PROPUESTA DE UNA VPN PROPIETARIA PARA LA MIGRACIÓN HACIA LA PLATAFORMA DE REDES COMO UNA SOLUCIÓN DE INTERCONEXIÓN DE LAS SUCURSALES NACIONALES DE LA EMPRESA VENEQUIP, S.A.

FALCÓN GRATEROL NELSON ANTONIO

UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"

Barquisimeto, 2006

UNIVERSIDAD CENTROCCIDENTAL

"LISANDRO ALVARADO"

DECANATO DE CIENCIAS Y TECNOLOGÍA

PROPUESTA DE UNA VPN PROPIETARIA PARA LA MIGRACIÓN HACIA LA PLATAFORMA DE REDES COMO UNA SOLUCIÓN DE INTERCONEXIÓN DE LAS SUCURSALES NACIONALES DE LA EMPRESA VENEQUIP, S.A.

Trabajo de Grado para optar al grado de Técnico Superior Especialista
En Tecnología de la Información y Comunicaciones

AUTOR: FALCÓN GRATEROL NELSON ANTONIO

TUTOR: PROF. WILLIAM POLANCO

Barquisimeto, 2006

DEDICATORIA

Dedico este trabajo a mi mama y a mi papa,

Por ser ustedes mi ejemplo a seguir y quienes me

Fortalecen cada día para seguir luchando y lograr

Las metas que me he propuesto

A mis hermanos y a mis hermanas por estar siempre pendientes de mí.

AGRADECIMIENTOS

A Dios Todo Poderoso, quien me guía, y me ayuda cada día en los momentos más difíciles de mi vida y con su luz me alumbra el camino correcto a seguir.

A mi Mama, por ser tú mi ángel protector, por darme todo ese amor incondicional y por ayudarme y apoyarme en todo y por estar siempre pendiente de mí y por que sé lo orgullosa que te sientes de este logro.

A mi Papa, ejemplo de constancia, por enseñarme las cosas buenas de la vida, por ser un gran ejemplo a seguir.

A mis Hermanas, Mariela y Yelitza, por que sé que también celebran conmigo este logro y por apoyarme en todo este tiempo.

A mis Hermanos, Eudy, Eliexer y Danilo, quienes han sido mis compañeros, gracias por apoyarme siempre.

A Krisselth, por estar presente en mi vida, impulsarme y darme aliento aún en los peores momentos.

Al Prof. Carlos Primera, por su apoyo incondicional en todo momento y por animarme y darme fuerzas para seguir adelante y terminar con éxito este trabajo.

A mi primo, Catire quien durante todas las fases de mis estudios universitarios realmente me ha hecho sentir que somos hermanos.

A mi Amiga, Zaida por que siempre serás mi amiga aun fuera del aula de clase

por estar siempre pendiente de que terminara este trabajo y por su ayuda incondicional prestada durante todo el periodo de clases.

A mis Amigos, Julio Inojosa, Agustín Castillo, Gabriel Silva, Miguel Quintero, por siempre estar pendiente en que terminara por brindarme su amistad y su apoyo, amigos incondicionales.

A la empresa VENEQUIP S.A., por permitirme desarrollar este trabajo en sus instalaciones y proporcionarme la información necesaria para culminar este trabajo.

Al Ing. William Polanco, por guiarme durante este proceso de aprendizaje y crecimiento personal.

A la Universidad Centroccidental Lisandro Alvarado por ser mi casa de estudios y un ente generador de personal capacitado para el campo laboral.

A todos, muchas gracias.

ÍNDICE

LISTA DE FIGURAS

FIGURAS **Pág.**

LISTA DE CUADROS

FIGURAS **Pág.**

UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGÍA
ESPECIALIZACION TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES

PROPUESTA DE UNA VPN PROPIETARIA PARA LA MIGRACIÓN HACIA LA PLATAFORMA DE REDES COMO UNA SOLUCIÓN DE INTERCONEXIÓN DE LAS SUCURSALES NACIONALES DE LA EMPRESA VENEQUIP, S.A.

Autor: Falcón Graterol, Nelson Antonio

Tutor: William Polanco

RESUMEN

El presente trabajo de investigación se realiza con la finalidad de encontrar una solución en cuanto a la sustitución del enlace de comunicación de cinco (5) de las sucursales de la empresa VENEQUIP S.A., las cuales son: Barquisimeto, Maracaibo, Caracas, Puerto La Cruz y Puerto Ordaz, para lo cual se realizó una fase de diagnóstico y así determinar la situación actual de estos enlaces. Se establecieron objetivos para el diseño, realizando a su vez un estudio de factibilidades técnica, operativa y económica para avalar dichos objetivos y el diseño propuesto. El presente estudio está enmarcado en la modalidad de proyecto factible de la línea de Investigación de redes de computación de la Universidad Centro Occidental Lisandro Alvarado, por que se logra a través del mismo, la solución del problema existente en la empresa. El diseño tiene como principal objetivo migrar del enlace existente hacia una nueva tecnología alternativa como en el caso de las conexiones Banda Ancha para establecer la red WAN de la empresa aumentando la velocidad de interconexión entre las LAN, disminuyendo costos y optimizando los procesos pertinentes a la empresa mediante la integración de voz y datos sobre una misma plataforma. Para brindar seguridad a las comunicaciones se creará una Red Privada Virtual (VPN) propietaria entre las sucursales en estudio la cual empleará los protocolos PPTP, CHAP e IPsec para el establecimiento de túneles, autenticación y encriptación de los datos respectivamente.

Palabras Claves: Enlace de comunicaciones, WAN, LAN, VPN.

INTRODUCCIÓN

El desarrollo de este trabajo propone una solución que permita optimizar el proceso de obtención de información de la empresa VENEQUIP S.A. a través de su red WAN de una manera eficaz y eficiente, en el menor tiempo posible para que esta pueda ser manipulada por el personal que en ella labora en las diferentes sucursales. Esto se alcanza realizando una sustitución del enlace existente por una nueva conexión de Voz y Datos empleando una VPN propietaria entre las sucursales de Barquisimeto, Maracaibo, Caracas, Puerto La Cruz y Puerto Ordaz, por ser estas las seleccionadas como piloto para la puesta en marcha de la plataforma, aplicando la tecnología de punta que actualmente marca pauta en el mercado. Una de estas tecnologías que resalta actualmente en dicho mercado y que es aplicable a la resolución del problema presentado por la empresa es la utilización de Acceso a Banda Ancha.

El enlace por medio de una VPN propietaria utilizando Banda Ancha permite llevar a cabo la obtención de la información de una manera más rápida, minimizando el costo del enlace que actualmente se emplea en la empresa como lo es FRAME RELAY.

El trabajo ha sido estructurado en cinco (5) capítulos en los cuales describen detalladamente los aspectos relacionados con la elaboración del proyecto.

En el primer capítulo, describe el planteamiento del problema, la justificación, así como también se plantean los objetivos tanto el general como los específicos, los

alcances y las limitaciones del trabajo.

El segundo capítulo, hace referencia a los fundamentos teóricos en los que se ha basado la investigación, los antecedentes y las bases teóricas que preceden al proyecto así como también la definición de términos básicos.

El tercer capítulo, se especifica y se describe la metodología en la que se basa el proyecto y se realiza un estudio de la factibilidad del mismo en el ámbito económico, operativo y técnico.

El cuarto capítulo, se presenta una descripción detallada de los resultados arrojados en el diagnóstico y la solución que se tomó como factible para la resolución del caso de estudio.

En el quinto capítulo, se desarrollan las conclusiones a las que se ha podido llegar durante el desarrollo del proyecto, así como también las recomendaciones que de alguna manera pudiesen optimizar la funcionalidad del diseño.

Y por último las referencias bibliográficas utilizadas para la realización de este trabajo.

CAPITULO I

EL PROBLEMA

En este capítulo se expresan aspectos básicos de la investigación como lo son: Planteamiento del Problema, Objetivo General, Objetivos Específicos, Justificación y Alcances.

PLANTEAMIENTO DEL PROBLEMA

Desde el inicio de los tiempos los individuos han tenido la necesidad de comunicarse unos con otros. Para lograrlo ha sido necesario el intercambio de información, y en la actualidad ésta se ha convertido en un factor fundamental en el desarrollo de toda la humanidad.

Con la evolución del hombre, comenzaron a formarse las comunidades, y en lo sucesivo las organizaciones donde confiablemente la comunicación se hacía mas necesaria, transformando las relaciones humanas, buscando el perfeccionamiento de la autopista de la comunicación, a través de las diferentes vías creadas hasta la actualidad, sin dejar de mencionar los factores siempre intervinientes en toda comunicación a saber, el emisor, el receptor y los canales los cuales con el avance del tiempo son cada vez mas numerosos.

En este sentido **Rodríguez (1.999)** señala: “La información ha representado, desde tiempos muy remotos, un papel muy importante en el desarrollo de la sociedad, evolucionando significativamente, presentándose de diversas formas, pero

manteniendo el mismo objetivo, la comunicación entre seres vivos". (P.10).

De acuerdo con **Rodríguez (1999)**, en la década de los sesenta las empresas desconocían la amplitud de los sistemas computacionales y la automatización de los procesos. Para ese entonces se realizaban de forma manual, por tal motivo se invertían grandes cantidades de horas hombre para realizar dichas actividades careciendo de confiabilidad y eficacia. Con la incursión de las computadoras las empresas comienzan a reducir costos y esfuerzos, aunque la automatización seguía siendo un tema del cual faltaba mucho por descubrir. Poco a poco las organizaciones comenzaron a aprovechar cada vez mas estas bondades llevando a la tecnología a consolidarse de una manera más práctica.

Según **Rodríguez (1999),** debido a las extensas cantidades de información intercambiada en las empresas, nace la necesidad de interconectar todos los departamentos, áreas y sucursales involucradas dentro de una organización buscando que el flujo de información que estas manejan se centralizara, y a su vez facilitar el acceso a ellas en el momento requerido. En la actualidad, la tecnología de redes es utilizada por todo tipo de empresas en el ámbito mundial, aunque cada vez las necesidades de comunicación e interconexión aumentan de una manera considerable permitiendo a la tecnología expandirse alrededor del mundo y abarcar zonas geográficas distantes entre sí, con la posibilidad de perfeccionar las negociaciones de las empresas y sus clientes, acortando distancias con solo marcar un número, pulsando un botón o con el uso de máquinas controladas por computadoras.

De acuerdo a la opinión de **Carlos Bellosta** (Presidente de Venequip), esta empresa no escapa a esta realidad, estando expandida por diferentes zonas geográficas del territorio nacional e internacional, requiriendo de los sistemas computacionales para permitir satisfacer las necesidades de sus clientes, generando un gran volumen de información manejada en la empresa. Información que debe estar continuamente actualizada para ser usada constantemente por las diversas áreas departamentales y áreas de negocios para la toma de decisiones de manera correcta.

De acuerdo a la información suministrada por el Sr. **Carlos Bellosta** esta empresa está dedicada a la venta y distribución de equipos y repuestos de maquinaria pesada caterpillar desde hace aproximadamente 80 años, siendo el único distribuidor autorizado de este producto en Venezuela, contando con una gran cantidad de clientes en las sucursales expandidas en todo el territorio nacional, como lo son: Barquisimeto, Caracas, Valencia, Maracaibo, San Cristóbal, Maturín, Punto Fijo, Puerto Ordaz, Puerto La Cruz, Guasare, y una sucursal ubicada en la cuidad de Miami: Venequip Machinary Sales Corporation (VMSC) y Curacao. Por el volumen de información que maneja esta empresa requiere una comunicación rápida, efectiva y confiable al momento de realizar sus negociaciones, tanto administrativas como técnicas entre las diferentes sucursales.

