UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"

PROPUESTA DE UN DISEÑO DE SISTEMA AUTOMATIZADO CLIENTE SERVIDOR PARA REDES PRIVADAS VIRTUALES DINAMICAS (DVPN) SOBRE BANDA ANCHA ADSL

ALIRIO JESUS MARQUEZ PERDOMO

Barquisimeto, 2005

UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGÍA
POSTGRADO EN CIENCIAS DE LA COMPUTACIÓN

PROPUESTA DE UN DISEÑO DE SISTEMA AUTOMATIZADO CLIENTE SERVIDOR PARA REDES PRIVADAS VIRTUALES DINAMICAS (DVPN) SOBRE BANDA ANCHA ADSL

Trabajo presentado para optar al grado de
Magíster Scientiarum

Por: ALIRIO JESUS MARQUEZ PERDOMO

Barquisimeto, 2005

PROPUESTA DE UN DISEÑO DE SISTEMA AUTOMATIZADO CLIENTE SERVIDOR PARA REDES PRIVADAS VIRTUALES DINAMICAS (DVPN) SOBRE BANDA ANCHA ADSL

Por: ALIRIO JESUS MARQUEZ PERDOMO

Trabajo de grado aprobado

_____	_____
(Jurado 1)	**(Jurado 2)**
Tutor	

_____

(Jurado 3)

Barquisimeto, ____ de _____ de 200_

UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGÍA
POSTGRADO EN CIENCIAS DE LA COMPUTACIÓN

PROPUESTA DE UN DISEÑO DE SISTEMA AUTOMATIZADO CLIENTE SERVIDOR PARA REDES PRIVADAS VIRTUALES DINAMICAS (DVPN) SOBRE BANDA ANCHA ADSL

Autor (a): Alirio Jesús Marquez Perdomo
Tutor (a): Arsenio Perez

RESUMEN

El presente trabajo se circunscribe en una investigación de campo bajo la modalidad de proyecto especial y tuvo como objetivo proponer un diseño de sistema cliente servidor que permitió crear redes privadas virtuales con direccionamiento IP dinámico (DVPN) sobre conexiones de acceso a Internet bajo tecnología banda ancha ADSL.

Para lograr este objetivo, se utilizó Internet para conectar las localidades remotas (Lara, Falcón y Portuguesa) con la sede principal (G&T Sistemas), empleando la encapsulación de la información transmitida para construir túneles o rutas virtuales seguras con la implementación de VPN, entre los usuarios de las diferentes localidades.

En la investigación se realizó el diagnóstico de las necesidades de implantación de conexiones DVPN, se determinó la factibilidad técnica de las conexiones DVPN, se propuso un diseño de DVPN y se construyó el software cliente servidor que permitió construir las redes privadas virtuales dinámicas. Finalmente se plantearon las conclusiones del estudio y algunas recomendaciones que dan pie a nuevas investigaciones en el campo.

Palabras Claves: Internet, Cliente-Servidor, Protocolo, Lan, Wan, ADSL, FTP, VPN

INDICE GENERAL

Página

INDICE DE GRÁFICOS

pág.

GRÁFICO

INDICE DE TABLAS

pág.

TABLA

INDICE DE FIGURAS

pág.

INTRODUCCIÓN

La comunicación entre los seres humanos es de obligatoria necesidad y, todas las ciencias conocidas, han contribuido decididamente al incremento, calidad y variedad en la transmisión de información, obteniendo un enorme crecimiento cultural, comercial e interpersonal, manifestado en una sociedad dinámica, educada y competitiva, que reclama una efectiva tecnología comunicacional que le interrelacione de forma permanente y ágil con su entorno y el mundo en general.

Actualmente Internet, contribuye a suplir esta necesidad, ofreciendo un servicio público de fácil acceso y de cobertura mundial, pero dada su vulnerabilidad es conveniente que las comunicaciones se realicen de forma segura, confiable y privada.

Este proyecto propuso un diseño de sistema automatizado cliente/servidor para crear redes privadas virtuales con direccionamiento IP dinámico (DVPN) sobre tecnología banda ancha ADSL, permitiendo la utilización de Internet como propuesta para interconectar localidades remotas (Lara, Falcón y Portuguesa) con la localidad principal de la empresa G&T sistema en Barquisimeto, no siendo necesaria direcciones IP fijas válidas para conectarse, obteniendo los usuarios una conexión de fácil acceso, bajo costo y transmisión de datos de forma confiable al utilizar protocolos de encriptamiento (L2TP, IPsec, entre otros).

El trabajo de grado está estructurado por capítulos, tal como se especifica:

El Capítulo I, comprende al planteamiento del problema, justificación, objetivos de la investigación, alcance y las limitaciones presentadas durante el desarrollo del estudio.

El Capítulo II, se refiere al Marco Teórico, que resumió antecedentes, fuentes bibliográficas y analíticas, sirviendo como base para el desarrollo de la investigación.

El Capítulo III, corresponde al Marco Metodológico de la investigación, especificando: tipo de investigación, población, muestra, técnicas de recolección de datos, instrumentos, validez y confiabilidad, fases de la metodología de la investigación y análisis de los datos.

El Capítulo IV, versa sobre el análisis de los resultados obtenidos, la creación y aplicación de la propuesta del diseño de sistema automatizado cliente/servidor.

El Capítulo V, trata lo concerniente a las conclusiones y recomendaciones.

El Capítulo VI, se refiere a la necesidad de elaborar un manual del sistema cliente/servidor que orientará a los usuarios.

CAPÍTULO I

EL PROBLEMA

Planteamiento Del Problema

El ser humano es por necesidad, un individuo sociable que ha venido a través de los tiempos experimentando significativos avances en su comunicación, adquiriendo así, conocimientos y conciencia de todo lo que sucede a su alrededor. En este interactuar sociable, el hombre ha empleado disímiles formas para comunicarse, desde la primitiva mímica a la escritura sobre piedras, pergaminos, sonidos, señales de humo y muchos otros métodos para tratar de expresar sus pensamientos y necesidades individuales y colectivas; ha inventado diversos sistemas de información, hasta lograr en nuestros días, poner a su servicio el milagro cibernético de las computadoras y los adelantos tecnológicos en el área de las telecomunicaciones. Esto le ha permitido interactuar con asombrosa rapidez desde cualquier parte del planeta y en fracciones de segundos transmitirse información actualizada sobre cualquier evento que suceda en el orbe (Veras, 2000).

El paso natural que sigue al intercambio electrónico de datos, es lograr que dos o más dispositivos que tienen almacenada información, independientemente del lugar geográfico donde se encuentren, la intercambien entre sí, lográndose de este modo una recíproca comunicación entre los usuarios. Esta es la misión de las redes de comunicación, las cuáles constituyen el medio a través del cuál, se enlazan los diversos puntos que contienen o reclaman la información. De igual forma, los canales o medios de comunicación, cumplen con la misión de ofrecer un soporte material al tráfico de datos que se genera entre la computadora emisora de la información y la que recibe ésta (Collado, 2003).

Por consiguiente para que las redes se comuniquen, es necesario un protocolo de red que es una especificación detallada de las "reglas" que deben seguir los diferentes programas que, empleados en una red de comunicaciones intercambian información. Para que éste sea útil, su especificación debe ser pública y debe ser aceptada por una parte significativa de la industria (Siles, 2002).

Cabe destacar que en 1960, el Protocolo de Control de Transporte o *Transport Control Protocol* (TCP) y el Protocolo de Internet o *Internet Protocol* (IP) actualmente denominado por el acrónimo TCP/IP, fueron desarrollados por la corporación RAND conjuntamente con el Instituto de Massachusetts de Tecnología y la Universidad de California en los Ángeles para el Departamento de Defensa de los Estados Unidos, por la necesidad de proveer rápida comunicación entre los diferentes dispositivos de red y es, sobre la base de estos protocolos que surge Internet, la red de redes (Leiner y otros, 1999).

De lo anterior, se desprende que en una red TCP/IP las computadoras se identifican mediante un número, que se denomina dirección de Protocolo de Internet o dirección IP. Dirección IP como identificador es un número único, global y estandarizado que permite al usuario a través de un computador, conectarse a Internet, transferir un archivo, enviar correos electrónicos entre otras bondades. Las direcciones IP deben estar asignadas por un proveedor de servicio de Internet o Internet Service Provider (ISP) y estas direcciones IP públicas en Internet pueden ser “Estáticas” o “Dinámicas”. Para el caso de Venezuela, tenemos como proveedores ISP a las siguientes empresas: CANTV, MOVISTAR, INTERCABLE, entre otros.

Considerando lo antes planteado, se puede definir a Internet como la gran colección de redes públicas, corriendo protocolos TCP/IP unidas dentro de la geografía mundial. Los navegantes de cualquier red, pueden usar los servicios que suministra TCP/IP para contactar usuarios en cualquiera de las otras redes, pero con la limitación de la seguridad en la información que transita por ésta. Internet es público, global, abierto a cualquiera que tenga una conexión y es vulnerable por atacantes que puedan consumir recursos del sistema (Tiempo de CPU, Ancho de

Banda de la Red, Memoria), así como también, pérdidas en la información (Siles, 2002).

Para utilizar a Internet como medio de conexión que enlaza localidades remotas, de manera segura en cuanto al envío y recepción de información, surge la necesidad de utilizar una Red Privada Virtual o *Virtual Private Network* (VPN). La VPN, proporciona un medio para usar el canal público de Internet, como un canal apropiado para comunicar los datos privados, a través de la creación de túneles o rutas virtuales, asegurando la confidencialidad de la información que se transmite, mediante la tecnología de encriptación y encapsulamiento de los datos (Cánovas y otros, 2001).

Siguiendo la misma línea, una Red Privada Virtual Dinámica (DVPN) se define como un modelo abierto, en el cuál, dos entidades quieren comunicarse de un modo seguro, flexible y de bajo costo y sin conocimiento previo de la otra parte (solamente teniendo en común una jerarquía de confianza) en donde se utilicen VPN, infraestructura de clave públicas y el uso de tarjetas inteligentes (Cánovas y otros, 2001).

Bajo las VPN, los túneles o rutas virtuales seguras, se construyen con direcciones IP públicas, estáticas o dinámicas, según la asignación hecha por el ISP a los equipos en los extremos (Computador Emisor, Computador Receptor). Las direcciones IP públicas, permiten que los usuarios puedan navegar en Internet, con los datos que viajan dentro del túnel, protegidos y encriptados (ABC analog, 2002).

Los proveedores de servicio de Internet (ISP) en Venezuela, específicamente en Barquisimeto estado Lara, ofrecen crear redes privadas virtuales a través de Internet, con soluciones dedicadas o permanentes. CANTV es un caso de ello, donde los clientes deben contratar sus servicios, en algunos de sus extremos con la finalidad de poder crear dicha red, para que sus usuarios puedan conectarse y verse a través del túnel de conexión con direcciones IP públicas estáticas. Este tipo de solución es muy costosa, ya que, al adquirir un circuito dedicado o permanente de conmutación de tramas o *Frame Relay* (FR), el mismo es arrendado mensualmente con costos

operativos en dólares. Otros proveedores ISP, como Intercable, prestan servicio de Internet por Megabytes consumidos mensualmente y para crear una VPN ofrecen una conexión a gran velocidad en uno de sus extremos, pero con un costo adicional por direcciones IP públicas certificadas, que permiten crear la VPN y un costo asociado al consumo mensual de Megabytes. Es así, que el problema principal de formar la VPN, radica en adquirir direcciones IP públicas, que permitan construir túneles o rutas virtuales seguras, entre los grupos de usuarios que se encuentran en diferentes zonas geográficas.

En la actualidad, existe una empresa llamada G&T Sistemas, ubicada en Venezuela, en la ciudad de Barquisimeto estado Lara, la cual se desempeña en el ramo de las operaciones de tecnología informática. Esta empresa, presta servicios a compañías que desean automatizar sus funciones, utilizando sistemas computarizados, en las áreas de construcción, administración, contabilidad, educación, entre otros. También asiste a algunos de sus clientes de manera remota (Lara, Falcón y Portuguesa) donde poseen oficinas, para realizar, actualizaciones y soportes en línea, entre otros servicios. La asistencia remota, es efectuada vía conexión telefónica, a través de un servidor de acceso remoto (RAS), donde se permite una sola conexión simultánea por cliente puesto que se dispone de una sola conexión telefónica, conectada a una tarjeta Fax/MODEM. La empresa G&T Sistemas tiene arrendado con el ISP de CANTV un servicio de banda ancha (ABA) sobre Línea de Abonado Digital Asimétrica o *Assymetric Digital Subscriber Line* (ADSL), siendo este, un servicio de conexión dedicada, pero con direcciones IP públicas dinámicas.

Considerando lo antes planteado, surgieron las interrogantes siguientes:

¿El servicio que actualmente presta la empresa G&T Sistemas puede ser sustancialmente mejorado con el uso de las DVPN?

¿Con una conexión de Red Privada Virtual Dinámica (DVPN), se podrá establecer comunicación con la red interna de un cliente con calidad en la conexión?

¿Se tendrá seguridad en la información que transita por los canales de

comunicación con los clientes que utilicen la solución DVPN?

¿La propuesta de interconexión DVPN se podrá realizar con los recursos tecnológicos con los que cuenta actualmente las localidades remotas?

El presente estudio tuvo como finalidad principal controlar el direccionamiento IP dinámico sobre las conexiones de acceso a Internet bajo tecnología banda ancha ADSL, a través, de un sistema cliente/servidor para construir y establecer redes virtuales privadas dinámicas (DVPN) entre la empresa G&T Sistemas y sus clientes remotos.

Objetivos

GENERAL

PROPONER UN DISEÑO DE SISTEMA AUTOMATIZADO CLIENTE SERVIDOR PARA LA CREACIÓN DE REDES PRIVADAS VIRTUALES DINÁMICAS (DVPN) SOBRE TECNOLOGÍA BANDA ANCHA ADSL

Específicos

1. Diagnosticar la necesidad de una interconexión de red a través de Internet a los clientes de la empresa G&T Sistemas, con la implantación de DVPN en Lara, Falcón y Portuguesa.
2. Determinar la factibilidad técnica para la implementación de una conexión DVPN a los clientes que se conectan telefónicamente con la empresa G&T Sistemas.
3. Proponer un diseño de conexión privada virtual dinámica a los clientes de la empresa G&T Sistemas en Barquisimeto.

Justificación e Importancia

ES IMPORTANTE SEÑALAR QUE EL NIVEL DE DESARROLLO ECONÓMICO, SOCIAL Y POBLACIONAL QUE SE ESTÁ ABRIENDO CAMINOS EN VENEZUELA, PROYECTA UNA EXIGENTE Y VARIADA PRODUCCIÓN DE SERVICIOS DE REDES TELEINFORMÁTICAS. DISPONE PARA ELLO, DE LOS RECURSOS TECNOLÓGICOS MAS AVANZADOS, QUE PROPORCIONAN UN CAMBIO RADICAL EN LAS ESTRUCTURAS OBSOLETAS, QUE POR TANTO TIEMPO HAN EXISTIDO, SIENDO NECESARIAS DERRUMBARLAS PARA PODER ENFRENTAR LOS RETOS MUNDIALES PRESENTES EN LA ACTUALIDAD, TALES COMO: GLOBALIZACIÓN, CONCENTRACIÓN, COMPETENCIA Y NUEVOS PRODUCTOS Y SERVICIOS. PARA ELLO LAS ORGANIZACIONES DEBEN DEPURARSE, SER MÁS HORIZONTALES, DESCENTRALIZAR SUS OPERACIONES Y MIGRAR HACIA UNIDADES DE NEGOCIO E INCORPORAR EL COMPONENTE TECNOLÓGICO QUE PERMITA OPTIMIZAR SU FUNCIONAMIENTO.

POR LO TANTO, SE HIZO NECESARIO QUE LA EMPRESA G&T SISTEMAS, IMPLEMENTE UN DISEÑO DE SISTEMA CLIENTE SERVIDOR, PARA REDES PRIVADAS VIRTUALES DINÁMICAS, APROVECHANDO LA INFRAESTRUCTURA DE RED PÚBLICA QUE POSEEN SUS RELACIONADOS, PARA CONECTARSE A SU RED PRIVADA, LO CUÁL LE PERMITIRÁ OPTIMIZAR SUS SERVICIOS, OPERANDO A VELOCIDADES SUPERIORES A LAS TELEFÓNICAS Y CON MAYOR SEGURIDAD EN LA INFORMACIÓN TRANSFERIDA.

Entre los beneficios directos que proporcionaría la implantación del sistema cliente servidor, para la conexión de red virtual privada dinámica, se encuentran:

- Permitirá mejorar la calidad de atención a los clientes, que realizan sus requerimientos de soporte y consultas a los sistemas vía Web, debido al aumento en velocidad, que tendrá con la utilización de la infraestructura de red interna de sus localidades y la estabilidad que brinda una conexión de banda ancha, que se traduce en disminución de tiempo de espera y en un aumento de

atención a varios clientes a la vez.

- Ofrecerá seguridad en las transacciones que se ejecuten, con las consultas efectuados por los clientes en las diferentes localidades en que se encuentran (Lara, Falcon y Portuguesa).
- Brindará, mayor operatividad en el servicio, por contar con redundancia en la conexión a la plataforma de red, de los sistemas con que cuenta la empresa G&T Sistemas, dado que el enlace principal, iría por la red Lan/Wan de la compañía y en caso de alguna falla, o intermitencia de la misma, se enlazaría vía conexión telefónica, pero contando con seguridad en la información, debido a los protocolos de encriptamiento utilizados por la solución DVPN.
- Permitirá un seguimiento y control, a nivel administrativo de los clientes que acceden a los sistemas en línea de la empresa G&T Sistemas, por estar enlazada a la red privada de esta, a través de una conexión dedicada ADSL, de este modo, el administrador de red de la empresa G&T Sistemas, podría conocer en línea el estado del enlace a través de herramientas de monitoreo.
- Permitirá reducir significativamente, la inversión que tendría que realizar G&T Sistemas en Barquisimeto, con la adquisición de una solución de red privada virtual.
- Permitirá a G&T Sistemas ofrecer a sus clientes, un mejor servicio con un costo operacional mas bajo.

Esta propuesta de solución, aunado a otros proyectos nacionales, afianzo el hecho de que se utilice la tecnología existente en nuestro país, lo cuál, ha cobrado una gran relevancia para las empresas, motivado por la situación económica por la que atraviesa Venezuela actualmente, contribuyendo al incremento de fuentes de empleo directas e indirectas.

Alcance y Limitaciones

Sobre la base de los objetivos antes expuestos, se presento una serie de consideraciones que definieron el alcance y las limitaciones del trabajo.

En lo que respecta a la investigación, se realizó en la empresa G&T Sistemas, específicamente en la sede administrativa ubicada en la Av. Venezuela, con calles 32 y 33, Edif. Don Martín, piso 1, ala sur, Departamento de Sistemas, Barquisimeto, Edo. Lara. El estudio se efectúo a los clientes ubicados a las empresas que presta soporte G&T Sistemas, en los estados (Lara, Falcon y Portuguesa), estos clientes cubren diferentes demandas de servicios en los mercados de Venezuela, en sus respectivas zonas.

Por consiguiente, solamente se estudio la creación de VPN con direccionamiento dinámico, sobre banda ancha ADSL en la sede de la empresa G&T Sistemas, utilizando un servidor principal bajo el sistema operativo Windows 2000 Server y para las localidades remotas se contará únicamente con estaciones de trabajo basadas en Windows 2000 y Windows XP.

El estudio se ajusta: 1) Implementación de DVPN en Barquisimeto sobre banda ancha ADSL, con un esquema cliente servidor para soportes y consultas y 2) Se utilizará la infraestructura de red de los clientes de la empresa G&T Sistemas, como una buena opción para el estudio de la creación de la red virtual privada dinámica.

CAPÍTULO II

MARCO TEÓRICO

Antecedentes de la Investigación

Hace unos años atrás todavía no era tan importante el conectar a usuarios a Internet para cuestiones de trabajo, pero a medida que ha pasado el tiempo las compañías han requerido que las redes de áreas locales o Local Area Network (LAN) trasciendan más allá del ámbito de la oficina. Estas redes demandan incluir el acceso a los trabajadores y centros de información de otros edificios, ciudades, estados o incluso otros países. Para lograr esta interconexión solicitada se tenían que invertir en hardware y servicios de telecomunicaciones costosos para crear redes amplias de servicio, denominadas Wide Area Network (WAN). Sin embargo, actualmente con Internet, las compañías tienen la posibilidad de crear una red privada virtual (VPN) que demanda una inversión relativamente pequeña de hardware y utiliza el Internet global para la conexión entre los puntos de la red y satisfacer los servicios de interconexión requeridos (Cabañas, 2000).

Este estudio se elaboró investigando temas relacionados con conexiones virtuales privadas, que permitió resolver el problema de interconexión de localidades remotas con sedes principales, utilizando la

tecnología ADSL para la conexión a Internet en ambos extremos, logrando construir una red virtual privada dinámica, aplicando el sistema cliente/servidor propuesto por el investigador.

Siguiendo la misma línea, en un estudio que realizó González y otros (2001) planteo una solución a los problemas de comunicación de la empresa SkyTEL S.A en cuanto a la movilidad de sus empleados, la velocidad de acceso a los datos de la central y la seguridad contra elementos externos que interferían en el buen funcionamiento de la empresa, para la interconexión de veinticinco (25) empleados remotos a la Intranet de la empresa. Los objetivos planteados fueron los siguientes:

- Proporcionar movilidad a los empleados.
- Acceso a la base de datos central sin utilización de operadores telefónicos.
- Interconexión total a la red de todos los comerciales (empleados), de forma segura a través de una infraestructura pública.
- Intercambio de información en tiempo real.
- Correo electrónico corporativo
- Acceso remoto a la información corporativa.
- Teletrabajo.
- Flexibilidad y facilidad de uso.
- Obtención de la máxima velocidad de transferencia de datos usando con eficiencia los recursos empleados.
- Fácil adaptación a las nuevas tecnologías.

González y otros (2001) adoptaron la solución de VPN fundamentalmente por dos (2) razones principales

- Costos, resultaba mucho más económico interconectar a los empleados utilizando una infraestructura pública que desplegar una red físicamente privada.
- Seguridad en las conexiones con la utilización del protocolo de túnel punto a punto o Point-to-Point Tunneling Protocol (PPTP) creando VPN. Este tipo de enlace proporciono un acceso seguro de los clientes a la red, con total movilidad y con independencia del Proveedor de Servicios de Internet (ISP) por el que se conecte.

En este orden de ideas, Espinera y otros (2003) platearon que una red privada virtual puede ser comparada con un sistema privado de telecomunicaciones que emplea líneas propias o alquiladas y que sólo puede ser utilizada por una compañía. En su estudio Espinera y otros (2003) indicaron al respecto:

- La idea de las VPN es otorgarle a las compañías, las mismas capacidades a costos mucho más bajos, usando la infraestructura pública compartida en lugar de una privada.
- Las compañías telefónicas han provisto de recursos compartidos seguros para mensajes de voz durante años. Una red privada virtual hace esto posible, pero para los datos.
- Hoy día, las compañías buscan usar una red privada virtual tanto para su Extranet como para su Intranet de área amplia.

Utilizar una red privada virtual involucra cifrar los datos antes de enviarlos a través de la red pública y descifrarlos instantes antes de entregarlos a su destino final. Un nivel adicional de seguridad, supone cifrar no sólo los datos sino también las direcciones de red de origen y destino (Espinera y otros 2003).

Cabe destacar que Espinera y otros (2003) describen a una VPN (Virtual Private Network) como una estructura de red corporativa implantada sobre una red de recursos de transmisión y conmutación públicos, 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 (Modo de Transmisión Asíncrona) o Frame Relay (Conmutación de Tramas). Adicionalmente, definió las

VPN como una red privada que se extiende, mediante procesos de encapsulación y cifrado, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte, como la Internet.

