección I.P. "200.23.242.x"; cuando completemos dicha "id. de red", observaremos que en "Nombre de la zona de búsqueda inversa" se mostrará el nombre "242.23.200.in-addr.arpa"clic en siguiente, figura 3.24.

Figura 3.24 *Búsqueda inversa*.

El tipo de actualizaciones que vamos a permitir en la zona, en un principio solo permitiremos las actualizaciones dinámicas. Si nos encontramos con algún tipo de problema, ya deberemos realizar un estudio a ver si debemos modificar este parámetro.Como lo muestra la figura 3.25 se deberá elegir la primera opción recomendada para un directorio activo.

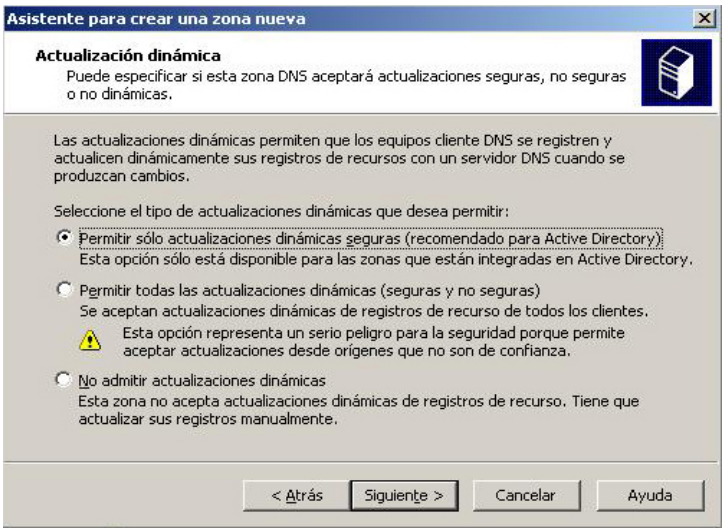

Figura 3.25 *Actualización dinámica*.

Por último dar clic en finalizar el asistente, figura 3.26.

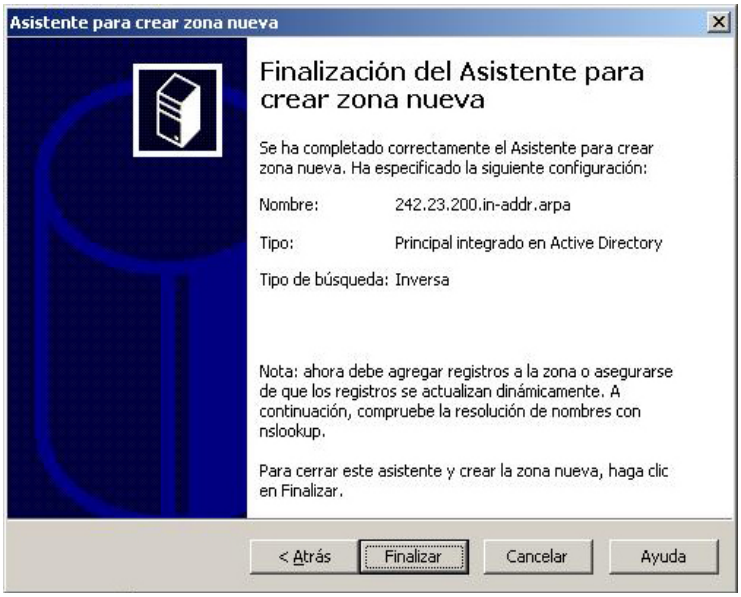

Figura 3.26 *Finalización del asistente.*

Ahora en el árbol desplegado elegir zona de búsqueda inversa/zona nueva y con clic derecho se elegirá nuevo puntero (PTR), figura 3.27.

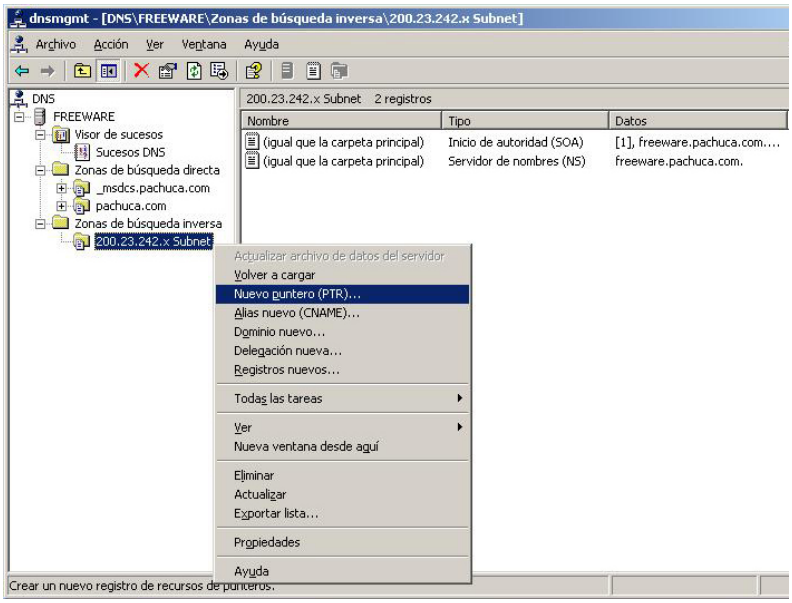

Figura 3.27 *Nuevo puntero.*

En la pantalla que desplegada se deberá teclear 193 en la IP del host, y en nombre de host www.pachuca.com, también existe la posibilidad de marcar la opción de permitir a cualquier usuario autenticado actualizar los registros DNS. Dar clic en aceptar y se cierra la ventana, figura 3.28.

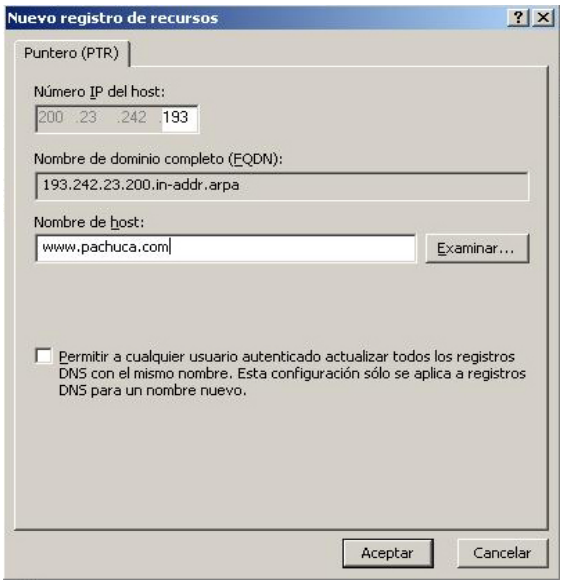

Figura 3.28 *Registro de recursos.*

3.5 Configuración DHCP

Cuando montamos una red, o cuando migramos alguna y tiene direccionamiento fijo nos acordamos de lo bueno q seria tener montado un servidor DHCP y olvidarnos del tema de ir puesto por puesto modificando cualquier dato de red. El DHCP sirve para ahorrar trabajo a un administrador de red, se configuran las IP's desde el servidor, se establece un rango de direcciones IP a asignar a los puestos y ya esta, podemos incluir además, todos los datos que nos interesen a parte de la IP, cómo por ejemplo, cual es la puerta de enlace, DNS, WINS y muchos más. Podemos asignar el tiempo de duración de las IP's en los cliente, por defecto son 8 días. Podemos reservar IP's por direcciones MAC. Y ver el listado de direcciones IP asignadas.La configuración del DHCP es fundamental para que el servidor pueda proveer de una configuración opcional a la computadora cliente y así asignar una dirección automáticamente para que pueda ser parte de la red, para su configuración se debe seguir la ruta Inicio/Herramientas Administrativas y clic en DHCP

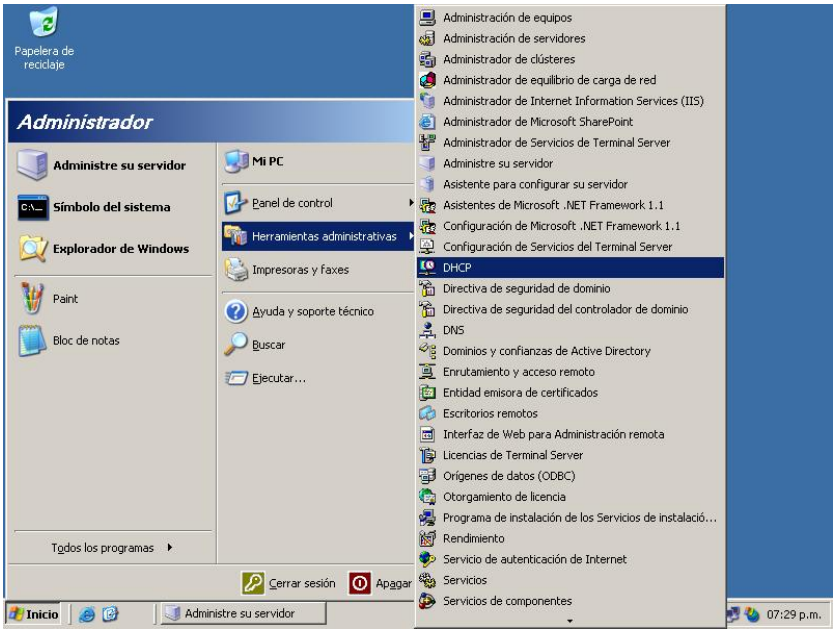

Figura 3.29 *Ruta DHCP.*

El árbol desplegado debe de ser parecido al de la figura 3.30.

Figura 3.30 *Despliegue del DHCP.*

Se puede dar clic derecho en ámbito y ver sus propiedades, aquí se podrá cambiar el nombre del ámbito y darle una descripción, el rango de IP del DHCP y la duración de la concesión de dichas para los clientes, figura 3.31.

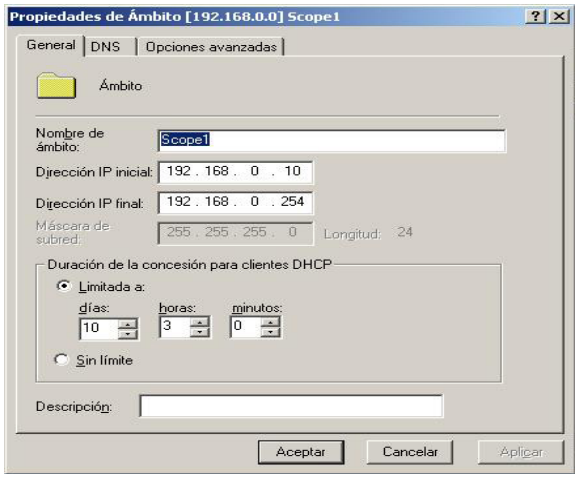

Figura 3.31 *Propiedades de ámbito DHCP.*

3.6 Configuración del enrutamiento y acceso remoto

Al agente encargado de realizar este encaminamiento de información entre redes se conoce como **enrutador** pudiendo ser de tipo hardware si es un dispositivo físico dedicado al encaminamiento y de tipo software en caso de propósito general que ejecutan lógica de encaminamiento. El **acceso remoto** permite a los clientes conectarse a los recursos de una red como si estuviesen físicamente conectados a la misma. Debe existir un agente encargado de recibir la petición del cliente, autentificarla y autorizarla, permitiendo

el acceso. Windows 2003 proporciona el servicio RRAS (Routing and Remote Access Service) que permite efectuar enrutamiento entre redes LAN, WAN y VPN (Virtual Private Network) sin la necesidad de disponer de un dispositivo encaminador dedicado, enrutamiento y acceso remoto se debe establecer debido a que proporciona servicios de enrutamiento de multiprotocolo LAN a LAN, LAN a WAN, red privada virtual (VPN) y traducción de direcciones de red (NAT). Enrutamiento y acceso remoto está destinado a administradores del sistema que ya estén familiarizados con protocolos y servicios de enrutamiento, y con protocolos enrutables como TCP/IP. Para ello se debe ingresar a herramientas administrativas/enrutamiento y acceso remoto, figura 3.32.

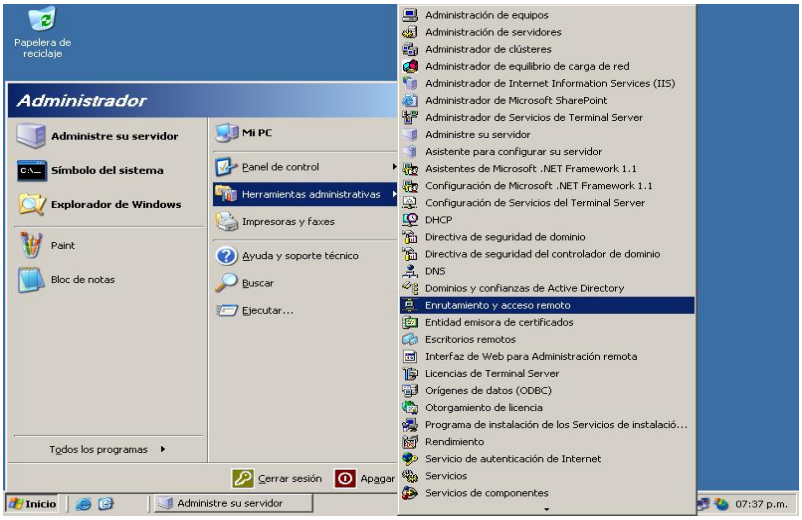

Figura 3.32 *Ruta Enrutamiento y acceso remoto.*

Se desplegará un árbol con estructura parecida a la figura 3.33.

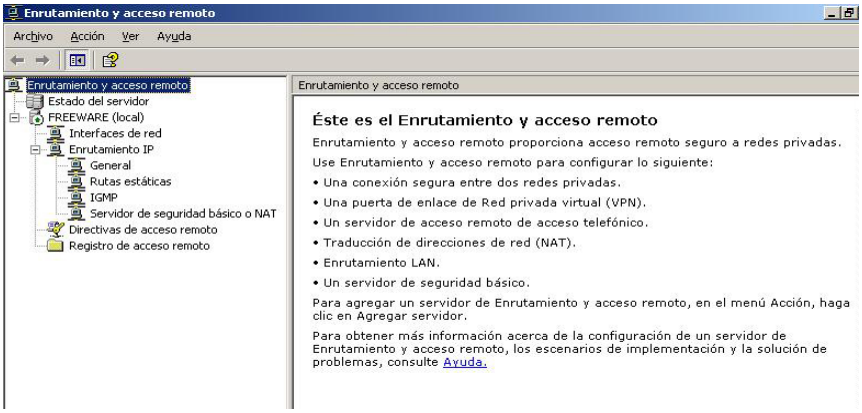

Figura 3.33 *Estructura.*

De la figura 3.34 se dará clic derecho en el servidor en este caso Freeware y de nuevo clic en deshabilitar Enrutamiento y acceso remoto, figura 3.34.

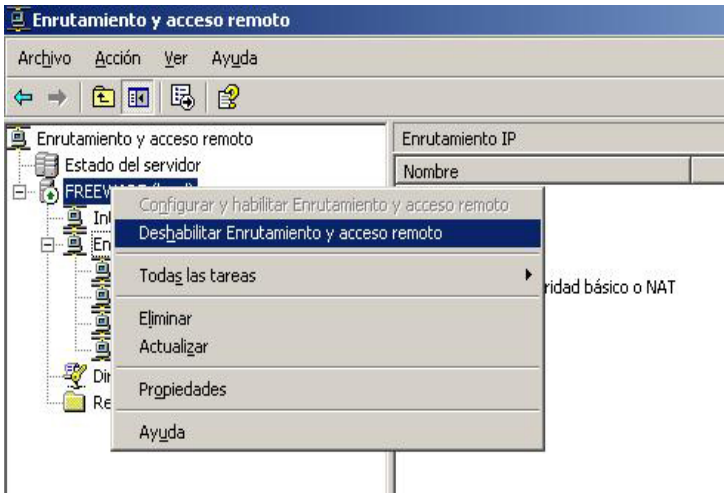

Figura 3.34 *Deshabilitar enrutamiento y acceso remoto.*

Ya deshabilitado el enrutamiento se procede a habilitarlo de acuerdo al asistente.