Esta organización siempre se ha visto en la imperiosa necesidad de mantener en sus telecomunicaciones tecnología de última generación. Desde sus inicios mantuvo conexión con líneas muertas entre sus sucursales, avanzando luego a servicios digitales dedicados, y en el presente cuenta con el servicio de

comunicaciones FRAME RELAY, el cual genera un alto costo en cuanto a arrendamiento, mantenimiento y monitoreo de los diferentes enlaces de comunicaciones existentes en la empresa. El servicio FRAME RELAY permite incrementar el ancho de banda de conexión y al requerir una ampliación del mismo, los costos de mantenimiento y monitoreo aumentan de manera proporcional.

VENEQUIP S.A. requiere ampliar el ancho de banda de los enlaces para poder mantener la operatividad y funcionalidad de sus transacciones, lo que según la gerencia nacional de sistemas les acarrearía un incremento considerable en los costos de mantenimiento y monitoreo de los enlaces FRAME RELAY, por lo que se sugiere migrar ésta a una tecnología tipo VPN propietaria que le permita mantener sus niveles de funcionamiento e incrementar su ancho de banda adaptándose a las necesidades actuales.

La prioridad de la empresa según su Misión y Visión es la satisfacción, el servicio y la atención al cliente y por tal motivo es en estas actividades donde invierte más tiempo y dinero. En este sentido, todos los usuarios de las diferentes sucursales consideran, al igual que las gerencias, que el manejo y la obtención de información de una manera eficaz, eficiente y oportuna, es una de las claves para el éxito, pues de ésta depende la satisfacción del cliente y en consecuencia la utilidad y productibilidad de la empresa.

Entre las innovaciones tecnológicas de hoy en día en el ámbito de las telecomunicaciones de voz y datos se encuentran los servicios de Banda Ancha y Las

Redes Virtuales Privadas (VPN). La primera nos ofrece rapidez de interconexión a Internet y menor costo en su utilización y la segunda nos proporciona acceso a redes privadas con niveles de seguridad garantizados mediante la autenticación y encriptación de los datos, empleando túneles de seguridad a través de Internet como medio de transporte; Dichas VPN pueden ser propietarias, en las cuales la administración de los recursos es realizada por el personal técnico de la empresa que decida implantarla, mientras que las VPN no propietarias o alquiladas corresponden a los diferentes proveedores en donde la administración es ejecutada por ellos, a tal efecto se propone el diseño de una VPN propietaria utilizando Banda Ancha para la migración de los enlaces de voz y datos FRAME RELAY existentes en las diferentes sucursales con que cuenta la empresa, como lo son: Barquisimeto, Valencia, Caracas, Maracaibo, Puerto La Cruz, Puerto Ordaz, Maturín, entre otras.

Surgen así algunas interrogantes a raíz de esta problemática, relacionadas con la disminución de costos y mejoramiento de la calidad del servicio: ¿Cuál es la situación actual de las redes de telecomunicaciones de voz y datos?, ¿Cuál es la factibilidad técnica, económica y operativa de la propuesta, ¿ Cuál es la configuración propuesta para la nueva plataforma de redes de comunicaciones de datos basada en VPN propietaria utilizando banda ancha que permita la interconexión de voz y datos de todas las sucursales nacionales de Venequip, S.A.?.

Estas interrogantes dan pie para el presente trabajo de investigación de tal forma que permita proponer el desarrollo de una plataforma de comunicaciones de voz y datos que permita dar solución a los problemas actuales en la empresa.

OBJETIVOS DE LA INVESTIGACION

OBJETIVO GENERAL

Proponer una VPN propietaria para la migración hacia la plataforma de redes basada en la tecnología vpn propietaria como una solución de interconexión de las sucursales nacionales de la empresa Venequip, S.A.

OBJETIVOS ESPECIFICOS

1. Diagnosticar la situación actual de las redes de comunicaciones de voz y datos entre las distintas sucursales nacionales de la empresa VENEQUIP S.A. realizadas a través del análisis del servicio Frame Relay existente.
2. Estudiar la factibilidad técnica, económica y operativa de la propuesta
3. Diseñar la nueva plataforma de redes de comunicaciones de datos basada en VPN propietaria utilizando banda ancha que permita la interconexión de voz y datos de todas las sucursales nacionales de Venequip, S.A.

JUSTIFICACION

El transcurrir del tiempo y el desarrollo de la sociedad han dado origen a transformaciones de índole tecnológica, económica y social, surgiendo la posibilidad de crear nuevos sistemas informáticos que satisfagan dichos cambios, con el fin de regular eficientemente el comportamiento del conglomerado social.

De acuerdo a la situación antes planteada, en el ámbito computacional, se visualiza una necesidad de cambio que se adapte a las nuevas tendencias, innovaciones, o nuevas plataformas de comunicación que ofrecen mayor valor agregado.

Por lo que a consecuencia surge la realización de este proyecto, con el propósito de ahondar en lo referente a los actuales sistemas computacionales relacionados con la interconexión de datos, el intercambio de información y las tecnologías de telecomunicaciones, de esta manera se propone una solución basada en las nuevas tendencias en tecnologías de telecomunicaciones.

Se justifica esta investigación, debido a que se pretende proporcionar a la empresa un enlace de comunicación de voz y datos para su conexión brindando rapidez y confiabilidad en las transacciones entre las diferentes sucursales. La propuesta de migración hacia una vpn propietaria y la utilización de la misma pretenden beneficiar enormemente a la empresa ya que con este servicio se incrementa el ancho de banda, y se contribuye a disminuir los costos en conexión, monitoreo y mantenimiento de los enlaces actuales. Paralelamente con esta tecnología de comunicaciones se lograra un gran impacto en cuanto a la confiabilidad de las transacciones realizadas, proporcionando altos niveles de seguridad de los datos y optimizar los procesos de obtención de información, todo ello gracias a los protocolos de comunicaciones, métodos de transporte de datos, métodos de autenticación y a los niveles de encriptación que soporta la tecnología propuesta.

Con esta tecnología los usuarios remotos podrán hacer sus transacciones desde cualquier ubicación geográfica con solo tener acceso a Internet, lo que permitirá que puedan tener acceso rápido a la información que requieren en cualquier lugar donde se encuentren. Si requieren conectarse desde sus casas también lo podrán hacer con solo tener acceso a Internet o a una línea telefónica.

Los resultados encontrados en la misma traerán beneficios a la sociedad y en especial al sector empresarial a quien les compete primordialmente esta materia, de interconexiones de sucursales y seguridad en sus transacciones entre las mismas, pues con ellos se aclaran las interrogantes formuladas y los objetivos propuestos. Asimismo, los resultados pueden significar un valioso aporte a la Universidad Centroccidental Lisandro Alvarado, específicamente al Decanato de Ciencias y Tecnología, por cuanto sus estudiantes y egresados pudieran obtener información precisa con relación a esta materia. Sirviendo también como antecedente y marco de referencia a nuevas investigaciones que tengan como propósito objetivos de esta índole.

ALCANCES Y LIMITACIONES

1. Integración de voz y datos en la misma plataforma.
2. Otorgar portabilidad a la red de la empresa Venequip, S.A.
3. De acuerdo a las necesidades de la empresa solo se realizara la migración a vpn propietaria a las sucursales de: Caracas, Maracaibo, Puerto La Cruz, Puerto Ordaz, Barquisimeto y Valencia.

4. Para la implementación y puesta en marcha de la propuesta solo se consideran los proveedores de acceso a Internet nacionales, que presten servicio en la zona donde este ubicada cada sucursal involucrada en la migración, entre ellos CANTV, MOVISTAR, entre otros.
5. A través de la puesta en marcha de la migración hacia vpn propietaria se tendrá acceso a los servicios de: Correo electrónico y acceso a los sistemas administrativos de la empresa.

CAPITULO II

MARCO TEORICO

Este capítulo está compuesto por varios puntos como lo son: Antecedentes, Bases Teóricas y Definición de Términos.

En los antecedentes se refieren los trabajos previos publicados (como trabajos especiales de grado, tesis y trabajos de ascenso) que guardan relación con la presente investigación. Las bases teóricas exponen la teoría que de una u otra forma está estrechamente relacionada con el tema de investigación como lo es todo lo relativo a redes virtuales privadas y las redes de área local y redes de área amplia. La definición de términos se refiere a conceptos no expuestos en las bases teóricas, pero que son necesarios de conocer para que cualquier persona que no sea especialista en el tema pueda entender fácilmente la teoría presentada.

El aporte que los siguientes antecedentes brindan a esta investigación radica en la información que suministran con respecto a la conformación y diseño de redes LAN y WAN, permitiendo así revisar y analizar diversidad de enfoques utilizando las diferentes plataformas de interconexión que existen en el mercado Nacional e Internacional haciendo mayor énfasis en el ámbito regional.

ANTECEDENTES DE LA INVESTIGACIÓN

Rodríguez, P. (2.003), en su trabajo titulado **"Interconexión de Voz, Datos y Video para la empresa Inversiones Tecnológicas C.A."**, para su trabajo de grado

de la Universidad Fermín Toro, propone diseñar una plataforma de interconexión que le permita a la empresa Inversiones Tecnológicas C.A. encontrar una solución a los problema que actualmente atraviesa en cuanto a la comunicación entre las diferentes sucursales que la conforman, pretende garantizar el manejo y obtención de la información de manera eficaz, eficiente y oportuna, basándose en la interconexión de Voz, Datos y Video de la empresa; buscando establecer la realización de videoconferencia entre las diferentes sucursales, transmisión de voz sobre el protocolo TCP/IP (VoIP) y dotar de portabilidad a la misma para centralizar toda la información mediante la plataforma VPN propietaria que le garantice la seguridad y optimización de sus comunicaciones.

En este trabajo se presenta un ejemplo muy claro acerca de las comunicaciones a través de voz sobre IP, en cuanto a conceptos y definiciones, ventajas y desventajas de la misma, protocolos de comunicación necesarios para el empleo de esta, equipos con tecnología de ultima generación capaz de soportar esta nueva herramienta de las telecomunicaciones, así como también la configuración y disponibilidad en el mercado nacional de estos equipos. De igual manera se explica la utilización de VPN propietaria, los equipos necesarios y la configuración de estos en cuanto a protocolos de seguridad y de distribución de ancho de banda para ser más óptima la interconexión entre sucursales.

Arévalo J. (2003), en su trabajo titulado **"Como escoger e implementar una vpn conceptos teóricos y prácticos"**, expone toda una serie de elementos tecnológicos que han sido usados desde el inicio de las telecomunicaciones para

interconectar sucursales de empresas. También explica en su trabajo en que consisten las tecnologías VPN, así como los protocolos usados para implementarlas, los tipos de vpn usadas actualmente, niveles y tipos de encriptamiento así como los tipos de túneles usados para tener acceso a las redes privadas de empresas. El propósito fundamental de este trabajo es mostrar las características más relevantes de las tecnologías vpn para así escoger aquella que se adapte a la realidad que se estudie. Este trabajo fue realizado en la universidad del Valle en Colombia.

Mendoza, M. (2.002), en su trabajo titulado **"Propuesta de la Instalación de una Red Privada Virtual (VPN) empleando la Red Híbrida Nodal de Fibra Óptica y Cable Coaxial (Hfc) de la empresa Intercable"**, propone la instalación de una Red Privada Virtual (VPN) empleando la Red Híbrida Nodal de Fibra Óptica y Cable Coaxial de la empresa Intercable. El proyecto se sustenta en la interacción de equipos de comunicación de red de los cuales forman una VPN para la región de Barquisimeto con visión de expansión hacia las principales ciudades de Venezuela. El servicio propuesto se basa en la autenticación y encriptación de los datos empleando túneles de seguridad a través de Internet como medio de transporte, bajo protocolo IP.