Las funcionalidades de una VPN están definidas más por el protocolo de transporte WAN, que por los dispositivos instalados en sus extremos, encargados de realizar la conexión con los elementos de la red de área local, en los puntos remotos a través de la WAN. Las VPN pueden enlazar las oficinas corporativas con aliados comerciales o asociados de negocio, usuarios móviles y sucursales remotas, mediante canales de comunicación seguros utilizando protocolos como IPSec (IP Secure), como se muestra en la figura 1 (Espinera y otros, 2003).

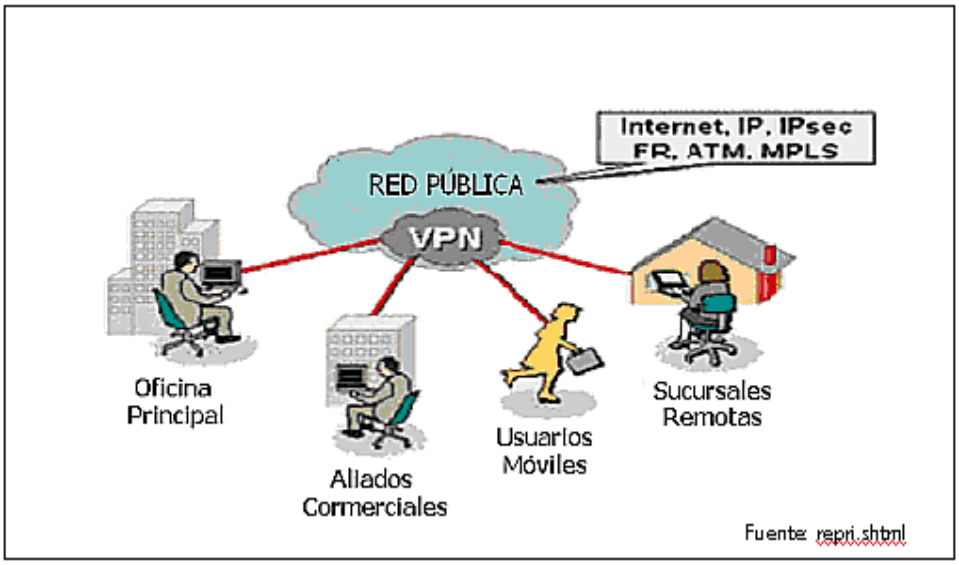

Figura 1. Conexión de la Red Corporativa a Través de una VPN

Fuente: **http://www.pc-news.com/detalle.asp?sid=&id=44&Ida=649**

Según las descripciones expuesta por Espinera y otros (2003) los paquetes de datos de una VPN viajan por medio de un "túnel" definido en la red pública. El túnel es la conexión definida entre dos puntos en modo similar a como lo hacen los circuitos en una topología WAN basada en paquetes. A diferencia de los protocolos orientados a paquetes, capaces de enviar los datos a través de una variedad de rutas

antes de alcanzar el destino final, un túnel representa un circuito virtual dedicado entre dos puntos. Para crear el túnel es preciso que un protocolo especial encapsule cada paquete origen en uno nuevo que incluya los campos de control necesarios para crear, gestionar y deshacer el túnel, tal como se muestra en la Figura 2.

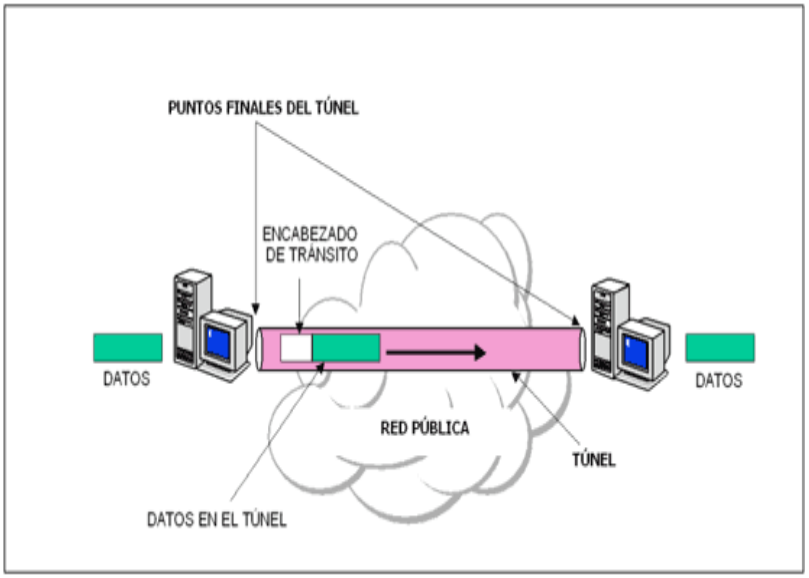

Figura 2. Túnel en una VPN

Fuente: **http://www.pc-news.com/detalle.asp?sid=&id=44&Ida=649**

Por su parte, Miranda (2003) planteó un Diseño de Interconexión de redes mediante VPN a la franquicia McDonald's para interconectar sus sedes remotas (cadenas de restaurantes) localizadas en el ámbito nacional con la sede principal del mismo, ubicada en Caracas Venezuela. Los objetivos de la investigación fueron los siguientes:

- Conocer los protocolos relacionados con VPN, así como todos aquellos conceptos que documenten su implementación.
- Determinar las ventajas y desventajas de cada modelo de implementación de VPN, de forma tal que se logre establecer un criterio que decida cual diseño se adecua a las necesidades del cliente.

- Establecer un modelo de diseño de interconexión basándose para ello en el resultado que arroje una matriz de parámetros y requisitos.
- Poner en marcha la propuesta de diseño con las herramientas prácticas disponibles.

Miranda (2003) en su investigación concluyó:

- Una VPN es una tecnología de interconexión construida sobre Internet que brinda seguridad, confiabilidad y disponibilidad propia de una red privada con líneas alquiladas.
- VPN puede sustituir a la tecnología de conmutación de tramas o Frame Relay (FR) en redes de bajo y mediano trafico. Adicionalmente, una VPN puede soportar implementaciones de Voz sobre sus túneles, sin modificar notablemente el desempeño de la misma.
- El costo es el elemento que mas destaca a la solución VPN, cuando se compara con otras tecnologías. Contrariamente, tiene sus desventajas como el retardo e indisponibilidad, producto del congestionamiento en la infraestructura pública de Internet, minimizan la calidad de servicios en tiempo real, como por ejemplo, voz mediante VPN, cosa que no ocurre con FR.
- La propuesta firewall watchGuard, es la solución mas apropiada para realizar el diseño VPN. las razones que motivan a esta conclusión, adicionando la preferencia del sistema Telcorp, fue el adecuado manejo de los siguientes parámetros: Flexibilidad, escalabilidad, soporte de direcciones IP dinámicas, seguridad y costos. También, por que se adapto de la mejor manera a los criterios de diseño implementados.
- La implementación de una topología estrella, cuyo centro es un datacenter, permite a Telcorp brindar el servicio VPN a diferentes clientes mediante la misma red, lo cual optimiza el uso del equipo principal ubicado en el datacenter.

- Las ofertas VPN ofrecidas por las empresas carrier de Venezuela: CANTV, COMSAT, TELCEL, presentan dos desventajas importantes que son: Costos y la necesidad de poseer direcciones IP fijas validas en todas las localidades. El diseño propuesto vence estas dificultades y ahora se presenta como un nueva alternativa para quienes necesitan redes privadas.

Del mismo modo, en un estudio reciente por Cánovas y otros (2003) presentaron una solución de VPN en la cual las entidades no conservaban secretos compartidos, sino que utilizan criptografía de clave pública para ofrecer seguridad a las comunicaciones, información criptográfica que no tiene que estar almacenada de forma estática, sino que es ofrecida al sistema cuando la necesita. Esta solución se consigue gracias a una Infraestructura de Clave Pública (PKI) propia y al uso de tarjetas inteligentes.

Los objetivos planteados fueron los siguientes:

- Conectar dos redes privadas A y B que van a ser protegidas por dos (2) puertas de enlaces o *Gateway* Seguros (SG).
- Los SG establecerán un túnel seguro basado en el protocolo de seguridad IP o *IP Security* (IPsec) y el Cambio de clave en Internet o *Internet Key Exchange* (IKE).
- La autenticación en los extremos será realizada usando certificados X.509 emitidos para los SG a través de sus correspondientes claves privadas.
- La implementación de los protocolos IPsec y IKE utilizada ha sido Linux FreeS/Wan por ser una solución completa de IPv4.

Cánovas y otros (2003) en su investigación concluyeron que:

- La implementación IPSec utilizada ha sido *KerneL IP Security* (KLIPS) incluida en el software FreeS/WAN. Esta solución permite establecer túneles seguros sobre redes no confiables, siendo los paquetes IP

enrutados entre los SGs separados por cualquier topología de red. El resultado es una conexión IP virtual que permitió definir la VPN.

- El software utilizado ha sido Pluto, la solución IKE que ofrece Linux FreeS/WAN. Pluto es un demonio que maneja intercambios de claves, verifica identidades y establece una política se seguridad para KLIPS. Pluto se basa en la autenticación de las entidades mediante secretos compartidos.
- Se ha modificado el software para unir realmente las soluciones de PKI y VPN. Esta modificación permitirá a cada entidad IPSec obtener la información criptográfica que necesite: certificados, claves privadas, entre otros, de un modo dinámico, con el único requerimiento de que tenga instalado un certificado de la Autoridad de Certificación deseada.
- La solución que ofrece los mecanismos y elementos necesarios de gestión de información criptográfica para el establecimiento de comunicaciones seguras es lo que se llama Infraestructura de Clave Pública o *Public Key Infrastructure* (PKI).
- Existen dos puntos de unión entre una PKI y una VPN. El primero es cuándo se deben emitir certificados para los usuarios, de modo que deba verificarse la identidad de cada entidad que lo solicite, siendo en este caso los administradores de red los responsables para la certificación de los sistemas. La información privada es almacenada en una tarjeta inteligente, mientras que la información pública es publicada en un directorio accesible para todos los usuarios de la organización.
- Una vez que los certificados han sido emitidos, los administradores pueden establecer canales seguros entres las redes. Es en este momento cuando Pluto obtendrá las informaciones criptográficas necesarias para la negociación, ya sea la clave privada a través de la tarjeta inteligente o su propio certificado o el del otro extremo mediante

el acceso al directorio de certificados.

En relación con estudios de VPN, García y Otros (2003) presentaron un proyecto llamado Prototipo de red multiservicio de muy altas prestaciones basada en IPV4/IPV6 sobre multiplexación por longitud de onda (PREAMBULO), es un proyecto perteneciente al plan nacional de Madrid España, que plantea la instalación, configuración y operación de una red de investigación de fibra óptica en la Comunidad de Madrid, que proporciono un servicio de transporte de datos utilizando IP directamente sobre división en longitud de onda o *Dense Wavelength División Multiplexer* (DWDM), entre los tres nodos de la red: la Universidad Carlos III de Madrid, la Universidad Politécnica de Madrid y la Empresa de telecomunicaciones Telefónica de España.

Como Objetivo García y Otros (2003) plantearon utilizar VPN nivel 2 manteniendo una única infraestructura basada en transporte sobre conmutación de etiquetas multi-protocolos o *Multi-Protocol Label Switching* (MPLS).

En este artículo presentaron la infraestructura de red óptica para soporte de IP directamente sobre DWDM del proyecto PREAMBULO, describiéndola tanto a nivel físico como a nivel lógico y comentando las principales alternativas que se dieron antes de optar por una solución definitiva que proporcionase la conectividad deseada entre las tres sedes que participaron en el proyecto.

Dicha solución se basó en mantener la conectividad a nivel 2 mediante conmutadores (con el algoritmo *Spanning Tree* deshabilitado), y utilizando VLANs para separar directamente a ese nivel el tráfico que va a circular por la red óptica.

Después presentaron las principales experiencias llevadas a cabo en el proyecto, indicando en el artículo, las experiencias con soluciones de redes privadas de nivel 2. Posteriormente realizaron una revisión de las principales líneas de investigación en lo referente a redes privadas virtuales (VPN), comentando la solución para VPNs de nivel 3, y haciendo especial énfasis en las soluciones de nivel 2.

Dichas soluciones se basaron en tecnologías que se encuentran actualmente en desarrollo, y para las que han comenzado recientemente a aparecer las primeras implementaciones en equipos comerciales. Si bien casi todas las propuestas se basan en el uso de túneles Martini, existen diferentes propuestas para el establecimiento de los circuitos virtuales.

Finalmente García y Otros (2003) analizaron la infraestructura que se ha probado dentro del proyecto PREAMBULO para dar soporte a una solución concreta VPN de nivel 2, Logical PE, propuesta por el fabricante Nortel Networks. De esta forma se demostró la viabilidad de esta tecnología de última generación, comprobando las ventajas respecto a soluciones previas que presentaban ciertos problemas de escalabilidad.

Sobre la base de los estudios consultados, se pudo conocer una alternativa de interconexión de sedes remotas que permitieron la disminución de costos, utilizando una red pública (Internet) con seguridad en la información que transita por la red, con la implementación de una solución VPN. Cabe destacar, que en los antecedentes revisados durante la investigación, no se encontró información sobre la creación de redes virtuales dinámicas sobre banda ancha ADSL utilizando una aplicación cliente/servidor.

Bases Teóricas

En esta sección se presentó el referencial teórico que permitió al investigador conocer de las tecnologías y estándares que sirvieron para la implementación del sistema cliente/servidor, estableciendo Redes Virtuales Privadas Dinámicas (DVPN) con los componentes de software y hardware necesarios para su funcionamiento.

Las bases teóricas del estudio, comenzaron con el modelo OSI, ya que es la

columna vertebral de las comunicaciones, en el cual se hizo énfasis en las capas que se utilizaron de este modelo para establecer una VPN dinámica. Dentro del contexto del Modelo OSI se hizo referencia al protocolo TCP/IP que se utilizó para establecer la comunicación en la red de área local (LAN), en las sedes remotas, y también permitió realizar la conexión de red de área amplia (Wan).

En este sentido se pudo indicar que el protocolo TCP/IP es la base de Internet, que sirvió para enlazar las computadoras, así como también, la tecnología ADSL que fue el medio escogido para la red Wan en el trabajo realizado.

Continuando en esta misma línea, se estudiaron conceptos como el de dirección IP, que permitió identificar el segmento de red de los equipos de las sedes remotas con el servidor principal, a su vez, entender el concepto cliente/servidor que contribuyó en la construcción de la propuesta del diseño de la aplicación DVPN.

De igual manera, dentro del contexto de los protocolos TCP/IP, el protocolo de capa de aplicación denominado FTP se utilizó para la publicación de la dirección IP del servidor de la empresa G&T Sistemas y la captura de éste, en los clientes de las sedes remotas.

Por último se investigo el concepto de VPN, cuales eran los requerimientos básicos para su construcción, la tecnología y su funcionalidad, que sirvieron para el encapsulamiento de los datos que transitaron por Internet desde la sedes remotas a la localidad principal utilizando el protocolo de túnel de capa dos (L2TP) y la Seguridad de protocolos Internet (IPsec).

Estándares en la Comunicación de Datos

Modelo de Referencia OSI

Para el trabajo de grado, se uso como marco referencial el modelo de Interconexión de Sistemas Abiertos o *Internacional Standards Organization* (OSI) en donde, se indico que los protocolos de comunicación estaban constituidos en siete niveles. Teniendo cada uno funciones muy específicas, que sé interrelacionan con las funciones de los niveles contiguos. Los niveles inferiores definen el medio físico, conectores y componentes que proporcionan comunicaciones de red, mientras que los

niveles superiores definen cómo acceden las aplicaciones a los servicios de comunicación.

Según Tanenbaum (1996), el modelo OSI tenía su origen en la Arquitectura de red sistemas o *System Network Architecture* (SNA) de IBM, que fue una descripción arquitectónica de los protocolos, formatos y estructuras necesarias para la transmisión de paquetes de información en un entorno de red. El modelo OSI fue desarrollado por la Organización Internacional para la Estandarización o *Open System Interconnection* (ISO) como un modelo de referencia de interconexión de sistemas abiertos. Las normas OSI fomentan los entornos abiertos de conexión de red que permite a los sistemas de computadoras de múltiples vendedores, comunicarse entre si, mediante el uso de protocolos que los miembros de ISO han aceptado internacionalmente.

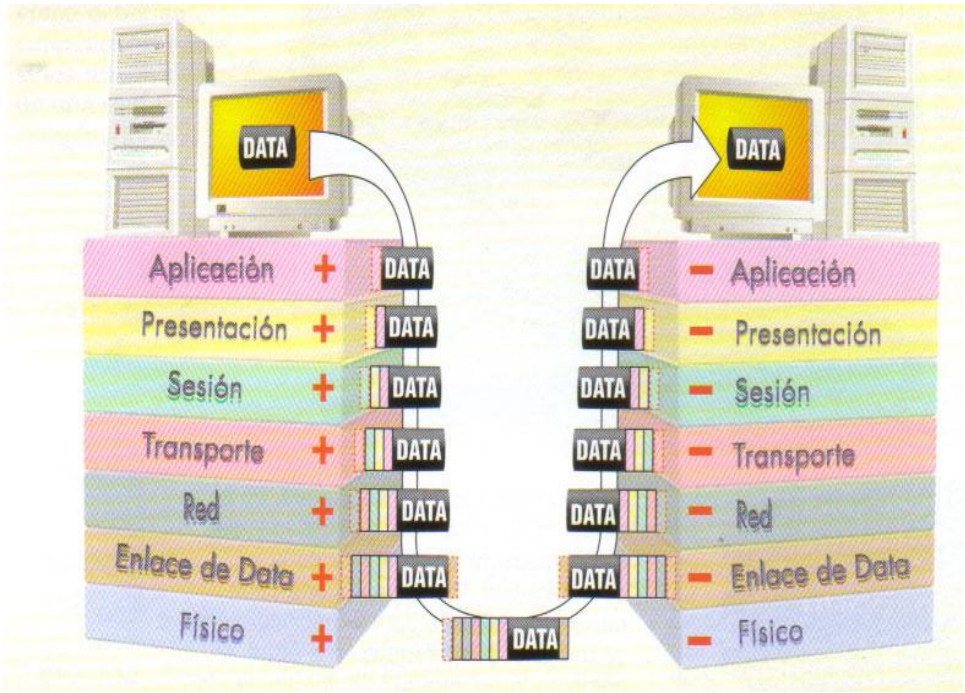

Figura 3. Arquitectura de la Red Basada en el Modelo OSI.

Fuente: http://coqui.lce.org/cadiaz/Cedu5240/contenido/ModeloOSI.html

Niveles del Modelo OSI

Nivel Físico

Según Millán (2005), la forma en que estarán físicamente conectadas las

estaciones en la red, el tipo de cable ó medio utilizado para la comunicación entre nodos, como viajará y será codificada la información eléctricamente en la red es definida por la capa física, en tal sentido, se conectaron los equipos (PC´s) físicamente en la red de área local (LAN), con cable par trenzado con sus conectores o lo que es lo mismo *Patch cord*, tanto las sedes remotas como la sede principal.

Nivel de Enlace de Datos

Según Millán (2005), los protocolos de este nivel son los responsables de transmitir sin errores y establecer conexiones lógicas entre estaciones. Esto se consigue empaquetando los bits procedentes de la capa física en bloques de datos (Tramas) y enviando estas tramas con la necesaria sincronización y orden.

Para la construcción de la DVPN se trabajo a nivel de control de acceso al medio con el estándar Ethernet, utilizando la Línea de Abonado Digital Asimétrica o *Assymetric Digital Subscriber Line* (ADSL) como la tecnología WAN que se escogió para conectarse a Internet, permitiendo el acceso de los cliente remotos (Localidades Remotas Lara, Portuguesa y Falcon) a la red de la localidad principal (Empresa G&T Sistemas), también se utilizó el protocolo de túnel de capa dos (L2TP) facilitando el entunelamiento de paquetes del protocolo punto a punto o *Point-to-Point Protocol* (PPP) a través de la red.

Nivel de Red

Según Millán (2005), esta capa decide el enrutamiento de los paquetes entre el origen y el destino. Esta orientación puede establecerse estáticamente (mediante tablas de rutas prefijadas) o bien dinámicamente (en función del tráfico de la red). Para la creación de la DVPN se utilizó el protocolo de Internet (IP) de manera

dinámica en ambos extremos.

Nivel de Transporte

Según Millán (2005), esta capa es la encargada de garantizar la transmisión de los datos. En ella podemos encontrar los protocolos UDP, TCP, entre otros. Para este estudio se utilizó el protocolo de control de trasporte o *Transmission Control Protocol* (TCP) garantizando la transmisión de los datos entre las localidades remotas y la localidad principal construyendo la DVPN.

Nivel de Sesión

Según Millán (2005), esta capa permite que usuarios de máquinas distintas establezcan sesiones entre ellos. También se encarga de la sincronización y de configurar el sentido del tráfico para que vaya en ambas direcciones a la vez o de forma alternativa. En otras palabras, tiene la responsabilidad de asegurar la entrega correcta de la información a la siguiente capa (capa de presentación). Según esta definición se utilizó esta capa en el trabajo propuesto de DVPN, estableciendo sesiones desde las localidades remotas con la implementación de la aplicación cliente al capturar la IP del servidor de hospedaje (Hosting) y luego realizando la conexión con la aplicación servidor instalada en el servidor de la empresa G&T Sistemas.

Nivel de Presentación

Según Millán (2005), la capa de presentación se ocupa de la sintaxis y semántica de la información que se transmite. Dentro de las tareas específicas se encuentran: Traslación de códigos, Encriptación y Compresión. Ejemplos de

protocolos de presentación: LPP, XDR, NetBIOS (Novell), NCP (Novell), X.25 PAD, entre otros.

Nivel de Aplicación

Según Millán (2005), esta capa ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico, gestores de bases de datos y servidor de aplicaciones. Utilizando la aplicación servidor desarrollada en esta investigación, se logro publicar la dirección IP del servidor de la localidad principal y la captura de esta IP en las PC o estaciones de trabajo de las localidades remotas utilizando la aplicación cliente, usando el Protocolo de Transferencia de Archivos o *File Transfer Protocol* (FTP) que se encuentra ubicada en la capa de aplicación del modelo OSI.

PROTOCOLO TCP/IP

SEGÚN SUÁREZ Y OTROS (1998), EL PROTOCOLO DE CONTROL DE TRANSMISIÓN/PROTOCOLO DE INTERNET (TCP/IP) ES LA DENOMINACIÓN QUE RECIBE UNA FAMILIA DE PROTOCOLOS DISEÑADOS PARA LA INTERCONEXIÓN DE COMPUTADORAS, INDEPENDIENTEMENTE DE SU ARQUITECTURA Y EL SISTEMA OPERATIVO QUE EJECUTEN. SON UN ESTÁNDAR DE FACTO DEBIDO A LA EXPANSIÓN DE

INTERNET, LA RED QUE CONECTA MILLONES DE MÁQUINAS POR TODO EL MUNDO.

SIGUIENDO LA MISMA LÍNEA, TCP/IP ES UN CONJUNTO DE PROTOCOLOS DISEÑADO CON UNA ARQUITECTURA EN CAPAS. LAS CAPAS PERMITIERON A LOS DISEÑADORES DEL PROTOCOLO DIVIDIR EN MÓDULOS LAS TAREAS Y SERVICIOS QUE REALIZARÁ EL MISMO. EL DISEÑO TAMBIÉN ESPECIFICA LA MANERA EN QUE UN MODULO INTERACTÚA CON OTROS. LA ARQUITECTURA EN CAPAS DE LOS PROTOCOLOS ESTÁ DISEÑADA COMO UNA PILA EN LA QUE LOS PROTOCOLOS DE MÁS ALTO NIVEL INTERACTÚAN CON PROTOCOLOS DE NIVELES MÁS BAJOS.