Figura 3.35 *Configurar enrutamiento.*

De la figura 3.36 se dará clic en siguiente.

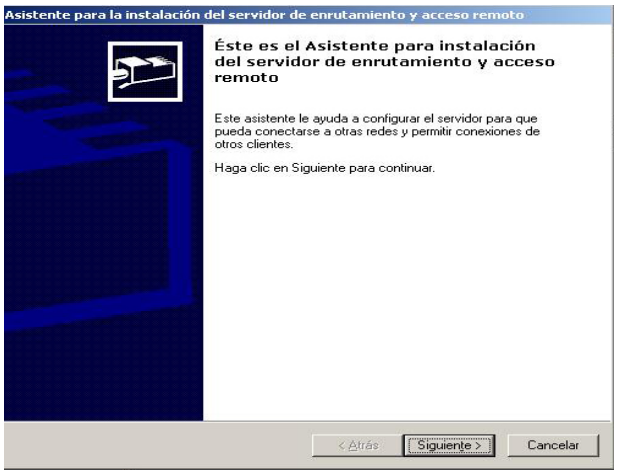

Figura 3.36 *Finalización del asistente.*

Después de elegir siguiente se elige acceso a red privada virtual (VPN) y NAT, con lo cual se permitirá la conexión de los clientes atreves de Internet figura 3.37.

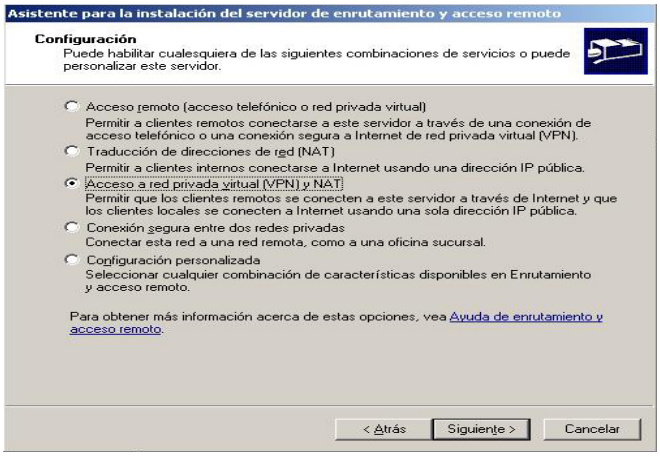

Figura 3.37 *VPN y NAT.*

En la siguiente pantalla se deberá elegir la conexión externa como interfaz a internet y que permitirá a los clientes entrar petición de acceso al servidor, clic en siguiente, figura 3.38.

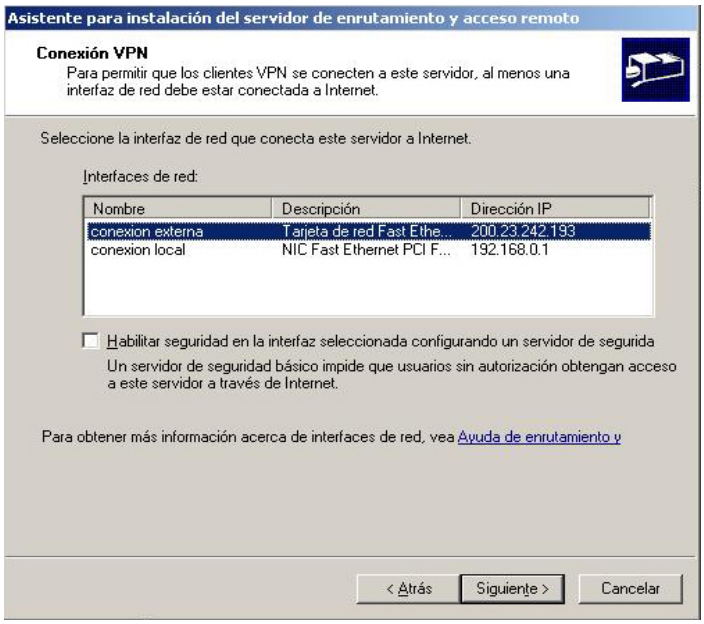

Figura 3.38 *Conexión VPN.*

De la siguiente ventana elegir Automáticamente, si es que tenemos configurado el DHCP correctamente, o elegir asignar un intervalo de direcciones manualmente, enseguida clic en siguiente, figura 3.39

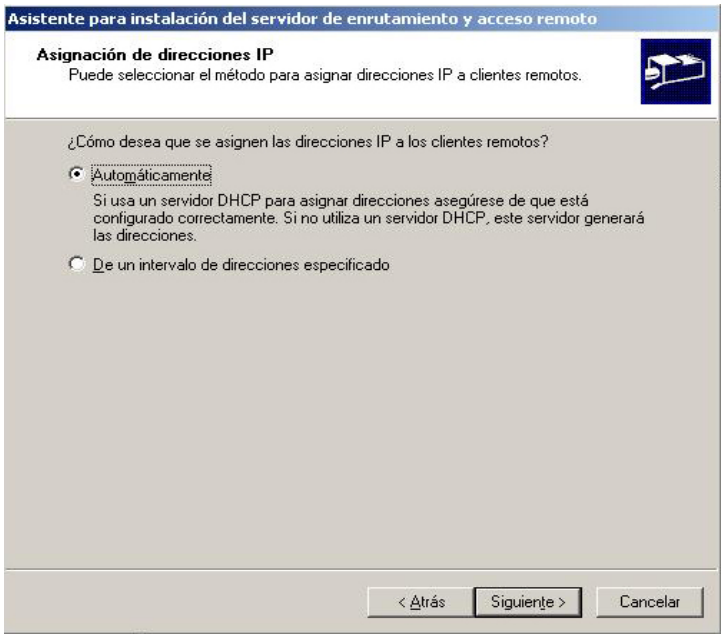

Figura 3.39 *Asignación de direcciones.*

Es importante elegir no usar la configuración de un servidor RADIUS, este protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP no se aplica. Utiliza el puerto 1813 UDP para establecer sus conexiones. Marcar la primera opción y con ello permitir que el enrutamiento y acceso remoto autentifique las solicitudes de conexión, clic en siguiente, figura 3.40.

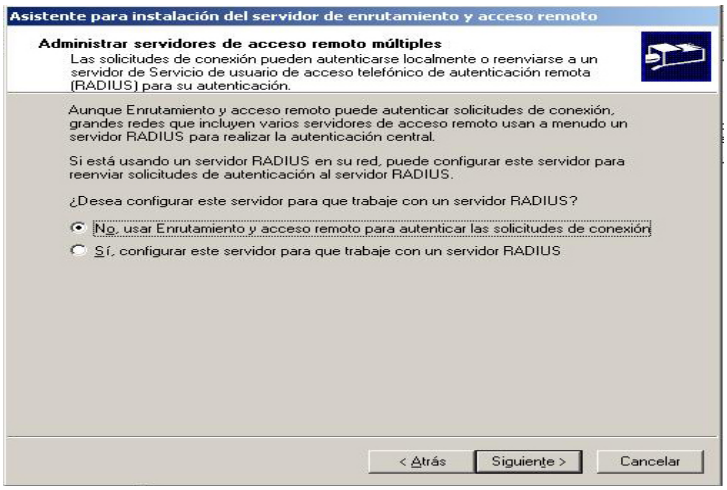

Figura 3.40 *Administrar servidor RADIUS.*

Después de siguiente se finaliza el asistente, figura 3.41.

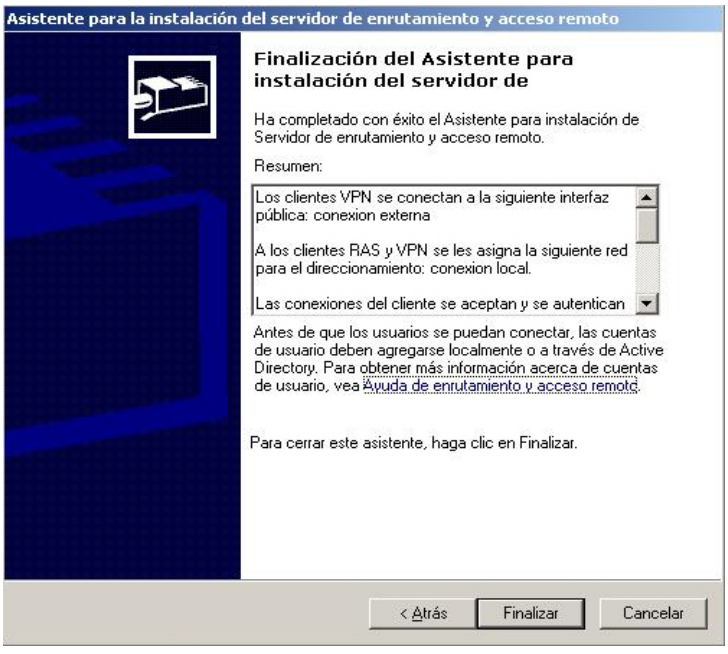

Figura 3.41 *Finalización del asistente.*

El árbol de enrutamiento ahora quedará parecido al de la figura 3.42.

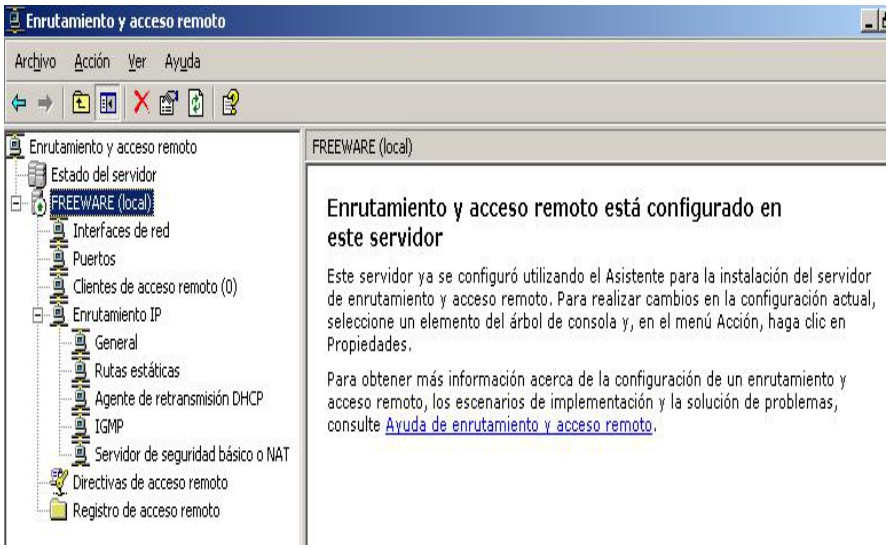

Figura 3.42 *Enrutamiento y acceso remoto.*

3.7 Creación de un usuario en el directorio activo

Active Directory proporciona la exclusiva función de administrar las identidades en Windows Server 2003 junto a las muchas identidades que están dispersas en otros sistemas y plataformas, además de su habilidad de controlar las directivas de seguridad y el acceso a otros recursos. Como resultado, Active Directory puede ser utilizado como un depósito autócrata para las identidades, para información sobre autenticación y autorización que puede ser extendida a otras aplicaciones, sistemas y plataformas. Ahora un usuario puede acceder de forma segura a los recursos de otros dominios con un solo inicio de sesión. Adicionalmente el directorio activo maneja usuarios, grupos o computadores como objetos definidos en él beneficiando sustancialmente a la empresa. Las cuentas de usuarios que gestiona Active Directory son almacenadas en la base de datos SAM (Security Accounts Manager), pero AD no sólo almacena información sobre los usuarios, sino que también mantiene información sobre servidores, estaciones de trabajo, recursos, aplicaciones, directivas de seguridad, etc. Por todo esto la instalación del Directorio Activo en nuestro servidor Windows 2003 es imprescindible si queremos sacar a nuestro sistema operativo servidor, todo el partido posible.

Se comenzará la creación del los usuarios siguiendo la siguiente ruta herramientas administrativas/usuarios y equipos de active directory, figura 3.43.

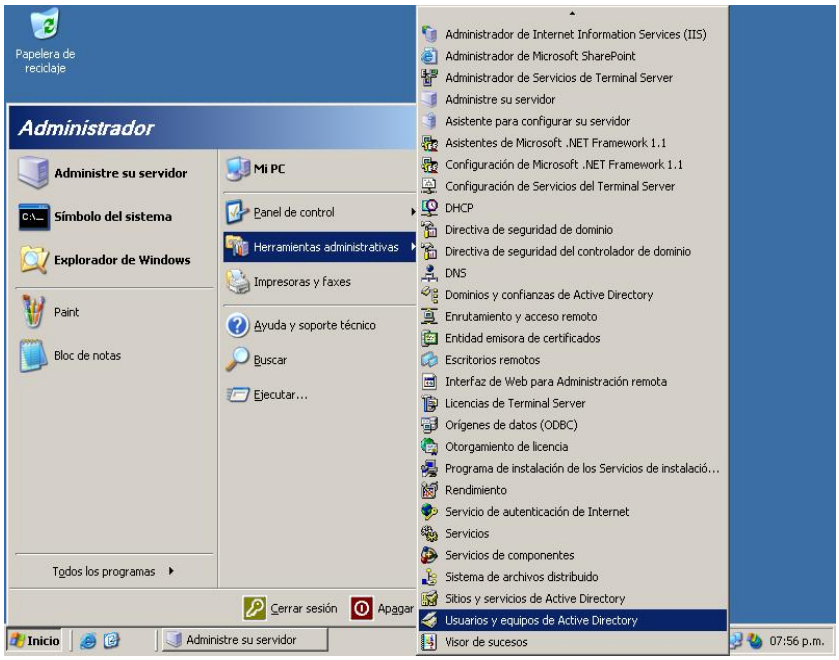

Figura 3.43 *Ruta Active Directory.*

Ahora dar de alta a un nuevo usuario que tendrá acceso con permisos de VPN, figura 3.44.

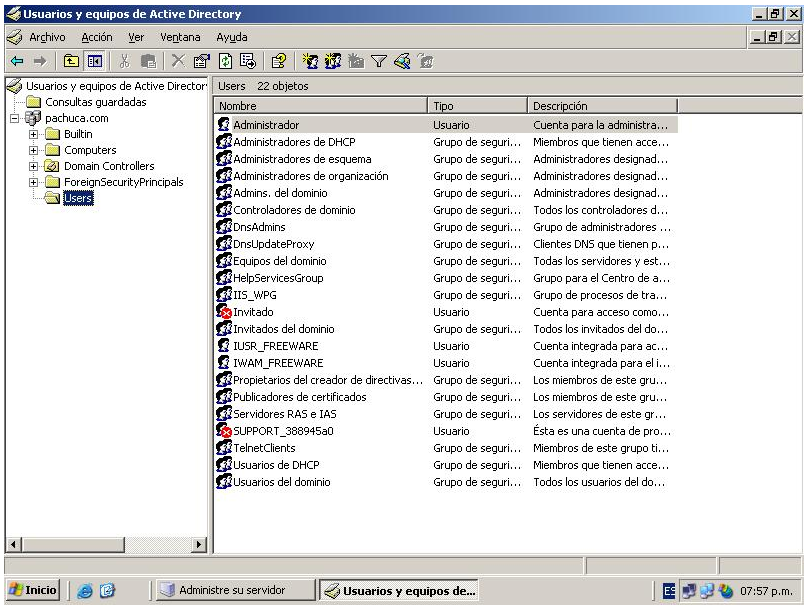

Figura 3.44 *Nuevo usuario (A).*

En la siguiente ventana como se muestra dar clic derecho en users/nuevo/usuario.