Este trabajo aporta información en cuanto a VPN, funcionamiento, ventajas y desventajas, protocolos de comunicación más factibles utilizados por la misma, nos presenta ejemplos de conexión y equipos necesarios para la configuración de la misma.

Jeanton, H. (2.002), en su trabajo titulado **"Proponer una Red de Área**

Extensa (WAN), para Interconectar las Redes Locales (LAN) de las Plantas Embotelladoras de Grupo Terepaima", propone una red extensa WAN para interconectar las redes LAN de las plantas embotelladoras del Grupo Terepaima. El proyecto busca alcanzar un avance tecnológico para la empresa, que aumente el rendimiento de las actividades de la misma, así como favorecer los procesos de toma de decisiones en cuanto a clientes, proveedores, empleados, entre otros. El proyecto permite la conexión de siete (7) plantas embotelladoras, que poseen redes locales y un depósito del mismo grupo. Cabe destacar que la propuesta abarca los detalles necesarios en cuanto a funcionamiento, seguridad y precios se refiere. Con esto cada sede de la embotelladora dispone de la información veraz, oportuna y completamente actualizada de las diferentes plantas cuando sea requerido.

Camacaro, D. (2.002), en su trabajo titulado **"Propuesta de Redes LAN y MAN para la Empresa ENELBAR",** se propone la implementación de redes de Área Local (LAN) y redes de Áreas Metropolitanas (MAN) para la Energía Eléctrica de Barquisimeto, C.A (Enelbar) basándose en una propuesta factible de redes de computadoras conformada por siete (7) redes de Área Local (LAN), una Red de Área Metropolitana (MAN) y una red de Área Extensa (WAN). Todas estas permitirán el acceso a los diferentes sistemas de información con que cuenta la empresa desde cada una de sus localidades. El diseño de las Redes se basa en una topología tipo estrella.

De los trabajos anteriormente citados puede observarse que se manifiesta en los mismos un gran interés por parte de las empresas involucradas en interconectar diversas sedes o sucursales, resaltando de manera muy importante la disponibilidad

de la información actualizada, usando como medio intermediario las tecnologías de información basadas en redes LAN y WAN, así como también enlaces de banda ancha y equipos tecnológicos de última generación.

BASES TEÓRICAS

La evolución de la tecnología a lo largo de los tiempos ha sido mencionada por el autor **Tanenbaum (2000)** como dominada por una sola en los tres últimos siglos. La etapa de los grandes sistemas mecánicos que acompañaron la Revolución Industrial se establece en el siglo XVIII. La época de la máquina de vapor marco la pauta durante el siglo XIX. Por ultimo el avance más relevante para la tecnología ha sido la recolección, procesamiento y distribución de información cuya etapa es del siglo XX. Entre otros adelantos, más importantes de la actualidad se destacan la instalación de redes telefónicas en todo el globo terráqueo, el descubrimiento de los medio de comunicación como la radio y la televisión, la invención y desarrollo de las computadoras, así como la puesta en orbita de los satélites de comunicación.

Todo lo antes expuesto ha dado origen a un procesamiento de información con mayor rapidez. Empresas con sucursales en diferentes zonas geográficas del país, con el pasar del tiempo tendrán la facilidad de acceder de manera rápida y directa a las operaciones que cada una de sus oficinas dependientes haya realizado con el único requisito de oprimir un botón. El crecimiento de las facilidades para la recolección, procesamiento y distribución de información, la solicitud de más modernos procesadores de información originan su desarrollo con gran celeridad.

Tanto las grandes empresas como las pequeñas, con el transcurrir del tiempo se han vuelto más y más dependientes del mundo de las computadoras, el cual ha crecido a pasos agigantados en un lapso de tiempo reducido. Anteriormente las compañías contaban con pocas computadoras, sin embargo el uso de estos equipos se ha vuelto indispensable, tomando en cuenta un gran número de computadoras separados pero interconectados, que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de *Redes de computadores*. Estas dan a entender una colección interconectada de computadores autónomos. Se dice que los mismos están interconectados, si son capaces de intercambiar información.

OBJETIVOS DE LAS REDES

El primero de los objetivos, según **Carballar (2002**), las redes en general, consisten en "compartir recursos", es decir, el hacer que todos los programas, datos y equipos estén accesibles para cualquier usuario de la red que lo solicite (sin interesar la ubicación física del recurso y del usuario). Esto significa que aunque exista una larga distancia entre el usuario y recursos, datos o programas, esto no seria impedimento para que los pueda manejar como si estuviese en el lugar de origen.

El segundo objetivo radica en proveer una gran confiabilidad, al poseer fuentes alternativas de suministro. Es decir, los archivos de una maquina pueden copiarse en dos o tres computadores mas, de forma tal que si una de ellas no se encuentra a la disposición del usuario, podría emplearse uno de los duplicados. Aunado a la existencia de varios equipos significando que si una de ellas deja de

trabajar, las resto de las máquinas son capaces de suplir de su labor, aunque el rendimiento global sea menor.

Un tercer objetivo es el ahorro económico, abaratando los costos. Los equipos pequeños poseen una relación de mejor costo/rendimiento, comparada con la ofrecida por las máquinas grandes. Estas son, a grandes rasgos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es miles de veces mayor. Este desequilibrio ha ocasionado que muchos diseñadores de sistemas construyan sistemas constituidos por poderosos computadores personales, uno por usuario, con los datos guardados en una o más máquinas que funcionan como servidor de archivos compartidos.

Una red, además, puede proporcionar un poderoso medio de comunicación entre personas que se encuentran geográficamente separados. Con una red es relativamente fácil para dos o más personas que se encuentran bajo estas condiciones, escribir informes juntos y cuando uno de ellos hace un cambio permite que el otro lo acceda de inmediato, en lugar de esperar varios días para recibirlos por carta. Esta rapidez hace que la cooperación entre grupos de individuos y que anteriormente había sido imposible de establecer, pueda hoy día realizarse.

Para la conceptualización de las redes es indispensable realizar una diferenciación entre el termino de redes físicas y de redes de comunicación.

Con relación a las redes físicas, **Huidobro (2000**), expresa en cuanto al término de la estructura física, los modos de conexión física, los flujos de datos, entre

otros; se señala que una red se puede constituir por dos o más computadores que comparten determinados recursos, bien sea hardware como impresoras, sistemas de almacenamiento, entre otros o software como aplicaciones, archivos, datos, entre otros.

En cuanto a las redes de comunicación, se manifiesta de manera óptima la utilización de las redes, es importante mencionar la existencia de diversos componentes en estas, como lo son, un componente humano que realiza la comunicación, un componente tecnológico encargado de suministrar equipos (computadoras, televisión, telecomunicaciones); y por último, un componente administrativo como organizaciones o instituciones que mantienen los servicios. Para definir una red, se ha de tener presente más que el uso de varias computadoras conectadas entre sí, constituidas por varias personas que solicitan, proporciona e intercambian experiencias e informaciones a través de sistemas de comunicación, con el principal objetivo de conseguir el mayor número de ventajas posibles.

Ahora bien, de esta manera queda determinado que una red se fundamenta en dos o más computadores entrelazados compartiendo recursos como programas, impresoras, carpetas, archivos, entre otros, y con la capacidad de comunicarse de forma electrónica. Los cables, las líneas de teléfono, las ondas de radio, los satélites, entre otros equipos pueden tomarse como los medios físicos por los cuales están entrelazadas las redes. El primordial objetivo de una red debe ser el de alcanzar que todos sus programas, datos, recursos, estén al acceso de cualquiera de los usuarios que integran la red, sin interesar la ubicación física del recurso y del usuario.

EL MODELO OSI

El modelo de referencia OSI es la arquitectura de red actual más prominente, el objetivo de este modelo es el de desarrollar estándares para la interconexión de sistemas abiertos (Open System Interconnection, OSI). Este término de OSI es el nombre dado a un conjunto de estándares para las comunicaciones entre computadoras, terminales y redes. Diferentes autores, como lo son **Tanenbaun (1.999**) y **Naranjo (2001)**, señalan que este modelo está diseñado para permitir la conectividad entre equipos con software y hardware diferentes.

Esto es posible ya que dicho modelo separa el problema de la conectividad en siete pequeños problemas, los cuales denomina capas, éste es un modelo de 7 capas, donde cada capa define los procedimientos y las reglas (protocolos normalizados) que los subsistemas de comunicaciones deben seguir, para poder comunicarse con sus procesos correspondientes de los otros sistemas, esto permite que un proceso que se ejecuta en una computadora, pueda comunicarse con un proceso similar en otra computadora, si tienen implementados los mismos protocolos de comunicaciones de capas OSI **(Ver Figura.1)**. Algunas de las funciones de cada capa o nivel se describen a continuación:

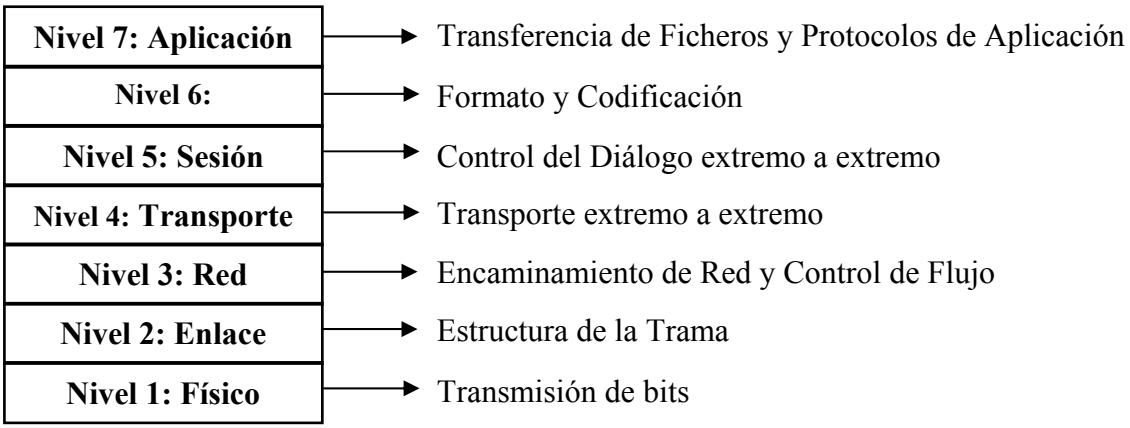

Figura 1
Modelo OSI de 7 Capas o Niveles.
Fuente: www.cisco.com

Capa 1. Capa Física

En esta capa es donde se definen las características físicas como lo son los componentes y conectores mecánicos, los niveles de tensión, es decir las condiciones eléctricas, y se determinan las características funcionales de la interfaz.

Esta capa recibe cuadros o paquetes de la capa 2, los convierte en señales eléctricas u ópticas equivalentes a los bits que componen aquellos, y los coloca en el medio de transmisión. El proceso se invierte en recepción.

Generalmente se reconocen cuatro aspectos principales:

- Solamente reconoce bits individuales, no reconoce caracteres ni tramas multicaracter. Por ejemplo RS-232 y RS-449.
- Mecánico: Se refiere básicamente al tipo de conector a usar, como RJ-11, RJ-45,

BNC, DB-9, DB-25, entre otros.

- Eléctrico: Niveles de tensión de transmisión y recepción (la señal de recepción tiene un nivel mucho menor), impedancia de la línea, interferencias, duración de los bits, forma de onda en recepción de los pulsos, entre otros.
- Procedimientos: Cómo se establece una comunicación y se intercambian datos. Es de particular importancia en las comunicaciones punto a punto.

Capa 2. Capa de Enlace de Datos

La capa de enlace de datos es la que proporciona los medios para asegurar confiabilidad a la cantidad de bits que se reciben de la capa física, y de esta forma se orienta a resolver los problemas planteados por la falta de fiabilidad de los circuitos de datos, agrupándose los datos recogidos del nivel de red para su transmisión, en ella se detectan y controlan los errores formando tramas que incluyen además bits de redundancia y control; además regula el flujo de las tramas para sincronizar su emisión y recepción.