EL MODELO DE TCP/IP ESTÁ FORMADO POR CUATRO CAPAS, SEGÚN MENCIONA, SUÁREZ Y OTROS (1998):

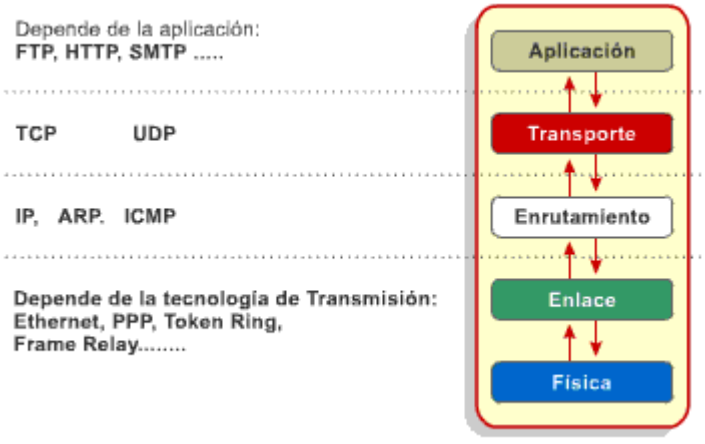

Figura 4. Diagrama en Bloques del Modelo TCP/IP

Fuente: http://www.newdevices.com/tutoriales/modelo-tcpip/2.html

- LA CAPA DE APLICACIÓN: ES LA CAPA MÁS ALTA DE LA PILA; ÉSTA PROVEE SERVICIOS DE ALTO NIVEL A LOS USUARIOS COMO TRANSFERENCIA DE ARCHIVOS, ENTREGA DE CORREO ELECTRÓNICO, Y ACCESO A TERMINALES REMOTOS. LOS PROGRAMAS DE APLICACIÓN ESCOGEN ENTRE DIFERENTES PROTOCOLOS DE TRANSPORTE DEPENDIENDO DEL TIPO DE SERVICIO DE TRANSPORTE QUE REQUIERAN. PARA EL TEMA EN ESTUDIO SE UTILIZARA FTP PARA PUBLICAR LA DIRECCIÓN IP DEL SERVIDOR PARA QUE LOS USUARIOS REMOTOS PUEDAN OBTENERLA CON LA IDEA DE ESTABLECER LA VPN DINÁMICA.
- LA CAPA DE TRANSPORTE TIENE SU PRINCIPAL FUNCIÓN EN PROVEER COMUNICACIÓN PUNTO A PUNTO ENTRE LAS APLICACIONES. LOS PROTOCOLOS DE TRANSPORTE (TCP Y UDP) USAN EL SERVICIO DE ENTREGA DE PAQUETES QUE PROVEE LA CAPA DE RED. SE UTILIZARA EL PROTOCOLO CONTROL DE TRASPORTE (TCP) PARA LA ENTREGA DE LOS PAQUETES EN ESTE PROYECTO.
- LA CAPA DE RED PROVEE EL SERVICIO DE ENTREGA DE PAQUETES DE UNA MÁQUINA A OTRA, POR MEDIO DEL PROTOCOLO DE INTERNET (IP). PARA EL TEMA EN ESTUDIO SE UTILIZARA EN ESTA CAPA EL PROTOCOLO

DE INTERNET O *INTERNET PROTOCOL* (IP) ES LLAMADO LA BASE TECNOLÓGICA DE TCP/IP QUE NOS SERVIRÁ PARA IDENTIFICAR EL SEGMENTO DE RED DE LOS EQUIPOS DE LAS SEDES REMOTAS CON EL SERVIDOR PRINCIPAL.

- LA CAPA DE ENLACE: ACEPTA DATAGRAMAS DE LA CAPA DE RED Y LOS ENVÍA FÍSICAMENTE. EL "MODULO" PARA EL ACCESO AL MEDIO ES CON FRECUENCIA UN CONTROLADOR DE DISPOSITIVO PARA UNA PIEZA PARTICULAR DE HARDWARE, Y LA "CAPA" DE ENLACE PUEDE CONSISTIR DE MÚLTIPLES MÓDULOS. PARA LA CREACIÓN DE LA DVPN SE UTILIZARA EN ESTA CAPA, EL PROTOCOLO DE TÚNEL DE CAPA DOS (L2TP) Y LA SEGURIDAD DE PROTOCOLOS INTERNET (IPSEC).

Tecnologías para Redes de Area Local

Red de Area Local (LAN)

Según Salvucci y otros (2003), una Red de Area Local (Lan) es un sistema de comunicación formado por un grupo de estaciones de trabajo o nodos, con capacidad de procesamiento local interconectados entre sí, para compartir recursos y transferir información entre ellos. Es importante mencionar que la red virtual privada virtual dinámica (DVPN) se probó únicamente para las tecnologías de red LAN Ethernet, a continuación se mencionan las tecnologías de redes LAN.

Tecnología de Red Lan Ethernet

Según Salvucci y otros (2003) la Norma o estándar (IEEE 802.3) que determina la forma en que las estaciones trabajo o nodos de la red envían y reciben datos sobre un medio físico compartido que se comporta como un bus lógico, independientemente de su configuración física. Originalmente fue diseñada para enviar datos a 10 Mbps, aunque posteriormente ha sido perfeccionado para trabajar a 100 Mbps, 1 Gbps o 10 Gbps y se habla de versiones futuras de 40 Gbps y 100 Gbps. Utiliza el protocolo de comunicaciones Acceso múltiple con detección de portadora y detección de colisiones o *Carrier Sense Multiple Access / Collision Detect* (CSMA/CD). Actualmente Ethernet es el estándar más utilizado en redes locales/LANs.

Tecnología de Red lan Token Ring

Según Salvucci y otros (2003) la red Token Ring es el segundo más usado después de la Ethernet. Fue desarrollado por IBM; y en términos generales su funcionamiento describe el siguiente comportamiento, es una red con topología en anillo y técnica de acceso de paso de testigo. Cumple el estándar IEEE 802.5.

Estas redes alcanzan una velocidad máxima de transmisión que oscila entre los 4 y los 16 Mbps.

Tecnología de Red Lan FDDI

Según Salvucci y otros (2003) la red internas de Datos Distribuida por Fibras o *Fiber distributed data interface* (FDDI) se define como una topología de red local en

doble anillo y con soporte físico de fibra óptica. Puede alcanzar velocidades de transmisión de hasta 100 Mbps y utiliza un método de acceso al medio basado en paso de testigo o *token passing*. Utiliza fibras multimodo y concentradores de cableado en topología física de estrella y lógica de doble anillo (anillo primario y anillo secundario). Es una red muy fiable gracias a la fibra y al doble anillo, sobre el que gira la información en direcciones opuestas.

Esta tecnología fue desarrollada a mediados de los años 80 cuando la tecnología ethernet y token ring no entregaban suficiente ancho de banda para aplicaciones.

FDDI, se compone de 4 especificaciones:

- Control de acceso al medio (Mac): Define la forma en que se accede al medio.
- Protocolo de capa física (PHY): Define los procedimientos de codificación o codificación.
- Medio de capa física (PMD): Define las características del medio de transmisión.
- Administración de estaciones (SMT): Define la configuración de la estación FDDI.

Topologías típicas en las redes LAN

Según Salvucci y otros (2003), la topología en las redes LAN es la disposición física en la que se conecta una red de computadoras. Las más comunes son:

- Anillo
- Árbol
- Malla
- Bus

- Estrella

Red de área amplia o Wide Area Network (WAN)

Según Wikipedia (2005), WAN es un acrónimo de red de área amplia o *Wide Area Network*. Un ejemplo de este tipo de redes sería la misma Internet o cualquier red en que no esté en un mismo edificio, localidad o sede. Opera en la capa física y de enlace del modelo de referencia OSI.

Debe señalarse que Muchas WAN son construidas por y para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de Internet o *Internet Service Provider* (ISP) para proveer de conexión a sus clientes.

En la construcción de la DVPN se utilizó Internet por ser pública estableciendo las conexiones de las sedes remotas con la sede principal a través de la tecnología de Línea de Abonado Digital Asimétrica o *Assymetric Digital Subscriber Line* (ADSL). A continuación se menciona la definición de Internet y de la tecnología ADSL.

Definición de Internet

Según Suárez y otros (1998), se puede definir como la red de redes, un grupo de redes que están conectadas físicamente, capaces de comunicarse y compartir datos y un conjunto de normas o protocolos de conexión entre computadoras, que engloba prácticamente la totalidad de las redes telefónicas del mundo entero, donde redes internacionales se muestran como si fueran pequeñas redes, permitiendo acceder y compartir información, gráficos, sonidos, texto, software, video, entre otros. Está basado en el protocolo TCP/IP.

Las computadoras y redes que forman parte de Internet deben estar de acuerdo, o sea hablar el mismo "idioma", o usar un intérprete. Este "lenguaje" es un software que permite que diferentes computadoras en distintas redes se puedan comunicar e intercambiar información.

Del mismo modo, una Intranet es un conjunto de contenido compartido por un grupo bien definido dentro de una organización y una Extranet es un conjunto de contenido compartido por un grupo bien definido, pero que atraviesa límites empresarios.

TECNOLOGÍA ADSL

SEGÚN CANTV.NET (2000), LA TECNOLOGÍA ADSL PERTENECE A UNA FAMILIA DE TECNOLOGÍAS CONOCIDAS COMO XDSL. LAS SIGLAS EN INGLÉS DE ADSL SIGNIFICAN ASSYMETRIC DIGITAL SUBSCRIBER LINE LO QUE EN ESPAÑOL VIENE A SER TRADUCIDO COMO LÍNEA DE ABONADO DIGITAL ASIMÉTRICA. EL ODJETIVO DE ASIMÉTRICO INDICA QUE LAS VELOCIDADES DE ENVÍO Y RECEPCIÓN DE INFORMACIÓN NO SON IDÉNTICAS. ADSL PERMITE COMPARTIR UNA PORCIÓN DEL RANGO DE FRECUENCIAS QUE PASA POR EL PAR DE COBRE TELEFÓNICO SIN INTERFERIR CON EL SERVICIO DE VOZ YA QUE LAS FRECUENCIAS UTILIZADAS SON DISTINTAS.

Podemos imaginar el par de cobre telefónico como una autopista de varios canales donde uno de ellos es utilizado para el viaje de voz, otro es utilizado para enviar datos y otro para la recepción. En el caso de los canales de datos el de recepción es mucho más grande que el de envío. Esto es así porque la tecnología ADSL fue pensada para el uso de Internet donde la cantidad de información recibida generalmente es mayor que la enviada.

La velocidad a la cual es enviada la información de datos es conocida como Upstream. Por el otro lado la velocidad de recepción es conocida como Dowstream. Ambas velocidades son medidas en Kbps (Kilobytes per second).

CLIENTE-SERVIDOR

Según Millán (2005), la arquitectura cliente-servidor llamado modelo cliente-servidor o servidor-cliente es una forma de dividir y especializar programas y equipos de cómputo a fin de que la tarea que cada uno de ellos realiza, se efectúe con la mayor eficiencia, y permita simplificar las actualizaciones y mantenimiento del sistema.

En esta arquitectura la capacidad de proceso está repartida entre el servidor y los clientes.

En la funcionalidad de un programa distribuido se pueden distinguir 3 capas o niveles:

- Manejador de Base de Datos (Nivel de almacenamiento)
- Procesador de aplicaciones o reglas del negocio (Nivel lógico) y
- Interface del usuario (Nivel de presentación)

En una arquitectura monolítica no hay distribución; los tres niveles tienen lugar en el mismo equipo.

En un comienzo, los mainframes concentraban la funcionalidad de almacenamiento y lógica y a ellos se conectaban terminales tontos, posiblemente ubicados en sitios remotos.

En el modelo cliente-servidor, en cambio, el trabajo se reparte entre dos computadores. De acuerdo con la distribución de la lógica de la aplicación hay dos posibilidades:

- Cliente delgado: si el cliente solo se hace cargo de la presentación.
- Cliente pesado: si el cliente asume también la lógica del negocio.

En la actualidad se suele hablar de arquitectura de tres niveles, donde la capa de almacenamiento y la de aplicación se ubican en (al menos) dos servidores diferentes, conocidos como servidores de datos y servidores de aplicaciones.

Ventajas de la arquitectura cliente-servidor

- El servidor no necesita tanta potencia de procesamiento, parte del proceso se reparte con los clientes.
- Se reduce el tráfico de red considerablemente. Idealmente, el cliente se conecta al servidor cuando es estrictamente necesario, obtiene los datos que necesita y cierra la conexión dejando la red libre.

Definiendo VPN

Según Carreon (2002), indicó que para minimizar los altos costos de interconexión de las empresas y en la búsqueda de obtener mayor seguridad, flexibilidad, implementación rápida y escalabilidad surgieron las Redes Privadas Virtuales, que solucionaron estos requerimientos.

Una definición simple es que se trata de una red de comunicaciones privada implementada sobre una infraestructura pública.

Sin embargo, la tecnología emergente de redes privadas virtuales se basa en los protocolos de Nivel 3 (Nivel de Red del modelo OSI), más específicamente en IP. Esta tecnología busca implementar redes de servicios privadas utilizando redes públicas o redes compartidas de IP, siendo la red publica mas conocida mundialmente es Internet.

Requerimientos Básicos de las VPN

De igual manera Carreon (2002) describió que implementando 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 auditoria 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.

Tipos de Redes Virtuales Privadas

Según Carreon (2002), las redes privadas virtuales se dividieron en 3 categorías de acuerdo con el servicio de conectividad que brinden, VPN de Acceso Remoto, VPN de Intranet y VPN de Extranet.

VPN de Acceso Remoto

Las VPN de Acceso Remoto o *Remote Acces VPNs*, proveen 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, sucursales remotas o *telecommuters*, 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.

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 características, extiende el modelo IP a través de la WAN compartida.

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.

Características:

- Extiende la conectividad a proveedores y clientes sobre una infraestructura compartida usando conexiones virtuales dedicadas.
- Los partners tienen diferentes niveles de autorización con listas de control de acceso o Access control lists, firewalls, filtros, según decida la empresa

Tecnología de las Redes Privadas Virtuales

Según Carreon (2002), la arquitectura de las VPN, se basaron en elementos esenciales de la tecnología, para proteger la privacidad, mantener la calidad, confiabilidad y asegurar la operatividad de la red en toda la empresa. Estos elementos son:

- **Seguridad:** uso de túneles, encriptación de datos, autenticación de usuarios y paquetes, control de acceso.
- **Calidad de Servicio:** uso de colas, manejo de congestión de red, priorización de tráfico, clasificación de paquetes.
- **Gestión:** implementación y mantenimiento de las políticas de seguridad y calidad de servicio a lo largo de la VPN.

Seguridad en las VPN

Un punto fundamental fue el particionamiento de las redes públicas o de uso compartido implementando las VPN que son disjuntas. Esto se logró mediante el uso de túneles que no son ni más ni menos que técnicas de encapsulado del tráfico. Las técnicas que se utilizan son: GRE, que permite que cualquier protocolo sea transportado entre dos puntos de la red encapsulado en otro protocolo, típicamente IP;

L2TP que permite el armado de túneles para las sesiones PPP remotas, y por último **IPSec** para la generación de túneles con autenticación y encriptado de datos.

Calidad de Servicio y Gestión en las VPN

La calidad de servicio permitió la asignación eficiente de los recursos de la red pública a las distintas VPN, obteniendo un performance predecible. A su vez, las VPN asignaron distintas políticas de calidad de servicio a sus usuarios, aplicaciones o servicios. Los componentes tecnológicos básicos fueron:

- **Clasificación de Paquetes:** asignación de prioridades a los paquetes basados en la política corporativa. Se pueden definir hasta siete clases de prioridades utilizando el campo de IP precedence dentro del encabezado del paquete IP.
- **Tarifa de Acceso Comprometida o *Committed Access Rate* (CAR):** garantiza un ancho de banda mínimo para aplicaciones o usuarios basándose en la política corporativa.
- **Formación de una cola de Espera o *Weighted Fair Queuing* (WFQ):** determina la velocidad de salida de los paquetes en base a la prioridad asignada a éstos, mediante el encolado de los paquetes.
- **Formación Aleatoria de Detección Anticipada o Weighted Random Early Detection (WRED):** complementa las funciones de TCP en la prevención y manejo de la congestión de la red, mediante el descarte de paquetes de baja prioridad.

Aspectos Básicos de Túneles en las VPN

Según Carreon (2002), al trabajar en un sistema de túnel, utilizando una infraestructura de la red para transferir datos de una red sobre otra; los datos que serán transferidos (o carga útil) pueden ser las tramas (o paquetes) de otro protocolo.

En lugar de enviar una trama a medida que es producida por el nodo promotor, el protocolo de túnel la encapsula en un encabezado adicional. Este proporciona

información de entubamiento de manera que la carga útil encapsulada pueda viajar a través de la red intermedia.

De esta manera, se pueden enrutar los paquetes encapsulados entre los puntos finales del túnel sobre la red (la trayectoria lógica a través de la que viajan los paquetes encapsulados en la red se denomina túnel). Cuando las tramas encapsuladas llegan a su destino sobre la red se desencapsulan y se envían a su destino final; nótese que este sistema de túnel incluye todo este proceso (encapsulamiento, transmisión y desencapsulamiento de paquetes).

De igual forma, existen muchos otros ejemplos de túneles que pueden realizarse sobre intranets corporativas. Y aunque la Red de redes, proporciona una de las intranets más penetrantes y económicas, las referencias a Internet en este artículo se pueden reemplazar por cualquier otra intranet pública o privada que actúe como de tránsito.

Según Carreon (2002), las tecnologías de túnel existen desde hace tiempo. Algunos ejemplos de tecnologías maduras incluyen:

- Túneles SNA sobre intranets IP. Cuando se envía tráfico de la Arquitectura de la red del sistema (SNA) a través de una intranet IP corporativa, la trama SNA se encapsula en un encabezado UPN Ej.: Túneles IPX para Novell NetWare, sobre intranets IP. Cuando un paquete IPX se envía a un servidor NetWare o ruteador IPX, el servidor o ruteador envuelve el paquete IPX en un encabezado UDP e IP y luego lo envía a través de una intranet IP.
- Protocolo de túnel de punto a punto (PPTP). Permite que se encripte el tráfico IP, IPX o NetBEUI, y luego se encapsule en un encabezado IP para enviarse a través de una red corporativa IP o una red pública IP, como Internet.
- Protocolo de túnel de nivel 2 (L2TP). Permite que se encripte el tráfico IP, IPX o NetBEUI, y luego se envíe sobre cualquier medio que dé soporte a la entrega de datagramas punto a punto, como IP, X.25, Frame Relay o ATM.

- Modo de túnel de seguridad IP (IPSec). Deja que se encripten las cargas útiles IP y luego se encapsulen en un encabezado IP, para enviarse a través de una red corporativa IP o una red pública IP como Internet.
- Formación de Trafico Genérico o ***Generic Traffic Shaping*** **(GTS),** reduce la velocidad de salida de los paquetes con el fin de reducir posibles congestiones de la red que tengan como consecuencia el descarte de paquetes.

Protocolos de Túneles

Según Carreon (2002), para que se establezca un túnel, tanto el cliente de éste como el servidor deberán utilizar el mismo protocolo de túnel. La tecnología de túnel se puede basar en el protocolo del túnel de Nivel 2 o e Nivel 3; estos niveles corresponden al Modelo de referencia de interconexión de sistemas abiertos (OSI).

Los protocolos de nivel 2 corresponden al nivel de Enlace de datos, y utilizan tramas como su unidad de intercambio. PPTP y L2TP y el envío de nivel 2 (L2F) son protocolos de túnel de Nivel 2, ambos encapsulan la carga útil en una trama de Protocolo de punto a punto (PPP) que se enviará a través de la red.

Los protocolos de Nivel 3 corresponden al nivel de la red y utilizan paquetes. IP sobre IP y el modo de túnel de seguridad IP (IPSec) son ejemplos de los protocolos de túnel de Nivel 3; éstos encapsulan los paquetes IP en un encabezado adicional antes de enviarlos a través de una red IP.

Funcionalidad de los Túneles en las Redes VPN

Según Carreon (2002), un túnel es similar a una sesión, tanto en las tecnologías de túnel de Nivel 2 como PPTP y L2TP; los dos puntos finales (Cliente/Servidor)

deben estar de acuerdo respecto al túnel, y negociar las variables de la configuración, como asignación de dirección o los parámetros de encriptación o de compresión. En la mayor parte de los casos, los datos que se transfieren a través del túnel se envían utilizando protocolos basados en datagramas (paquetes de información); se utiliza un protocolo para mantenimiento del túnel como el mecanismo para administrar al mismo.

Por lo general, las tecnologías del túnel de Nivel 3 suponen que se han manejado fuera de banda todos los temas relacionados con la configuración, normalmente a través de procesos manuales; sin embargo, quizás no exista una fase de mantenimiento de túnel. Para los protocolos de Nivel 2 (PPTP y L2TP) se debe crear, mantener y luego concluir un túnel.

Cuando se establece el túnel, es Posible enviar los datos a través del mismo. El cliente o el servidor utilizan un protocolo de transferencia de datos del túnel a fin de preparar los datos para su transferencia.

Por ejemplo, cuando el cliente del túnel envía una carga útil al servidor, primero adjunta un encabezado de protocolo de transferencia de datos de túnel a la carga útil. Luego, el cliente envía la carga útil encapsulada resultante a través de la red, la que lo enruta al servidor del túnel. Este último acepta los paquetes, elimina el encabezado del protocolo de transferencia de datos del túnel y envía la carga útil a la red objetivo. La información que se envía entre el servidor del túnel y el cliente del túnel se comporta de manera similar.

Los Protocolos y los Requerimientos básicos del Túnel

Según Carreon (2002), menciona que los protocolos de Nivel 2 (PPTP v L2TP) heredan un conjunto de funciones útiles, ya que se basan en protocolos PPP bien definidos. Como se señala adelante, estas funciones y sus contrapartes de Nivel 3 cubren los requerimientos básicos de la VPN.

- Autenticación de usuario. Los protocolos de túnel Nivel 2 heredan los esquemas de autenticación del usuario de PPP. Muchos de los esquemas

de túnel de Nivel 3 suponen que los puntos finales han sido bien conocidos (y autenticados) antes de que se estableciera el túnel. Una excepción es la negociación IPSec ISAKMP que proporciona una autenticación mutua de los puntos Finales del túnel. (Nótese que la mayor parte de las implementaciones IPSec dan soporte sólo a certificados basados en equipo, más que en certificados de usuarios; como resultado, cualquier usuario con acceso a uno de los equipos de punto final puede utilizar el túnel. Se puede eliminar esta debilidad potencial de seguridad cuando se conjunta el IPSec con un protocolo de Nivel 2, como el L2TP.)

- Soporte de tarjeta de señales. Al utilizar el Protocolo de autenticación ampliable (EAP), los protocolos de túnel Nivel 2 pueden ofrecer soporte a una amplia variedad de métodos de autenticación, incluidas contraseñas de una sola vez, calculadores criptográficos y tarjetas inteligentes. Los protocolos de túnel Nivel 3 pueden utilizar métodos similares; por ejemplo, IPSec define la Autenticación de los certificados de llaves públicas en su negociación ISAKMP/Oakley.
- Asignación de dirección dinámica**.** El túnel de Nivel 2 da soporte a la asignación dinámica de direcciones de clientes basadas en un mecanismo de negociación de protocolos de control de la red en general los esquemas del túnel de nivel 3 suponen que ya se ha asignado una dirección antes de la iniciación del túnel. Cabe mencionar que los esquemas para la asignación de direcciones en el modo de túnel IPSec están actualmente en desarrollo, por lo que aún no están disponibles.
- Compresión de datos. Los protocolos de túnel Nivel 2 proporcionan soporte a esquemas de compresión basados en PPP Por ejemplo, las implementaciones de Microsoft tanto de PPTP como L2TP utilizan Microsoft Point to Point Compression (MPPC). La IETF está investigando mecanismos similares (como la compresión IP) para los protocolos de túnel Nivel 3.