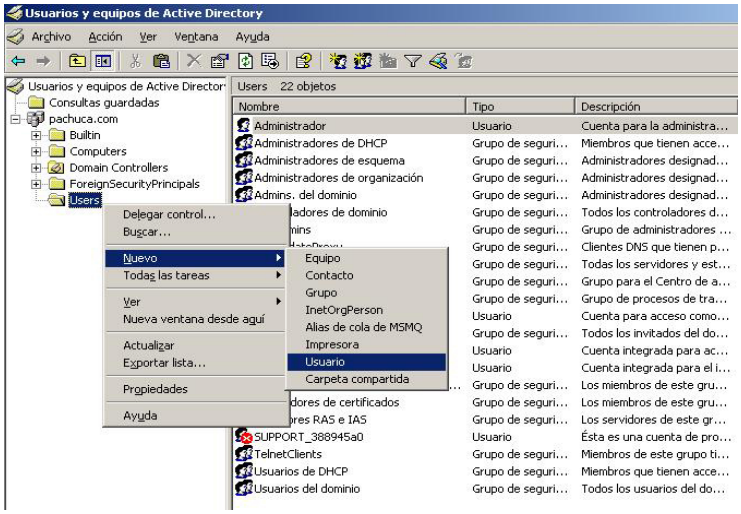

Figura 3.45 *Nuevo usuario (B).*

Se requisitarán los datos como por ejemplo el nombre del usuario sus iniciales, apellidos y automáticamente el sistema dará un nombre completo en base a los 3 primeros datos introducidos, lo siguientes es el nombre de inicio de sesión con la posibilidad de cambiar el nombre de inicio de sesión para loguearse en sistemas de 16 bits o anteriores a Windows 2000, ya que si no hace esto habrá conflictos por símbolos o extensión del nombre de usuario no soportadas en estas versiones. En seguida clic en siguiente, figura 3.46.

Figura 3.46 *Ingresar datos del usuario.*

Ahora se debe considerar que la contraseña debe contener letras y números ya que si es muy simple la seguridad del servidor no aceptará el password, cabe mencionar que se puede habilitar la opción de cambiar la contraseña al iniciar una nueva sesión, que el usuario pueda cambiar la contraseña, la contraseña nunca caduca o la deshabilitar la cuenta si es que el usuario ha infringido alguna norma, una vez hecho esto dar clic en siguiente, figura 3.47.

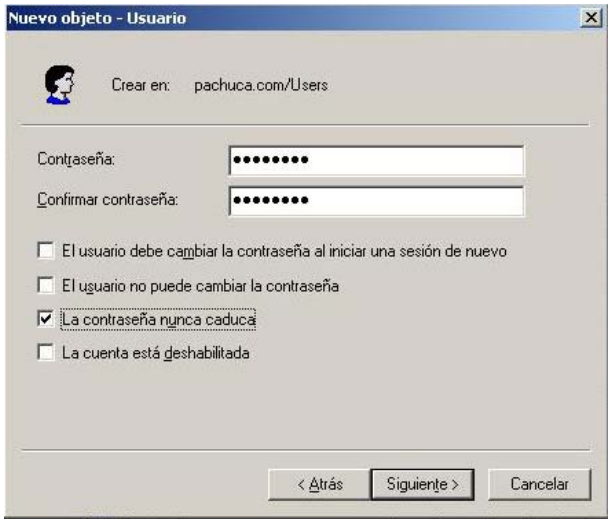

Figura 3.47 *Contraseña.*

La última figura mostrará el resumen del usuario creado con todas las características habilitadas, dar clic en la opción atrás para cambiar algún dato o finalizar, figura 3.48.

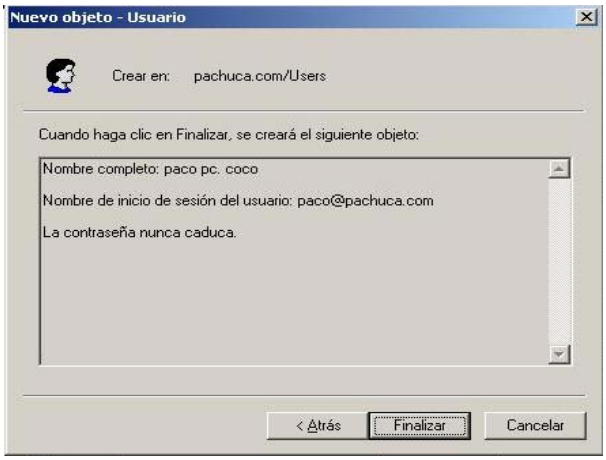

Figura 3.48 *Resumen de los datos del usuario.*

Ya que el usuario ha sido creado posicionarse sobre el usuario creado, y dar clic derecho sobre él, se selecciona la opción propiedades, figura 3.49.

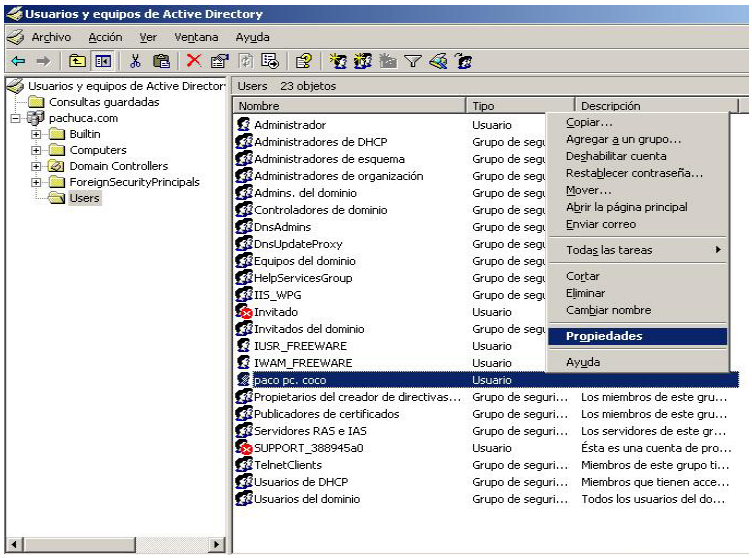

Figura 3.49 *Propiedades del usuario.*

En las propiedades del usuario dirigirse a la pestaña marcado y se deberá elegir permitir acceso o denegar, hay pestañas como la General, donde lo interesante es tener bien puesto sus datos y el "Nombre para mostrar", en la pestaña "Cuenta", podemos indicar en que horas del día puede iniciar sesión, en que equipos puede iniciar sesión, cuando le caduca la cuenta de usuario, la de control remoto es para el uso exclusivo de los servicios de TS (Terminal Server), si queremos que este usuario controle remotamente sesiones de otros usuarios, y si necesita permiso del usuario a controlar, si queremos que sólo vea o que también controle la sesión, en la Ruta de acceso al perfil: Si tenemos perfiles móviles, aquí indicar cuando el usuario inicie sesión de donde cogerá los datos del perfil, la de perfil de servicios de Terminal Server es igual que la de perfil y solo se aplicara cuando un usuario inicie sesión en un Terminal Server (TS). Es importante marcar la ultima opción, que es donde le daremos permiso a un usuario para que inicie sesión o no en un servidor de TS, en "Miembro de" es a que grupos pertenece el usuario, Si queremos que cuando un usuario inicie sesión en un servidor de TS en vez que vea el escritorio tenga acceso sólo a un programa determinado se le indica el path y el ejecutable y ya está. Además tenemos las opciones de que se instalen las impresoras del usuario en el servidor para cuando le de a imprimir imprima por las suyas, en la pestaña sesión *Finalizar una sesión desconectada:* Una sesión desconectada es cuando se cierra la ventana del cliente de TS sin haberle dado a cerrar sesión, es el tiempo que se espera hasta que se finaliza la sesión.

Limite de sesión activa: El tiempo máximo que puede estar logueado un usuario sin cerrar sesión.

Limite de sesión inactiva: El tiempo máximo que puede estar cerrada una sesión desconectada en el servidor TS.

Cuando se alcanza el limite de una sesión o se pierde la conexión: Que hace el servidor cuando un usuario desconecta la sesión o cuando no tiene conexión con el servidor. Si la deja desconectada o la finaliza.

Permitir volverse a conectar: Cuando se desconecta una sesión y se tiene que volver a conectarse el usuario, desde donde se le deja volver a conectarse, si sólo desde su puesto o desde cualquier otro PC. Finalmente al terminar de rellenar cada una de las opciones dar clic en aceptar y cerrar la ventana, figura 3.50.

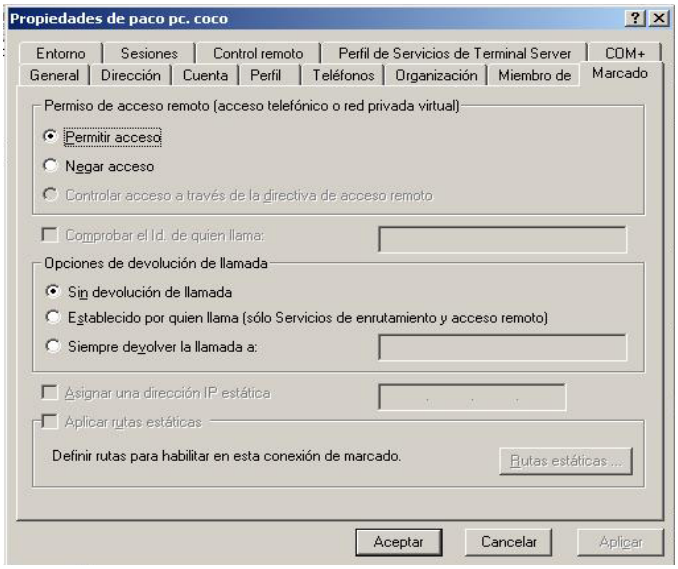

Figura 3.50 *Pestaña marcado.*

Ahora ya se tiene implementado el servidor, configurado y listo para recibir peticiones de VPN, para el siguiente capitulo se tratará como crear un cliente remoto con diferentes sistemas operativos. La figura 3.51 muestra como desde una PC remota con IP 200.23.242.194 se conecta al servidor por medio de VPN y el servidor por medio del servicio de DHCP asigna a dicho cliente una IP 192.168.0.19, y con ello ya se esta dentro del sistema.

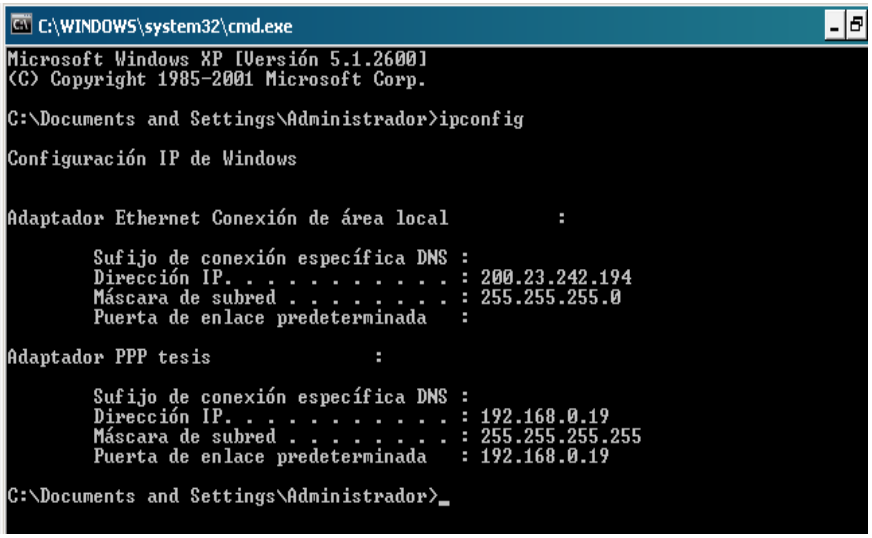

Figura 3.51 *Muestra de la conexión PPP.*

3.8 Seguridad en la VPN

La seguridad interna de la red es, las más veces, menospreciada por sus administradores. Muy a menudo, dicha seguridad incluso no existe, permitiendo a un usuario acceder fácilmente al equipo de otro usuario utilizando debilidades bien conocidas, relaciones de confianza y opciones predeterminadas. La mayor parte de estos ataques necesitan poca o ninguna habilidad, poniendo la integridad de una red en riesgo. La mayoría de los empleados no necesitan y no deben tener acceso al resto de equipos, funciones administrativas, dispositivos de red, etcétera. Sin embargo, debido a la cantidad de flexibilidad necesaria para la función normal, las redes internas no pueden permitirse una seguridad máxima. Por otro lado, sin ninguna seguridad, los usuarios internos pueden ser una importante amenaza para muchas redes corporativas. Un usuario de la empresa ya tiene acceso a muchos recursos internos y no necesita evitar cortafuegos u otros mecanismos de seguridad que previenen que las fuentes no confiables, como usuarios de Internet, accedan a la red interna. Dichos usuarios internos, equipados con mucha habilidad, pueden penetrar satisfactoriamente y conseguir derechos de administración remota de red mientras que asegura que su abuso sea difícil de identificar o incluso de detectar. Una pobre seguridad de red también significa que, si un informantico externo fuerza un equipo de su red, podrá acceder al resto de la red interna más fácilmente. Esto habilitaría a un atacante sofisticado leer y posiblemente filtrar correo y documentos confidenciales; equipos basura, haciendo creer en pérdidas de información; y más. Por no mencionar que entonces utilice su red y recursos para volverse e iniciar el ataque a otros sitios, que cuando sean descubiertos le apuntarán a usted y a su empresa, no al informático.

Es por lo anterior la importancia de la seguridad, la Autenticación y Encripción son conceptos básicos utilizados en seguridad. La autenticación es utilizada para asegurar que todos los usuarios pueden identificarse para auditorias o permisos de acceso. Es un método para verificar que el emisor y el receptor sean realmente quienes pretenden ser, y desde luego, que estén autorizados. Por su parte, la encripción provee confidencialidad de la información. Es el resultado de la utilización de algoritmos matemáticos para convertir información legible en información ilegible o cifrada. Quienes están involucrados en una comunicación segura tienen que ser autenticados al principio de su sesión con el objeto de establecer una relación de confianza entre ellos. Como parte de este proceso, las llaves de encripción/desencripción son generadas e intercambiadas. Esas llaves son usadas por los puntos de comunicación finales para transmitir mensajes sobre el ambiente o equipo no confiable.

Una seguridad manejada por los sistemas operativos de Windows server así como clientes incluido Linux es KERBEROS. Kerberos es un protocolo utilizado en el directorio activo de validación de identificación, basado en una variación del Needham−Schroeder; se llama así por un perro de varias cabezas de la mitología griega que solía cuidar la entrada al averno (supuestamente para mantener fuera a los indeseables). Kerberos se diseñó en el M.I.T. para permitir a los usuarios de estaciones de trabajo el acceso a recursos de una manera segura; su principal diferencia respecto del protocolo de Needham−Schroeder es el supuesto de que todos los relojes están bastante bien sincronizados. La arquitectura de Kerberos está basada en tres objetos de seguridad: Clave de Sesión, Ticket y Autenticador.

Existen tres protocolos principales que son de propósito para construir VPN's [Kosiur, 1998], son:

- IPSec,
- PPTP, y
- L2TP

Estos protocolos definen cómo los paquetes son encapsulados y como se forman los túneles, así de cómo los paquetes son asegurados. Los protocolos de seguridad también ofrecen un acuerdo entre los que envían y reciben información en la VPN, ya que son necesarios para manejar y administrar los secretos y métodos de autenticación.

IPsec – IPSecurity El protocolo TCP/IP no incluye características de seguridad inherentemente. Para proporcionar al paquete de IP un nivel de seguridad, la IETF ha estado desarrollando en protocolos IPSec. El primer protocolo que abarca IPSec, para autenticación y encripción de datagramas IP, fue publicado por la IETF como RFCs 1825 al 1829 en 1995. IPSec se ha implementado extensamente para poner en ejecución las Redes Privadas Virtuales. IPSec es la abreviación de IP Security, es un conjunto de protocolos que se usan en el intercambio seguro de paquetes en la capa IP, utiliza dos modos de cifrado: transporte y túnel. El modo del transporte cifra solamente la porción de los datos (carga útil) de cada paquete, y la cabecera sale intacta. El modo del túnel seguro cifra ambos. En la recepción un dispositivo IPSec esclavo desencripta cada paquete. Maneja dos tipos de cabeceras según el caso: el AH para la autenticación (Autenthication Header) y el ESP (Encapsulating Security Payload) para la encripción. Está construido alrededor de un número de tecnologías de algoritmos criptográficos que proveen confidencialidad, integridad en datos y autenticación: Diffie-Hellman, Llave Pública, DES y certificados Digitales. Para que IPSEC trabaje, los dispositivos que envían y de recepciones deben compartir una clave pública. Esto se logra con un protocolo conocido como Protocolo de asociación de Seguridad en Internet y Administración de llave (ISAKMP/Oakley), que permite que el receptor obtenga una clave pública y autentifique el remitente usando certificados digitales.