Capa 3. Capa de Red

En esta capa se determina el establecimiento de la ruta, es decir observa las direcciones del paquete para determinar los métodos de conmutación y enrutamiento y controla el nivel de congestión, proporcionando los medios para establecer, mantener y liberar la conexión y el intercambio de datos entre el origen y el destino, a través de una red donde existe una malla de enlaces y nodos, entre sistemas abiertos.

Capa 4. Capa de Transporte

Esta capa se ocupa de asegurar que se reciban todos los datos y en el orden adecuado, aceptando los datos del nivel de sesión, fragmentándolos en unidades más pequeñas en caso necesario y los pasa al nivel de red. Regula el control de flujo del tráfico de extremo a extremo.

Su misión es optimizar los servicios del nivel de red y corregir las posibles deficiencias del servicio, proporciona los procedimientos de transporte precisos, con independencia de la red o del soporte físico empleado y reconoce los paquetes duplicados.

Capa 5. Capa de Sesión

Provee mecanismos para organizar y estructurar diálogos entre procesos de aplicación. Actúa como un elemento moderador capaz de coordinar y controlar el intercambio de los datos. A partir de la capa de Sesión las relaciones principales son con las propias aplicaciones, de hecho en muchos casos los protocolos de esta capa se integran con los de las capas superiores de presentación y aplicación. Controla la integridad y el flujo de los datos en ambos sentidos.

Esta capa básicamente administra el establecimiento, mantenimiento y terminación entre dos entidades de presentación, que establecen una conexión o sesión, y se sincroniza la sesión. Se trata entonces de controlar el diálogo que mantienen dichas entidades.

Capa 6. Capa de Presentación

En esta capa se efectúa la conversión de datos entre códigos diferentes, el formateo o transformación de sintaxis de dichos datos por ejemplo para su presentación en pantalla o ventanas de ella, incluyendo el manejo de caracteres, la compresión y descompresión de datos, y el encriptado y desencriptado de la información.

En muchos casos los protocolos de esta capa son parte del sistema operativo y hasta de las propias aplicaciones.

Capa 7. Capa de Aplicación

Esta capa provee el acceso al ambiente de una red de las aplicaciones propiamente dichas. Las funcionalidades principales radican en cuestiones administrativas referidas a la red. Así como servicio de directorios, procesamiento de transacciones, manejo de correo electrónico, terminales virtuales y transferencia de archivos (FTP).

CLASIFICACIÓN DE LAS REDES

Huidobro (2002), afirma que si las computadoras se encuentran dentro de un mismo ámbito geográfico como una habitación, un edificio o un campus (como máximo del orden de 1 Km.) se denominan con el nombre de red de área local LAN (Local Area Network). Si la distancia es del orden de la decena de kilómetro entonces se está ante una red denominada con el nombre de red de área metropolitana MAN

(Metropolitan Area Network). Si la distancia es de varios cientos de kilómetros entonces se habla de una red de área extensa WAN (Wide Area Network) y si se trata de una red que cubre todo el planeta entonces se habla de Internet.

Hay tres (3) parámetros característicos en una red de computadores: su tamaño, su tecnología de transmisión y su topología.

Las LAN están restringidas en cuanto a su tamaño y por ello se puede calcular su velocidad de transmisión. El medio de transmisión consiste en un cable al que están conectadas todas las máquinas. Su topología, es decir la forma en que enlazan las computadoras puede ser en bus o en anillo, entre otros; tal y como se verá más adelante.

Las redes de área amplia o WAN están formadas por un conjunto de máquinas destinadas a ejecutar programas de aplicación llamadas Host las cuales están a su vez conectadas por una subred. Esta subred tiene dos componentes distintos: las líneas de transmisión que mueven bits de una máquina a otra y los elementos de conmutación que conectan dos o más líneas de transmisión con el objeto de escoger una línea de salida para reenviarlos.

Por último, se debe indicar la existencia de interredes formadas por redes LAN y WAN a veces diferentes entre sí, conectadas mediante pasarelas que son máquinas que efectúan la labor de conexión y traducción.

Redes de Área Local LAN

Según Tanenbaum (2000), una red de área local es un conjunto de elementos físicos y lógicos que proporcionan interconexión a una gran variedad de dispositivos de comunicación de información en un área privada restringida (recinto, edificio, campus, entre otros.)

En esta definición formal aparecen los siguientes elementos con significado propio: conjunto de elementos físicos y lógicos que proporcionan interconexión, es decir, son un conjunto de elementos que configuran una red de comunicación que facilita la transmisión de bits entre un dispositivo y otro. Por otra parte, se habla de una gran variedad de dispositivos de comunicación, esto es, a la red pueden conectarse dispositivos de todo tipo tales como computadoras, terminales, periféricos, sensores, aparatos telefónicos, equipos facsímil, entre otros.

Otro aspecto incluido en la definición es el ámbito geográfico de la red local que, en general, es pequeño y no sale más allá de los límites de un departamento situado en un edificio o conjunto de edificios próximos. Por último cabe destacar el carácter privado de una red local que, generalmente, no necesita otros medios de comunicación suministrados por empresas o redes de comunicación.

Las características más representativas de una red de área local son las siguientes:

- **Alcance.** El área de conexión se limita a una extensión moderada, generalmente desde unos pocos metros a unos pocos kilómetros.
- **Velocidad de transmisión.** En estas redes, la velocidad es elevada en

comparación con otros circuitos de comunicación, variando entre 1 y 100 Mbps.

- **Conectividad.** Además de que todos los dispositivos conectados a una red de área local puedan comunicarse entre sí, también se incluye la capacidad de conexión con otras redes locales o de área extensa como pueden ser la red telefónica conmutada o las redes SNA, X.25, TCP/IP, entre otros.
- **Propiedad Privada.** Una red de área local es propiedad de la organización o empresa en lugar de ser un elemento público para otros usos externos. Por lo general, la organización es propietaria de la red y todo el conjunto de dispositivos conectados a ella.
- **Fiabilidad.** Estas redes presentan una baja tasa de error en las transmisiones de datos en comparación con el resto de modalidades de comunicación.
- **Compartición de recursos.** Permiten la integración en la misma red de una gran diversidad de dispositivos. Los recursos de almacenamiento, las impresoras y los elementos de comunicación pueden ser utilizados por todas las estaciones de trabajo.

Las ventajas más significativas que proporcionan las redes de área local son:

- **Recursos compartidos.** Los dispositivos conectados a la red comparten datos, aplicaciones, periféricos y elementos de comunicación.
- **Conectividad a nivel local.** Los distintos equipos que integran la red se encuentran conectados entre sí con posibilidades de comunicación.

- **Proceso distribuido.** Las redes de área local permiten el trabajo distribuido, es decir, cada equipo puede trabajar independientemente o cooperativamente con el resto.
- **Flexibilidad.** Una red local puede adaptarse al crecimiento cuantitativo referido al número de equipos conectados, así como adaptarse a cambios cualitativos de tipo tecnológico.
- **Disponibilidad y fiabilidad.** Un sistema distribuido de computadoras conectadas en red local es inherentemente más fiable que un sistema centralizado.
- **Cableado estructurado.** Estas redes por sus cableados y conexiones, facilitan mucho la movilidad de los puestos de trabajo de un lugar a otro
- **Optimización.** Las redes de área local permiten la máxima flexibilidad en la utilización de recursos, estén estos en la computadora central, el procesador departamental o la estación de trabajo, facilitando, por tanto, la optimización del coeficiente prestaciones/precio del sistema.

El estado actual del hardware y software de redes de área local hace que las desventajas expuestas puedan paliarse mediante el empleo de las técnicas adecuadas, normalmente realizadas por programas de comunicaciones, gestión de red y seguridad.

Estándares de Redes Lan

Ethernet

Huidobro (2000), refiere que, Xerox Parc, construyó un sistema de 2.94 Mbps, para conectar más de 100 estaciones de trabajo utilizando un cable de 1 kilómetro, se denominó Ethernet (red de éter). Es hoy en día uno de los estándares para las redes de área local, se define como un modo de acceso múltiple Access/collision detection (CSMA/CD). Cuando una estación quiere acceder a la red escucha si hay alguna transmisión en curso, si no hay ninguna, ésta transmite.

Puede ocurrir que dos estaciones emitan al mismo tiempo, se producirá una colisión, lo cual queda resuelto con los sensores de colisión que detectan esta situación y fuerzan a una retransmisión de la información.

Ethernet es la arquitectura de red más popular en todo el mundo. Sigue la norma 802.3 de la lEEE, usa el método de acceso CSMA/CD y funciona a velocidad de 10 Mbps.

Puede usar fácilmente protocolos de comunicaciones como el TCP/IP del Unix hoy mucho más extendido gracias al Internet. De esta manera se pueden acceder computadoras de mayor porte.

Si bien la topología original del Ethernet es de un bus lineal, es decir, de una conexión que va de un extremo a otro, a lo largo del cual, se van "colgando" los diferentes equipos, hoy en día más del 95 % de las instalaciones nuevas se hacen con

la topología en estrella.

El sistema se llama 10 BASE-T. El 10 es de 10 Mbps. Base indica que la información se transmite tal como se genera (los electrónicos dicen banda base) sin trasladarse en el espectro de frecuencias, y la T se refiere al medio de conexión que es el par trenzado sin blindar, más conocido como UTP.

La configuración se basa en un dispositivo central llamado hub, que hace de repetidor de las señales que circulan entre las PCs **(Ver Figura 2)**. Entonces el paquete que genera un equipo aparece en todas las ramas de la estrella.

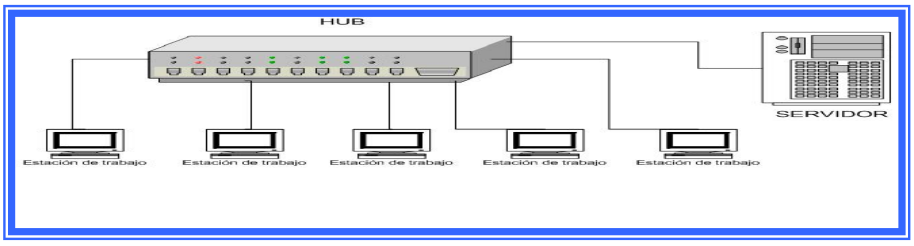

Figura 2
Configuración 10 Base T (UTP)
Fuente : www.cisco.com

Local Talk

Fue desarrollado por Apple Computer Inc. para computadores Macintosh, al igual que el método de acceso al medio CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Este método se diferencia en que el computador anuncia su transmisión antes de realizarla.

Mediante el uso de adaptadores Local Talk y cables de par tranzado (UTP)

especiales, se puede crear una red de computadoras a través del puerto serie. El sistema operativo de estos establece relaciones punto a punto sin necesidad de software adicional.

Con este protocolo se pueden utilizar topologías de bus, estrella o árbol usando cable UTP, pero la velocidad de transmisión es muy inferior a la de Ethernet.

Token Ring

El protocolo Token Ring fue desarrollado por IBM a mediados de los años 80, el modo de acceso al medio está basado en el traspaso del testigo o token passing, en una red Token Ring, las computadoras se conectan formando un anillo y un testigo o token electrónico pasa de una computadora a otra.

Cuando este testigo es recibido, se está en la disposición de emitir datos, los cuales viajan por el anillo hasta llegar a la estación receptora. Las redes Token Ring se montan sobre topologías estrella, cableadas con par trenzado o fibra óptica.