- Encriptación de datos**.** Los protocolos de túnel Nivel 2 dan soporte a mecanismos de encriptación de datos basados en PPP. Por su parte, la implementación de Microsoft de PPTP da soporte al uso opcional de Microsoft Point to Point Encription (MPPE), basado en el algoritmo RSA/RC4. Los protocolos de túnel Nivel 3 pueden utilizar métodos similares; por ejemplo, IPSec define varios métodos de Encriptación opcional de datos que se negocian durante el intercambio ISAKMP/Oaklev. La implementación de Microsoft del protocolo L2TP utiliza la encriptación IPSec para proteger el flujo de datos del cliente al servidor del túnel.
- Administración de llaves. MPPE, un protocolo de Nivel 2, se basa en las claves iniciales generadas durante la Autenticación del usuario y luego las renueva en forma periódica. IPSec negocia explícitamente una llave común durante el intercambio ISAKMP y también las renueva de manera periódica.
- Soporte de protocolo múltiple. El sistema de túnel de Nivel 2 da soporte a protocolos múltiples de carga útil, lo que facilita a los clientes de túnel tener acceso a sus redes corporativas utilizando IP, IPX, NetBEUI, entre otros.

En contraste, los protocolos de túnel Nivel 3, como el modo de túnel IPSec, por lo común dan soporte sólo a redes objetivo que utilizan el protocolo IP.

Tipos de Túneles

Según Carreon (2002), se pueden crear túneles en diferentes formas. Túneles voluntarios: Una computadora de usuario o de cliente puede emitir una solicitud VPN para configurar y crear un túnel voluntario. En este caso, la computadora del usuario es un punto terminal del túnel y actúa como un cliente de éste.

Túneles obligatorios: Un servidor de acceso de marcación capaz de soportar una VPN configura y crea un túnel obligatorio. Con uno de éstos, la computadora del

usuario deja de ser un punto termina¡ de¡ túnel. Otro dispositivo, el servidor de acceso remoto, entre la computadora de¡ usuario y el servidor del túnel, es el punto terminal del túnel y actúa como el cliente del mismo.

A la fecha, los túneles voluntarios han probado ser el tipo más popular de túnel. Las siguientes secciones describen cada uno de estos tipos con mayor detalle.

Túneles Voluntarios

Un túnel voluntario ocurre cuando, una estación de trabajo o un servidor de entubamiento utilizan el software del cliente del túnel, a fin de crear una conexión virtual al servidor del túnel objetivo; para lograr esto se debe instalar el protocolo apropiado de túnel en la computadora cliente. Para los protocolos que se analizan en este artículo, los túneles voluntarios requieren una conexión IP (ya sea a través de una LAN o marcación).

En determinadas situaciones, el cliente debe establecer una conexión de marcación con el objeto de conectarse a la red antes de que el cliente pueda establecer un túnel (éste es el caso más común). Un buen ejemplo es el usuario de Internet por marcación, que debe marcar a un ISP y obtener una conexión a Internet antes de que se pueda crear un túnel sobre Internet.

Para una PC conectada a una LAN, el cliente ya tiene una conexión a la red que le puede proporcionar un entubamiento a las cargas útiles encapsuladas al servidor del túnel LAN elegido. Este sería el caso para un cliente en una LAN corporativa, que inicia, un túnel para alcanzar una subred privada u oculta en la misma LAN (como sería el caso de la red de Recursos Humanos).

Es falso que las VPN requieran una conexión de marcación, pues sólo requieren de una red IP. Algunos clientes (como las PC del hogar) utilizan conexiones de marcación 1 Internet para establecer transporte IP; esto es un paso preliminar en la preparación para la creación de un túnel, y no es parte del protocolo del túnel mismo.

Túneles Obligatorios

Diversos proveedores que venden servidores de acceso de marcación han implementado la capacidad para crear un túnel en nombre del cliente de marcación. La computadora o el dispositivo de red que proporciona el túnel para la computadora del cliente es conocida de varias maneras: Procesador frontal (FEP) en PPTP, un Concentrador de acceso a L2TP (LAC) en L2TP o un gateway de seguridad IP en el IPSec. En este artículo, el término FEP se utilizará para describir esta funcionalidad, sin importar el protocolo de túnel.

Para realizar esta función, el FEP deberá tener instalado el protocolo apropiado de túnel y ser capaz de establecer el túnel cuando se conecte la computadora cliente.

En el ejemplo de Internet, la computadora cliente coloca una llamada de marcación al NAS activado por los túneles en el ISP; puede darse el caso de que una empresa haya contratado un ISP para instalar un conjunto nacional de FEP.

Esta configuración se conoce como "túnel obligatorio" debido a que el cliente está obligado a utilizar el túnel creado por FER Cuando se realiza la conexión inicial, todo el tráfico de la red de y hacia el cliente se envía automáticamente a través del túnel.

En los túneles obligatorios, la computadora cliente realiza una conexión única PPP, y cuando un cliente marca en el NAS se crea un túnel y todo el tráfico se enruta de manera automática a través de éste. Es posible configurar un FEP para hacer un túnel a todos los clientes de marcación hacia un servidor específico del túnel. De manera alterna, el FEP podría hacer túneles individuales de los clientes basados en el nombre o destino del usuario.

A diferencia de los túneles por separado creados para cada cliente voluntario, un túnel entre el FEP y servidor puede estar compartido entre varios clientes de marcación. Cuando un segundo cliente marca al servidor de acceso (FEP) a fin de alcanzar un destino no hay necesidad de crear una nueva instancia del túnel entre el FEP y el servidor del túnel.

Sistema de Variables

Una hipótesis bien formulada debe contener elementos o términos que fueron observables, y en consecuencia, sujetos a medición (Besarón y otros 2000). Por consiguiente, en una comunicación cliente/servidor, sobre la cual se crea una DVPN, se necesita que los procesos clientes se comuniquen con un proceso servidor. Sobre esta base se puede establecer un túnel de comunicación que involucre la publicación de una dirección IP en el proceso servidor y la captura de dicha IP por el proceso cliente. Por tanto, para crear una VPN que involucre IP dinámicas es necesario poder controlar esas direcciones IP tanto en el cliente como en el Servidor.

Con base a esta definición se propusieron para este estudio la hipótesis nula y su hipótesis alternativa.

HO: Las direcciones IP dinámicas no se pueden controlar por lo tanto no se pueden crear DVPN entre Cliente/Servidor con direcciones IP dinámicas.

H1: Las direcciones IP dinámicas se pueden controlar y por lo tanto se pueden crear DVPN entre Cliente/Servidor con direcciones IP dinámicas.

Sobre las hipótesis planteadas se desprendieron las variables independientes y dependientes, como se muestran en la Tabla 1. Las variables independientes, estuvieron formadas por: el sistema automatizado cliente/servidor y el servidor de alojamiento (Hosting) conformado por el proceso cliente, que corre bajo el sistema Operativo Windows en las

localidades remotas de cada usuario, permitiendo la captura de la dirección IP publicada en el servidor de alojamiento (hosting) y estableciendo la conexión con el servidor principal a través del enlace banda ancha ADSL y el proceso servidor que presta los servicios en la localidad principal, obteniendo la dirección IP del servidor en la sede principal y posteriormente a través del protocolo de transferencia de archivo (FTP) permitió publicar la dirección IP al servidor de hospedaje o servidor hosting de CANTV.net, que prestó el servicio de alojamiento de la dirección IP.

Por otra parte, la variable dependiente fue la red virtual privada dinámica (DVPN) creada entre los clientes y el servidor con el control de las direcciones IP dinámicas, en vista de que existe una relación causa efecto entre éstas. Diseñar un sistema cliente servidor bajo una DVPN trae como consecuencia controlar las direcciones IP dinámicas para poder establecer una DVPN.

Para definir los indicadores de estas variables, se comenzó por una definición conceptual que permitió entender la variable dependiente DVPN. La variable dependiente (DVPN) es la capacidad de crear una red privada virtual con direccionamiento IP dinámico en una conexión remota. Considerando lo antes planteado, los indicadores de la variable dependiente fueron las diferentes conexiones DVPN que se establecieron entre clientes remotos que usaron sistemas operativos Windows y el Servidor que uso igualmente sistema operativo Windows 2000 Server.

Tabla 1. Operacionalización de las Variables

Variable Independiente	Dimensiones	Indicadores
Aplicación Cliente	Sistema o agente local en el cliente para capturar la IP	Conexión
Aplicación Servidor	Sistema o agente local en el servidor para publicar la IP	Conexión
Servidor de Alojamiento (Hosting)	Servidor publico donde se almacena la dirección IP	Capacidad de Alojamiento
Variable Dependiente	**Dimensiones**	**Indicadores**
DVPN	Conexión DVPN	Conexión DVPN entre procesos clientes y procesos servidor

CAPÍTULO III

MARCO METODOLÓGICO

Tipo de Investigación

El trabajo de grado se enmarcó en función de los objetivos planteados en una investigación de campo bajo la modalidad de proyecto especial. En donde textualmente el Manual de la Universidad Centroccidental Lisandro Alvarado (2002) define esta investigación de la siguiente manera:

> se entenderá por investigación de campo a la aplicación del método científico en el tratamiento de un sistema de variables y sus relaciones, las cuales conducen a conclusiones y al enriquecimiento de un campo del conocimiento o disciplina inherente a la especialidad, con la sustentación de los experimentos y observaciones realizadas. (p.4).

Según el manual de la UPEL (2002) el trabajo se encontró en la modalidad de proyecto especial, ya que se enmarcó en una de las categorías señaladas, a continuación se cita textualmente:

> trabajos que lleven a creaciones tangibles, susceptibles de ser utilizadas como soluciones a problemas demostrados o que respondan a necesidades de intereses de tipo cultural. Se incluyen en esta categoría los trabajos de elaboración de libros de textos y de materiales de apoyo educativo, el desarrollo de software, prototipos y de productos tecnológicos en general…. (p.8).

En tal sentido, en esta investigación se pretendió proponer un diseño de software cliente/servidor que permitió crear redes virtuales privadas dinámicas sobre banda ancha ADSL en la empresa G&T Sistemas.

Población y Muestra

Según Tamayo (1998), una población está determinada por sus características definitorias. Por lo tanto, el conjunto de elementos que posea esta característica se denomina *población* o *universo*. Población es la totalidad del fenómeno a estudiar, donde las unidades de población poseen una característica común, la que se estudia y da origen a los datos de la investigación.

De acuerdo a esto, una población es el conjunto de todas las cosas que concuerdan con una serie determinada de especificaciones. Un censo, por ejemplo, es el recuento de todos los elementos de una población.

Para la realización de este estudio se tomaron como población o universo a setenta y Ocho (78) empresas, de las cuales setenta y siete (77) representaron el universo de las localidades remotas, estando distribuidas por estado de la siguiente manera: treinta y siete empresas (37) en el estado Lara, veinticuatro (24) en el estado Falcón y dieciséis (16) en el estado Portuguesa, estando la localidad principal (G&T Sistemas) ubicada en el estado Lara.

Tabla 2. Población de la Investigación.

N.-	Nombre de la Empresa	Conexión a Internet	Estado
1	DIGINET, C.A.	Dial Up	Falcón
2	C.D.C. PUNTO FIJO, C.A.	Dial Up	Falcón
3	TELECOMUNICACIONES LA MONTAÑA, C.A.	Frame Relay	Falcón
4	INVERSIONES DON JOSE GLOBAL COMUNICATION, C.A.	Frame Relay	Falcón
5	CORPORACION GEOSATELITAL, C.A.	ADSL	Falcón
6	INVERSIONES G & J, C.A.	Frame Relay	Falcón
7	REPRESENTACIONES SOUSA-PINTO, C.A.	ADSL	Falcón
8	AZAP, BUSINESS.COM, C.A.	ADSL	Falcón
9	CORPORACION DIGITAL SERVICE, C.A.	ADSL	Falcón
10	TWIN TELECOM, C.A.	Frame Relay	Falcón
11	COMERCIAL OMAR, C.A.	ADSL	Falcón
12	ALIATEL, C.A.	Frame Relay	Falcón
13	INSABASA, S.A.	Dial Up	Falcón
14	DROGUERIA FARMACOS PARAGUANA, C.A.	ADSL	Falcón
15	INVERSIONES JUDINECA, C.A.	ADSL	Falcón
16	DITHOMP CONEXIÓN, C.A.	ADSL	Falcón
17	EXTINFAL, C.A.	ADSL	Falcón

18	TWIN TELECOM, C.A.	ADSL	Falcón
19	TU COMUNICACIÓN, C.A.	ADSL	Falcón
20	INVERSIONES UNIVERSITARIAS FALCONIANAS, C.A.	ADSL	Falcón
21	INVERSIONES GOMA, C.A.	ADSL	Falcón
22	DATA COMP SERVICIOS, S.A.	ADSL	Falcón
23	BODEGÓN Y LICORERÍA COCUY, C.A	ADSL	Falcón
24	CONSORCIO D & C, C.A.	ADSL	Falcón
25	D & S TELECOMUNICACIONES, C.A.	Frame Relay	Lara
26	GRUPO MIDAS, C.A.	ADSL	Lara
27	ALO.NET, C.A.	Dial Up	Lara
28	CONSTRUCTORA CUATRO ENE, C.A.	Frame Relay	Lara
29	WELCOME.COM, C.A.	Frame Relay	Lara
30	INVERSIONES ZZ, C.A.	ADSL	Lara
31	ON LINE.COM, C.A.	ADSL	Lara
32	TOTAL CONSULTING 2000, C.A.	ADSL	Lara
33	TEL. C. SERVI, C.A.	Frame Relay	Lara
34	GRUPO MIDAS, C.A.	Frame Relay	Lara
35	TITEL C.A.	Frame Relay	Lara
36	N.G.C. TELECOMUNICACIONES, C.A.	Frame Relay	Lara
37	H.R. COMUNICACIONES, C.A.	Frame Relay	Lara
38	ADMINISTRADORA C.A. LARA YARACUY	Frame Relay	Lara
39	AGH INVERSIONES C.A.	ADSL	Lara
40	FONO-TEL C.A.	Dial Up	Lara
41	MAGNACIM, C.A.	Frame Relay	Lara
42	ELECTRONICA Y SONIDO ELECTRO-SONI, C.A.	Frame Relay	Lara
43	ELECTRONICA Y SONIDO ELECTRO-SONI, C.A.	Frame Relay	Lara
44	SERVICIOS SAN JOSE, C.A.	Frame Relay	Lara
45	INVERSIONES EMI.NET, C.A. (Transporte Carlos López, C,A.)	Frame Relay	Lara
46	SERVICIOS SAN JOSE, C.A.	Frame Relay	Lara
47	RODA.COM, C.A.	Frame Relay	Lara
48	A.T.J. TELECOMUNICACIONES, C.A.	Frame Relay	Lara
49	INVERSIONES EXITOS S.G., C.A.	Frame Relay	Lara
50	ALO.NET, C.A.	Frame	Lara

		Relay	
51	VIKINGO 2002, C.A.	Frame Relay	Lara
52	INVERSIONES ROCKEFELLER, C.A.	Frame Relay	Lara
53	ELECTRONICA Y SONIDO ELECTRO SONI, C.A.	Frame Relay	Lara
54	INVERSIONES HMV, C.A.	ADSL	Lara
55	ABC TELECOMUNICACIONES, C.A	ADSL	Lara
56	CENTRO DE COMUNICACIONES BABILON	Dial Up	Lara
57	INVERSIONES P.L.B. COMUNICACIONES, C.A.	No tiene	Lara
58	CENTRO DE COMUNICACIONES LAS TRINITARIAS	No tiene	Lara
59	CENTRO DE COMUNICACIONES FAETON	No tiene	Lara
60	COMPUSERVER, C.A.	No tiene	Lara
61	TERRITORIO DIGITAL, C.A.	ADSL	Lara
62	RUIZ COMUNICACIONES & SISTEMAS, C.A.	ADSL	Portuguesa
63	INVERSIONES COMFAXTEL, C.A.	Frame Relay	Portuguesa
64	TELUN, C.A.	ADSL	Portuguesa
65	COMSA, COMUNICACIONES, S.A.	Frame Relay	Portuguesa
66	REPRESENTACIONES M&R, C.A.	Frame Relay	Portuguesa
67	TELECOMUNICACIONES TUREN, C.A.	Frame Relay	Portuguesa
68	DURAN COMUNICACIONES (DUCOCA), C.A.	Dial Up	Portuguesa
69	COMUNICACIONES INTEGRALES J & S, C.A	ADSL	Portuguesa
70	TELECOM LA FUENTE, C.A.	ADSL	Portuguesa
71	MARLA, C.A.	ADSL	Portuguesa
72	INVERSIONES COLLECORVINO, C.A.	ADSL	Portuguesa
73	MUNDO MOVIL, C.A	ADSL	Portuguesa
74	ASTUR SERV, C.A.	ADSL	Portuguesa
75	CENTRO DE COMUNICACIONES NASSER, C.A	ADSL	Portuguesa
76	INVERSIONES TELCOM, C.A.	Dial Up	Portuguesa
77	MICROTEC, C.A.	ADSL	Portuguesa

Según Tamayo (1998), cuando se seleccionan algunos elementos con la intención de averiguar algo sobre una población determinada, se hace referencia a este grupo de elementos como *muestra*.

Para la investigación se seleccionó una muestra no probabilística, que es aquella en la cual el investigador procede a seleccionar la muestra en forma convencional, sin considerar el error muestral que pueda existir; las muestras no probabilísticas mas utilizadas son las llamadas intencionales u opináticas, por cuotas y accidentales.

Para el desarrollo de la investigación se seleccionó una muestra de tipo intencional opinática, que exige un conocimiento de la población a estudiar.

El investigador seleccionó como muestra a las empresas que cumplieron con dos condiciones fundamentales, 1) Que las empresas poseyeran conexiones a Internet vía Dial-up y 2) Que las empresas tuvieran conexiones a Internet vía ADSL, el hecho de tener conexión Dial-up fue tema de estudio en los objetivos específicos de la investigación e igualmente que la conexión ADSL, por ser la tecnología que se escogió para poder establecer la DVPN con la localidad principal (G&T Sistemas).

De acuerdo a lo antes señalado, la muestra del presente estudio estuvo constituida en cuarenta y tres (43) empresas, de las cuales cuarenta y dos (42) correspondieron a las localidades remotas, distribuidas por estado de la siguiente manera: diecinueve (19) en Falcón, once (11) en Lara y doce (12) en Portuguesa, estando la localidad principal (G&T Sistemas) ubicada en el estado Lara.

Tabla 3. Muestra de la Investigación.

N.-	Nombre de la Empresa	Conexión a Internet	Estado
1	DIGINET, C.A.	Dial Up	Falcón
2	C.D.C. PUNTO FIJO, C.A.	Dial Up	Falcón
3	CORPORACION GEOSATELITAL, C.A.	ADSL	Falcón
4	REPRESENTACIONES SOUSA-PINTO, C.A.	ADSL	Falcón
5	AZAP, BUSINESS.COM, C.A.	ADSL	Falcón
6	CORPORACION DIGITAL SERVICE, C.A.	ADSL	Falcón
7	COMERCIAL OMAR, C.A.	ADSL	Falcón
8	INSABASA, S.A.	Dial Up	Falcón
9	DROGUERIA FARMACOS PARAGUANA, C.A.	ADSL	Falcón
10	INVERSIONES JUDINECA, C.A.	ADSL	Falcón
11	DITHOMP CONEXIÓN, C.A.	ADSL	Falcón
12	EXTINFAL, C.A.	ADSL	Falcón
13	TWIN TELECOM, C.A.	ADSL	Falcón
14	TU COMUNICACIÓN, C.A.	ADSL	Falcón
15	INVERSIONES UNIVERSITARIAS FALCONIANAS, C.A.	ADSL	Falcón
16	INVERSIONES GOMA, C.A.	ADSL	Falcón
17	DATA COMP SERVICIOS, S.A.	ADSL	Falcón
18	BODEGÓN Y LICORERÍA COCUY, C.A	ADSL	Falcón
19	CONSORCIO D & C, C.A.	ADSL	Falcón
20	GRUPO MIDAS, C.A.	ADSL	Lara
21	ALO.NET, C.A.	Dial Up	Lara
22	INVERSIONES ZZ, C.A.	ADSL	Lara
23	ON LINE.COM, C.A.	ADSL	Lara
24	TOTAL CONSULTING 2000, C.A.	ADSL	Lara
25	AGH INVERSIONES C.A.	ADSL	Lara

26	FONO-TEL C.A.	Dial Up	Lara
27	INVERSIONES HMV, C.A.	ADSL	Lara
28	ABC TELECOMUNICACIONES, C.A	ADSL	Lara
29	CENTRO DE COMUNICACIONES BABILON	Dial Up	Lara
30	TERRITORIO DIGITAL, C.A.	ADSL	Lara
31	RUIZ COMUNICACIONES & SISTEMAS, C.A.	ADSL	Portuguesa
32	TELUN, C.A.	ADSL	Portuguesa
33	DURAN COMUNICACIONES (DUCOCA), C.A.	Dial Up	Portuguesa
34	COMUNICACIONES INTEGRALES J & S, C.A	ADSL	Portuguesa
35	TELECOM LA FUENTE, C.A.	ADSL	Portuguesa
36	MARLA, C.A.	ADSL	Portuguesa
37	INVERSIONES COLLECORVINO, C.A.	ADSL	Portuguesa
38	MUNDO MOVIL, C.A	ADSL	Portuguesa
39	ASTUR SERV, C.A.	ADSL	Portuguesa
40	CENTRO DE COMUNICACIONES NASSER, C.A	ADSL	Portuguesa
41	INVERSIONES TELCOM, C.A.	Dial Up	Portuguesa
42	MICROTEC, C.A.	ADSL	Portuguesa

PROCEDIMIENTO

La investigación se desarrolló en un periodo de seis meses siguiendo las seis (6) fases indicadas a continuación:

Fase 1. Diagnóstica

Esta fase tuvo como finalidad diagnosticar los problemas de soporte técnicos entre las localidades remotas (Lara, Falcón y Portuguesa) con la localidad principal de la empresa G&T Sistema y la necesidad de proveer una herramienta que permita establecer una red virtual privada dinámica con la empresa G&T Sistema en línea,

dicha información se recolectó, a través de un cuestionario con preguntas cerradas, aplicado mediante una entrevista a los representantes de las localidades remotas y en lo referido a la localidad principal se aplicó un cuestionario dirigido al representante del departamento de informática de la empresa G&T Sistemas para recabar la información necesaria.

La validez de estos instrumentos (Cuestionarios) se realizaron a través del juicio de expertos quienes determinaron la relación que existe entre el objetivo del estudio, las variables, las dimensiones, los indicadores y los ítems que contiene el instrumento.

Todos los documentos y formularios requeridos para recabar información pertinaz y oportuna para una mayor comprensión y fluidez del presente estudio, tuvieron la debida aprobación y validación por parte de los profesores involucrados en el proyecto, quienes fueron: ingenieros Arsenio Pérez, profesor en el área de Teleproceso, el profesor Jesús León Subero, docente de Metodología de la Investigación adscrito al Decanato de Ingeniería Civil y Rey González como Gerente de sistemas de la empresa G&T Sistemas.

Estos expertos evaluaron los cuestionarios de la siguiente forma: Se les entregó una carpeta a cada uno con el siguiente contenido: (a) una hoja de solicitud de validación (ver Anexo C), (b) dos ejemplares preliminares de los cuestionarios (ver Anexo A y B) y (c) un formato para la evaluación de la pertinencia, claridad y congruencia de cada ítem en relación al objetivo definido. Para opinar sobre dichos aspectos los expertos podrán seleccionar en los recuadros Si ó No, además de escribir sus observaciones, opiniones y sugerencias para cada ítem y para el instrumento en general (ver Anexo E y F)

Fase 2. Documentación Bibliográfica

Como apoyo bibliográfico del presente estudio, se elaboraron los antecedentes basados en diferentes investigaciones relacionadas con el tema tratado, estas fuentes han permitido sustentar científicamente los conceptos, opiniones y esquemas generales, obteniendo así, una mejor comprensión de los objetivos plasmados en este trabajo.