3.9 Conclusiones

Como se detalló en este capitulo, la implementación de un servidor VPN es compleja y es importante tomar en cuenta la instalación de los servicios que la VPN por su naturaleza utiliza para funcionar con exactitud. Estas funciones fueron detalladas suponiendo que en el servidor no habían sido instaladas al igual que la implementación del servidor, es decir se realizó la configuración tomando como si estuviera recién instalado el Windows Server.

CAPÌTULO IV
CONFIGURACIÓN DEL CLIENTE VPN

4.1 Introducción

Cada vez es más habitual moverse en escenarios en donde se requiere el acceso a recursos remotos desde cualquier lugar, incluso recursos que no están disponibles directamente en Internet, pero sí en nuestra intranet. Una VPN permite un bajo coste de implementación. Por ejemplo, en cualquier sistema operativo podemos encontrar software para establecer una sesión como cliente, porque soportan el protocolo IPSec. Aunque sea una forma lenta de comunicación (es necesario cifrar y encapsular los datos) resulta insignificante con las velocidades que nos brinda hoy la banda ancha. Es extremadamente escalable, con un sólo servidor, cualquier cliente puede conectarse desde cualquier lugar, y, sobre todo, es muy seguro.Mediante una VPN podemos acceder de forma segura a todos los recursos de nuestra intranet usando una conexión pública como Internet y trabajar como si estuviésemos en la red local. La mejor forma de entender y ver como funciona es creando el cliente VPN, y eso es lo que se hará en este capitulo. La PC cliente de un servidor de VPN realizado en diferentes sistemas operativos.

4.2 Configuración del cliente VPN en Windows XP

Windows XP (cuyo nombre en clave inicial fue Whistler) es una línea de sistemas operativos que fueron hechos públicos el 25 de octubre de 2001 por Microsoft. Se considera que están en el mercado 400 millones de copias funcionando. Las letras "XP" provienen de la palabra experience ("experiencia" en español). Es por ello que es el sistema más usado en los equipos de cómputo de la Presidencia de Pachuca de Soto Hidalgo. Los ordenadores que ejecutan Windows XP Professional son ordenadores clientes. Los ordenadores clientes pueden compartir recursos, como archivos, impresoras y conexiones a Internet,

creando o accediendo a una red. Es recomendable que se actualice la versión de XP al sp2 o al sp3 para evitar problemas de seguridad en el sistema.

- Se abre la carpeta de "Conexiones de red" y en el menú Archivo se selecciona "Nueva conexión" como se muestra en la figura 4.10. En el asistente para conexión nueva se elige "Conectarse a la red de mi lugar de trabajo" la cual es una red de negocios usando la VPN para que puedan trabajar desde casa, oficina de campo u otra ubicación, dar clic en el botón siguiente.

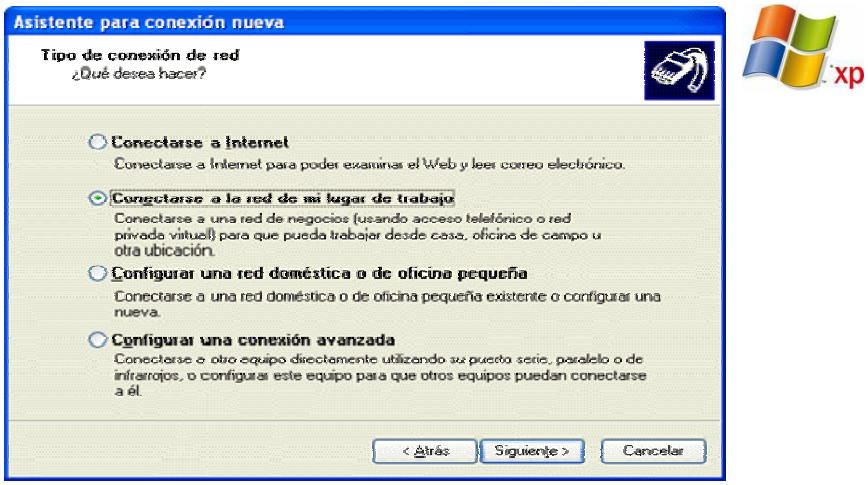

Figura 4.1 *Tipo de conexión de red.*

- Seleccionar "Conexión de Red Privada Virtual" figura 4.2, y después pulsar siguiente.

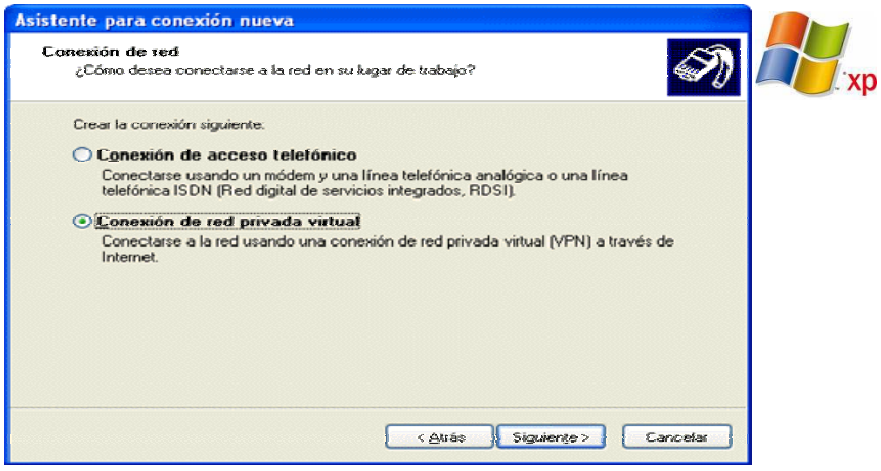

Figura 4.2 *Conexión de red privada virtual.*

En la siguiente ventana, se deberá marcar la opción "no usar conexión inicial" a menos que se requiera que con la vpn se utilice otra de las conexiones a internet, si se indica que al activar esta conexión se active antes otra conexión, por ejemplo una conexión telefónica, se conectará primero a Internet y luego se establecerá la VPN. Si se dispone de cable o ADSL no es necesario activar ninguna de estas conexiones. Tampoco lo es si se está conectado a Internet cuando se activó la conexión VPN o no se requiere que ésta marque ninguna conexión.

Por último indicar la dirección IP del servidor VPN como se muestra en la figura 4.3, esta es la dirección IP pública, es decir, la que tiene en Internet en el momento de establecer la conexión entre los clientes y el servidor.

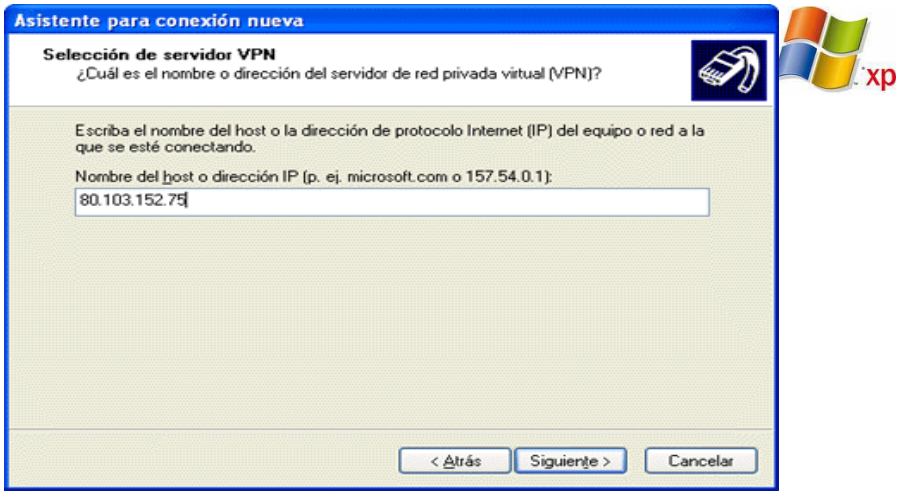

Figura 4.3 *Nombre del host o dirección IP del servidor*.

- Al finalizar el asistente ya se tendrá la conexión lista para activarse. Ahora debemos indicar el usuario y password que se ha activado en el servidor y ya se podrá conectar con el servidor como se muestra en al figura 4.4. Si el servidor VPN se conecta a Internet usando un modem o Cable la IP puede cambiar (IPs dinámicas) por lo que será necesario indicarle la IP que tiene en cada momento.

Figura 4.4 *Conexión del cliente VPN.*

Ahora ya se tiene la conexión VPN lista para funcionar.

Si se está trabajando con conexiones lentas (módem de 64kbs o similar) la VPN también irá lenta. Es recomendable disponer de conexiones de banda ancha para aprovechar todos los privilegios que ofrecen este tipo de conexiones. Para realizar las comunicaciones usando la VPN se deberán usar las IPs de la VPN, es decir, además de la IP de Internet que tiene el servidor y los clientes se han generado otras IPs internas de la VPN, pues esas se deberán usar para comunicarnos con los equipos de la VPN, estas se obtendrán como las habituales, pero en el icono de la nueva conexión que aparece en la barra de notificación (junto al reloj).En conexiones lentas, el Explorador de Windows no será capaz de mostrar los otros equipos de la red, o le llevará mucho tiempo, en ese caso, se podrá acceder a ellos escribiendo en la barra de direcciones del Explorador de Windows "\\ip_en_la_VPN" o "\\nombre_maquina" de la máquina a la que se quiere acceder, por ejemplo, si la IP (en la VPN) de la otra máquina es 169.254.3.117 se tendrá que escribir \\169.254.3.117 en la barra de direcciones del Explorador de Windows y de esta forma ya se tendrá acceso a los ficheros e impresoras de la máquina indicada. Para usar otros recursos, como servidores de base de datos, etc. Simplemente se deberá usar la IP en la VPN de la maquina destino. Además, si los equipos no tienen realizada la configuración de red adecuadamente, o tienen mal asignados los permisos puede ocurrir que no se pueda acceder a recursos. Esto no es un problema de la VPN sino de cómo se tienen establecidos los permisos en cada ordenador, al igual que pasa en una red local. Por último, y como recomendación final, es aconsejable mantener el equipo actualizado e instalar los parches y services packs que va publicando Microsoft. Al tratarse de un servicio de red es muy vulnerable a ser atacado y si no está convenientemente actualizado la red podrá ser víctima de ataques, o los datos quizás no viajen lo suficientemente seguros como se espera.

4.3 Configuración de una VPN en Linux del lado del cliente

Red Hat Enterprise Linux es compatible con IPsec para la conexión entre hosts y redes remotos utilizando un túnel seguro en un transportador de red común tal como la Internet. IPsec se puede implementar usando una conexión host-a-host (una computadora a la otra) o de red-a-red (una LAN/WAN a la otra). La implementación IPsec en Red Hat Enterprise Linux utiliza el *Intercambio de Llaves en Internet* (*IKE*), el cual es un protocolo implementado por el Internet Engineering Task Force (IETF), a ser usado para la autenticación mutua y asociaciones seguras entre sistemas conectándose.

Una conexión IPsec se divide en dos fases lógicas. En la fase 1, un nodo IPsec inicializa la conexión con el nodo o red remota. El nodo/red remota verifica las credenciales del nodo solicitante y ambos lados negocian el método de autenticación para la conexión. En sistemas Red Hat Enterprise Linux, una conexión IPsec utiliza el método de *llave pre-compartida* o *pre-shared key* de autenticación de nodo IPsec.

La fase 2 de la conexión IPsec es donde se crea una *asociación de seguridad* (SA) entre nodos IPsec. Esta fase establece una base de datos SA con información de configuración, tal como el método de encriptación, parámetros de intercambio de llaves secretas y más. Esta fase maneja realmente la conexión IPsec entre nodos y redes.

La implementación de Red Hat Enterprise Linux de IPsec utiliza IKE para compartir las llaves entre hosts a través de la Internet. El demonio `racoon` de manejo de llaves se encarga de la distribución e intercambio de llaves IKE.

En la figura 4.5 se puede ver la pantalla del escritorio en la cual posicionaremos el cursor en el icono del sombrero que dice aplicaciones, la ruta de acceso a la configuración de red en Linux Red Hat, se deberá dar clic en aplicaciones, configuración de sistema, red.

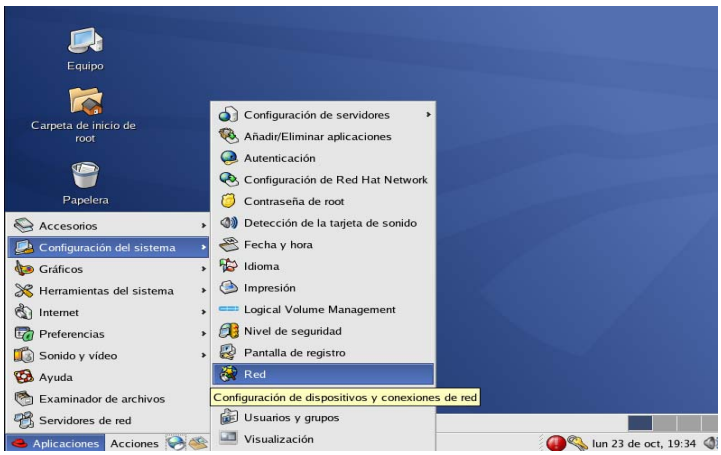

Figura 4.5 *Configuración de dispositivos y configuraciones red.*

- En la figura 4.6 se muestran las pestañas de configuración de red

Figura 4.6 *Configuración de red.*

- Seleccionar la pestaña con el protocolo Ipsec y dar clic en activar figura 4.7

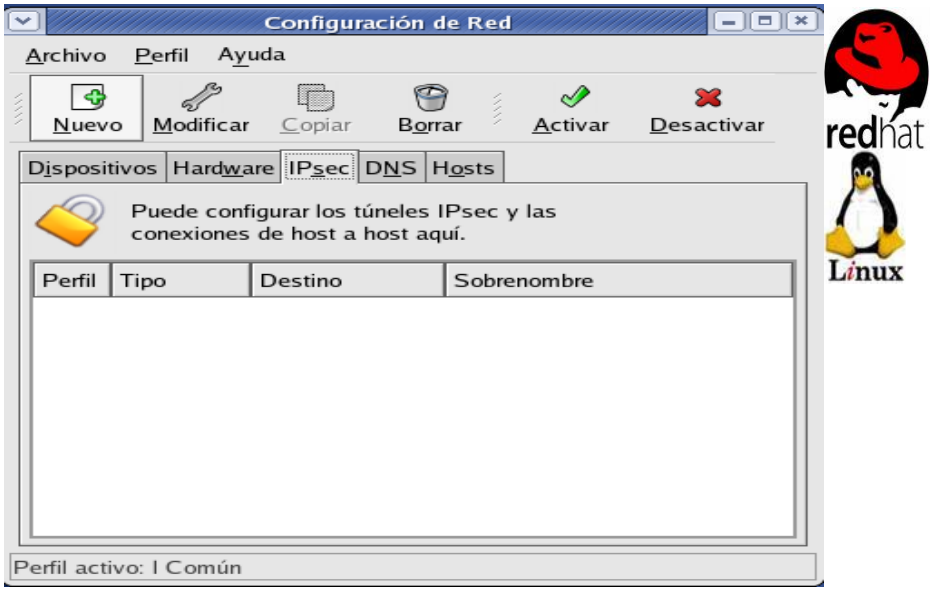

Figura 4.7 *Pestaña configuración IPsec.*

- Dar siguiente en la ventana de configuraciones ipsec figura 4.8.