Topología de Redes

Según Naranjo, Alice los nodos de red (las computadoras), necesitan estar conectados para comunicarse. A la forma en que están conectados los nodos se le llama topología. Una red tiene dos diferentes topologías: una física y una lógica. La topología física es la disposición física actual de la red, la manera en que los nodos están conectados unos con otros. La topología lógica es el método que se usa para comunicarse con los demás nodos, la ruta que toman los datos de la red entre los

diferentes nodos de la misma. Las topologías físicas y lógica pueden ser iguales o diferentes. Las topologías de red más comunes son: bus, anillo y estrella.

Red en Bus

En una topología de bus, cada computadora está conectada a un segmento común de cable de red. El segmento de red se coloca como un bus lineal, es decir, un cable largo que va de un extremo a otro de la red, y al cual se conecta cada nodo de la misma. El cable puede ir por el piso, por las paredes, por el techo, o puede ser una combinación de éstos, siempre y cuando el cable sea un segmento continuo. (Ver Figura 3).

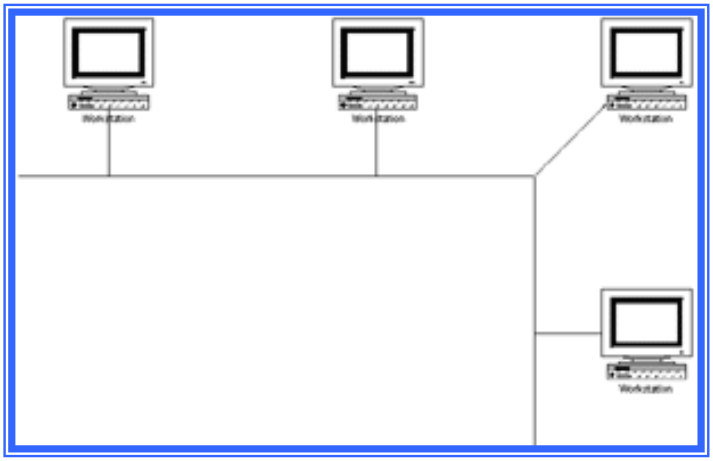

Figura 3
Topología Bus
Fuente: www.cisco.com

Red en anillo

Una topología de anillo consta de varios nodos unidos formando un círculo lógico. Los mensajes se mueven de nodo a nodo en una sola dirección. Algunas redes de anillo pueden enviar mensajes en forma bidireccional, es decir, pueden enviar y

recibir información, no obstante, sólo son capaces de enviar mensajes en una dirección cada vez. La topología de anillo permite verificar si se ha recibido un mensaje. En una red de anillo, las estaciones de trabajo envían un paquete de datos conocido como flecha o contraseña de paso. **(Ver Figura** 4**)**.

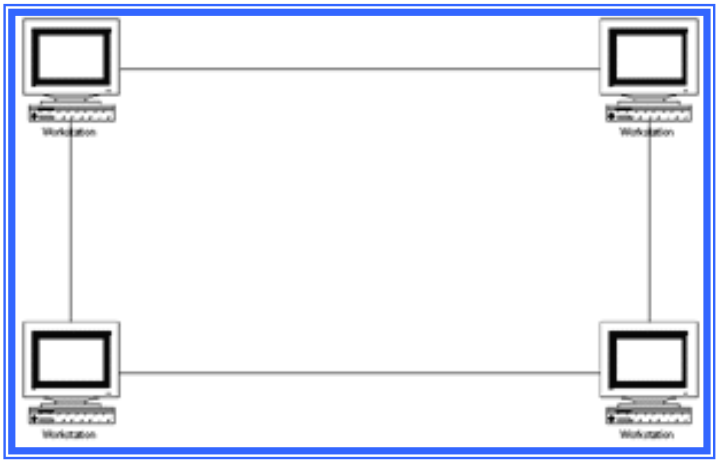

Figura 4
Topología Anillo
Fuente: www.cisco.com

Red en estrella

Uno de los tipos más antiguos de topologías de redes es la estrella, la cual usa el mismo método de envío y recepción de mensajes que un sistema telefónico, ya que todos los mensajes de una topología LAN en estrella deben pasar a través de un dispositivo central de conexiones conocido como concentrador de cableado, el cual controla el flujo de datos. **(Ver Figura 5)**.

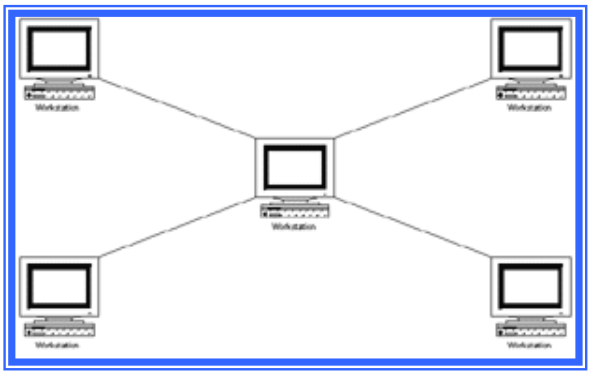

Figura 5
Topología Estrella
Fuente: www.cisco.com

Redes de Área Extensa (WAN)

Según Tanenbaum (2000), cuando se llega a un cierto punto deja de ser poco práctico seguir ampliando una Red de área local LAN. A veces esto viene impuesto por limitaciones físicas, aunque suele haber formas más adecuadas o económicas de ampliar una red de computadoras. Dos de los componentes importantes de cualquier red son la red de teléfono y la de datos. Son enlaces para grandes distancias que amplían la LAN hasta convertirla en una red de área extensa (WAN). Casi todos los operadores de redes nacionales (como DBP en Alemania o British Telecom en Inglaterra) ofrecen servicios para interconectar redes de computadoras, que van desde los enlaces de datos sencillos y a baja velocidad que funcionan basándose en la red pública de telefonía hasta los complejos servicios de alta velocidad (como FRAME RELAY y SMDS - Synchronous Multimegabit Data Service, entre otros) adecuados para la interconexión de las LAN. Estos servicios de datos a alta velocidad suelen denominarse conexiones de banda ancha. Se prevé que proporcionen los enlaces

necesarios entre LAN para hacer posible lo que han dado en llamarse autopistas de la información.

Una WAN se extiende sobre un área geográfica amplia, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar aplicaciones, estas máquinas se llaman Hosts. Los hosts están conectados por una subred de comunicación. El trabajo de una subred es conducir mensajes de un hosts a otro. La separación entre los aspectos de comunicación de la red y los aspectos de aplicación, simplifica enormemente el diseño total de la red.

En muchas redes de área amplia, la subred tiene dos componentes distintos: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión, también llamadas circuitos o canales mueven los bits de una máquina a otra.

Los elementos de conmutación son computadoras especializadas que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación debe escoger una línea de salida para enviarlos. Aunque no existe una terminología estándar para designar estas computadoras, se les denomina nodos conmutadores de paquetes, sistemas intermedios y centrales de conmutación de datos. También es posible llamarles simplemente enrutadores.

En casi todas las WAN, la red contiene numerosos cables o líneas telefónicas, cada una conectada a un par de enrutadores. Si dos enrutadores que no comparten un cable desean comunicarse, deberán hacerlo indirectamente, por medio de otros dos enrutadores. Cuando se envía un paquete de un enrutador a otro a través de uno o más

enrutadores intermedios, el paquete se recibe completo en cada enrutador intermedio, se almacena hasta que la línea de salida requerida está libre, y a continuación se reenvía. Una subred basada en este principio se llama, de punto a punto, de almacenar y reenviar, o de paquete conmutado. Casi todas las redes WAN excepto aquellas que usan satélites tienen subredes de almacenar y reenviar. Cuando los paquetes son pequeños y el tamaño de todos es el mismo, suelen llamarse celdas.

Una posibilidad para una WAN es un sistema de satélite o de radio en tierra. Cada enrutador tiene una antena por medio de la cual puede enviar y recibir. Todos los enrutadores pueden oír las salidas enviadas desde el satélite y en algunos casos pueden oír también la transmisión ascendente de los otros enrutadores hacia el satélite. Algunas veces los enrutadores están conectados a una subred punto a punto de gran tamaño, y únicamente algunos de ellos tienen una antena de satélite. Por su naturaleza las redes de satélite son de difusión y son más útiles cuando la propiedad de difusión es importante.

Constitución de una Red de Área Extensa (WAN)

Según Tanenbaum (2000), la red consiste en computadores de conmutación (ECD) interconectados por canales alquilados de alta velocidad. Cada ECD utiliza un protocolo responsable de encaminar correctamente los datos y de proporcionar soporte a los computadores y terminales de los usuarios finales conectados a los mismos. La función soporte del ETD se denomina a veces PAD (ensamblador / desamblador de paquetes). Para los ETD, el ECD es un dispositivo que los aísla de la

red. El centro de control de red (CCR) es el responsable de la eficiencia y fiabilidad de las operaciones de la red.

Componentes Físicos

Línea de Comunicación: Medios físicos para conectar una posición con otra con el propósito de transmitir y recibir datos.

Hilos de Transmisión: En comunicaciones telefónicas se utiliza con frecuencia el termino "pares" para describir el circuito que compone un canal. Uno de los hilos del par sirve para transmitir o recibir los datos, y el otro es la línea de retorno eléctrico.

Clasificación de las Líneas de Conmutación

Líneas Conmutadas: Un servicio de línea conmutada no requiere conexiones permanentes entre dos puntos fijos. En su lugar, permite a los usuarios establecer conexiones temporales entre múltiples puntos cuya duración corresponde a la de la transmisión de datos. Existen dos tipos de servicios conmutados: servicios de conmutación de circuitos, similares a los servicios utilizados en las llamadas telefónicas; y los servicios de conmutación de paquetes, que se ajustan mejor a la transmisión de datos.

Líneas Dedicadas: Líneas de comunicación que mantienen una permanente conexión entre dos o más puntos. Estas pueden ser de dos o cuatro hilos.

Líneas Punto a Punto: Enlazan dos DTE

Líneas Multipunto: Enlazan tres o más DTE

Líneas Digitales: En este tipo de línea, los bits son transmitidos en forma de señales digitales. Cada BIT se representa por una variación de voltaje y esta se realiza mediante codificación digital.

Tipos de Redes WAN

Conmutadas por Circuitos: Redes en las cuales, para establecer comunicación se debe efectuar una llamada y cuando se establece la conexión, los usuarios disponen de un enlace directo a través de los distintos segmentos de la red.

Conmutadas por Mensaje: En este tipo de redes el conmutador suele ser un computador que se encarga de aceptar tráfico de los computadores y terminales conectados a él. El computador examina la dirección que aparece en la cabecera del mensaje hacia el que debe recibirlo. Esta tecnología permite grabar la información para atenderla después. El usuario puede borrar, almacenar, redirigir o contestar el mensaje de forma automática.

Conmutadas por Paquetes: En este tipo de red los datos de los usuarios se descomponen en trozos más pequeños. Estos fragmentos o paquetes, estás insertados dentro de informaciones del protocolo y recorren la red como entidades independientes.

Redes Orientadas a Conexión: En estas redes existe el concepto de multiplexión de canales y puertos conocido como *circuito o canal virtual*, debido a que el usuario

aparenta disponer de un recurso dedicado, cuando en realidad lo comparte con otros pues lo que ocurre es que atienden a ráfagas de tráfico de distintos usuarios.

Redes no orientadas a conexión: Llamadas Datagramas, pasan directamente del estado libre al modo de transferencia de datos. Estas redes no ofrecen confirmaciones, control de flujo ni recuperación de errores aplicables a toda la red, aunque estas funciones si existen para cada enlace particular. Un ejemplo de este tipo de red es INTERNET.

Red Pública de Conmutación Telefónica (PSTN): Esta red fue diseñada originalmente para el uso de la voz y sistemas análogos. La conmutación consiste en el establecimiento de la conexión previo acuerdo de haber marcado un número que corresponde con la identificación numérica del punto de destino.