Fase 3. Recolección de la Información

Se aplicó un cuestionario de seis interrogantes (6) que contestaron los usuarios de las localidades remotas (Lara, Falcón y Portuguesa) mediante el formulario (ver Anexo A). Igualmente, se aplicó un cuestionario de ocho preguntas (8) que contestó, el representante de la localidad principal (G&T Sistemas) mediante formulario (ver Anexo B).

Fase 4. Procesamiento y Análisis de resultados

Una vez que se procedió a administrar el instrumento, se analizó y tabuló con base a técnicas de análisis estadísticos o de asignación de porcentajes simples de acuerdo a las tendencias presentes en las respuestas que otorgaron los entrevistados. La presentación de los resultados se reforzó con cuadros y gráficos.

Fase 5. Elaboración del modelo

De acuerdo al resultado obtenido mediante el debido análisis de la información procesada, se construyó el modelo cliente/servidor y se procedió a la elaboración del software cliente y el software servidor, igualmente se realizaron las pruebas de publicación y captura de direcciones IP con el servidor de hospedaje de CANTV.net, y se realizaron pruebas de conexión enviando mensajes entre el servidor y el cliente.

Fase 6. Elaboración de Conclusiones y Recomendaciones

Con base al análisis y la elaboración del modelo, se presentaron las conclusiones de la investigación, donde se plantearon los aportes del trabajo y las recomendaciones para investigaciones futuras.

CAPÍTULO IV

ANÁLISIS DE LOS RESULTADOS Y ELABORACIÓN DEL MODELO CLIENTE/SERVIDOR

Análisis de la Encuesta

El análisis de los resultados fue una etapa decisiva en el proceso de la investigación, por cuanto es un paso previo que permitió interpretar los datos obtenidos y soportarlos con los conocimientos teóricos que fundamentaron el estudio.

El diagnóstico que sustentó la propuesta, se basó en el análisis cuantitativo de la data recolectada donde se expuso a través de gráficos los resultados de las respuestas obtenidas en cada ítem y se reforzó con el análisis cualitativo fundamentado en la experiencia profesional del autor y sus habilidades como investigador. Esta etapa de análisis de las encuestas dio respuesta a los dos (2) primeros objetivos específicos de la investigación, que fueron:

4. Diagnosticar la necesidad de una interconexión de red a través de Internet a los clientes de la empresa G&T Sistemas, con la implantación de DVPN en Lara, Falcón y Portuguesa.
5. Determinar la factibilidad técnica para la implementación de una conexión DVPN a los clientes que se conectan telefónicamente con la empresa G&T Sistemas.

A continuación se presentan los resultados obtenidos para cada uno de los ítems de la encuesta realizada en forma tabular y su gráfico asociado.

Ítem N.- 1. ¿Ha tenido lentitud o retardo con las actualizaciones de las aplicaciones que usted adquirió con la empresa G&T Sistemas?

En la tabla 4 y el gráfico 1 se muestran los resultados obtenidos para este ítem.

Tabla 4. Diagnosticar los problemas o inconvenientes presentes en las Actualizaciones.

1. ¿Ha tenido lentitud o retardo con las actualizaciones de las aplicaciones que usted adquirió con la empresa G&T Sistemas?	Estado	Conexión a Internet	Total	%
Frecuentemente	Falcón	ADSL	15	36
		Dial Up	3	7
	Total Falcón		**18**	**43**
	Lara	ADSL	7	17
		Dial Up	3	7
	Total Lara		**10**	**24**
	Portuguesa	ADSL	9	21
		Dial Up	2	5
	Total Portuguesa		**11**	**26**
Total Frecuentemente			**39**	**93**
Muy Poco	Falcón	ADSL	1	2
	Total Falcón		**1**	**2**
	Lara	ADSL	1	2
	Total Lara		**1**	**2**
	Portuguesa	ADSL	1	2
	Total Portuguesa		**1**	**2**
Total Muy Poco			**3**	**7**
Total general			**42**	**100**

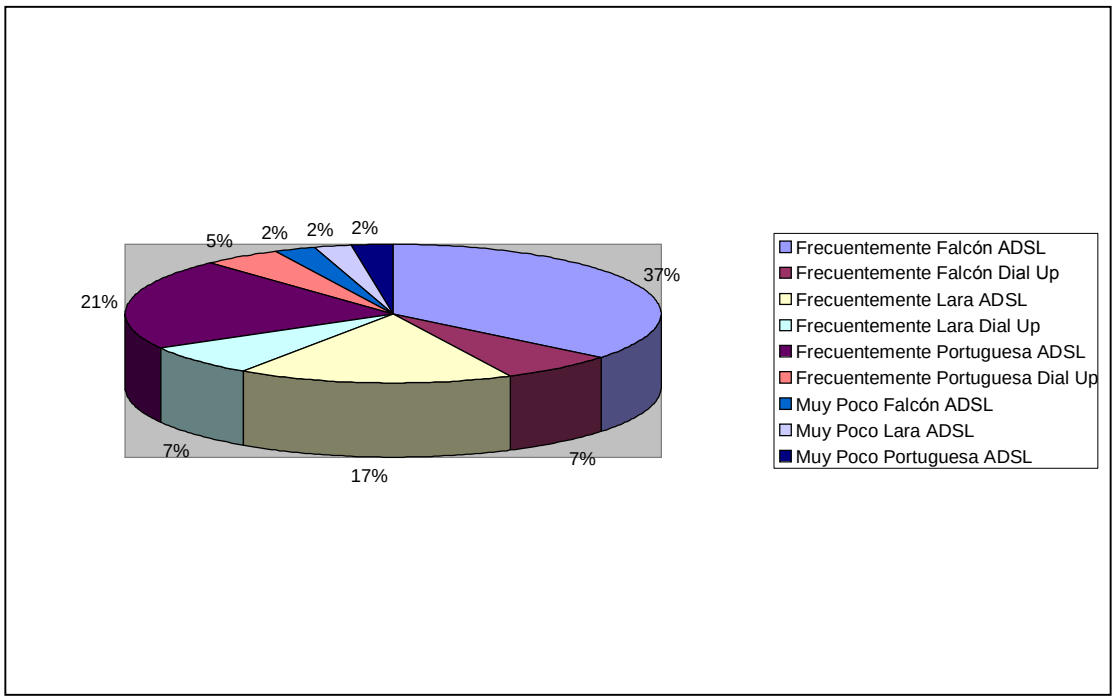

Gráfico No. 1: Distribución Porcentual de Fallas Presentes en las Actualizaciones de las Aplicaciones Clientes.

De acuerdo a este resultado, como se muestra en la tabla 4, se puede inferir que actualmente la forma en que la empresa G&T Sistemas esta realizando las actualizaciones, es decir, trasladando personal al sitio para realizar las mismas o efectuando asistencia remota, vía Dial-up, donde se permite una sola conexión simultánea por cliente, por la limitante que tiene el RAS de una sola tarjeta FAX-MODEM, demuestra que no está llenando las expectativas de sus clientes, ya que, solamente 3 empresas indicaron que muy poco tienen problemas con las actualizaciones y esto corresponde a un 7 % de la muestra.

Es importante acotar que el 74% de las empresas con conexión ADSL contestaron que frecuentemente tuvieron problemas de retardo y solamente 3 con conexión ADSL contestaron que muy poco presentaron problemas como lo indica el gráfico 1, esto nos da la idea, que sería interesante utilizar la banda ancha de estos clientes, para efectuar las actualizaciones o soportes de aplicaciones que actualmente no se realizan por esta vía.

Ítem N.- 2. ¿Los soportes a las aplicaciones que usted adquirió con la empresa G&T como los califica?

En la tabla 5 y el gráfico 2 se muestran los resultados obtenidos para este ítem.

Tabla 5. Diagnosticar la Calificación de los Soportes.

2. ¿Los soportes a las aplicaciones que usted adquirió con la empresa G&T como los califica?	Estado	Total	%
Bueno	Falcón	2	5
	Lara	2	5
	Portuguesa	1	2
Total Bueno		**5**	**12**
Excelente	Falcón	1	2
	Portuguesa	1	2
Total Excelente		**2**	**4**
Malo	Falcón	5	12
	Lara	5	12
	Portuguesa	4	10
Total Malo		**14**	**34**
Regular	Falcón	11	26
	Lara	4	10
	Portuguesa	6	14
Total Regular		**21**	**50**
Total general		**42**	**100**

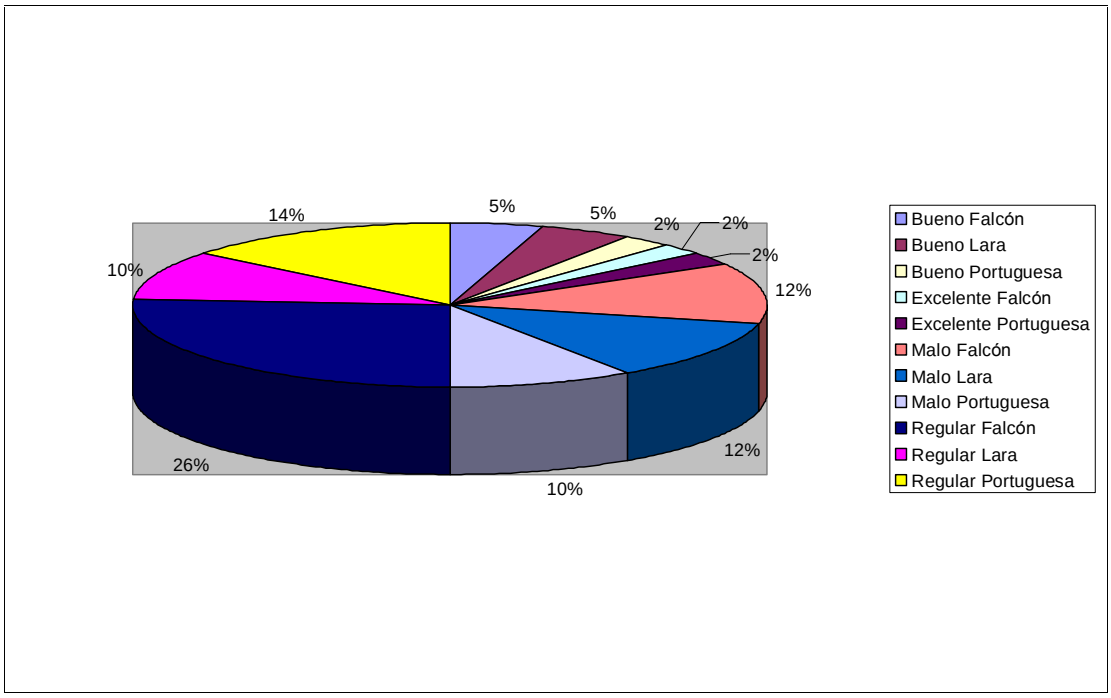

Gráfico No. 2: Distribución Porcentual de la Aplicación de los Soportes.

Con base a los resultados de la tabla 5, el 84 % de la muestra seleccionada opinó que el soporte que esta brindando la empresa G&T Sistemas a sus aplicaciones requiere cambios, ya que, lo califican mayoritariamente entre dos opciones: Regular y Malo. Apoyándonos en el gráfico 2, el 50 % de las empresas opinaron que el soporte es regular y un 34 % lo clasifican como malo. Esta percepción la consideran porque la asistencia telefónica es limitada por la capacidad de atender a un cliente a la vez y al no poder solventar por teléfono la falla debe trasladar personal al sitio para solucionar el problema, trayendo como consecuencia retardos en las soportes por no contar con una conexión en línea que permita optimizar las funciones de soporte.

Ítem N.- 3. ¿Desea conectarse en Línea con G&T para mejorar la calidad del servicio?

En la tabla 6 y en el gráfico 3 se presentan los resultados obtenidos para este ítem.

Tabla 6. Diagnosticar la Demanda de las Empresas que Desean Conectarse en Línea con la Empresa G&T Sistemas.

3. ¿Desea conectarse en Línea con G&T para mejorar la calidad del servicio?	Conexión a Internet	Estado	Total	%
NO	ADSL	Falcón	1	2
		Lara	1	2
		Portuguesa	1	2
	Total ADSL		**3**	**7**
Total NO			**3**	**7**
SI	ADSL	Falcón	15	36
		Lara	7	17
		Portuguesa	9	21
	Total ADSL		**31**	**74**
	Dial Up	Falcón	3	7
		Lara	3	7
		Portuguesa	2	5
	Total Dial Up		**8**	**19**
Total SI			**39**	**93**
Total general			**42**	**100**

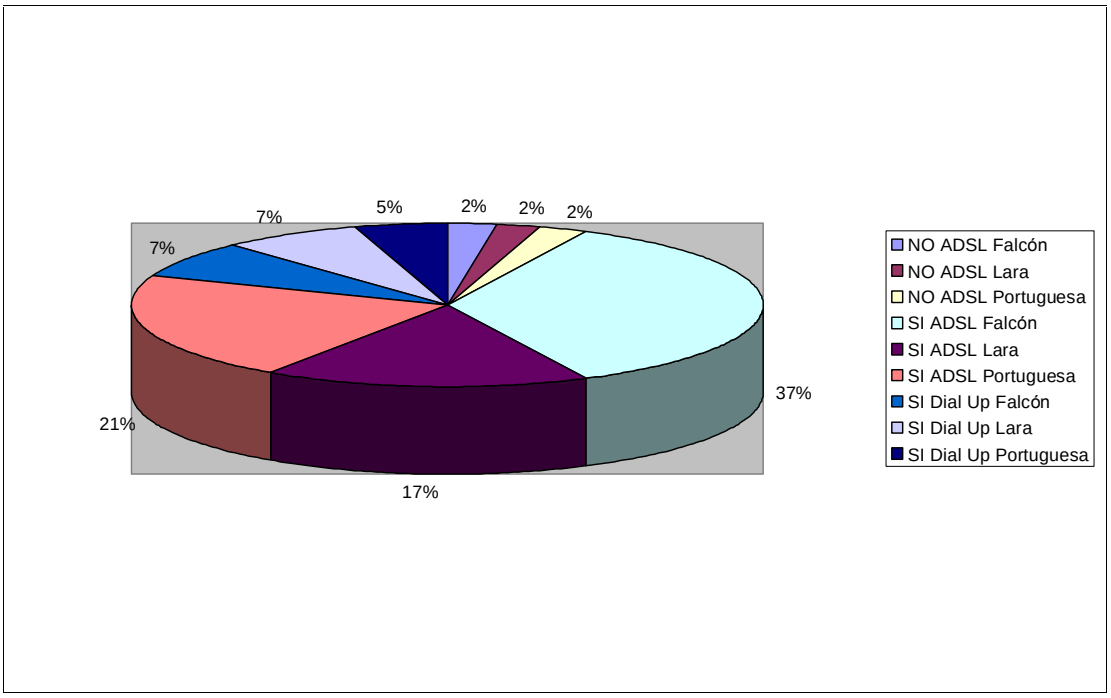

Gráfico No. 3: Distribución Porcentual de la Necesidad de Conexión de los Clientes con la Empresa G&T Sistemas.

Al aplicarse el instrumento se obtuvo que el 93 % de la muestra seleccionada, opinó que desea conectarse en línea con G&T Sistemas como lo indica la Tabla 6, con la finalidad de mejorar la calidad en el servicio y que esto se traduzca en mejoras operativas, tanto para el cliente remoto como para la propia empresa G&T, tomando en cuenta que los soportes y actualizaciones funcionarían en línea; solamente un 7 % opinó que no desea conectarse en línea con G&T Sistemas como lo muestra la gráfica 3.

Ítem N.- 4. ¿Que Tipo de Conexión tiene su empresa?

En la tabla 7 y en el gráfico 4 se presentan los resultados obtenidos para este ítem.

Tabla 7. Factibilidad Técnica de Conexión.

4. ¿Que Tipo de Conexión tiene su empresa?	Estado	Total	%
ADSL	Falcón	16	38
	Lara	8	19
	Portuguesa	10	24
Total ADSL		**34**	**81**
Dial Up	Falcón	3	7
	Lara	3	7
	Portuguesa	2	5
Total Dial Up		**8**	**19**
Total general		**42**	**100**

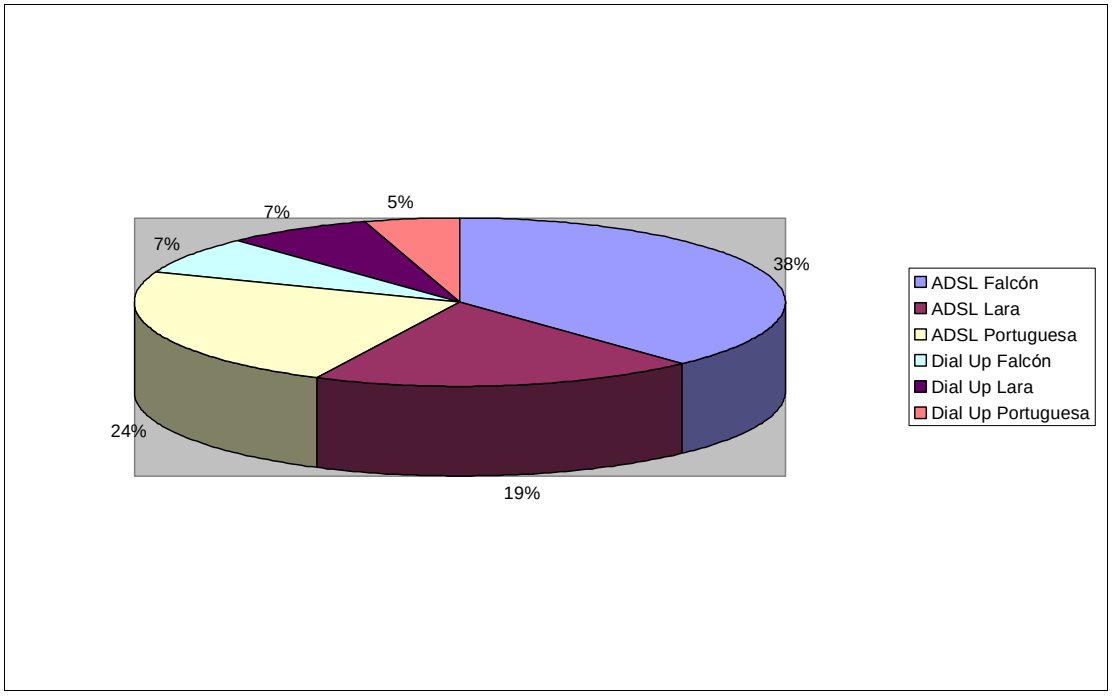

Gráfico No. 4: Distribución Porcentual de Factibilidad Técnica.

El 81% de la muestra seleccionada tiene conexión ADSL como podemos observar en la Tabla 7, esto nos indicó que 34 empresas pudieran estar conectadas con G&T Sistemas de manera automática, cumpliendo así, con la premisa de tener

una tecnología de banda ancha ADSL, que les permitiría cubrir la factibilidad técnica para la conexión de una red privada virtual dinámica, por otro lado, como se indica en el gráfico 4, tenemos solamente un 19 % con conexión Dial-Up que representan 8 empresas.

Ítem N.- 5. ¿Si su conexión es Dial-up, estaría dispuesto a cambiar este tipo de conexión a ADSL, con la idea de mejorar el soporte de G&T Sistemas?

En la tabla 8 y en el gráfico 5 se presentan los resultados obtenidos para este ítem.

Tabla 8. Factibilidad Técnica de Migrar la Conexión Dial-up a Tecnología ADSL.

5. ¿Si su conexión es Dial-up, estaría dispuesto a cambiar este tipo de conexión a ADSL, con la idea de mejorar el soporte de G&T Sistemas?	Total	%
SI	8	100
Total general	8	100

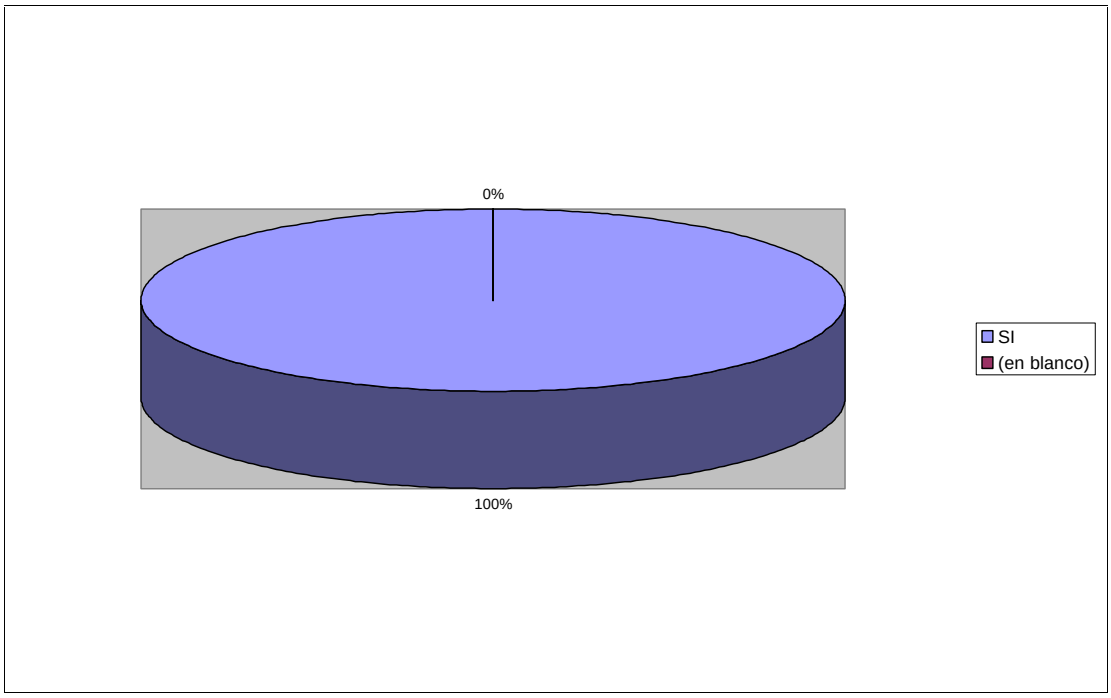

Gráfico No. 5: Distribución Porcentual de Migrar la Conexión Dial-up a Tecnología ADSL en los Clientes.

Con base a los resultados de la Tabla 8, el 100 % de las empresas están dispuestas a migrar a una conexión más estable como lo es ADSL, ya que, permite tener un acceso dedicado o permanente a Internet y con una velocidad superior a la conexión Dial-up, con la finalidad de poder contar con un mejor soporte por parte de la empresa G&T de las aplicaciones que actualmente estos adquirieron, incidiendo positivamente en sus operaciones.

Ítem N.- 6. ¿Que tipo de S.O Windows tiene el PC donde esta(n) la(s) aplicación(es) de G&T Sistemas?

En la tabla 9 y en el gráfico 6 se presentan los resultados obtenidos para este ítem.

Tabla 9. Factibilidad Técnica de Contar con un S.O que Permita la Creación de la DVPN.