Figura 4.8 *Configuraciones IPsec.*

- Asignar un sobrenombre para la conexión y también existe la posibilidad de activar el inicio del dispositivo al iniciar el ordenador figura 4.9

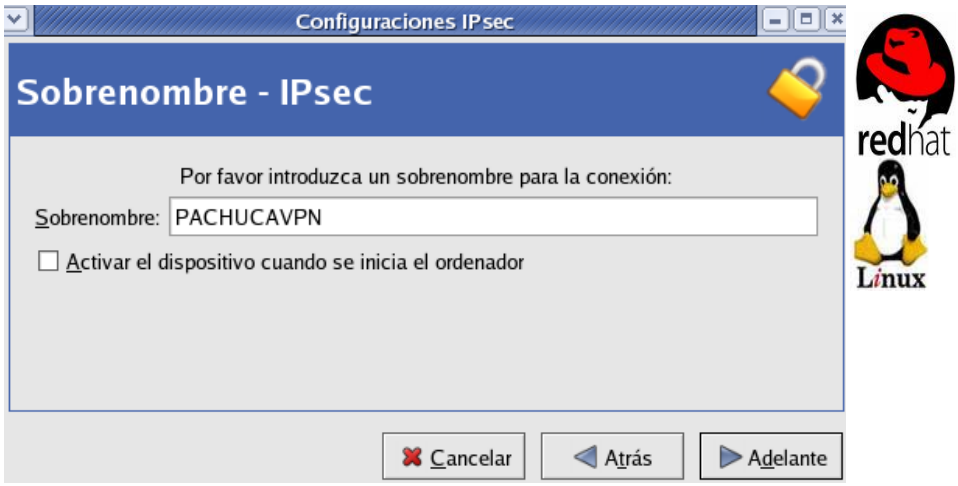

Figura 4.9 *Sobrenombre IPsec.*

En la figura 4.10 IPsec se puede configurar para conectar un escritorio o estación de trabajo a otro a través de una conexión host-a-host. Este tipo de conexión utiliza la red a la cual están conectados los hosts para crear un túnel seguro entre ellos. Los requerimientos de una conexión host-a-host son mínimos, como lo es la configuración de IPsec en cada host. Los hosts solamente necesitan una conexión dedicada al transportador de red (tal como la Internet) y Red Hat Enterprise Linux para crear la conexión IPsec. IPsec

también se puede configurar para conectar una red completa (tal como una LAN o una WAN) a una red remota a través de una conexión red-a-red. Una conexión de red-a-red requiere la configuración de enrutadores IPsec en cada lado de las redes conectantes para procesar y enrutar la información de forma transparente desde un nodo en una LAN a otro nodo en una LAN remota. En este caso utilizar encriptación de red a red (VPN).

Figura 4.10 *Nombre de conexión.*

- Seleccionar un modo de encriptación en este caso a través de IKA (racoon) figura 4.11

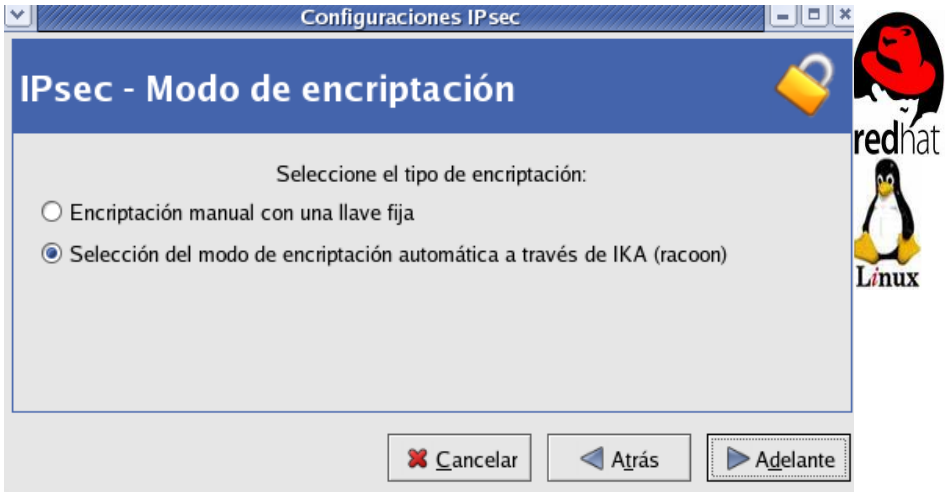

Figura 4.11 *Modo de encriptación del protocolo IPsec.*

En la parte de **Red local**, introduzca la información siguiente información:

Dirección de red local: La dirección IP del dispositivo en el enrutador IPsec conectado a la red privada.

Máscara de subred local: La máscara de la subred de la dirección IP de red local.

Puerta de enlace de red local: La puerta de enlace para la red privada.
Introducir los datos de la configuración de red local figura 4.12

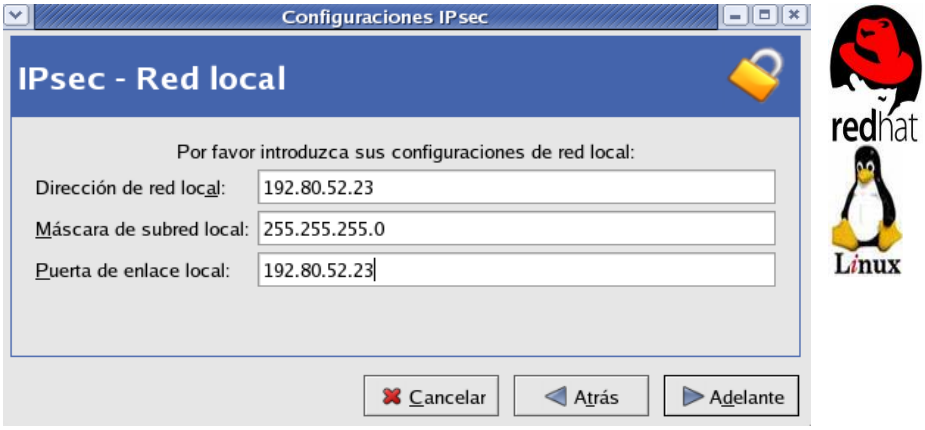

Figura 4.12 ***C****onfiguración IPsec red local*.

En la parte de **Red remota**, ingrese la siguiente información:

Dirección IP remota: La dirección IP públicamente direccionable del enrutador IPsec para la *otra* red privada.

Dirección de red remota: La dirección de red de la subred privada detrás del *otro* enrutador IPsec.

Máscara de la subred remota: La máscara de la subred de la dirección IP remota.

Puerta de enlace remota: La dirección IP de la puerta de enlace para la dirección de red remota.

Insertar de los datos de red del servidor remoto al cual se quiere conectar como cliente figura 4.13

Figura 4.13 *Configuraciones IPsec.*

- El siguiente paso es generar la llave de autenticación y nos da la opción de ingresar una o que el mismo asistente la genere figura 4.14

Figura 4.14 *Llave de autenticación.*

- Al final se muestra un resumen con los datos de la configuración figura 4.15

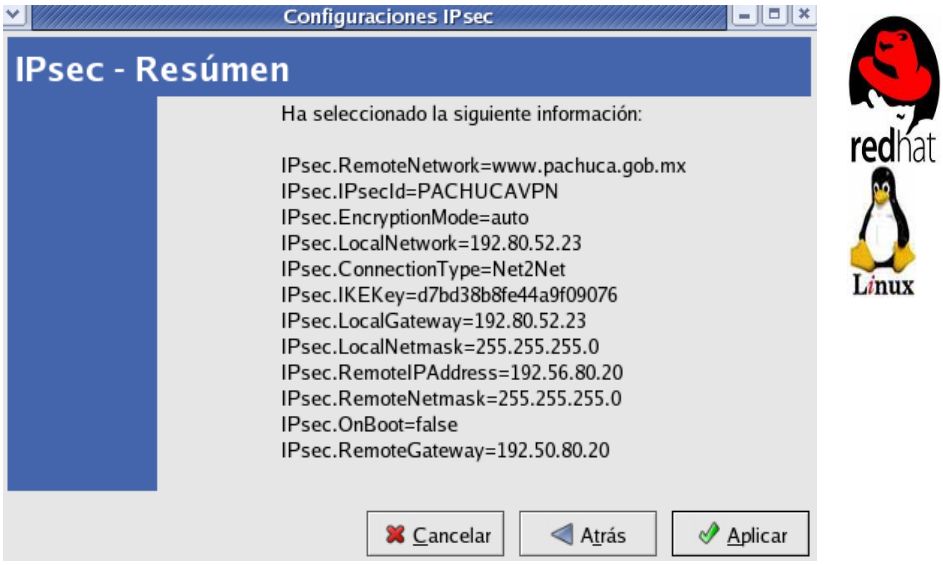

Figura 4.15 *IPsec resumen.*

- Volver a la pestaña de configuración figura 4.16 de IPsec y ahí muestra la conexión del túnel ipsec realizada

Figura 4.16 *Túnel IPsec configurado.*

- Se Guardan los cambios figura 4.17

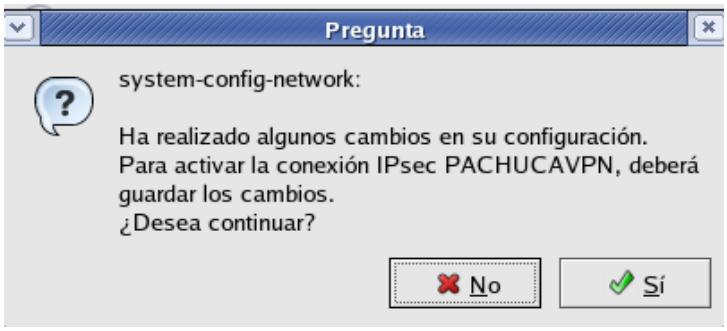

Figura 4.17 *Guardar cambios de la configuración.*

- Y Dar en aceptar en la ultima pantalla figura 4.18

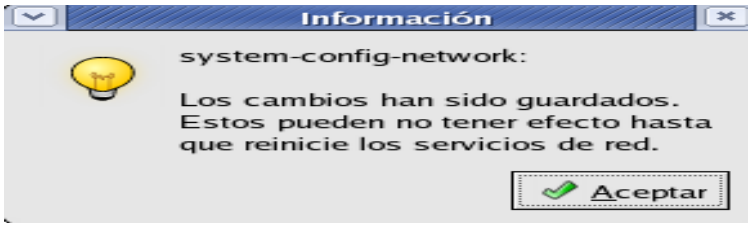

Figura 4.18 *Aceptar la configuración.*

4.4 Instalación y configuración de un cliente PPTP en Windows Vista

Windows Vista ofrece una infraestructura avanzada centrada en el trabajo, aplicaciones móviles de productividad y una experiencia de primera para la diversión digital en casa, todo ello en un único producto. Windows Vista Ultimate brinda todas las características ofrecidas en Windows Vista Home Premium, incluidos Windows Media Center, Windows Movie Maker con compatibilidad para alta definición y Windows DVD Maker. También ofrece todas las características de Windows Vista Business, por ejemplo, las redes de empresa, las herramientas de administración centralizada y las características avanzadas de copia de seguridad del sistema, estas características son de gran importancia para la creación del cliente VPN. Y, aparte de todo lo anterior, Windows Vista Ultimate dispone de todas las nuevas características de seguridad y protección de datos que otorgan a Windows Vista un grado excepcional de confiabilidad. Desde el botón Iniciar, hacer clic en Conectar a aparecerá la siguiente ventana mostrando todas las redes a las que se puede conectarse:

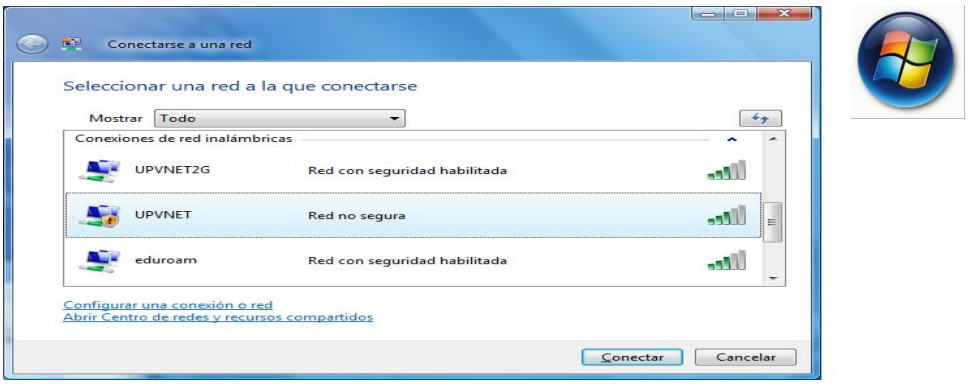

Figura 4.19 *Configurar una conexión de red.*

En la figura 4.19 aparece el enlace **Configurar una conexión de red**. Se tiene que hacer clic sobre él y emergerá una nueva ventana figura 4.20.

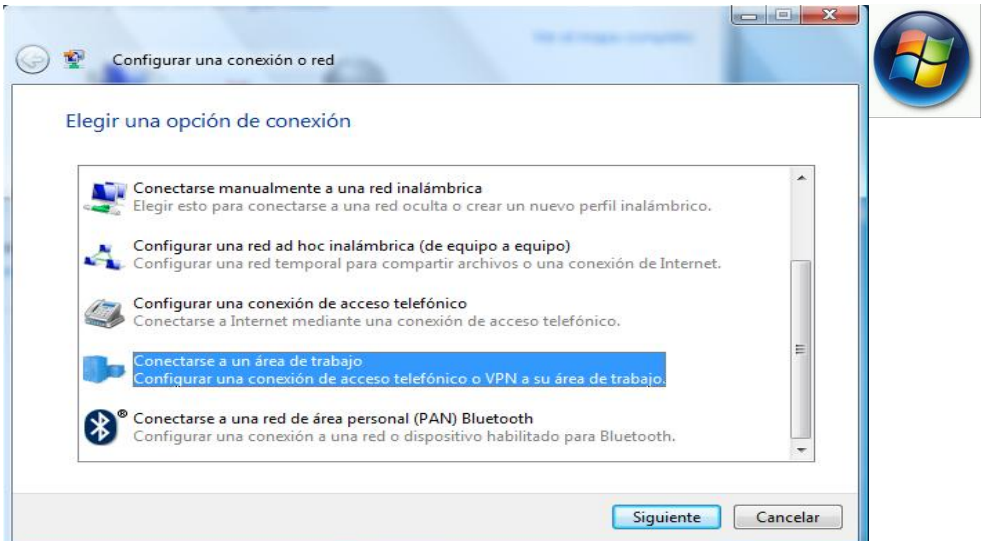

Figura 4.20 *Conectarse a una área de trabajo.*

En la ventana se deberá escoger la opción de Conectarse a un área de trabajo y dar Clic en el botón **Siguiente.**

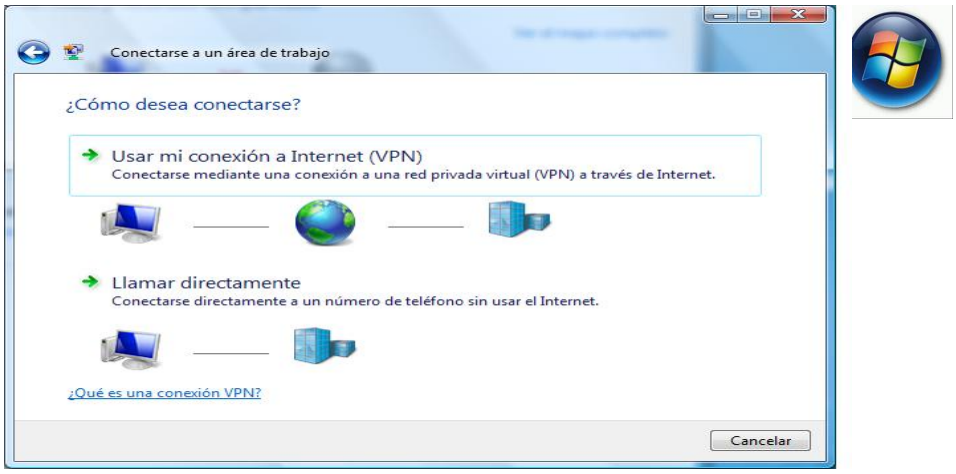

Figura 4.21 *¿Cómo desea conectarse.*

En la nueva ventana figura 4.21 elegir la opción Usar mi conexión a Internet (VPN).