Topologías

Para poder visualizar el sistema de comunicación en una red es conveniente utilizar el concepto de topología, o estructura física de la red. Las topologías describen la red físicamente y también nos dan información acerca de el método de acceso que se usa (Ethernet, Token Ring, entre otros.).

Cuando se usa una subred punto a punto, una consideración de diseño importante es la topología de interconexión del enrutador. Las redes WAN típicamente tienen topologías irregulares.

Redes Públicas

Las redes públicas son los recursos de telecomunicación de área extensa pertenecientes a las operadoras y ofrecidos a los usuarios a través de suscripción.

Estas operadoras incluyen a:

- Compañías de servicios de comunicación local. Entre estas compañías tenemos a CANTV.
- Compañías de servicios de comunicación a larga distancia. Una compañía de comunicación a larga distancia es un operador de telecomunicaciones que suministra servicios de larga distancia Entre ellos tenemos CANTV, MOVISTAR.
- Proveedores de servicios de valor añadido. Los proveedores de servicio de valor añadido (VACs: Value-added carriers) como CANTV, ofrecen con frecuencia, servicios de comunicación de área amplia como complemento a su verdadero negocio.

Redes Privadas

Una red privada es una red de comunicaciones construida, mantenida y controlada por la organización a la que sirve según **Arévalo J. (2003),** como mínimo una red privada requiere sus propios equipos de conmutación y de comunicaciones. Puede también, emplear sus propios servicios de comunicación o alquilar los servicios de una red pública o de otras redes privadas que hayan construido sus

propias líneas de comunicaciones.

Aunque una red privada es extremadamente cara, en compañías donde la seguridad es imperante así como también lo es el control sobre el tráfico de datos, las líneas privadas constituyen la única garantía de un alto nivel de servicio. Además, en situaciones donde el tráfico de datos entre dos puntos remotos excede de seis horas al día, emplear una red privada puede ser más rentable que utilizar la red pública.

Líneas Analógicas y Digitales

Las líneas analógicas son las típicas líneas de voz desarrolladas inicialmente para llevar tráfico de voz. Este tipo de líneas son parte del servicio telefónico tradicional, por lo que se encuentran en cualquier lugar. Aunque el tráfico de datos digitales no es compatible con las señales de portadora analógica, se puede transmitir tráfico digital sobre líneas analógicas utilizando un módem, el cual modula las señales digitales sobre servicios de portadora analógica, a diferencia de las líneas digitales que están diseñadas para transportar tráfico de datos, que es digital por naturaleza. En vez de utilizar un módem para cargar datos sobre una señal portadora digital, utilizará un canal de servicio digital / unidad de servicio de datos, el cual únicamente proporciona una interfaz a la línea digital. Las líneas digitales pueden transmitir tráfico de datos a velocidades superiores a las líneas analógicas y están disponibles tanto para servicios dedicados como conmutados.

Protocolos y Niveles de las WAN

Los protocolos de capa física WAN describen cómo proporcionar conexiones eléctricas, mecánicas, operacionales, y funcionales para los servicios de una red de área amplia. Estos servicios se obtienen en la mayoría de los casos de proveedores de servicio WAN tales como las compañías telefónicas, portadoras alternas, y agencias de Correo, Teléfono, y Telégrafo (PTT: Post, Telephone and Telegraph).

Los protocolos de enlace de datos WAN describen cómo los marcos se llevan entre los sistemas en un único enlace de datos. Incluyen los protocolos diseñados para operar sobre recursos punto a punto dedicados, recursos multipunto basados en recursos dedicados, y los servicios conmutados multiacceso tales como Frame Relay.

Los estándares WAN son definidos y manejados por un número de autoridades reconocidas incluyendo las siguientes agencias:

International Telecommunication Union-Telecommunication Standardization Sector (ITU-T), antes el Consultative Committee for Intenational Telegraph and Telephone (CCITT).

- Intenational Organization for Standardization (ISO).
- Intenet Engineering Task Force (IETF).
- Electronic Industries Association (ETA).

Los estándares WAN describen típicamente tanto los requisitos de la capa física

como de la capa de enlace de datos.

Capa Física: WAN

La capa física WAN describe la interfaz entre el equipo Terminal de datos (DTE) y el equipo de conexión de los datos (DCE). Típicamente, el DCE es el proveedor de servicio, y el DTE es el dispositivo asociado. En este modelo, los servicios ofrecidos al DTE se hacen disponibles a través de un módem o unidad de servicio del canal/unidad de servicios de datos.

Algunos estándares de la capa física que especifican esta interfaz son:

- EIA/TIA-232D: Esta norma fue definida como una interfaz estándar para conectar un DTE a un DCE.
- EIA/TIA-449: Junto a la 422 y 423 forman la norma para transmisión en serie que extienden las distancias y velocidades de transmisión más allá de la norma 232.
- V.35: Según su definición original, serviría para conectar un DTE a un DCE síncrono de banda ancha (analógico).
- X.21: Estándar CCITT para redes de conmutación de circuitos. Conecta un DTE al DCE de una red de datos pública.
- G.703: Recomendaciones del ITU-T, antiguamente CCITT, relativas a los aspectos generales de una interfaz.
- EIA-530: Presenta el mismo conjunto de señales que la EIA-232D.

- High-Speed Serial Interfase (HSSI): Estándar de red para las conexiones seriales de alta velocidad sobre conexiones WAN.

Capa de Enlace de Datos: Protocolos WAN

Las tramas más comunes en la capa de enlace de datos, asociadas con las líneas seriales sincrónicas se enumeran a continuación:

- Synchronous Data Link Control (SDLC). Es un protocolo orientado a dígitos desarrollado por IBM. SDLC define un ambiente WAN multipunto que permite que varias estaciones se conecten a un recurso dedicado. SDLC define una estación primaria y una o más estaciones secundarias. La comunicación siempre es entre la estación primaria y una de sus estaciones secundarias. Las estaciones secundarias no pueden comunicarse entre sí directamente.
- High-Level Data Link Control (HDLC). Es un estándar ISO. HDLC no pudo ser compatible entre diversos vendedores por la forma en que cada vendedor ha elegido cómo implementarla. HDLC soporta tanto configuraciones punto a punto como multipunto.
- Link Access Procedure Balanced (LAPB). Utilizado sobre todo con X.25, puede también ser utilizado como transporte simple de enlace de datos. LAPB incluye capacidades para la detección de pérdida de secuencia o extravío de marcos así como también para intercambio, retransmisión, y reconocimiento de marcos.
- Frame Relay. Utiliza los recursos digitales de alta calidad donde sea

innecesario verificar los errores LAPB. Al utilizar un marco simplificado sin mecanismos de corrección de errores, Frame Relay puede enviar la información de la capa 2 muy rápidamente, comparado con otros protocolos WAN.

- Point-to-Point Protocol (PPP). Descrito por el RFC 1661, dos estándares desarrollados por el IETF. El PPP contiene un campo de protocolo para identificar el protocolo de la capa de red.
- X.25. Define la conexión entre una Terminal y una red de conmutación de paquetes.
- Integrated Services Digital Network (ISDN). Un conjunto de servicios digitales que transmite voz y datos sobre las líneas de teléfono existentes.

FRAME RELAY

Frame Relay es una tecnología de conmutación rápida de paquetes de datos, llamados tramas, que puede utilizarse como un protocolo de transporte y acceso en redes públicas o privadas, a fin de brindar servicios de telecomunicaciones según la revista electrónica **aprendiendo más y más primera parte**. Frame Relay ha sido especialmente adaptado para velocidades de hasta 2 Mbps, aunque nada le impide superarlas.

La tecnología Frame Relay está basada en el concepto de uso de Circuitos Virtuales (Virtual Circuit). Un Circuito Virtual son dos vías, definidas por software, de un trayecto entre dos puertos que actúa como una línea privada en la red.

La aparición de Frame Relay se debe a los trabajos realizados por un consorcio de compañías entre las que se encontraban Cisco, Northern Telecom, Digital Equipment, Stratacom y Convex Computer, que se involucraron activamente en la generación de la norma. Fue en este contexto donde se escogió un subconjunto de LAPD como protocolo generador y núcleo de Frame Relay.

El primer servicio público basado en Frame Relay apareció en Estados Unidos en 1992 bajo los auspicios de AT&T y BT North América. Los primeros nodos se situaron en las ciudades más importantes de forma que sus habitantes podían acceder al servicio de forma directa; para los usuarios situados en el resto de ciudades el acceso al servicio de los nodos se proporcionaba mediante unos puntos de presencia (lugares físicos donde un portador de larga distancia sitúa el interfase con un LEC o Local Exchange Carrier) facilitados por las compañías telefónicas locales.

El protocolo Frame Relay se basa en los tres (3) principios siguientes:

a. El medio de transmisión y las líneas de acceso están prácticamente libres de errores.
b. La corrección de errores se proporciona por los niveles superiores de los protocolos de las aplicaciones de usuario.
c. La red, en estado normal de operación, no está congestionada, y existen mecanismos estándares de prevención y tratamiento de la congestión.

El primer principio básico señala que muchos de los protocolos más antiguos,

tales como X.25, se diseñaron para operar mediante circuitos analógicos con errores. Esto exigía al protocolo de comunicación el uso de procedimientos complejos de control de errores y confirmación de información transmitida y recibida correctamente. Con la aparición de líneas de transmisión digitales, se redujo considerablemente la necesidad de estos procedimientos.

Esto permite el segundo principio básico de Frame Relay. Se requiere menos carga de proceso en la red para asegurar que los datos se transportan de manera fiable. Por tanto, es lógico el uso de procedimientos simplificados como los de Frame Relay. Esta tecnología ofrece mejor velocidad y rendimiento, porque realiza solamente un mínimo control de errores. Si se produce un error, el protocolo se limita a desechar los datos. Cuando Frame Relay desecha datos erróneos, puede hacerlo sin comprometer la fiabilidad de los datos de usuario, porque los niveles superiores de los protocolos transportados sobre FR proporcionarán la corrección de errores.

El tercer principio básico de Frame Relay es que existe una congestión limitada dentro de la red. Frame Relay supone que existe una cantidad ilimitada de ancho de banda disponible. Si se produce una congestión, el protocolo desecha los datos e incluye mecanismos para "notificar explícitamente" al usuario final la presencia de congestión, y confía en que reaccionará ante estas notificaciones explícitas.

ANCHO DE BANDA

Rango de frecuencias asignadas a un canal de transmisión. Se corresponde con

las situadas entre los puntos en que la atenuación de la señal es de 3dB. El ancho de banda es la máxima cantidad de datos que pueden pasar por un camino de comunicación en un momento dado, normalmente medido en segundos. Cuanto mayor sea el ancho de banda, más datos podrán circular por ella al segundo. Según la página Web en Internet: http://www.learnthenet.com/spanish/glossary/bandwth.htm

RED PRIVADA VIRTUAL VPN

Según **Mason (2002)**, una Red Privada Virtual ó VPN es un servicio que ofrece una conectividad confiable, segura pasando a través de la estructura de red pública como es Internet.

Cuando se desea enlazar las oficinas centrales con alguna sucursal u oficina remota existen tres (3) tres opciones:

a. Modem: Las desventajas es el costo de la llamada, ya que el costo de esta llamada sería por minuto conectado, además sería una llamada de larga distancia, aparte no contaría con la calidad y velocidad adecuadas.

b. Línea Privada: Tendría que tender el cable ya sea de cobre o fibra óptica de un punto a otro, en esta opción el costo es muy elevado porque si por ejemplo se necesita enlazar una oficina central con una sucursal que se encuentra a 200 Kilómetros de distancia el costo sería por la renta mensual por kilómetro sin importar el uso.

c. VPN: Los costos son bajos porque solo se realizan llamadas locales, además de tener la posibilidad de que los datos viajen encriptados y seguros, con

una buena calidad y velocidad.