6. ¿Que tipo de S.O Windows tiene el PC donde esta(n) la(s) aplicación(es) de G&T Sistemas?	Conexión a Internet	Estado	**Total**	**%**
W2000	ADSL	Falcón	1	2
		Portuguesa	1	2
	Total ADSL		2	5
Total W2000			**2**	**5**
W95	ADSL	Lara	1	2
	Total ADSL		1	2
Total W95			**1**	**2**
WXP	ADSL	Falcón	15	36
		Lara	7	17
		Portuguesa	9	21
	Total ADSL		31	74
	Dial Up	Falcón	3	7
		Lara	3	7
		Portuguesa	2	5
	Total Dial Up		8	19
Total WXP			**39**	**93**
Total general			**42**	**100**

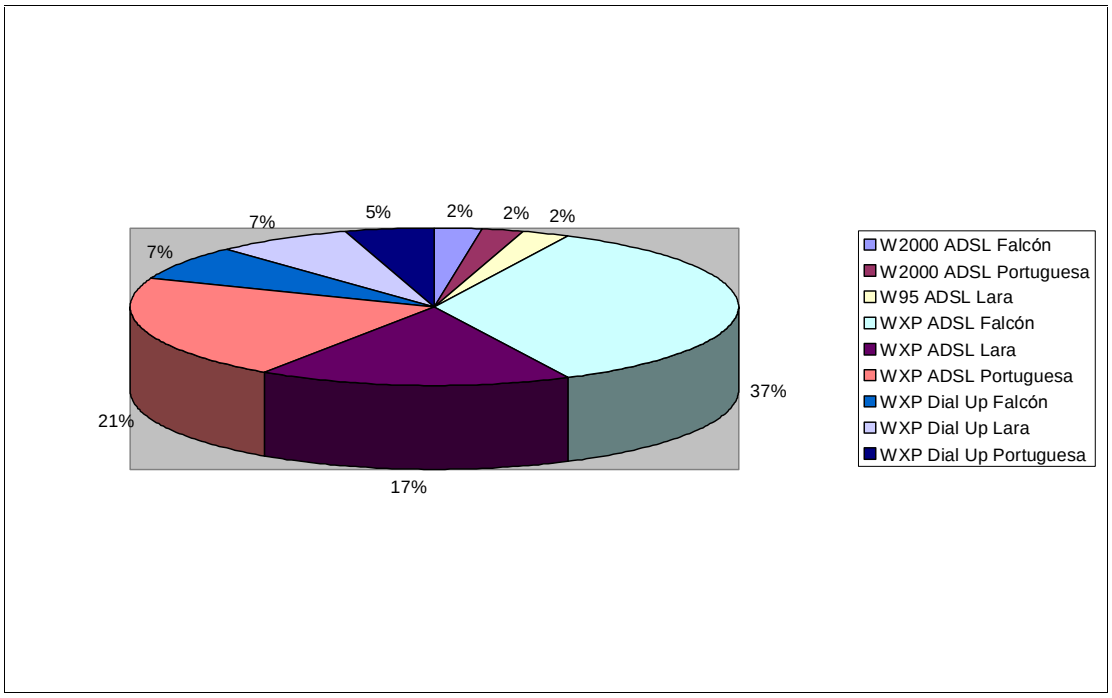

Gráfico No. 6: Distribución Porcentual de los S.O Clientes.

Con base a la Tabla 9, podemos determinar claramente que 39 empresas que corresponden a un 93 % como se indica en la gráfica 6 de la muestra, tienen sistemas operativos Windows XP y que 31 empresas que corresponde a un 74 % de la muestra tienen conexión ADSL, estas dos características cumplen con la factibilidad técnica para crear una red privada virtual dinámica (DVPN).

En otro orden de ideas, revisando el cuestionario de la localidad principal se obtuvo lo siguiente:

Se aplicó un cuestionario de ocho (8) preguntas a la empresa G&T Sistemas (Anexo D), que permitió conocer la necesidad de optimizar los servicios con sus clientes y los recursos con que contaban para poder implementar la propuesta del diseño de sistema automatizado cliente/servidor para crear la DVPN sobre banda ancha ADSL. De la información obtenida se pudo entender que las actualizaciones o

soportes que brinda la empresa G&T Sistemas a sus clientes, se realizan por dos vías: Dial-up y En Sitio. La primera tiene una limitante que es la de aceptar una sola conexión a la vez, porque el equipo RAS de la localidad principal tiene una sola tarjeta Fax-MODEM y la segunda opción es de realizar actualizaciones o soportes en sitio, lo que trae como consecuencia, que se tiene que, desplazar personal de G&T Sistemas a todas las empresas y como tienen clientes remotos en otros estados, el impacto económico y de tiempo respuesta afectarían de manera negativa tanto a la empresa G&T Sistemas como a sus clientes.

Siguiendo la misma línea, la empresa G&T Sistemas utiliza el correo electrónico para transmitir archivos con sus clientes, pero con la limitante de capacidad de almacenamiento que tienen los buzones de cada cliente. Además, de la limitante propia del tamaño del archivo que se puede enviar en un momento determinado, como por ejemplo lo indica el proveedor ISP CANTV.net en su correo, el tamaño total del mensaje debe ser menor a 6Mb y los archivos deben tener menos de 3Mb de tamaño cada uno.

Por otro lado, la empresa G&T Sistemas no cuenta con un servidor de hospedaje ni con una aplicación automatizada que permita estar en línea con sus clientes para agilizar los procesos de soportes o de actualizaciones, pero si cuentan con un servidor Windows 2000 Server, además de poseer una conexión ADSL.

De acuerdo al análisis efectuado a la empresa G&T Sistemas, se pudo observar que existía la necesidad de contar con una herramienta que permitiera estar en línea con sus clientes, lo cuál mejoraría su calidad de servicio ya que tienen los insumos necesarios, para montar una red privada virtual.

Elaboración del Modelo Cliente/Servidor

Esta etapa de análisis del modelo propuesto respondió el tercer (3er.) objetivo específico de la investigación, el cuál fue: Proponer un diseño de conexión privada virtual dinámica a los clientes de la empresa G&T Sistemas en Barquisimeto.

Para la elaboración de este modelo, el investigador se basó en la necesidad que tenía la empresa G&T Sistemas en conectarse en línea con sus localidades remotas y poder brindar un mejor servicios a sus clientes. Para esto se hacía importante establecer, si sus clientes también adolecían de esta necesidad, para lo cuál, se aplicaron cuestionarios a los clientes, que permitieron conocer dichas necesidades obteniendo información útil para la elaboración de la propuesta del modelo.

El análisis inicial de esta investigación nos permitió proponer una red privada virtual, con el propósito de establecer conexiones en línea de manera segura y estable entre G&T y sus clientes remotos. Para esto se propuso investigar cuáles eran las condiciones que se necesitaban y con cuáles recursos se contaban.

La Empresa G&T Sistemas contó con los siguientes recursos:

- Enlace principal Banda Ancha con tecnología ADSL.
- Un Servidor con sistema operativo Windows 2000 Server.

Al Realizar un estudio de cómo trabaja la tecnología ADSL, nos permitió conocer que el proveedor de servicio a Internet (ISP) CANTV, suministra direcciones IP válidas certificadas, pero de manera dinámica, es decir, cada cierto tiempo cambia la dirección IP. El hecho que CANTV asigne direcciones dinámicas implicó realizar un estudio mas profundo de la solución para poder establecer o crear una red privada virtual puesto que se necesitaba una IP fija válida para asignarla al servidor, que a su vez, se encargaría de brindar los servicios de VPN los clientes conectados.

Por tal motivo, se propuso un diseño de sistema automatizado cliente servidor que permita la creación de la red virtual privada pero de forma dinámica, ya que, el acceso a Internet será por ADSL. Por lo antes expuesto se creó un esquema de interconexión de forma tal, que se pueda establecer la red privada virtual dinámica, entre clientes remotos y la sede principal. Para tener una mejor visión del modelo propuesto, a continuación se muestra diagrama del mismo.

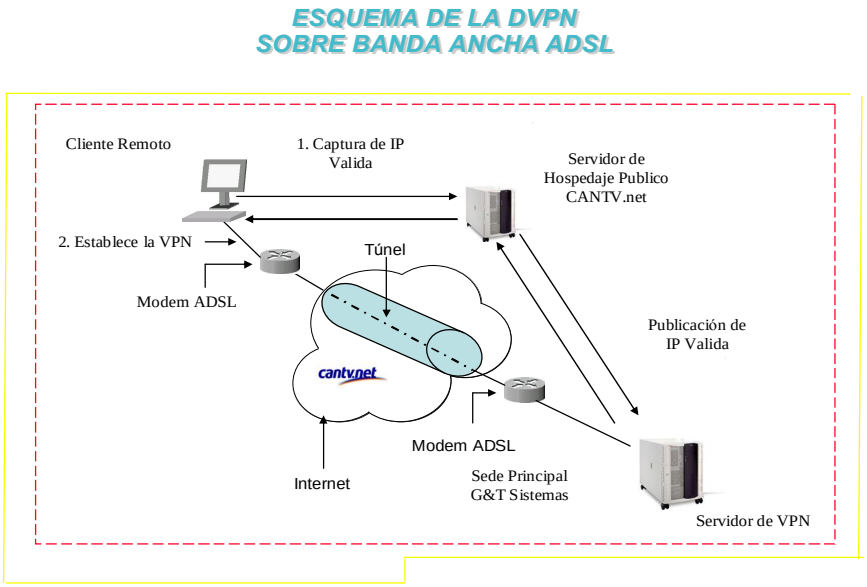

Figura 5. Esquema de Interconexión DVPN entre los Clientes Remotos y G&T

Fuente: MARQUEZ (2005)

El esquema de interconexión propuesto tiene en consideración que las direcciones IP en ambos extremos son dinámicas y el punto focal donde los clientes se conectarán para realizar la VPN es el servidor Windows 2000 Server. Para ello se buscó un servidor intermedio que sirvió de puente entre los clientes remotos y el servidor principal ubicado en la empresa G&T Sistemas, con el propósito de almacenar la dirección IP que tenga en un determinado momento el servidor principal. También este servidor sirve a su vez como punto de captura de la dirección IP requerida por los clientes remotos antes de establecer la VPN, el cuál se denominó servidor de hospedaje (Hosting). Este servidor de hospedaje debería ser público para que las máquinas puedan reconocerlos en la red. En esta investigación se tomó como servidor Hosting el de CANTV.net y dicho servidor se registra con el nombre de mipagina.cantv.net en Internet. Es importante acotar que para esta investigación se utilizó el login y password de la cuenta de correo del investigador para poder realizar la publicación y captura de la IP.

Una vez que se concibió el modelo para la creación de DVPN dinámicas, se procedió a efectuar el diseño del sistema automatizado, escogiendo una aplicación cliente/servidor que permite comunicar programas entre si, pudiendo procesar información a través de la red pública Internet. Tomando en cuenta que Internet es vulnerable a la seguridad, se le agregaron los protocolos propios de encriptamiento usados por los sistemas operativos de la empresa Microsoft para tener conexiones seguras, con la finalidad de crear la VPN dinámica.

Para el desarrollo de la aplicación cliente en la creación de DVPN se utilizaron los siguientes insumos:

Hardware:

- Un (1) equipo HP Pentium IV
- Procesador 1,70 GHZ
- 256 MB de RAM
- Disco Duro de 40 GB
- Unidad de CD/RW

Software:

- Sistema Operativo Windows XP

Lenguaje de Programación Utilizado:

- Microsoft Visual Basic 6.0

En el desarrollo de la aplicación Servidor se utilizó un control en Visual Basic 6.0 llamado Winsock, el cuál permite conectarse a un equipo remoto e intercambiar información con el protocolo control de transmisión (TCP). A continuación se describe la lógica del desarrollo de esta aplicación servidor:

a) Basándonos en el análisis del esquema de conexión, lo primero que debe realizar la aplicación servidor es averiguar cuál IP tiene, con la idea de publicarla en Internet almacenándola en el servidor mipagina.cantv.net, el control Winsock tiene varias propiedades, entre ellas esta **LocalIP** que permite conocer cuál dirección IP tiene el equipo en ese momento, apoyándonos en esta propiedad, el sistema automáticamente captura la IP del equipo servidor y lo copia en un archivo tipo texto

llamado pubip.txt realizando la publicación de éste, a través del procolo de transferencia de archivos (FTP), para esta publicación se utilizó un control en visual Basic 6.0 llamado Internet Transfer (Inet). Al realizar este paso de manera exitosa, la aplicación servidor que esta corriendo en el servidor de G&T se mantiene escuchando, es decir, esperando conexiones clientes, es importante acotar que para establecer esta comunicación se tomó como puerto el 878.

b) Para el desarrollo de la aplicación Cliente se utilizó el control Inet que permite realizar un FTP al servidor mipagina.cantv.net con la finalidad de capturar la dirección IP que tiene el servidor, al tener ésta, se procede a establecer una conexión, utilizando el control Winsock de visual Basic y nos apoyamos en la libreta de teléfonos de marcado que tiene el S.O Windows XP para establecer o crear la VPN, esta libreta de conexiones tiene como nombre rasphone.pbk, pero antes de ejecutar dicha libreta, la aplicación cliente debe actualizar la dirección IP que tiene en ese momento el servidor, con la finalidad de crear la VPN.

c) Luego del desarrollo de la aplicación cliente/servidor, se planteó realizar una prueba de verificación en una empresa en Barquisimeto, se tomó como premisa que su conexión a Internet fuera ADSL y que el equipo cliente tuviera S.O Windows XP.

d) Cumplido estos requisitos, se procedió a instalar la aplicación cliente en el equipo remoto, igualmente se instaló la aplicación servidor en el equipo servidor VPN de G&T Sistemas, se desactivaron los corta fuego (Firewall) que coloca CANTV.net de protección a la red en el ADSL, tanto en el cliente como en G&T Sistema, logrando que el servidor de VPN publicara su dirección IP en el servidor Hosting de CANTV.net y que la aplicación cliente recibiera esta dirección para luego establecer la VPN, al crear el túnel se pudo tomar control remoto de la máquina del cliente con la herramienta conexión a escritorio remoto, observando rapidez, dicha conexión se mantuvo por un período de una (1) hora, comprobándose que las pruebas lograron el objetivo propuesto.

Para corroborar las hipótesis que fueron planteadas en el capítulo dos (2):

HO: Las direcciones IP dinámicas no se pueden controlar por lo tanto no se pueden crear DVPN entre Cliente/Servidor con direcciones IP dinámicas.

H1: Las direcciones IP dinámicas se pueden controlar y por lo tanto se pueden crear DVPN entre Cliente/Servidor con direcciones IP dinámicas.

Se realizó una segunda prueba con el cliente de la empresa G&T Sistemas, para validarlas.

Las pruebas aplicadas y sus resultados son las siguientes:

1. Establecer la conexión con la aplicación Cliente/Servidor solamente sin realizar la conexión VPN, se pudo observar que hubo conexión realizando envió y recepción de mensajes.
2. Establecer la VPN conociendo la IP del Servidor sin ejecutar la aplicación Cliente/Servidor, al realizar la prueba se verificó si la dirección IP del servidor era reconocida en Internet con el comando ping y el resultado fue positivo, luego se procedió a realizar la conexión VPN solamente configurando dicha IP y no hubo conexión.

De estas pruebas se demostró que la DVPN dependió de que se estableciera una conexión cliente-servidor, condición necesaria para que se pueda crear la VPN porque cuando se controló las direcciones IP dinámicas con la aplicación Cliente/Servidor se logró establecer el túnel de conexión que permitió crear la VPN.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Las experiencias adquiridas diariamente a través del trabajo y de la observación, permitió constatar que puede haber una tecnología susceptible de ser mejorada ó innovada, el uso de Internet por ser pública, nos invita a investigar como podemos sacar provecho de esta infraestructura para lograrlo. En el estudio realizado, el investigador se apoyó en esta gran red, con el fin de aportar una solución que permitió dar respuesta a las interrogantes que se plantearon, cumplir con los objetivos específicos de la investigación, corroborar las dos hipótesis propuestas y lograr el objetivo general el cual fue la creación de una red virtual privada dinámica sobre banda ancha ADSL, con el uso de un sistema automatizado cliente/servidor.

A continuación se mencionan las conclusiones de esta investigación.

1. Con la recopilación de la información, luego de la aplicación del instrumento a los clientes remotos y de haber efectuado el análisis de los datos, se concluye que existe la necesidad de realizar cambios en el servicio que actualmente presta la empresa G&T Sistemas, con el uso de herramientas automatizadas que les permita conectarse en línea con G&T Sistemas optimizando la eficiencia en sus operaciones.
2. La empresa G&T Sistemas no posee una herramienta que le permita actualizar en línea las aplicaciones que tiene con sus clientes remotos, por lo cual debe trasladar personal a los distintos clientes, esto genera retraso en las actualizaciones generando inconformidad en el cliente sobre el servicio

prestado. Esto hace deseable una herramienta que facilite la actualización en línea de las aplicaciones que G&T tiene implantadas en sus clientes

3. Con la realización de la prueba del establecimiento de un red privada virtual efectuada en una empresa de la ciudad de Barquisimeto (Cliente de la empresa G&T Sistemas), se logró el objetivo propuesto y su implementación eficaz, dando como resultado un desempeño cabal en cuanto a rapidez, confidencialidad y seguridad en la transmisión de los datos.
4. Se concluyó que el 74 % de los clientes de G&T Sistemas tienen conexión a Internet ADSL y cuentan con estaciones de trabajo con Sistema Operativo Windows XP, dos (2) condiciones fundamentales en donde se implantó el sistema cliente/servidor, esto garantiza que se podrán crear y establecer la conexión DVPN de una manera factible y segura, lo cual se traduce en una disminución del tiempo de respuesta de atención a clientes y en un aumento de varios clientes atendidos a la vez por parte de la empresa G&T Sistemas.
5. Se demostró con la segunda prueba efectuada al cliente de la empresa G&T Sistemas, que la creación de la DVPN dependía de las variables: aplicación cliente, Servidor de Hospedaje (Hosting) y aplicación servidor.
6. Se concluyó que al no controlar las direcciones IP Dinámicas no se podían establecer o crear la DVPN y que al controlar las direcciones IP Dinámicas con la aplicación cliente/servidor se pudo establecer la DVPN.
7. Según el modelo planteado las VPN no solamente se crean bajo un ambiente de direcciones IP estáticas si no también con accesos a Internet que tienen direccionamiento dinámico y sistemas operativos propietarios como Windows.

Recomendaciones

Dado los resultados positivos conseguidos en el estudio efectuado, el investigador recomienda:

1. La implementación de la solución tanto en la empresa G&T Sistemas como al 74 % de sus clientes que cumplen las premisas de instalación.
2. Evaluar la generalización del diseño propuesto de DVPN a otras redes que usen otras tecnologías para el acceso a Internet.
3. Evaluar el diseño propuesto de DVPN para otros sistemas operativos diferentes de Windows XP.
4. Implementar corta fuegos (Firewall) que permitan proteger y administrar los accesos de servicios a Internet de la red interna local, tanto de los clientes remotos como de la propia empresa G&T Sistemas.
5. La aplicación de la propuesta cliente/servidor para implementarlo en otras empresas que requieran conectar sus sedes remotas a su sede principal, con la creación de la DVPN sobre banda ancha ADSL.

CAPÍTULO VI

SOFTWARE DE IMPLEMENTACION DEL MODELO CLIENTE/SERVIDOR PROPUESTO PARA LA CREACION DE DVPN

De conformidad con los objetivos planteados en este trabajo de grado, se explica a continuación la implementación del software cliente y del software servidor, que se aplicó en los clientes remotos y la localidad principal de la empresa G&T Sistema respectivamente.

Para agilizar la puesta en marcha del sistema cliente/servidor, se crearon dos (2) programas de instalación con la herramienta de asistente de empaquetado y distribución de software, del lenguaje de programación Visual Basic 6.0, cada programa de instalación tiene de nombre Setup.exe, el programa Setup.exe del software cliente, contiene el ejecutable de la aplicación (clientes.exe) y las librerías ó componentes propios del lenguaje de programación visual Basic que se utilizaron en el desarrollo del software cliente. El programa Setup.exe del software servidor, contiene el ejecutable de la aplicación (servidor.exe), el archivo plano (pupip.txt) y las librerías propias de Visual Basic que se utilizaron en el desarrollo del software servidor.

El software clientes.exe se desarrolló en visual Basic 6.0 y su creación se baso en resolver dos (2) problemas esenciales, 1) como conectarse a un equipo servidor cuando no conocemos su dirección IP y 2) como podemos establecer una conexión segura, confiable entre un equipo cliente y un equipo servidor.

1) Para resolver el primer problema, se utilizó un control en Visual Basic 6.0 llamado Winsock, el cuál permite conectarse a un equipo remoto e intercambiar información con el protocolo control de transmisión (TCP), siempre y cuando se conozca la dirección IP del equipo destino y se establezca el puerto de la conexión. El control Winsock tiene una propiedad llamada, RemotePort que sirve para devolver o establecer el puerto de conexión con el equipo remoto (Servidor de la empresa G&T

Sistemas), se utilizó el puerto de comunicación 878 para indicar al protocolo TCP que la conexión entre la máquina cliente y la máquina servidor se efectuara por el puerto 878; para conocer cuál es la dirección IP que tiene el servidor de G&T Sistemas, se utilizó un servidor de hospedaje de la empresa CANTV.net que tiene como nombre mipagina.cantv.net, dicho servidor permite almacenar información hasta un máximo de capacidad de 5 MB, en este espacio podemos copiar, eliminar, modificar, leer información almacenada, utilizando el protocolo de transferencia de archivos (FTP).

Siguiendo la misma línea, la aplicación cliente utilizó un control de visual Basic 6.0 llamado INET, que permitió capturar la dirección IP que publicó el servidor de la empresa G&T Sistemas en el servidor de hospedaje, y esto se efectúa, realizando FTP al servidor mipagina.cantv.net (Servidor Hosting), donde se copia la información del archivo plano pubip.txt que contiene la IP del servidor en un archivo plano llamado recibe.txt en la máquina del cliente, al tener copiado el archivo plano recibe.txt, se efectúa una lectura de este archivo para conocer cuál es la IP del servidor. Al descubrir la IP del equipo remoto, en este caso el servidor y conociendo el puerto de conexión (Puerto Remoto 878), podemos establecer la comunicación entre la aplicación cliente y la aplicación servidor.

2) Para resolver el segundo problema de contar con una conexión segura y confiable, el investigador se apoyó en los protocolos de encriptamiento y encapsulación (L2TP, IPsec) propios del sistema operativo Windows XP en español, que se utilizan cuando se crean redes privadas virtuales (VPN); la aplicación cliente luego de establecer la conexión con el servidor, actualiza la dirección IP del servidor en la libreta de conexiones DVPN que tiene como nombre en el S.O Windows XP rasphone.pbk y muestra al usuario en la máquina cliente, la pantalla de conexión para establecer la VPN, culminando así el problema planteado.

El software servidor.exe se desarrolló en visual Basic 6.0 y su creación se baso en resolver el problema de publicación de la dirección IP dinámica del equipo servidor de la sede principal (G&T Sistemas) al servidor de hospedaje de CANTV.net, con el fin de que los equipos remotos con la aplicación cliente capturen la IP y puedan establecer conexiones con el servidor de la sede principal utilizando el

puerto de conexiones 878; explicando lo del puerto de comunicación, se menciona que dentro de la máquina servidor podemos tener varios servicios (Correo, Ftp, www, clientes.exe ó servidor.exe) y cuando llega uno de esos paquetes que contienen información, la máquina servidor debe saber reconocer a que servicio está destinado. Eso lo sabe mediante el Puerto de Comunicación al que va dirigido el paquete, por tal razón, tanto la aplicación cliente como la aplicación servidor se le programó que su conexión se realizará por el puerto 878.

En el desarrollo de la aplicación Servidor se utilizó un control en Visual Basic 6.0 llamado Winsock, el cuál permite conectarse a un equipo remoto e intercambiar información con el protocolo control de transmisión (TCP). Basándonos en resolver el problema de la publicación de la IP en el servidor de hospedaje (Hosting), lo primero que debe realizar la aplicación servidor es averiguar cuál IP tiene, con la idea de publicarla en Internet almacenándola en el servidor mipagina.cantv.net, el control Winsock tiene varias propiedades, entre ellas se encuentra **LocalIP** que permite conocer cuál dirección IP tiene el equipo en ese momento, apoyándonos en esta propiedad, el sistema automáticamente captura la IP del equipo servidor y lo copia en un archivo de texto llamado pubip.txt realizando la publicación de éste, a través del procolo de transferencia de archivos (FTP). Para esta publicación se utilizó un control en visual Basic 6.0 llamado Internet Transfer (Inet).

Al realizar la publicación de manera exitosa, la aplicación servidor se mantiene escuchando, es decir, esperando conexiones clientes con la propiedad **listen** del control Winsock, es importante acotar que para establecer esta comunicación se tomo como puerto local el # 878 utilizando la propiedad **LocalPort** del control Winsock.