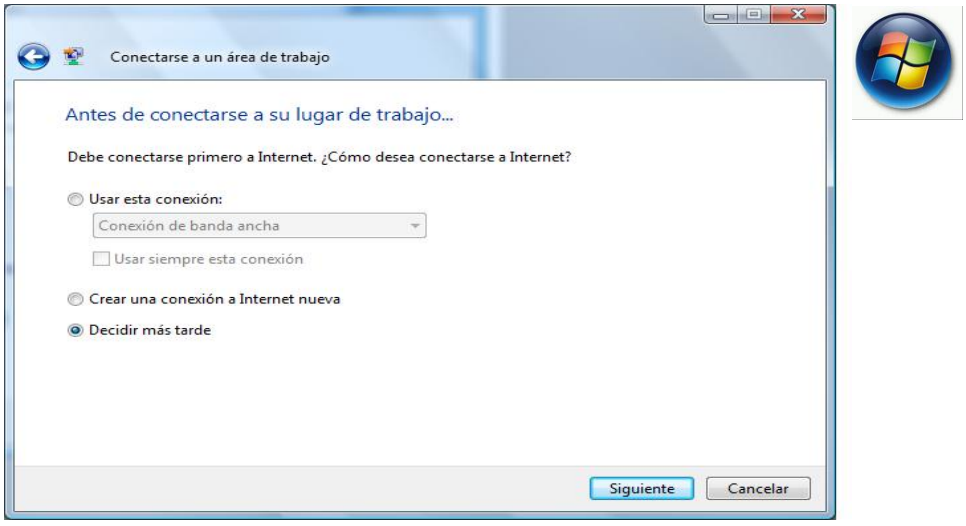

Figura 4.22 *¿Cómo desea conectarse a Internet?*

En la figura 4.22 deberá marcar la casilla 'Decidir más tarde'. Ahora se solicitan los datos de la conexión.

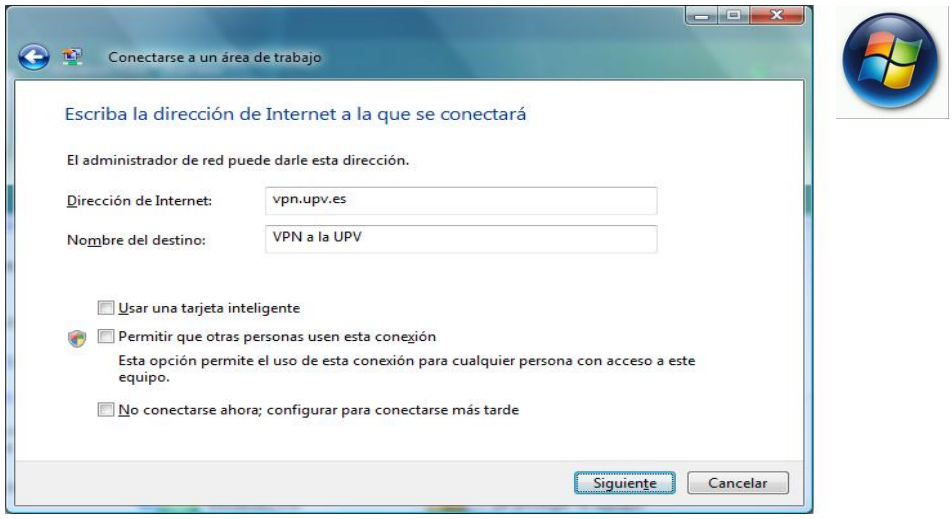

Figura 4.23 *Escribir la dirección de internet a la que se conectará.*

En el campo 'Dirección de Internet' se introduce el nombre del servidor de túneles pachuca.com y en el campo 'Nombre del destino' se debe escoger un nombre descriptivo para la conexión figura 4.23 dar clic en el botón 'Siguiente'.

Ahora llega el momento de autenticarse como usuario:

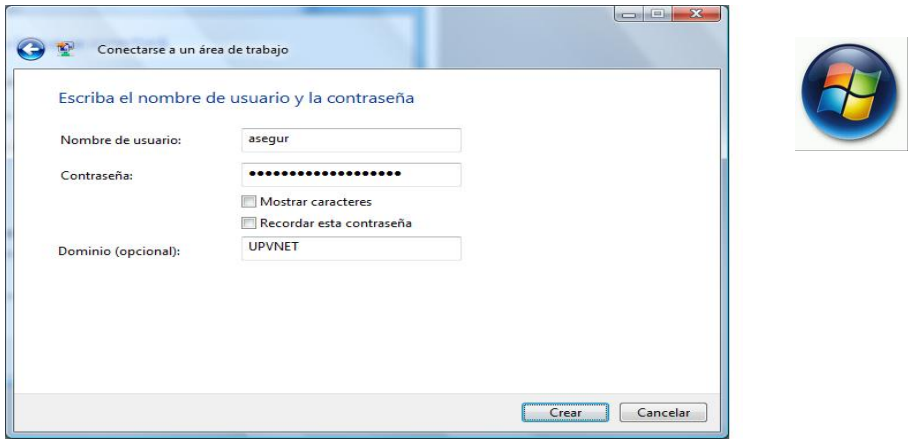

Figura 4.24 *Nombre de usuario y contraseña.*

Ahora se debe introducir el nombre de usuario, contraseña y dominio (PACHUCA, ALUMNO, AAA). Clic en el botón 'Crear', ya solo se debe tener en cuenta que se debe de permitir la conexión en el firewall que maneje ya sea el propio del sistema o firewalls de terceros figura 4.24.

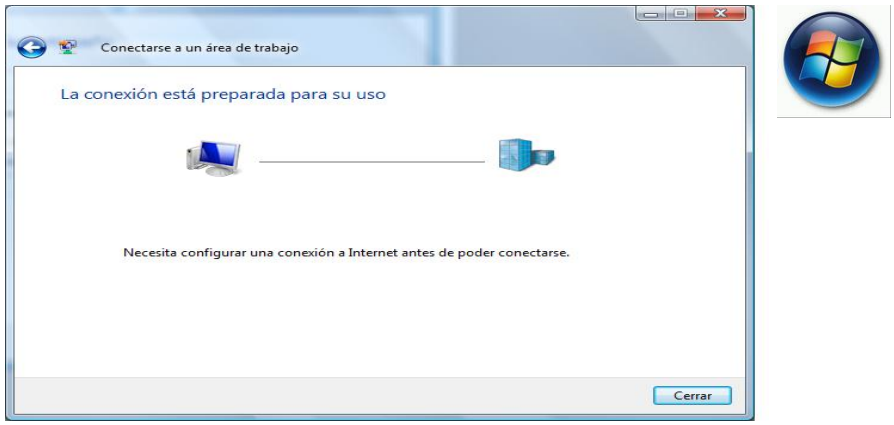

Figura 4.25 *Finalización del asistente.*

Clic en el botón 'Cerrar' figura 4.25.

4.5 Conclusiones

La configuración de la VPN del lado del cliente fue, como se detalló en este capitulo de manera sencilla y funcionable, el parámetro más relevante que vale la pena retomar y considerar para realizar el acceso es que en el Servidor ya se halla dado de alta el usuario con su nombre y su contraseña.

Ya una vez realizada la conexión se podrá tener acceso a los recursos compartidos y disponibles del servidor. Los clientes VPN representan una gran solución cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha vuelto un tema importante, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro, el único inconveniente que pudieran tener las VPN es que primero se deben establecer correctamente las políticas de seguridad y de acceso porque si esto no está bien definido pueden existir consecuencias serias.

CAPITULO V
ESTRUCTURA DE LA RED DE PRESIDENCIA DE PACHUCA DE SOTO HIDALGO

5.1 Introducción

En toda red existen computadoras para correr programas de usuario (aplicaciones). Muchas de ellas comúnmente son usadas vía red remota o para llevar a destinos locales y remotos. El diseño completo de la red se simplifica notablemente cuando se separan los aspectos puros de comunicación de la red (la subred), de los aspectos de aplicación (los hostales). Las líneas de transmisión (conocidas como circuitos, canales o troncales), se encargan de mover bits entre máquinas. Los elementos de conmutación son ordenadores especializados que se utilizan para conectar dos o más líneas de transmisión. La red de Presidencia de Pachuca de soto Hidalgo está estructurada pensando en un crecimiento a corto, mediano y largo plazo, lo cual garantiza la vida útil de la infraestructura y aplicaciones futuras como lo es la Red Privada Virtual.

5.2 Red general de datos de Presidencia de Pachuca de Soto Hidalgo.

En las figuras 5.1 y 5.2 se muestra el diagrama general de la red de datos de presidencia municipal de Pachuca de soto hidalgo y la ubicación de las secretarias. Secretaría General Municipal: Provee a la ciudadanía de la información relacionada a la Administración Pública Municipal para transparentar el manejo de los recursos, favoreciendo la rendición de cuentas a la ciudadanía de forma oportuna, veraz y confiable. Secretaría de Administración: La Secretaría de Administración es la dependencia que tiene por objeto la aplicación y control de los procesos y acciones de apoyo a la operación de los servicios municipales a través de las áreas de Informática; Recursos Humanos, Compras, Concursos y Licitaciones; Servicios Básicos de Conservación y Limpieza de Instalaciones, Control y Mantenimiento Vehicular con el

fin de promover la productividad, eficiencia y eficacia de las Dependencias del Municipio, al contar las áreas con el personal y los recursos materiales necesarios para la eficaz operación de la Administración Municipal. Secretaría de Contraloría Municipal, Secretaría de Tesorería Municipal, Secretaría de Seguridad Pública: es la que Garantiza los servicios de seguridad pública, vialidad y protección civil con apego a derecho, estableciendo políticas, sistemas y programas para la prevención e inhibición del delito; el desarrollo de las vías de circulación de móviles; y el auxilio, recuperación y apoyo a la ciudadanía. Secretaría de Obras Públicas: es la que Responde con eficacia y eficiencia a las exigencias actuales de la sociedad en atención a sus demandas para impulsar el crecimiento, la belleza y la modernidad que requiere la ciudad y así incrementar el nivel de beneficio para su población. Secretaría de Servicios Municipales: tiene como compromiso atender las necesidades de la ciudadanía, ofreciendo servicios de calidad con calidez, coadyuvando en la generación de un ambiente de confianza y certidumbre entre la sociedad y la administración municipal. Secretaría de Desarrollo Económico: es la instancia donde la voz de los empresarios y la sociedad civil es valorada para generar políticas públicas en materia económica que habrán de efectuarse en el municipio de Pachuca. Todas estas secretarias están intercomunicadas por medio de una antena de microondas instalada en el cerro de cubitos, cuentan con conexión a Internet, "Casa Rule" cuenta con un E1 de 2 megas de velocidad, las demás con acceso de mínimo de un mega con el servicio de Prodigy Infinitum. Cuenta la red de presidencia d Pachuca de soto hidalgo con un total de 288 equipos en red incluido el servidor.

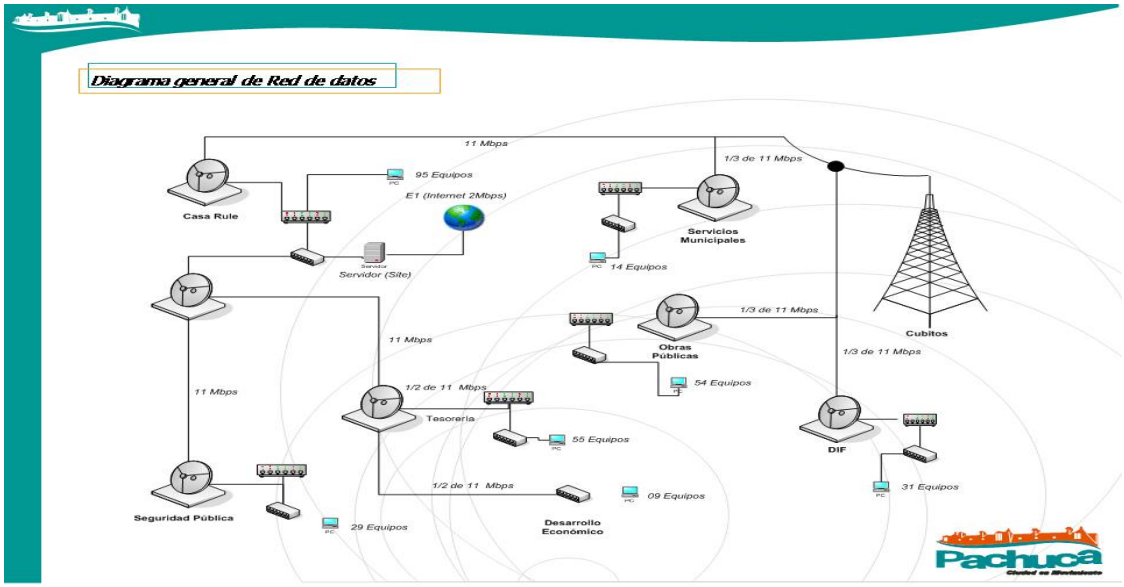

Figura 5.1 *Diagrama general de Red de datos.*

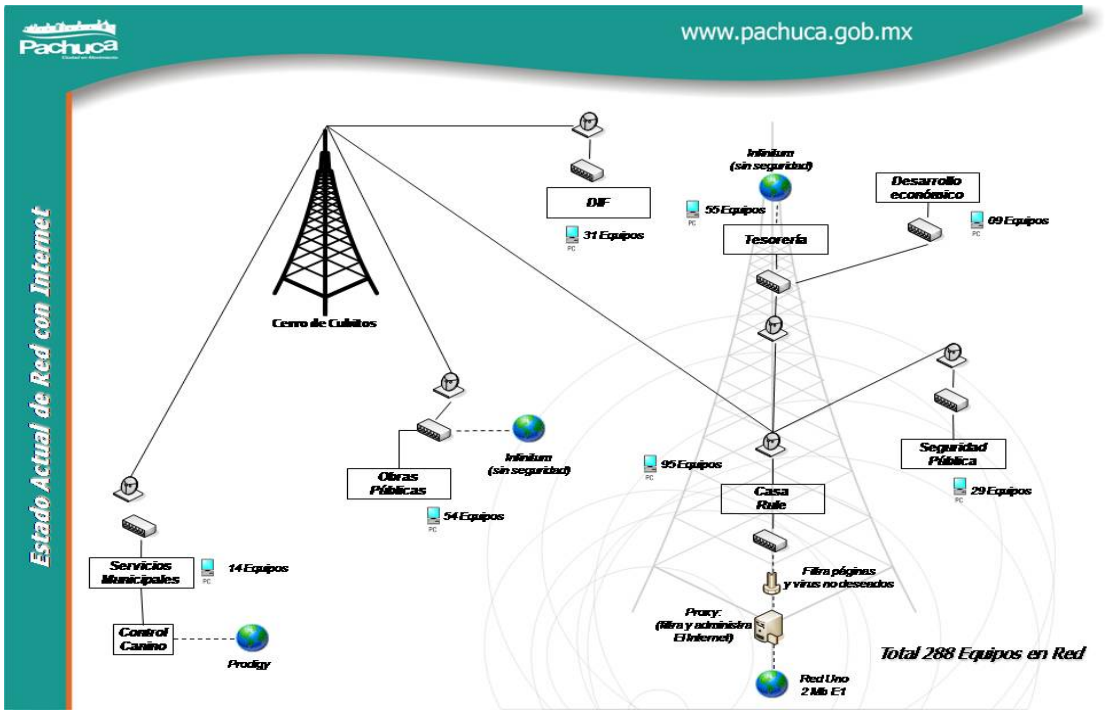

Figura 5.2 *Estado actual de Red con internet.*

5.3 Site de Telecomunicaciones

Figura 5.3 *Rack del Site de Presidencia de Pachuca de Soto Hidalgo.*

En la figura 5.3 se encuentra el rack dentro del Site de presidencia de Pachuca, el cual cuenta con PATCH PANEL, que es arreglo de conectores hembra RJ 45 que se utiliza para realizar conexiones cruzadas (diferente a cable cruzado) entre los equipos activos y el cableado horizontal. Permite un gran manejo y administración de los servicios de la red, ya que cada punto de conexión del patch panel maneja el servicio de una salida de telecomunicaciones, permite interconexión entre equipos por tanto deben ser de primera calidad debido a que por sus puntos transitan señales de alta velocidad.
La idea del Patch-Panel además de seguir estándares de redes, es la de estructurar o manejar los cables que interconectan equipos en una red, de una mejor manera.