Una Red Virtual Privada (VPN- Virtual Prívate Network) es una red privada que se extiende, mediante un proceso de encapsulación y encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte.

En estos particulares, la palabra virtual, indica la conectividad dinámica en la red. Esta característica es debido a las necesidades de las organizaciones actuales, donde no existe un estándar en su conectividad y van creciendo incrementalmente. Este término también se puede asociar a la flexibilidad de los dispositivos que se presentan en la comunicación, adaptándose a los medios y características de transmisión que existan.

De igual forma, privada señala la seguridad y garantía que debe tener la información que se envía por la red. La disponibilidad de esta para los usuarios autorizados. Esta característica es un reto sobre todo cuando se habla de transmisión de datos en Internet. La privacidad es típicamente considerada como el hecho de ocultar información. La red utilizando VPN podrá ser tan segura como la red interna.

Las razones que empujan el mercado en ese sentido son, fundamentalmente de costes: resulta mucho más barato interconectar sucursales utilizando una infraestructura pública que desplegar una red físicamente privada. En el otro extremo, por supuesto, es necesario exigir ciertos criterios de privacidad y seguridad, por lo

que normalmente debemos recurrir al uso de la criptografía. Los paquetes de datos de la red privada (VPN) viajan por medio de un "túnel" definido en la red pública (Ver Figura 6).

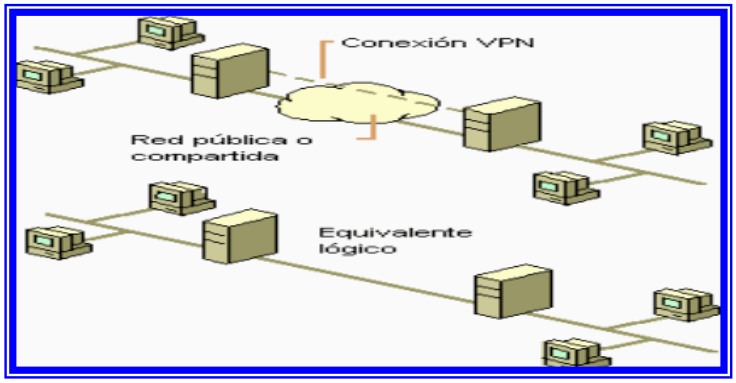

Figura 6
Red Privada Virtual VPN
Fuente: www.cisco.com

Tecnología de Túnel

El manejo del caso general de lograr la interacción de dos redes diferentes es difícil. Sin embargo, hay un caso especial común que puede manejarse. Este caso es cuando el host de origen y el de destino están en la misma clase de red, pero hay una red diferente en medio. Para esto las redes privadas virtuales crean un túnel o conducto de un sitio a otro para transferir datos, **(Ver Figura 7),** a esto se le conoce como encapsulación además los paquetes van encriptados de forma que los datos son ilegibles para los extraños.

La tecnología de túneles -Tunneling- es un modo de transferir datos entre 2 redes similares sobre una red intermedia. También se llama "encapsulación", a la

tecnología de túneles que encierra un tipo de paquete de datos dentro del paquete de otro protocolo, que en este caso sería TCP/IP. La tecnología de túneles VPN, añade otra dimensión al proceso de túneles antes nombrado -encapsulación-, ya que los paquetes están encriptados de forma que los datos son ilegibles para los extraños. Los paquetes encapsulados viajan a través de Internet hasta que alcanzan su destino, entonces, los paquetes se separan y vuelven a su formato original. La tecnología de autenticación se emplea para asegurar que el cliente tiene autorización para contactar con el servidor. Los proveedores de varios firewall incluyen redes privadas virtuales como una característica segura en sus productos.

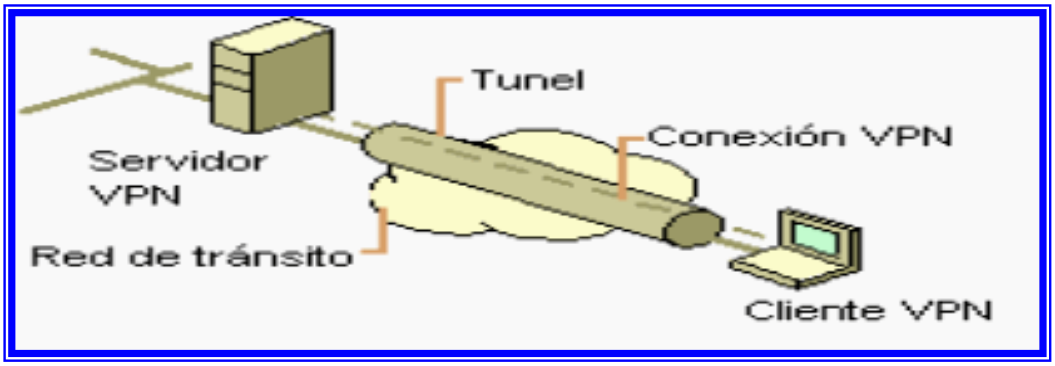

Figura 7
Tecnología de Túnel
Fuente: www.cisco.com

Los datos viajan través de una VPN ya que el servidor dedicado del cual parten los datos, llegando a firewall que hace la función de una pared para engañar a los intrusos a la red, después los datos llegan a la nube de Internet donde se genera un túnel dedicado únicamente para nuestros datos, **(Ver Figura 8)**, para que estos con una velocidad garantizada, con un ancho de banda también garantizado lleguen a su

vez al firewall remoto y terminen en el servidor remoto.

Figura 8
Funcionamiento de una VPN
Fuente: www.monografias.com

Las VPN pueden enlazar diversas oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos como Internet, IP, IPSec, Frame Relay, entre otros.

Por lo general existen dos tipos de Redes Privadas Virtuales (VPN), como lo son los enlaces Cliente-Red y los enlaces Red-Red.

Enlaces Cliente-Red

En estos enlaces se encapsula, típicamente, PPP (Point-to-Point Protocol). Las tramas del cliente se encapsulan en PPP, y el PPP resultante se encapsula para crear el VPN. Se emplean, entre otras muchas cosas, para:

a. Acceso seguro de un cliente a la red.

b. Clientes móviles (para independizarlos de la topología física).

c. Puntos de acceso remoto. Por ejemplo, un "pool" de módems en otra ciudad, o clientes nuestros entrando por otro ISP.

d. Rutado de tramas no utilizables en Internet. Por ejemplo, tramas NetBEUI, IPX, SNA o DECNET.

Enlaces Red-Red

En estos casos se está encapsulando el tráfico de una red local, por lo que nos ahorramos el paso PPP anterior. Las tramas de la LAN se encapsulan directamente para crear el VPN. Se utiliza para:

a. Fundir dos (2) redes locales a través de Internet, para que parezcan una sola.

b. Establecer canales con privacidad, autenticidad y control de integridad, entre dos redes independientes.

c. Rutado de tramas no utilizables en Internet. Por ejemplo, tramas NetBEUI, IPX, SNA o DECNET.

Requerimientos Básicos

Por lo general cuando se desea implantar una VPN hay que asegurarse que esta proporcione:

a. Identificación de usuario.

b. Administración de direcciones.

c. Codificación de datos.

d. Administración de claves.

e. Soporte a protocolos múltiples.

f. Identificación de usuario.

g. La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la misma a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien accedió, qué información y cuando.

h. Administración de direcciones: La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

i. Codificación de datos: Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

j. Administración de claves: La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

k. Soporte a protocolos múltiples: La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de Internet (IP), el intercambio de paquete de Internet (IPX) entre otros.

Herramientas

1. VPN Gateway.

2. Software.

3. Firewall

4. Router.

Ventajas que nos proporciona una VPN

a. La integridad, confidencialidad y seguridad de los datos.

b. Reducción de costos.

c. Sencilla de usar.

d. Sencilla instalación del cliente en cualquier PC Windows.

e. Control de Acceso basado en políticas de la organización herramientas de diagnóstico remoto.

f. Los algoritmos de compresión optimizan el tráfico del cliente.

g. Evita el alto costo de las actualizaciones y mantenimiento a las PCs remotas.

Desventajas de una VPN

a. Al usar una red pública como transporte para los túneles VPN, la seguridad se ve severamente afectada, los datos privados atraviesan una red pública en su transito desde los extremos del túnel VPN.

b. Si bien es cierto se pueden mantener las puertas cerradas de la red privada, no hay que olvidar que la VPN es una fuente de acceso a nuestra red, por lo tanto desde el punto de vista de seguridad de redes, las VPN están en ambos extremos de la balanza, o son muy seguras o muy inseguras, no hay

términos medios

c. Por ello es muy importante la elección de los protocolos a usar en los túneles VPN, los cifrados en la data y en la autentificación de los usuarios VPN, además de considerar al pie de la letra las recomendaciones de claves de acceso en un nivel aceptable y seguro.

Protocolo IPSec

IPSec es un grupo de extensiones de la familia del protocolo IP que representa la tendencia a largo plazo hacia las redes seguras. IPSec provee servicios criptográficos de seguridad basado en técnicas de cifrado y protocolos de seguridad, de acuerdo a la página Web **http://www.openbsd.com**. Como no requiere cambios en las aplicaciones o en los protocolos, IPSec se puede instalar fácilmente en las redes existentes.

Estos servicios permiten la autenticación, integridad, control de acceso, y confidencialidad, pero a nivel de redes, de un modo que es completamente transparente para sus aplicaciones y mucho más robusto. Es transparente porque sus aplicaciones no necesitan tener ningún conocimiento de IPSec para poder usarlo. Se puede usar cualquier protocolo IP sobre IPSec. Se pueden crear túneles cifrados (VPN), o simple cifrado entre computadoras (ordenadores). Debido a que dispone de tantas opciones, IPSec es más bien complejo.

IPSec proporciona autenticación en el nivel de equipo y cifrado de datos para conexiones VPN que utilicen el protocolo L2TP, IPSec negocia entre el equipo y el

servidor de túnel remoto antes de establecer la conexión L2TP, por lo que protege tanto las contraseñas como los datos.

L2TP utiliza protocolos de autenticación estándar basados en PPP, como EAP, CHAP, y PAP con IPSec.

El cifrado está determinado por la asociación de seguridad IPSec o IPSec SA. Una asociación de seguridad es una combinación de una dirección de destino, un protocolo de seguridad y un valor de identificación único, denominado índice de parámetros de seguridad (SPI). Los cifrados disponibles son:

Estándar de cifrado de datos (DES) con una clave de 56 bits, que se ha diseñado para uso internacional y cumple la legislación de cifrado para exportación de datos de EE.UU.

Triple DES (3DES), que utiliza dos claves de 56 bits y se ha diseñado para entornos de alta seguridad de Norteamérica. De un modo lógico, IPSec funciona en cualquiera de estos tres modos:

a. Anfitrión-a-Anfitrión

b. Anfitrión-a-Red

c. Red-a-Red

En cualquier escenario en el que haya una red, el concepto de enrutador está implícito, como en Anfitrión-a-Enrutador (y este enrutador controla y cifra el tráfico para una Red particular).

IPSec se puede usar como túnel de tráfico para conexiones de «redes privadas virtuales» (VPN, Virtual Primate Networks). Sin embargo, su utilidad va más allá de las VPN. Con un registro central de «intercambio de claves de Internet» (IKE, Internet Key Exchange), cada máquina en Internet podría comunicarse con otra y usar cifrado y autenticación de alto grado.