A continuación se describe como se realiza la instalación del software cliente:

1. Se debe ejecutar el archivo 

para iniciar la instalación, este ejecutable se encuentra en el subdirectorio Instalador\Cliente y la unidad donde se encuentre el instalador dependerá del dispositivo de almacenamiento (CD, Zip, Memoria extraíble, entre otros).

2. Aparece una pantalla de instalación donde se copiaran archivos (Mswinsck.ocx, Msinet.ocx, Msvbvm60.dll, entre otros) de configuración en la máquina destino.

3. Se muestra la Figura 6, que permite la instalación, para comenzar se debe ejecutar Clic en el Botón Aceptar ó ↵

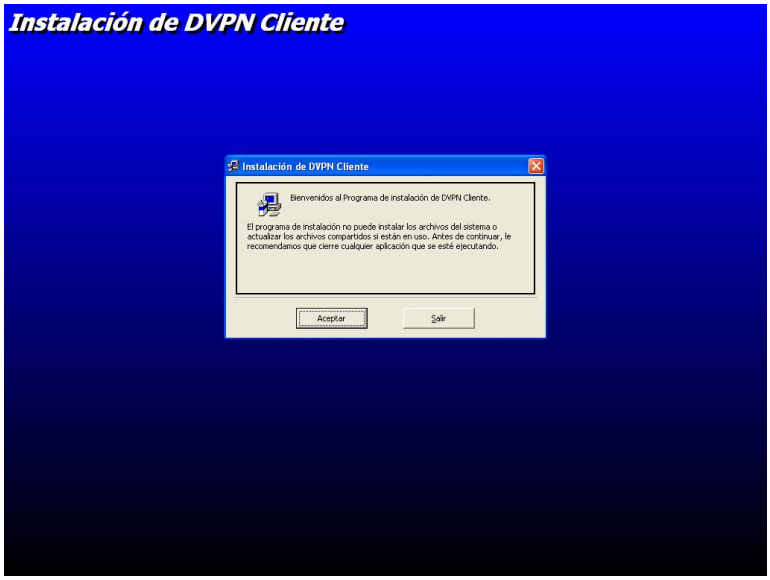

Figura 6. Módulo Inicial de Instalación de la Aplicación Cliente.

4. Aparecerá la Figura 7, Clic en el Botón  ó ↵

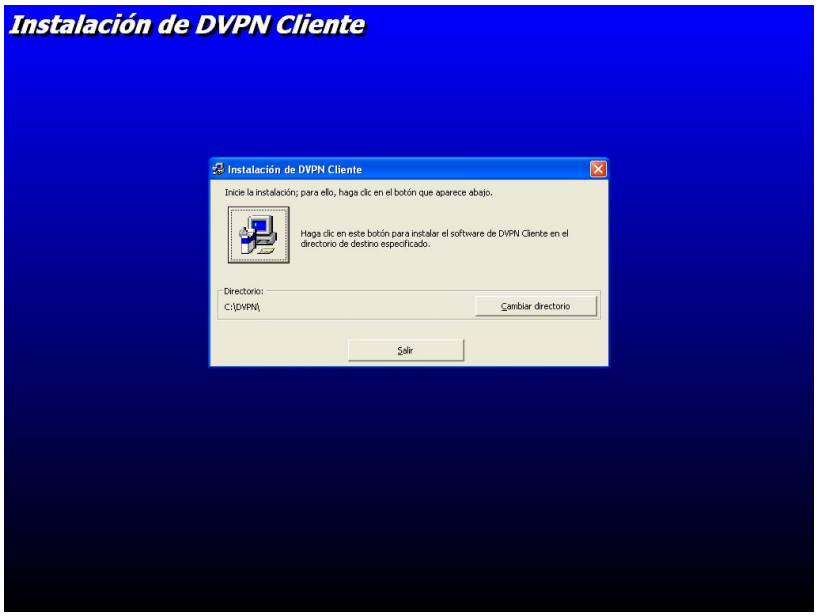

Figura 7. Instalación de la Aplicación Cliente en la Ruta: C:\DVPN.

5. Aparecerá la Figura 8, Clic en el Botón Continuar ó ↵

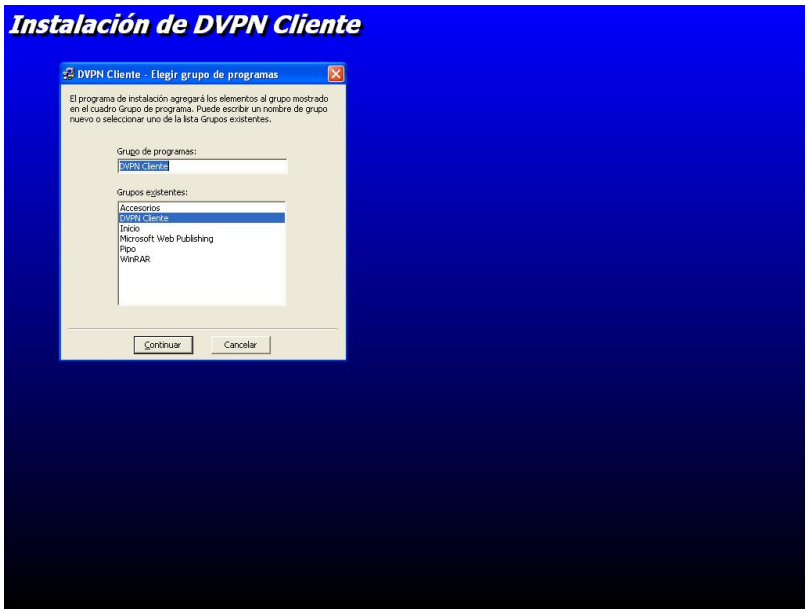

Figura 8. Creación de Grupo de Programa Cliente DVPN.

6. Finalización de la instalación de la aplicación cliente, tal como se muestra en la Figura 9.

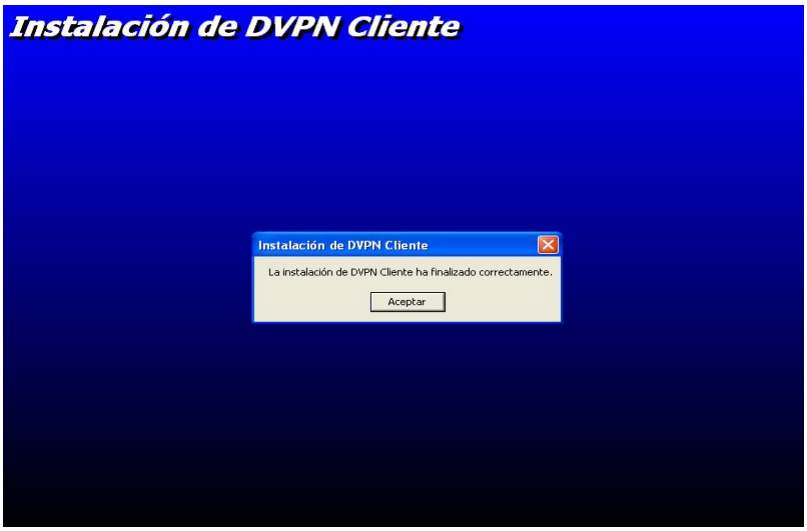

Figura 9. Finalización de la Instalación del Programa Cliente DVPN.

Seguidamente se describe la aplicación cliente:

1. La aplicación cliente se instala en el grupo de programas DVPN Clientes, como se muestra en la Figura 10.

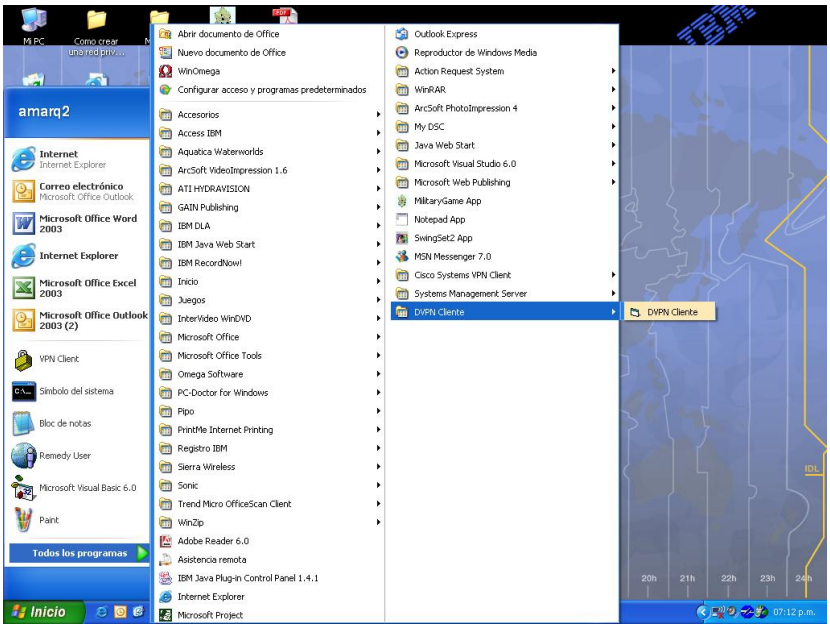

Figura 10. Grupo del Programa Cliente DVPN.

2. Para comenzar a trabajar con la aplicación cliente, se debe ejecutar el botón conectar que aparece en la Figura 11, cuando se acciona, la aplicación cliente realizará una conexión a Internet utilizando FTP para conectarse al servidor mipagina.cantv.net, ubica la dirección IP que publicó el servidor de G&T Sistemas y muestra la dirección IP en el cuadro de texto que tiene la etiqueta IP del Servidor

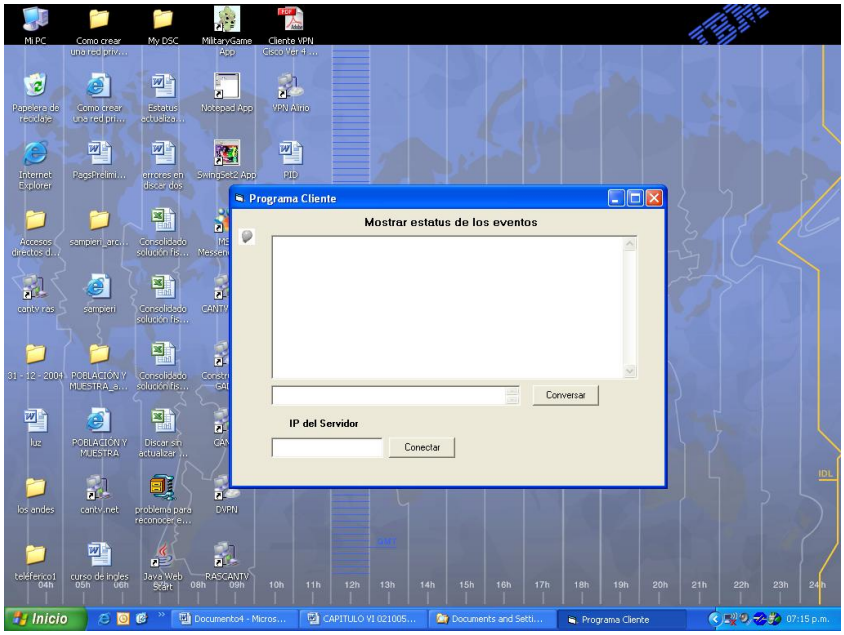

Figura 11. Pantalla del Programa Cliente DVPN.

3. En la Figura 12, se muestra la conexión con el servidor, específicamente en el cuadro de texto identificado con el nombre Mostrar estatus de los eventos entre el cliente y el servidor, en ese momento ya el cliente tiene conexión con el servidor de G&T Sistemas y todavía no se ha establecido la VPN, internamente la aplicación cliente actualiza la libreta de teléfonos rasphone.pbk con la dirección IP del Servidor de G&T y muestra el cuadro de diálogo (Conexiones de red), para establecer la VPN se debe accionar el botón Conectar de la pantalla Conexiones de red.

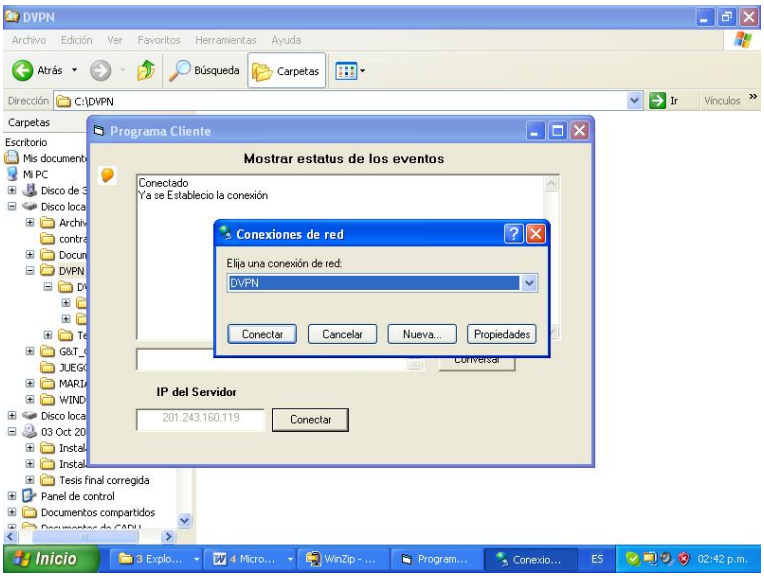

Figura 12. Estatus de Conexión Cliente/Servidor.

4. En la figura 13. presenta el login del cliente, se debe colocar el password o contraseña y se prosigue a darle clic al botón Conectar.

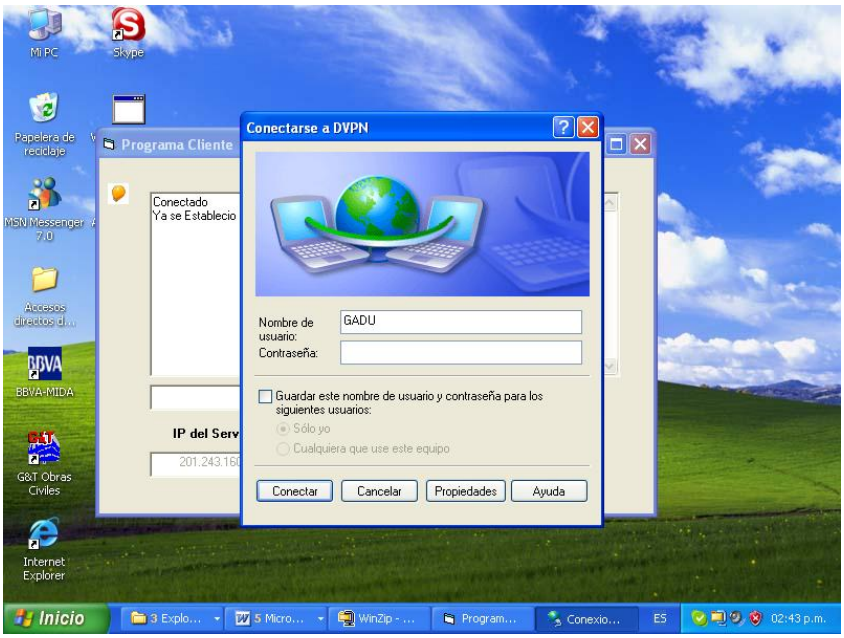

Figura 13. Pantalla de Conexión DVPN Cliente/Servidor.

5. En la Figura 14, se muestra la autenticación de VPN de la máquina cliente.

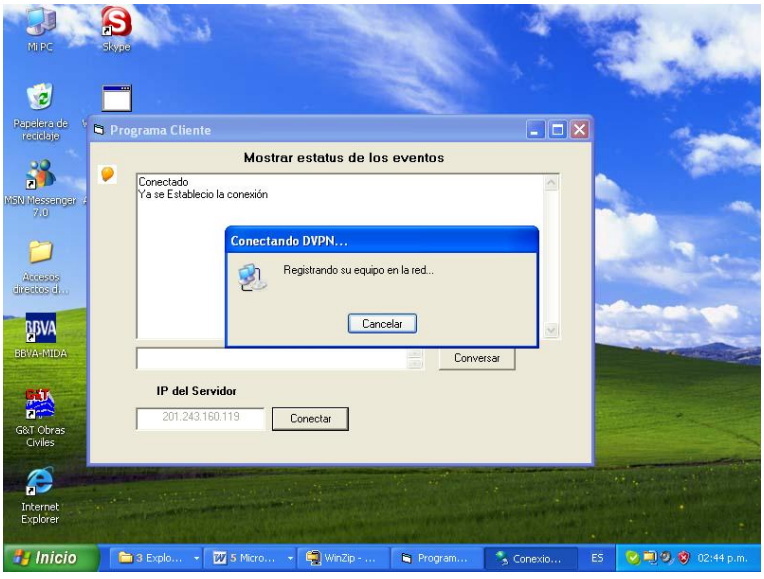

Figura 14. Pantalla de Registro de la Conexión DVPN Cliente/Servidor.

6. En la Figura 15, se muestra la conexión DVPN realizada con la aplicación cliente/servidor.

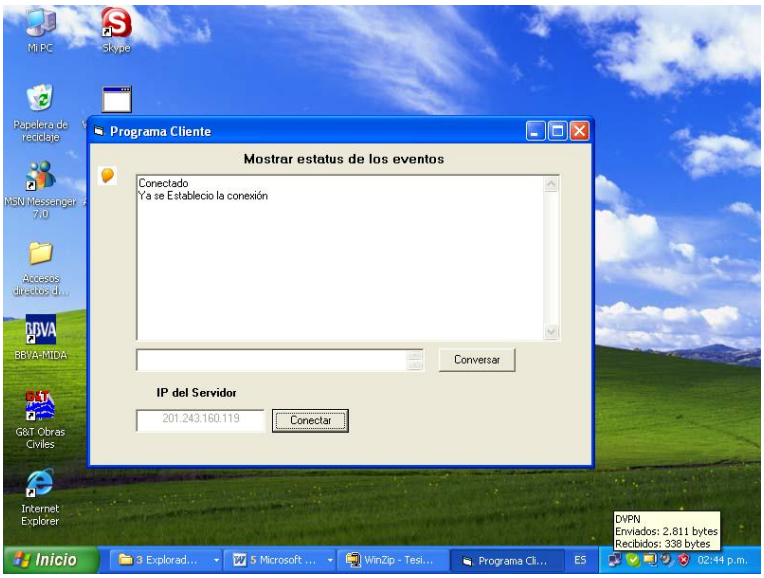

Figura 15. Pantalla de la Creación DVPN Cliente/Servidor.

7. La Figura 16, muestra el botón conversar, que sirve para intercomunicarse enviando y recibiendo mensajes de forma segura que garantiza la confidencialidad requerida, las respuestas del servidor son colocadas en el cuadro de texto con nombre Mostrar estatus de los eventos (Entre el cliente y el Servidor).

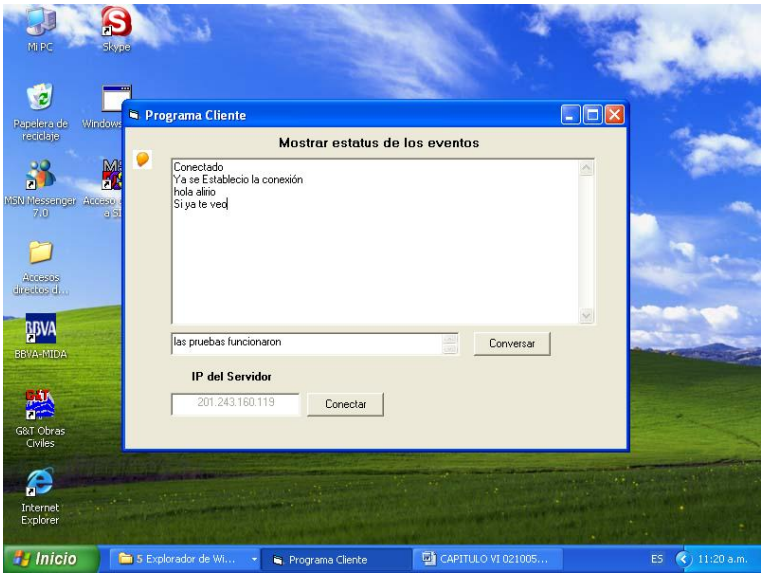

Figura 16. Pantalla de Estatus de Eventos Cliente.

A continuación explicaremos como se realiza la instalación del software Servidor:

1. Se debe ejecutar el archivo 

para iniciar la instalación, este ejecutable se encuentra en el subdirectorio Instalador\Servidor y la unidad donde se encuentre el instalador dependerá del dispositivo de almacenamiento (CD, Zip, Memoria extraíble, entre otros).
2. Aparece una pantalla de instalación donde se copiaran archivos (Mswinsck.ocx, Msinet.ocx, Msvbvm60.dll, entre otros) de configuración en la máquina destino.

3. Aparecerá la Figura 17 para iniciar la instalación, hacer Clic en el Botón Aceptar ó ↵

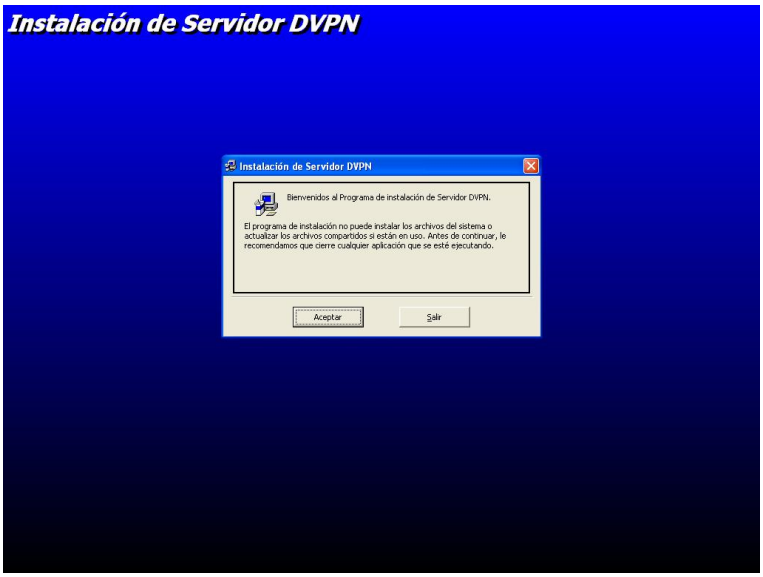

Figura 17. Módulo Inicial de Instalación de la Aplicación Servidor.

4. Aparecerá la Figura 18, hacer Clic en el Botón  ó ↵

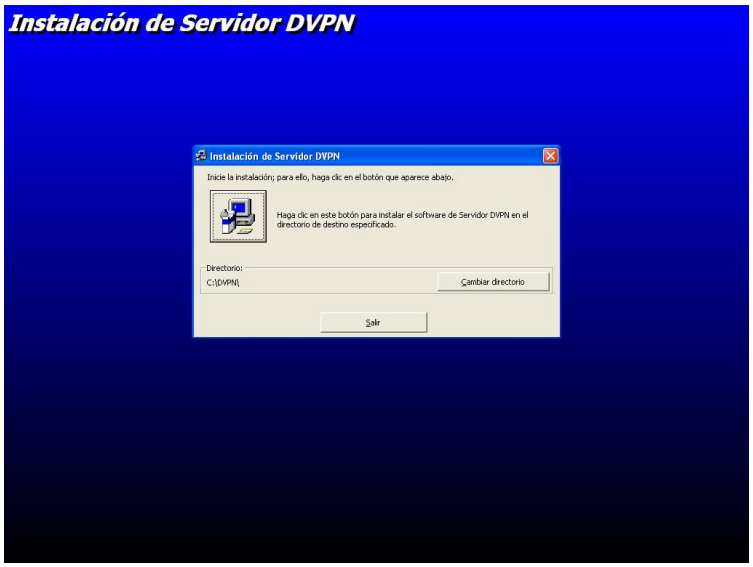

Figura 18. Instalación de la Aplicación Servidor en la Ruta: C:\DVPN.