Características

- La ventaja de los patch panels modulares, es que aceptan las mismas rosetas que se ubican en los puestos de trabajo en cualquier orden, tipo y color.
- Poseen además un opcional para montar en pared, o se puede utilizar directamente para instalar en rack con frente estándar de 19".
- Tienen la ventaja de ser modelos compactos permitiendo ahorrar el espacio disponible en el rack. Utilizando el correspondiente ordenador de patch cords y etiquetando cada puerto con su correspondiente puesto de trabajo, se asegura una perfecta administración de la red una vez concluida la instalación. Por tanto se tiene un control y registro sobre los equipos con determinados servicios. Las características claves de un sistema de cableado abierto son que todos las tomas (salidas para conexión) del área de trabajo son idénticamente conectados en estrella a algún punto de distribución central, usando una combinación de medio y hardware que puede aceptar cualquier necesidad de aplicación que pueda ocurrir a lo largo de la vida del cableado; para lo cual estos elementos se prestan de forma oportuna y eficiente para la transmisión de datos, voz, video, etc.

Figura 5.4 *Servidor ubicado en el site de presidencia de Pachuca de Soto Hidalgo.*

En las figuras 5.3 y 5.4 se observa el Site de telecomunicaciones de la presidencia de Pachuca de Soto Hidalgo.

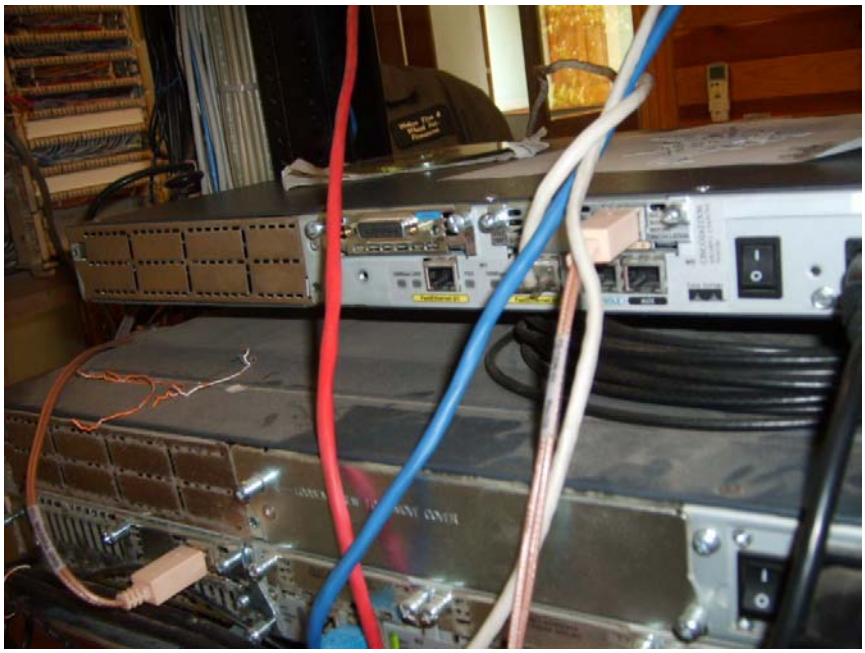

Figura 5.5 *Vista de la parte de atrás de los routers cisco 2600 y cisco 3700.*

Figura 5.6 *Vista frontal de los routers cisco 2600 y cisco 3700.*

En las figuras 5.5 y 5.6 se encuentran los routers cisco 2600 y cisco 3700, hardware para interconexión de redes de las computadoras que opera en la capa tres (nivel de red) del modelo OSI. El router interconecta segmentos de red, o algunas veces hasta redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red, El Cisco 2600 y el 3700 son modular multiservice routers, ofrecen versatibilidad, integración, y poder para ramificar las oficinas de presidencia de Pachuca. Con 50 módulos de redes e interfaces, la arquitectura modular de los routers Cisco Series fácilmente permite interfaces para ir ascendiendo o acomodar la expansión de red.

Figura 5.7 *Firewall cisco pix 506 E.*

El firewall cisco pix 506 E figura 5.7 se encarga de cerrar puertos para evitar intrusiones no deseadas y dejar puertos abiertos con accesos solo de entrada/salida o ambos, proporciona un alto grado de seguridad, fácil de instalar y con un rendimiento sobresaliente. Le permite proteger rigurosamente la red interna del mundo exterior con una completa protección de seguridad, la Presidencia de Pachuca de Soto Hidalgo a bloqueado los puertos 135 - 137 - 138 - 139 - 445 - 5000 – 1900 entre otros por seguridad, algunos solo tienen salida de datos pero no de entrada .

Figura 5.8 *Access Point*.

En la figura 5.8 se muestra el Access Point Wireless-G de Linksys que tiene Velocidades de transferencia de datos hasta de 54 Mbps en el modo Wireless-G (802.11g) y hasta 11 Mbps en el modo Wireless-B (802.11b). La función de configuración mediante un botón permite una configuración inalámbrica segura y sencilla. Seguridad inalámbrica avanzada: encriptación WPA de 128 bits, filtrado de MAC, este equipo se ha instalado en Presidencia de Pachuca para proporcionar acceso inalámbrico a determinados usuarios móviles.

Figura 5.9 *Patch panel y switches 3com*.

El Site de presidencia cuenta con 2 Switch 3com de 24 puertos dando servicio a 46 equipos de computo en presidencia de Pachuca, su auto-negociación ajusta la velocidad del puerto con la del dispositivo de comunicación. Cualquiera de los 24 puertos del switch puede ofrecer Ethernet 10BASE-T para usuarios con requerimientos promedio de ancho de banda, o Fast Ethernet 100BASE-TX para usuarios de potencia con conexiones de red más nuevas como la de base 1000-tx, que conectan los cables utp cat 5 al usuario final de las diferentes aéreas internas de Presidencia, figura 5.9.

Figura 5.10 *Equipo SDSL Watson 4*.

El equipo SDSL de la familia WATSON 4 transmite y recibe señales digitales de 2 Mbit/s sobre un solo par de cobre sobre distancias de hasta 6 kilómetros y utiliza el código de línea CAP. Posibles interfaces a su equipo son E1 (G.703/G.704), V.35, V.36 y X.21, actualmente solo se usa para eventos especiales.

Figura 5.11 *Conmutador telefónico*.

Se encarga de gestionar la telefonía, cuenta con troncales de respuesta rápida.

Figura 5.12 *Tellabs 8110*.

La unidad de terminal de red es el Tellabs 8110 que proporciona Telmex para el enlace a internet, figura 5.12.

Figura 5.13 *Servidor de Presidencia de Pachuca de Soto Hidalgo.*

El servidor de la Presidencia de Pachuca de Soto

Arquitectura escalable creada para los procesadores de doble núcleo futuros, Escala de desempeño de alto nivel con bus de sistema de 800 MHz, dual, independiente y con corrección de errores (crc), E/S rápida y flexible, latencia de memoria reducida y E/S PCI Express, Desempeño mejorado y menor consumo de energía con la memoria DDR2, colocándosele 2 memorias de 2 gigas haciendo un total de 4 gigas funcionando a una frecuencia de 800 MHz con disipadores térmicos y tecnología de corrección de errores, memoria con disponibilidad extremadamente alta, reforzada contra cualquier error debido al sistema RAID de memoria integrado, la compatibilidad con módulos de conexión en caliente, bajo consumo de energía cuando la plataforma está inactiva o con una carga de trabajo moderada gracias a la Conmutación según demanda (DBS), Capacidad de crecimiento con la Tecnología de memoria ampliada Intel® 64 (Intel® EM64T). Protección adicional contra una clase determinada de ataques de virus malintencionados con la tecnología del Bit de desactivación de la ejecución. 2 disco duros sata II, uno de ellos alberga el sistema operativo y el otro base de datos, este tipo de discos proporciona una velocidad de 300 mb por segundo de información, girando a una velocidad de 10,000 rpm, una fuente de poder de 1200 watts termaltake con la suficiente capacidad para soportar dispositivos actuales y un crecimiento a futuro. La placa madre es una

S3000AHV de Intel con 1 x PCI Express x8, 1 x PCI Express x4, 2 x PCI 32-bit 33MHz, Controlador Gráfico: ATi ES1000 - con 16MB, 6 puertos usb 2.0. 2 tarjetas de red Intel **82573**E/V Ethernet Gigabit **10**/**100**/**1000** Mbps. Un lector óptico de DVD LG. Este servidor Se encarga de administrar a los usuarios asignando permisos y delimitando accesos, tiene instalado Microsoft Windows 2003 server, un procesador Intel Xeon de 3.2 gigas de doble núcleo, figura 5.13.

5.4 Conclusiones

A lo largo de la historia los ordenadores (o las computadoras) nos han ayudado a realizar muchas aplicaciones y trabajos, el hombre no satisfecho con esto, buscó mas progreso, logrando implantar comunicaciones entre varias computadoras, o mejor dicho: "implantar Redes en las computadoras"; hoy en día la llamada Internet es dueña de las redes, en cualquier parte del mundo una computadora se comunica, comparte datos, realiza transacciones en segundos, gracias a las redes. En los Bancos, las agencias de alquiler de vehículos, las líneas aéreas, instituciones gubernamentales y casi todas las empresas tienen como núcleo principal de la comunicación a una RED. Gracias a la denominada INTERNET, familias, empresas, y personas de todo el mundo, se comunican, rápida y económicamente. Las redes agilizaron en un paso gigante al mundo, por que grandes cantidades de información se trasladan de un sitio a otro sin peligro de extraviarse en el camino. La red estructurada de presidencia de Pachuca de soto Hidalgo cuenta con la tecnología adecuada para los servicios que ofrece, un diseño factible para la implementación de una Red Privada Virtual.

CONCLUSIONES

Es necesario que el ingeniero comprenda los conceptos básicos de la red privada virtual para que tenga un buen criterio en el diseño de estos elementos. Gracias a la combinación de la tecnología actual y las nuevas técnicas de ingeniería es posible producir un elemento estructural de economía, eficiencia y seguridad, lográndose así diseños de comunicación muy eficientes. Existen instituciones, empresas entre otros que sólo son posibles gracias al empleo de la tecnología comunicativa. En esta tesis se investigó solamente sobre la implementación de la VPN en Presidencia municipal de Pachuca de soto por ser de suma utilidad según datos arrojados, sin manejar planos estructurales, más que de los de la propia red instalada ya que por seguridad no se presentan en la culminación. Las VPN representan una gran solución para las empresas e instituciones en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha vuelto un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro. Como vemos, la creación de una VPN ha dado solución a la mayoría de los retos que le habíamos impuesto. Ahora, gracias a que podemos tener direcciones IP correspondientes a una misma subred IP, podemos cumplir el punto de requisitos que nos pedía mayor facilidad para la administración de la red. El punto de requisitos que mencionaba la necesidad (o quizás el deseo) de que las aplicaciones deberían seguir funcionando sin tener que modificarlas debido a la creación de la VPN no se va a cumplir enteramente. Esto es debido a que algunas aplicaciones que trabajen directamente a un nivel inferior que el de IP (que deberían de ser aquellas que monitoricen la red, por ejemplo) van a "darse cuenta" de que hay dos redes físicamente separadas, ya que, por ejemplo, no serán capaces de analizar el tráfico que suceda entre dos hosts de otras subredes, que sí serían capaces de analizar en un segmento de una auténtica LAN. Esto se puede solucionar, si es una necesidad crítica, usando un protocolo que trabaje sobre el nivel 2 OSI (L2), como sería por ejemplo L2TP, que está pensado para `juntar', en un principio, un host con una subnet, pero que puede servirnos para comunicar dos gateways de las subnets a unir por el VPN.

Finalmente las pruebas hechas al red privada virtual implementada en el servidor de presidencia de Pachuca de soto hidalgo han sido satisfactorias, observando que la VPN es una herramienta muy importante en las telecomunicaciones de hoy día, También se observa que las topologías virtuales entre las delegaciones, son adecuadas siempre a las necesidades del momento y permitiendo la inclusión de nuevas sedes o centros remotos de forma rápida y transparente al usuario.

GLOSARIO DE TERMINOS

Red: La comunicación mediante computadoras es una tecnología que facilita el acceso a la información científica y técnica a partir de recursos informáticos y de telecomunicaciones. Por eso, decimos que una red es, fundamentalmente, una forma de trabajo en común, en la que son esenciales tanto la colaboración de cada miembro en tareas concretas, como un buen nivel de comunicación que permita que la información circule con fluidez y que pueda llevarse a cabo el intercambio de experiencias. [14]

VPN: es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet. El ejemplo más común es la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo esto utilizando la infraestructura de Internet.

Para hacerlo posible de manera segura es necesario proveer los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación: Autenticación y autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.

- Integridad: La garantía de que los datos enviados no han sido alterados.
- Confidencialidad: Dado que los datos viajan a través de un medio potencialmente hostil como Internet, los mismos son susceptibles de interceptación, por lo que es fundamental el cifrado de los mismos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma. [20]

Protocolo: Un protocolo de red es como un lenguaje para la comunicación de información. Son las reglas y procedimientos que se utilizan en una red para comunicarse entre los nodos que tienen acceso al sistema de cable. Los protocolos gobiernan dos niveles de comunicaciones:

- Los protocolos de alto nivel: Estos definen la forma en que se comunican las aplicaciones.

- Los protocolos de bajo nivel: Estos definen la forma en que se transmiten las señales por cable.

Como es frecuente en el caso de las computadoras el constante cambio, también los protocolos están en continuo cambio. Actualmente, los protocolos más comúnmente utilizados en las redes son Ethernet, Token Ring y ARCNET. Cada uno de estos esta diseñado para cierta clase de topología de red y tienen ciertas características estándar. [15]

Internet: INTerconnected NETworks. La red de redes. Red de telecomunicaciones nacida en 1969 en los EE.UU. a la cual están conectadas centenares de millones de personas, organismos y empresas en todo el mundo, mayoritariamente en los países más desarrollados, y cuyo rápido desarrollo está teniendo importantes efectos sociales, económicos y culturales, convirtiéndose de esta manera en uno de los medios más influyentes de la llamada Sociedad de la Información y en la Autopista de la Información por excelencia. Fue conocida como ARPANET hasta 1974.

Internet es una Red informática de transmisión de datos para la comunicación global que permite el intercambio de todo tipo de información (en formato digital) entre sus usuarios. El nombre proviene del acrónimo de las palabras inglesas International Network (red internacional). [16]

Routian - Enrutamiento y acceso remoto proporciona servicios de enrutamiento de multiprotocolo LAN a LAN, LAN a WAN, red privada virtual (VPN) y traducción de direcciones de red (NAT). Enrutamiento y acceso remoto está destinado a administradores del sistema que ya estén familiarizados con protocolos y servicios de enrutamiento, y con protocolos enrutables como TCP/IP y AppleTalk [15]

Forwardiag - Reenvío

Transceiver - (Transductor) Dispositivo que recibe la potencia de un sistema mecánico, electromagnéntico o acustico y lo transmite a otro, generlamente en forma distinta. El microfono y el altavoz son ejemplos de transductores. En comunicaciones (informática) es un transmisor/receptor de señales de radio frecuencia (RF), sirve para conectar aparatos por via inalámbrica [5]

Mulfiport repeater - Son equipos que van conectados a un transceiver y que tienen varias puertas de salida para equipos. La única limitación que tienen es que mediante estos equipos no se pueden interconectar equipos que conecten redes entre sí [17]

Conector RJ45: El conector es una pieza de plastico transparente en donde se inserta el cable. El Jack es tambien de plastico, pero en este se inserta el conector. Las siglas RJ significan Registro de Jack y el 45 especifica el esquema de numeracion de pins. El cable se inserta en el conector, este se conecta al jack que puede estar en la pared, en la tarjeta de red la computadora o en el Switch [23].

Broadcast: Aquellas redes en las que la transmisión de datos se realiza por un sólo canal de comunicación, compartido entonces por todas las máquinas de la red. Cualquier paquete de datos enviado por cualquier máquina es recibido por todas las de la red [24].
Backup: Interconexión de segmentos de una red que es usado solamente como respaldo en caso de que un nodo no redundante no esté activo [25].

Bridgíng: Terminología del había inglesa que denomina un respaldo [26].

DTE: Data Terminal Equipment (equipo terminal de datos, ETD). Se considera ETD a cualquier equipo informático, sea receptor o emisor al final de los datos. Si los procesa y los envía a un tercero sería un ETCD (por ejemplo un módem). También definido como. Equipo Terminal de Datos. Lado de una interfaz que representa al usuario de los servicios de comunicación de datos en una norma como RS232C o X.25. Los ETD son generalmente computadoras o terminales de computadora [27].

ÁUI y BNC: Attachment Unit Interface (cable o interfase de unión de unidades) y Bayonet Neilí Concelmann (cierre de bayoneta, une 2 cables coaxiales) [28].

LAT (DECnet): LAT al igual que DECnet son protocolos y/o software de red para las microcomputadoras DEC (DECnet = Digital Network Architecture) [29].

Browser: Es lo mismo que navegador www, browser www o web browser. Programa utilizado para visualizar las páginas almacenadas en senadores de la Word Wide Web. Utilizando una definición un poco más técnica, un browser es un programa cliente que permite acceder, generalmente por medio de una interfase gráfica, información diversa en formato de hipertexto (no igual que HTML) almacenadas en senadores locales o remotos [30].

Throughput: Rendimiento total efectivo. Rendimiento total de una computadora que se cuantifica por su capacidad para enviar datos a través de todos los componentes del sistema, incluidos los dispositivos de almacenamiento secundario, como las unidades de disco [31].

Carrierr: Significa "Portadora". Es un tono continuo establecido por dos módems conectados entre sí. Los datos se comunican alterando la portadora [25].

Windowing: Es un esquema de control de flujo en el cual el dispositivo fuente requiere un reconocimiento del destino después que un cierto número de paquetes han sido transmitidos. Por ejemplo con un tamaño de ventana de tres, la fuente requiere de un mensaje de reconocimiento después que *hs.* enviado tres paquetes para poder continuar con la transferencia [32].

Timeslot: En español significa "Ranura de tiempo", son utilizados para transmitir información en un tiempo determinado y estos son asignados por la tecnología de red que se esté utilizando [37],

SLIP: Siglas de Serial Line Internet Protocol. SLIP es un protocolo que permite utilizar el TCP/IP en una línea telefónica por medio de un módem. Tiende a ser reemplazado por el PPP [34].
Autenticación: Es una fase opcional de PPP, pero por lo general es implementada por todas las ISP's, con el fin de verificar la información de usuarios conmutados [15]

Frame: Grupo estructurado, Marco. Un frame es una porción de datos transmitidos por un modem con fines de verificación de errores en otros datos transmitidos [35].

NAT: Es un protocolo de traslación de direcciones, con el cual se logra que por medio de una sola dirección IP publica, puedan acceder a una red como Internet; un rango de direcciones IP privadas [35].

DHCP: El protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) es un estándar IP diseñado para simplificar la administración de la configuración IP del host. El estándar DHCP permite el uso de servidores DHCP para administrar la asignación dinámica a los clientes DHCP de la red, de direcciones IP y otros detalles de configuración relacionados [36].

DNS: Es una abreviatura para Sistema de nombres de dominio (Domain Name System), un sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios. La asignación de nombres DNS se utiliza en las redes TCP/IP, como Internet, para localizar equipos y servicios con nombres descriptivos. Cuando un usuario escriba un nombre DNS en una aplicación, los servicios DNS podrán traducir el nombre a otra información asociada con el mismo, como una dirección IP [37].

TCP / IP: Se han desarrollado diferentes familias de protocolos para comunicación por red de datos para los sistemas UNIX. El más ampliamente utilizado es el Internet Protocol Suite, comúnmente conocido como TCP / IP.

Es un protocolo DARPA que proporciona transmisión fiable de paquetes de datos sobre redes. El nombre TCP / IP Proviene de dos protocolos importantes de la familia, el Transmission Contorl Protocol (TCP) y el Internet Protocol (IP). Todos juntos llegan a ser más de 100 protocolos diferentes definidos en este conjunto.

El TCP / IP es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local y área extensa. TCP / IP fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en el ARPANET una red de área extensa del departamento de defensa. [17]

OSI: En 1977, la Organización Internacional de Estándares (ISO), integrada por industrias representativas del medio, creó un subcomité para desarrollar estándares de comunicación de datos que promovieran la accesibilidad universal y una interoperabilidad entre productos de diferentes fabricantes. El resultado de estos esfuerzos es el Modelo de Referencia Interconexión de Sistemas Abiertos (OSI).

El Modelo OSI es un lineamiento funcional para tareas de comunicaciones y, por consiguiente, no especifica un estándar de comunicación para dichas tareas. Sin embargo, muchos estándares y protocolos cumplen con los lineamientos del Modelo OSI. [18]

Frame Relay: es un servicio de transmisión de voz y datos a alta velocidad que permite la interconexión de redes de área local separadas geográficamente a un costo menor. Es una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de marcos (“frames”) para datos, perfecto para la transmisión de grandes cantidades de datos. [19]

ACRÓNIMOS

ASNl: Abstract Syntax Notation One (Notación Sintáctica Abstracta Uno)

ARP: Address Resolution Protocol (Protocolo de Resolución de Direcciones)

ATM: Asynchronous Transfer Mode (Modo de Transferencia Asincrono)

CSMS-CB: Cali Sense Múltiple Access-Collision Detect (Acceso Múltiple de Sentido de Llamada-Detección de Colisión)

DAN: Desktop Área Network (Red de Área de Escritorio)

DNS: Domain Name Server (Servidor de Nombre de Dominio)

GAN: Global Área Network (Red de Área Global)

ICMP: Internet Control Message Protocol (Protocolo Internet de Control de Mensajes)

IP: Internet Protocol

IPIP: IP in IP Tunneling (Entunelamiento IP en IP)

IPSec: Internet Protocol Security (Protocolo Internet de Seguridad)

IPX: Internet Package Exchange (intercambio de Paquetes de Internet)

ISO: International Organisation for Standarisation (Estandarización para Organismos Internacionales)

ISDN: Red Digital de Servicios Integrados.

ISP: Internet Service Provider (Proveedor de Servicios de Internet)

L2TP: Layer 2 Tunneling Protocol (Protocolo de Entunelamiento de Nivel 2)

LAN: Local Area Network (Red de Área Local)

MAN: Metropolitan Área Network (Red de Área Metropolitana)

MPPE: Microsoft Point-to-Point Enciypíion (Protocolo de Encriptación Punto-a-Punto de Microsoft)

NAP: Network Access Point (Punto de acceso a red)

NAS: Neíwork Access Server (Servidor de Acceso Remoto)

NAT: Network Access Translator (Traductor de Direcciones de Red)

NFS: Network File Server (Servidor de Archive de Red)

NIC: Network Interface Card (Tarjeta de Interface de Red)

OSI: Open Systems Interconection (Interconexión de Sistemas Abiertos)

POP: Point of Presence (Punto de Presencia)

PPP: Point to Point Protocol (Protocolo Punto a Punto)

PROFECG: Procuraduría Federal del Consumidor

PVC: Permanent Virtual Circuit (Circuitos Virtuales Permanentes)

RADIUS: Remote Authentication Dial-In User Service (Autenticación Remota de Mareado Interno a Servicios de Usuario)

RAS: Remote Access Server (Servidor de Acceso Remoto)

RPC: Remote Procedure Calls (Llamadas de Procedimiento Remoto)

RRAS: Remote and Routing Access Service (Servicios de Acceso Remoto y de Enrutamiento)

SMDS: Synchronous iviultimegabit Data Service (Servicio de Datos Síncrono Multimegabit)

SMTP: Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correo)

SNMP: Simple Network Management Protocol (Protocolo Simple de Administración de Red)

SSL: Secure Sockets Layer (Nivel de Conectares Seguros)

SVC: Circuitos Virtuales Conmutados

TCP/IP: Transmission Control Protocol / Internet Protocol (Protocolo de Control de Transmisión / Protocolo internet)

TCP: Transmission Control Protocol

TFTP: Trivial File Transfer Protocol (Protocolo Trivial de Transferencia de Archivos)

UDP: User Datagram Protocol (Protocolo de Datagrama de Usuario)

UNI: User Network Interface

VC: Virtual Channels (Canales Virtuales)

VCI: Virtual Channel Identifiers (Identificadores de Canales Virtuales)

VLAN: Virtual Local Área Network (Red de Área Local Virtual) •

VP: Virtual Patlis (Caminos Virtuales)

VPI: Virtual Patlis Identifiers (Identificadores de Caminos Virtuales)

VPN: Virtual Private Network (Red Privada Virtual)

WAN: Wide Area Network (Red de Área Extensa)

REFERENCIAS BIBLIOGRÁFICAS

REFERENCIAS BIBLIOGRÁFICAS

[1] http://dis.eafit.edu.co/eursos/st059/material/fundamentacion//introredes.pdf

[2] http://www.newdevices.com/tutoriales/modeIo-tcpip/'2.html

[3] http://glosarium.com/term/1452,14,xhtml

[4] http://www.pchardware.org/redes/redes_osi.php

[5] http://www.cyclades.com.pe/Documentacion/Tecnologia/VPN_Tecnologia.htm

[6] http://www/.xombra.com/go_articulo.php?articulo=36

[7] http://landatel.com/html/glosario.html

[8] http://www.gestinet.info/es/vpn.asp

[9] http://www.nti.educa.rcanaria.es/conocernos_rnejor/paginas/introduccion.html

[10] http://www.interlan.com.co/vpns.htm

[11] http://www.digitian.com/html/vpn.htm

[12] http://www.angelfire.com/alt/arashi/red.htm

[13] http://www.microsoft.com

[14] http://www.definicion.org/intern

[15] http://www.mailxmail.com/curso/informatica/redes/capitulo10.htm

[16] http://es. definicion. org/internet

[17] http://www.cisco.com/warp/public/cc/techno/protocol/iprout/tech/tcpip_pc.htm

[18] http://www.cisco.com/warp/public/cc/techno/protocol/iprout/tech/osi_pc.htm

[19] http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/frame.htm

[20] http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/vpn.htm

[21] http://www.uaslp.mx/Plantilla.aspx?padre=1026

[22] http://mx.microsotf.com/alfonsoaraujocardenas/redes.html

[23] http://www.alegsa.com.ar/Dic/

[24] http://www.consulintel.es/html/productos/Perle/ipipxbr.htm#Bridging

[25] http://www.angelfire.com/art3/arturocaicedo/

[26] http://www.arqhys.com/arquitectura/bnc-conector.html

[27] http://www.linktionary.com/d/decnet.html

[28] http://jamillan.com/v_brows.htm

[29] http://www.m-w.com/cgi-bin/dictionary?va=throughputs
[30] http://www.sateliteinfos.com/diccionario/index.asp/termino/Windowing
[31] http://www.btwsa.com.ar/siteDocs/t.asp
[32] http://www.learnthenet.com/Spanish/glossary/slip.htm
[33] http://informatica.uv.es/iiguia/AER/Tema9.pdf
[34] http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/DHCP
[35] http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/DNS
[36] http://www.dei.uc.edu.py/tai2003/vpn/protocol.htm

REFERENCIAS BIBLIOGRÁFICAS

[36] Introducción a las Redes Locales Autor: José Félix Rábano Editorial Anaya.

[37] Redes locales y TCP/IP Autor: José luís Raya Editorial AlfaOmega

[38] Autor: Grupo NAP Edita: Colegio oficial de ingenieros de telecomunicación C/Aimagro,2. 28010 Madrid

[39] Revista PC/Tips Byte pag 94-98 articulo: "Redes inalámbricas" Abril 1992 Nicolás Baran.

[40] Wireless Security Modeis, Threats, and Solutions -Randall K. Nichols, Panos C. Lekkas McGraw-Hill

[41] Edita: COLE-GIOOFICIAL DE INGENIEROS DE TELECOMUNICACIÓN C/Almagro,2. 28010 Madrid

[42] Redes Inalámbricas (Wi-Fi) Aplicaciones y Proyectos Técnicos Fidel García, Jose F.Kukielka, Alonso Fernandez, Jose 1. Alonso

[41] Redes de Acceso de Banda Ancha". Arquitectura, prestaciones, servicios y evolución. Ministerio de Ciencia y Tecnología

[43] Measured Performance of 5 GHZ 802.11a Wireless LAN systems", by James C.Chen, Jeffrey M. Gilbert, Atheros Communications, 08/27/2001

[44] Introducción a las Redes Locales. José Félix Rábano. Editorial Anaya.

[45] Redes locales y TCP/IP. José Luís Raya Editorial AlfaOmega
[45] Como construir una Intranet con Windows 2003 Server. José Luís Raya Editorial AlfaOmega. Junio 2001, Colombia.

[46] Fundamentos de redes. Bruce A. Hallberg Editorial Mc. Hill. Primera Edición 2003.

[47] Comunicación entre computadoras y tecnologías de red. Michael A. Gallo, William M. Hancock. Editorial Thomson, Ed. 2002, México, D.F.

[48] Tirn Parker, “Leaming TCP/ÍP in 14 days", 1st edition, Sams Publishing & Prentice Hall, 1995.
[49] Intemetworking Technologies Handbook, Cisco Press. Ford, Kim Lew, Spanier and Stevenson. 1997.

VITA

Raúl Ramírez Arzate nació en Ixmiquilpan, Hidalgo, el 30 de octubre de 1978. Sus padres son Lorenzo Ramírez Muñoz y Emma Arzate Magaña. Realizó sus estudios de licenciatura en el Instituto de Ciencias Básicas e Ingeniería de la Universidad Autónoma del Estado de Hidalgo. Su experiencia laboral comienza en el año 2000-2002 siendo supervisor de escuelas primarias en el estado de Hidalgo, a partir del 2002 como catedrático en Algebra y Física en el CONAFE.
Su desempeño profesional inició en septiembre de 2005 ingresando a Cetha Logística un asociado de la empresa internacional Qualita, funcionando como Ingeniero de mantenimiento de cómputo y red, entre los más destacados Banamex, Telmex y Wyeth; a partir de marzo de 2005 se desempeña como profesional independiente.

- Dirección permanente: Reforma No. 106-d Int. 2 Colonia Centro
- Pachuca, Hidalgo, CP 42000. México
- Teléfono fijo:----------
- Teléfono celular: 044 771 140 7111
- Correo electrónico: raraul70@hotmail.com, raraul70@gmail.com

Marcos Aurelio Guzmán Vite nació en Pachuca, Hidalgo, el 29 de marzo de 1982. Sus padres son A. Aurelio Guzmán Vite y Angelina Vite Hernández. Realizó sus estudios de licenciatura en el Instituto de Ciencias Básicas e Ingeniería de la Universidad Autónoma del Estado de Hidalgo. Su desempeño profesional inició en julio de 2005 ingresando a Cetha Logística un asociado de la empresa internacional Qualita, funcionando como Ingeniero de mantenimiento de cómputo y red, entre los sitios más destacados atendidos son Banamex, Telmex y Wyeth; a partir de enero de 2007 se desempeña como encargado del Departamento de Capacitación de la Presidencia Municipal de Pachuca de Soto Hidalgo donde aplica todos los conocimientos adquiridos durante sus estudios, administración, asesorías en áreas como Computación, electrónica, redes, entre otras, al par se desarrollo como profesional independiente prestando a la comunidad pachuqueña servicios informáticos.

- Dirección permanente: Andador 2, Manzana M, No. 309, Col. Plutarco Elias Calles.
- Pachuca, Hidalgo, CP 42035. México
- Teléfono fijo: 71 34767
- Teléfono celular: 044 771 1896678
- Correo electrónico: marguvi_29@hotmail.com