5. Aparecerá la Figura 19, hacer Clic en el Botón Continuar ó ↵

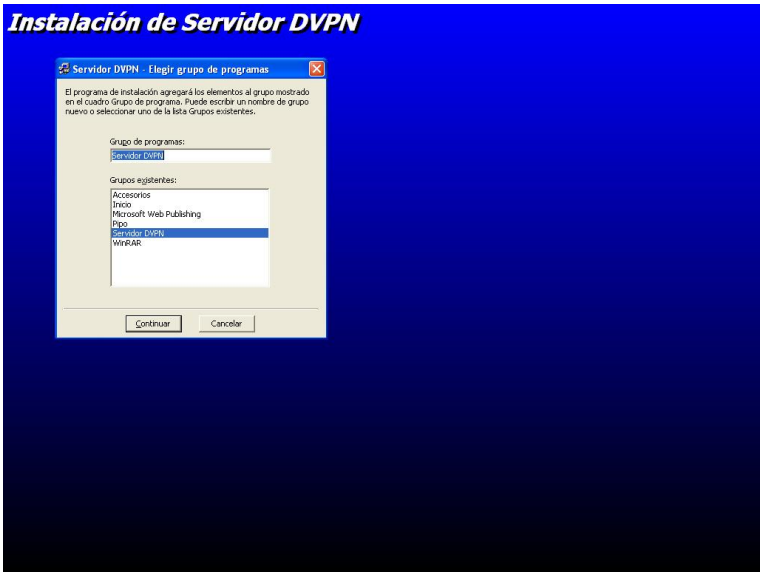

Figura 19. Creación de Grupo de Programa Servidor DVPN.

6. La Figura 20 muestra la Finalización de la instalación de la aplicación Servidor, hacer clic en el botón Aceptar.

Figura 20. Finalización de la Instalación del Programa Servidor DVPN.

A continuación se describe la aplicación servidor:

1. La aplicación Servidor se instala en el grupo de programas Servidor DVPN, como se muestra en la Figura 21.

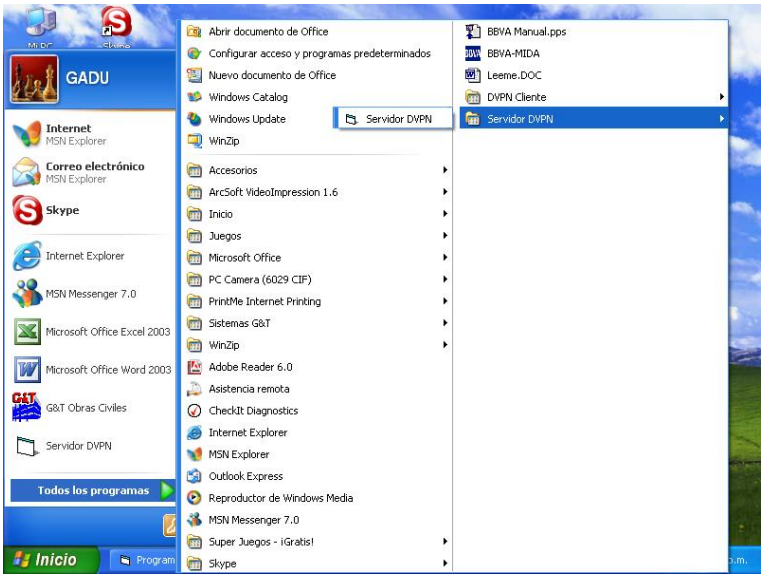

Figura 21. Grupo del Programa Servidor DVPN.

2. En la Figura 22, se muestra automáticamente la Dirección IP que tiene el servidor G&T Sistemas, para publicarla al servidor Hosting de CANTV.net, hacer clic en el botón Publicar IP, la aplicación servidor realizará una conexión a Internet utilizando FTP para conectarse al servidor mipagina.cantv.net, publicando la dirección IP que tiene y se mantiene esperando conexiones (Escuchando por el puerto 878).

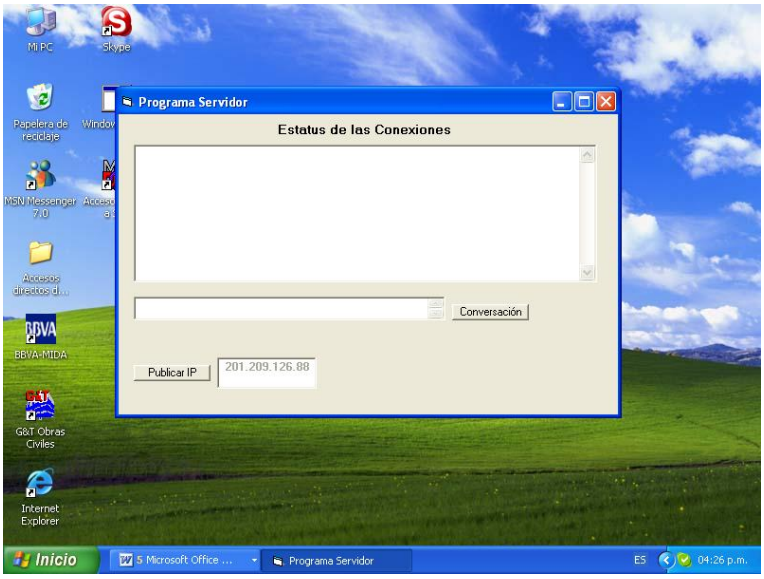

Figura 22. Pantalla del Programa Servidor DVPN.

3. En la Figura 23, se muestra una conexión entre una empresa cliente y el servidor, en el cuadro de texto con Estatus de las Conexiones, se observa la conexión de la máquina cliente y el mensaje enviado por éste, para responderle se debe ubicar el cursor en el cuadro de texto de la conversación y luego de escribir hacer en el botón Conversación.

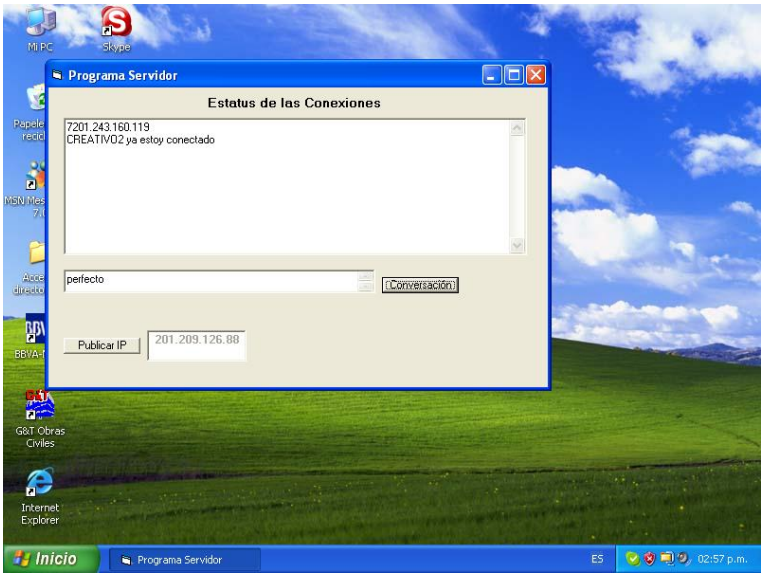

Figura 23. Pantalla de Estatus de Eventos Servidor.

La implementación del software propuesto demostró la factibilidad práctica del modelo en esta investigación, ya que, permitió corroborar que la creación de la DVPN sobre conexiones a Internet bajo tecnología ADSL es posible controlando las direcciones IP dinámicas asignadas por los proveedores de servicio.

REFERENCIAS BIBLIOGRAFICAS

ABC analog s.l (2001). "Enrutadores WAN para CABLE y ADSL Vigor2200".Recuperado Abril 12 de 2003 de URL: http:// http://www.abcnet.es.

Aldo, N., Peralta, G., Sandmann, F.,Simunic, M. (2005). Arquitectura TCP/IP.Recuperado 03 de Marzo 2005 de URL http://web.frm.utn.edu.ar/comunicaciones/tcp_ip.html#5

Besarón, P., Muler, H. (2000). Operacionalización de las variables de una Hipótesis. Recuperado 09 de Marzo de 2005 de URL: http://www.escribimos.com/operacion.htm

CANTV.net (2000). "Internet Sobre Banda Ancha". Recuperado Septiembre 20 de 2003 de URL: http://www.cantv.net/aba/ir_a.asp?2_aba_acerca.

Centro de Comunicaciones CSIC RedIRIS (2002). "Enrutadores VPN". Recuperado Marzo 10 de 2003 de URL: http://www.rediris.es/rediris/boletin/54-55/sumario.html.

Centro de Comunicaciones CSIC RedIRIS (2001). "Redes Privadas Virtuales Dinámicas".Recuperado Marzo 13 de 2003 de URL: http://www.rediris.es/rediris/boletin/54-55/sumario.html.

Cabañas, A. (2000). ¿Son importantes las VPN?. Recuperado 11 de Marzo de 2004 de URL:http://microasist.com.mx/noticias/internet/achin2401.shtml

Carreon, R. (2002), Redes Privadas Virtuales (VPN), recuperado 10 de Octubre de 2004 de URL: http://www.monografias.com/trabajos11/repri/repri.shtml

Dumith, F. (1999), Telecomunicaciones. Recuperado 5 de Marzo de 2004 de URL: http://www.a-venezuela.com/venezuela/telecom.shtml

Fortea, V. (1999). Diseño e Implementación de un cliente FTP bajo Windows 95. Recuperado 25 de enero 2005 de URL: http://members.tripod.com/vteforte/index2.html

Guenul, O. (2001). Redes. Recuperado 10 de Octubre de 2004 de URL: http://www.monografias.com/trabajos5/redwan/redwan.shtml

Leiner, B., Cerf, V., Clark, D., Kahn, R., Kleinrock, L., Lynch, D., Postel, J., Lawrence, R., Wolf, S. (1999), Una breve historia de Internet. Recuperado 11 de Marzo de 2004 de URL: http://www.ati.es/DOCS/internet/histint/

Mudd, S., Moncada, Á., Béjar, J. (2002). Organización de las Redes Wireless - v1.2. Recuperado Junio 20 de 2003 de URL: http://www.wl0.org/~sjmudd/wireless/network-structure/html/index.html.

Millán, A. (2005), Tutorial: La Internet (La Web) introducción a la herramienta que acondicionara el futuro, Recuperado 06 de marzo de 2005 de URL:http://www.zator.com/Internet/

Neolab S.A. de C.V. (2001). "Telefonía por Internet". Recuperado 15 de Agosto de 2003 de URL: http://www.ipstar.com.mx/Default.html.

Salvucci, G., Virues, L. (2003). Recuperado 20 de enero 2005 de URL: http://www.monografias.com/trabajos12/redlan/redlan.shtml

Suárez, A., Losinno, E. (1998). Tutorial sobre Servicios en Internet. Revisado

22 de enero 2005 de URL: http://www.linti.unlp.edu.ar/frames/tesisdeg.htm

Teo Veras S.A. (2004). "Orígenes De La Comunicación Humana Y Desarrollo De La Comunicación Eléctrica". Recuperado Octubre 10 de 2004 de URL: http://www.teoveras.com.do/Origenes%20Telecoms.htm

Tanenbaum, S. (1996). "Redes De ordenadores". Revisado 15 de enero 2005 de URL: http://www.tau.org.ar/base/lara.pue.udlap.mx/redes/rede196.htm

Tamayo, M. (1998). El proceso de la Investigación Científica. Recuperado 10 de marzo de 2005 de URL: http://server2.southlink.com.ar/vap/poblacion.htm

Universidad Centroccidental "Lisandro Alvarado". (2002). Manual para la Presentación del Trabajo Conducente al Grado Académico de: Especialización, Maestría y Doctorado.

Universidad Pedagógica Experimental Libertador. (2002). Manual de Trabajos de Grado de Especialización, Maestría y Tesis Doctórales. Caracas – Venezuela.

ANEXO A

UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIA
MAESTRIA EN CIENCIAS DE LA COMPUTACION
MENCION REDES DE COMPUTADORAS

PROPUESTA DE UN DISEÑO DE SISTEMA AUTOMATIZADO CLIENTE SERVIDOR PARA REDES PRIVADAS VIRTUALES DINAMICAS (DVPN) SOBRE BANDA ANCHA ADSL

ENCUESTA LOCALIDADES REMOTAS	**Fecha:**
DATOS DEL LUGAR	
NOMBRE DE LA EMPRESA:	**ESTADO:**
Dirección:	
NOMBRE DEL ENTREVISTADO:	**CARGO:**
DEPARTAMENTO:	
DATOS BÁSICOS	

1. ¿Ha tenido lentitud o retardo con las actualizaciones de las aplicaciones que usted adquirió con la empresa G&T Sistemas?	**2. ¿Los soportes a las aplicaciones que usted adquirió con la empresa G&T como los califica?**	**3. ¿Desea conectarse en Línea con G&T para mejorar la calidad del servicio?**

Frecuentemente ☐	Muy Poco ☐	Nunca ☐	Excelente ☐	Bueno ☐	Regular ☐	Malo ☐	Si ☐	No ☐

4. ¿Que Tipo de Conexión tiene su empresa?					**5. ¿Si su conexión es Dial-up, estaría dispuesto a cambiar este tipo de conexión a ADSL, con la idea de mejorar el soporte de G&T Sistemas?**		**6. ¿Que tipo de S.O Windows tiene el PC donde esta(n) la(s) aplicación(es) de G&T Sistemas?**			
Dial-Up ☐	ADSL ☐	FR ☐	Otro ☐	No Tiene ☐	Si ☐	No ☐	W95 ☐	W98 ☐	W2000 ☐	WXP ☐

ANEXO B

UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIA
MAESTRIA EN CIENCIAS DE LA COMPUTACION
MENCION REDES DE COMPUTADORAS

PROPUESTA DE UN DISEÑO DE SISTEMA AUTOMATIZADO CLIENTE SERVIDOR PARA REDES PRIVADAS VIRTUALES DINAMICAS (DVPN) SOBRE BANDA ANCHA ADSL

ENCUESTA LOCALIDAD PRICIPAL	**Fecha:**10/02/2011
DATOS DEL LUGAR	
NOMBRE DE LA EMPRESA:	**ESTADO**:
Dirección:	

NOMBRE DEL ENTREVISTADO:	CARGO:
DEPARTAMENTO:	

DATOS BÁSICOS

1. ¿Los actuales soportes con sus clientes remotos los clasifica en:?				2. ¿Como realiza G&T los soportes o actualizaciones con sus clientes remotos?			3. ¿G&T cuenta con una Herramienta para transmitir archivos con sus clientes?	
Excelente □	Bueno □	Regular □	Malo □	En Sitio □	Dial-Up □	Por Correo □	Si □	No □

4. ¿G&T cuenta con una aplicación que permita establecer una conexión en línea con sus clientes?		5. ¿Desea crear DVPN con sus localidades Remotas para mejorar la calidad en el servicio?		6. ¿Posee Servidor Windows 2000 Server?	
Si □	No □	Si □	No □	Si □	No □

7. ¿G&T cuenta con un servidor de Hospedaje?		8. ¿Que tipo de Conexión tiene?			
Si □	No □	Dial-Up □	ADSL □	FR □	Cable-Modem □

ANEXO C

Carta de Solicitud de Validación a los Expertos

UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGÍA

Barquisimeto, Junio de 2005

Ciudadano (a):_____

Reciba un cordial saludo en mi nombre. Sirva la presente para solicitarle la colaboración en calidad de experto para determinar la validez de contenido del cuestionario con el cual se pretende recopilar información necesaria para el Trabajo de Grado titulado "**PROPUESTA DE UN DISEÑO DE SISTEMA AUTOMATIZADO CLIENTE SERVIDOR PARA REDES PRIVADAS VIRTUALES DINAMICAS (DVPN) SOBRE BANDA ANCHA ADSL**", el cual será aplicado a las localidades Remotas en Lara, Portuguesa y Yaracuy, estas localidades son clientes de la empresa G&T Sistemas.

Para tal propósito se anexa a la presente: 1) Formatos de Validación con sus respectivas instrucciones; 2) Cuestionario que se aplicarán a la muestra.

Su opinión al respecto representa un gran aval para esta investigación, dada la excelente labor docente, de investigación y extensión que ha realizado en pro de la formación profesional en la Universidad.

Sin otro particular al cual hacer referencia y agradeciendo de antemano su colaboración, quedo de usted

Atentamente,

_____

Ing. Alirio Marquez.
C.I.: 10.282.156

ANEXO D

UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIA
MAESTRIA EN CIENCIAS DE LA COMPUTACION
MENCION REDES DE COMPUTADORAS

PROPUESTA DE UN DISEÑO DE SISTEMA AUTOMATIZADO CLIENTE SERVIDOR PARA REDES PRIVADAS VIRTUALES DINAMICAS (DVPN) SOBRE BANDA ANCHA ADSL

ENCUESTA LOCALIDAD PRICIPAL	**Fecha:**

DATOS DEL LUGAR

NOMBRE DE LA EMPRESA:	**ESTADO**:
Dirección:	
NOMBRE DEL ENTREVISTADO:	**CARGO:**
DEPARTAMENTO:	

DATOS BÁSICOS

1. ¿Los actuales soportes con sus clientes remotos los clasifica en?:				**2. ¿Como realiza G&T los soportes o actualizaciones con sus clientes remotos?**			**3. ¿G&T cuenta con una Herramienta para transmitir archivos con sus clientes?**	
Excelente □	Bueno □	Regular X	Malo □	En Sitio X	Dial-Up X	Otra □	Si X	No □

4. ¿G&T cuenta con una aplicación automatizada que permita establecer una conexión en línea con sus clientes?		**5. ¿Desea crear DVPN con sus localidades Remotas para mejorar la calidad en el servicio?**		**6. ¿Posee Servidor Windows 2000 Server?**	
Si □	No X	Si X	No □	Si X	No □

7. ¿G&T cuenta con un servidor de Hospedaje?		**8. ¿Que tipo de Conexión tiene a Internet?**			
Si □	No X	Dial-Up □	ADSL X	FR □	Cable-Modem □

ANEXO E

Formato de Validación del Instrumento

UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIA
POSTGRADO EN CIENCIAS DE LA COMPUTACION
MENCION REDES DE COMPUTADORA

PROPUESTA DE UN DISEÑO DE SISTEMA AUTOMATIZADO CLIENTE SERVIDOR PARA REDES PRIVADAS VIRTUALES DINAMICAS (DVPN) SOBRE BANDA ANCHA ADSL

Formato de Validación del Instrumento (Ver Anexo A)

Ciudadano (a): _____

Para efectos de la evaluación correspondiente a los ítems planteados se determinará la validez de cada instrumento en los siguientes términos:

Se tomarán en cuenta los siguientes aspectos: a) **Pertinencia:** Es la correspondencia del ítem con el aspecto; b) **Claridad:** se refiere a la redacción precisa y sencilla del ítem; y c) **Congruencia:** entendida como la lógica interna del ítem.

Se le agradece seleccionar una de las 2 posibles opciones (Si/No) para cada ítems con el objetivo de señalar el grado de pertinencia, claridad y congruencia de los ítems.

	PERTINENCIA		CLARIDAD		CONGRUENCIA		
Ítem	SI	NO	SI	NO	SI	NO	OBSERVACIONES
1	□	□	□	□	□	□	_____
2	□	□	□	□	□	□	_____
3	□	□	□	□	□	□	_____
4	□	□	□	□	□	□	_____
5	□	□	□	□	□	□	_____
6	□	□	□	□	□	□	_____

ANEXO F

Formato de Validación del Instrumento

UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIA
POSTGRADO EN CIENCIAS DE LA COMPUTACION
MENCION REDES DE COMPUTADORA

PROPUESTA DE UN DISEÑO DE SISTEMA AUTOMATIZADO CLIENTE SERVIDOR PARA REDES PRIVADAS VIRTUALES DINAMICAS (DVPN) SOBRE BANDA ANCHA ADSL

Formato de Validación del Instrumento (Ver Anexo B)

Ciudadano (a): _____

Para efectos de la evaluación correspondiente a los ítems planteados se determinará la validez de cada instrumento en los siguientes términos:

Se tomarán en cuenta los siguientes aspectos: a) **Pertinencia:** Es la correspondencia del ítem con el aspecto; b) **Claridad:** se refiere a la redacción precisa y sencilla del ítem; y c) **Congruencia:** entendida como la lógica interna del ítem.

Se le agradece seleccionar una de las 2 posibles opciones (Si/No) para cada ítems con el objetivo de señalar el grado de pertinencia, claridad y congruencia de los ítems.

	PERTINENCIA		CLARIDAD		CONGRUENCIA		
Ítem	SI	NO	SI	NO	SI	NO	OBSERVACIONES
1	□	□	□	□	□	□	_____

2	□	□	□	□	□	□	
3	□	□	□	□	□	□	
4	□	□	□	□	□	□	
5	□	□	□	□	□	□	
6	□	□	□	□	□	□	
7	□	□	□	□	□	□	
8	□	□	□	□	□	□	

Barquisimeto, 18 de marzo del 2005

Prof.

Willian Polanco

Coordinador del Programa

Maestría en Ciencias de la Computación Mención: Redes de Computadoras

Yo, Alirio Jesús Marquez Perdomo titular de la C.I. N^{o} 10.282.156. En mi carácter de participante del Programa Maestría, cumpliendo con todos los requisitos exigidos por el Reglamento de Estudio de Postgrado de la Universidad Centroccidental "Lisandro Alvarado", someto a consideración de la Comisión de Estudios de Postgrado del Decanato de Ciencias y Tecnología el Proyecto del Trabajo de Grado, Titulado: Propuesta de un Diseño de Sistema Cliente Servidor para crear Redes Virtuales Privadas Dinámicas (DVPN) sobre Banda Ancha ADSL. Para optar el titulo de: Maestría en Ciencias de la Computación Mención: Redes de

Computadora. Anexo a la presente solicitud, constancia de notas y solvencia administrativa expedida por la Coordinación de Postgrado del Decanato.

Atentamente

Alirio Jesús Marquez Perdomo
C.I. 10.282.156

Barquisimeto, 18 de marzo del 2005

Prof.
Darwin Romero
Coordinador de Postgrado
Decanato de Ciencias y Tecnología

Sirva la presente para notificarle que he aceptado la Tutoría del Trabajo de Grado titulado: "Propuesta de un Diseño de Sistema Cliente Servidor para crear Redes Virtuales Privadas Dinámicas (DVPN) sobre Banda Ancha ADSL". Presentado por el Ciudadano: Alirio Jesús Marquez Perdomo para optar al titulo de: Maestría en Ciencias de la Computación. Así mismo anexo a la presente Currículo Académico y copia simple del Titulo de Postgrado.

Datos del Tutor:

Apellidos y Nombres: Pérez Arsenio.
Cédula de Identidad: 3.876.192
Profesión: Profesor
Postgrado:
Instituto donde labora: Universidad Centroccidental “Lisandro Alvarado”

ACEPTACIÓN DEL TUTOR

Por medio de la presente, en mi carácter de Tutor del Trabajo Especial de Grado titulado: “**PROPUESTA DE UN DISEÑO DE SISTEMA AUTOMATIZADO CLIENTE SERVIDOR PARA REDES PRIVADAS VIRTUALES DINAMICAS (DVPN) SOBRE BANDA ANCHA ADSL**”, presentado por el ciudadano: **ALIRIO JESUS MARQUEZ PERDOMO**, **C.I: 10.282.156**, para optar al Grado de **Magíster Scientiarum en Ciencias de la Computación**, Mención **Redes de Computadoras**, una vez realizada la correspondiente lectura y revisión considero que el mencionado trabajo reúne los requisitos y méritos suficientes para ser sometido a la evaluación por parte del jurado que se designe.

En la ciudad de Barquisimeto, al seis (06) días del mes de octubre del año dos mil cinco (2005).

ARSENIO A. PEREZ P.

C.I.: 3.876.192