Direcciones IP

La dirección de origen y destino en la cabecera IP es una dirección global de Internet de 32 bits. De estos 32 bits, algunos identifican al computador y el resto a la red. Estos campos son variables en extensión para poder ser flexibles al asignar direcciones de red. Hay diferentes tipos de redes que se pueden implantar en la dirección de red. Unas son grandes (con muchas subredes), otras medianas y otras pequeñas. Es posible y adecuado mezclar en una dirección los tres tipos de clases de redes.

Internet Protocol (IP)

El IP está incluido en el nivel de red, y se encarga de enviar los paquetes de información a sus destinos correspondientes. El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet.

IP está en todos los computadores y dispositivos de encaminamiento y se encarga de retransmitir datos desde un computador a otro pasando por todos los

dispositivos de encaminamiento necesarios.

Los servicios que proporciona IP a TCP son: Send (envío) y Deliver (entrega).

TCP utiliza Send para solicitar el envío de una unidad de datos y Deliver es utilizada por IP para notificar a TCP que una unidad de datos ha llegado. Los campos incluidos en estas dos llamadas son: dirección origen y destino de los datos, usuario IP, identificador de bloque de datos, indicador sobre si está permitida la segmentación del bloque, tipo de servicio, tiempo de vida, longitud de los datos, datos.

Transmission Control Protocol (TCP)

Provee una conexión confiable que permite la entrega sin errores de un flujo de bytes desde una máquina a alguna otra en la red, parte el flujo en mensajes discretos y los monta de nuevo en el destino, además maneja el control de flujo.

De igual forma, **Black (2002)** afirma, que una de las grandes ventajas del TCP/IP es que se encarga de que la comunicación entre todos los computadores de clases diferentes sea posible, esto se debe a que este protocolo es compatible con cualquier sistema operativo y con cualquier tipo de hardware.

TCP proporciona una comunicación segura a través de diversos tipos de redes y conjuntos de redes interconectadas. Además garantiza seguridad (todos los datos llegarán a su destino) y precedencia (se garantiza que el orden de envío se establecerá correctamente en el destino).

TCP está implementado sólo en los computadores y se encarga de suministrar a IP los bloques de datos y de comprobar que han llegado a su destino.

Cada computador debe tener una dirección global a toda la red. Además, cada proceso debe tener un puerto o dirección local dentro de cada computador para que TCP entregue los datos a la aplicación adecuada.

La cabecera de segmento de TCP es única y de un gran tamaño. Entre sus campos, destacan: puerto de origen, puerto de destino, número de secuencia, número de confirmación, longitud de cabecera, indicadores, ventana, suma de verificación, puntero urgente, entre otros.

Para transmitir información a través de TCP/IP, ésta debe ser dividida en unidades de menor tamaño, las cuales reciben el nombre de datagrama (datagram), y son un conjunto de datos que se envían mensajes independientes.

TCP/IP

Black (2002), refiere que TCP/IP es el protocolo común utilizado por todos los computadores conectados a Internet, de manera que éstos puedan comunicarse entre sí. Tiene como objetivos la conexión de redes múltiples y la capacidad de mantener conexiones aún cuando una parte de la subred esté perdida. La red es packed- switched (paquetes ruteados) y está basada en un nivel de Internet sin conexiones.

Los host pueden introducir paquetes en la red, los cuales viajan

independientemente al destino. Se define el Internet Protocol (IP) que provee el ruteo y control de congestión.

TCP/IP no es un único protocolo, sino lo que en realidad se conoce con este nombre es un conjunto e protocolos que cubren los distintos niveles del modelo OSI, los protocolos más importantes son el TCP (Transmisión Control Protocol) y el IP (Internet Protocol).

Protocolos de Túnel

PPP Protocol

Es un protocolo de acceso remoto usado por el PPTP para enviar datos a través de redes basadas en TCP/IP. El PPP encapsula paquetes IP, IPX y NetBEUI entre marcos PPP y envía los paquetes encapsulados creando un link point-to-point entre los ordenadores de origen y destino.

Muchas de las sesiones PPTP comienzan con la llamada de un cliente y un ISP. El protocolo PPP es usado para crear la conexión entre el cliente y el servidor de acceso a la red y presenta las siguientes funciones:

a. Establece y termina la conexión física. El protocolo PPP usa una secuencia definida en el RFC 1661 para establecer y mantener la conexión entre dos ordenadores remotos.

b. Autentifica usuarios. Los clientes PPTP son autentificados usando PPP. Limpieza de texto, encriptado o MS-CHAP pueden ser usados por el

protocolo PPP.

c. Crea datagramas PPP. Que contienen paquetes IPX, NetBEUI o TCP/IP

Protocolo PPTP

El PPTP es un protocolo de red que permite el tráfico seguro de datos desde un cliente remoto a un servidor corporativo privado, estableciéndose así una Red Privada Virtual (VPN) basada en TCP/IP. PPTP soporta múltiples protocolos de red (IP, IPX y NetBEUI) y puede ser utilizado para establecer dichas redes virtuales a través de otras redes públicas o privadas como líneas telefónicas, redes de área local o extensa (LANs y WANs) e Internet u otras redes públicas basadas en TCP/IP.

El punto fuerte del PPTP es su habilidad para proveer en la demanda, multi-protocolo soporte existiendo una infraestructura de área de trabajo, como INTERNET. Esta habilidad permitirá a una compañía usar Internet para establecer una red privada virtual (VPN) sin el gasto de una línea alquilada.

Esta tecnología que hace posible el PPTP es una extensión del acceso remoto del PPP (point-to-point-protocol.....RFC 1171). La tecnología PPTP encapsula los paquetes PPP en datagramas IP para su transmisión bajo redes basadas en TCP/IP. El PPTP es ahora mismo un boceto de protocolo esperando por su estandarización. Las compañías "involucradas" en el desarrollo del PPTP son Microsoft: P. Ascend Communications, 3com / Primary Access, ECI Telematics y US Robotics.

Protocolo PPTP y VPN

El protocolo Point-To-Point Tunneling Protocol viene incluido con Windows NT 4.0 Server y Workstation. Los PCS que tienen corriendo dentro de ellos este protocolo pueden usarlo para conectar con toda seguridad a una red privada como un cliente de acceso remoto usando una red publica como Internet.

Una característica importante en el uso del PPTP es su soporte para VPN. La mejor parte de esta característica es que soporta VPN`s sobre public-switched telephone networks (PSTNs) que son los comúnmente llamados accesos telefónicos a redes.

Usando PPTP una compañía puede reducir en un gran porcentaje el coste de distribución de una red extensa, la solución del acceso remoto para usuarios en continuo desplazamiento porque proporciona seguridad y comunicaciones encriptadas sobre estructuras de área de trabajo existentes como PSTNs o Internet.

Distribución Standard del PPTP

En la práctica general hay normalmente tres ordenadores involucrados en una distribución:

a. Un cliente PPTP.

b. Un servidor de acceso a la red.

c. Un servidor PPTP.

En una distribución típica de PPTP comienza por un PC remoto o portátil que será el cliente PPTP. Este cliente PPTP necesita acceso a la red privada (private network) utilizando un ISP (Internet service provider). Los clientes que usan Windows NT Server o Workstation como sistema operativo, usaran el Dial-up networking y el protocolo PPP para conectar a su ISP. Son también conocidos como Front-End Processors (FEP`s) o Point-Of-Presence servers (POP`s). Una vez conectados, el cliente tiene la capacidad de extraer datos de Internet. Los "network access servers" usan el protocolo TCP/IP para el mantenimiento de todo el tráfico.

Después que el cliente ha hecho la conexión PPP inicial al ISP, la segunda llamada Dial-up es hecha a través de la conexión PPP ya establecida. Los datos enviados usando la segunda conexión son en forma de datagramas IP que contienen paquetes PPP. Es la segunda llamada la que crea la conexión VPN a un servidor PPTP en la red privada. Esto es llamado un TUNEL.

El Tunneling, es el proceso de intercambio de datos de un ordenador en una red privada de trabajo enrutándolos sobre otra red. Los otros enrutamientos de la otra red no pueden acceder porque esta en la red privada. Sin embargo, el tunneling activa el enrutamiento de la red para transmitir el paquete a un ordenador intermediario, como un servidor PPTP. Este servidor PPTP esta conectado a ambas, a la red privada de la compañía y a la red de enrutamiento, que en este caso es Internet. Ambos, el cliente PPTP y el servidor PPTP usan el tunneling para transmitir paquetes de forma segura a un ordenador en la red privada.

Cuando el servidor PPTP recibe un paquete de la red de enrutamiento (Internet) lo envía a través de la red privada hasta el ordenador de destino. El servidor PPTP hace esto procesando el paquete PPTP para obtener el nombre del ordenador de la red privada o la información de la dirección que esta encapsulada en el paquete PPP.

PPTP encapsula el encriptado y comprimido paquete PPP en datagramas IP para su transmisión a través de Internet. Estos datagramas IP son enrutados a través de Internet como un paquete PPP y después son desencriptados usando el protocolo de red de la red privada. Los protocolos soportados por el PPTP, son: TCP/IP, IPX/SPX y NetBEUI.

Transmisión de Datos PPTP

Después de que el Túnel PPTP ha sido creado, los datos del usuario son trasmitidos entre el cliente y el servidor PPTP. Los datos son enviados en datagramas IP conteniendo paquetes PPP. El datagrama IP es creado usando una versión modificada de la versión de Generic Routing Encapsulation (GRE) protocol (RFC1701-2).

Prestando atención a la construcción del paquete, podrás ver como es capaz de ser transmitido a través de Internet desmenuzando las cabeceras. La cabecera de envío del PPP proporciona información necesaria para el datagrama para atravesar Internet. La cabecera GRE es usada para encapsular el paquete PPP sin el datagrama IP. El paquete PPP es creado por RAS. El paquete PPP es encriptado y si es

interceptado, será ilegible.

Seguridad PPTP

El PPTP usa la estricta autentificación y encriptación de seguridad disponible por los ordenadores que corren RAS bajo Windows NT Server v 4.0.El PPTP puede también proteger el servidor PPTP y la red privada ignorando todo excepto el trafico PPTP. A pesar de esta seguridad es fácil configurar un firewall para permitir al PPTP acceder a la red interna.

Control de Acceso

Después del "auth", todo el acceso a la LAN privada continúa usando las estructuras de seguridad basadas en NT. El acceso a recursos en devices NTFS u otros recursos de la red requieren los permisos correctos, tal como si estuvieses conectado dentro de la LAN.

Encriptación de los Datos

Para la encriptación de datos, el PPTP usa el proceso de encriptación RAS "shared secret". Es referido a un "shared-secret" porque ambos terminan la conexión "sharing" the encryption key. Bajo la implantación del RAS de MS, el secreto "shared" es el pass del usuario (Otros métodos incluyen llave pública de encriptación. El PPTP usa la encriptación PPP y los métodos de compresión PPP. El CCP (Compression Control Protocol es usado para negociar la encriptación usada. El nombre de usuario y el password esta disponible al servidor y sustituida por el cliente.

Una llave de encriptación es generada usando una mínima parte del password situados en cliente y servidor. El RSA RC4 Standard es usado para crear estos 40 bits (128 dentro de EEUU y Canadá) de llave de sesión basada en el password de un cliente. Esta llave es después usada para encriptar y desencriptar todos los datos intercambiados entre el servidor PPTP y el cliente. Los datos en los paquetes PPP son encriptados. El paquete PPP que contiene un bloque de datos encriptados es después metido en un largo datagrama IP para su ruteo.

Filtrado de Paquetes PPTP

La seguridad de la red contra intrusos puede ser mejorada activando el filtro PPTP en el servidor PPTP. Cuando el filtro PPTP esta activado, el servidor PPTP en la red privada acepta y rutea solo paquetes PPTP. Esto previene de todos los tipos de paquetes de la red entera. El tráfico PPTP usa el puerto 1723.

Protocolo de Túnel de Capa 2

El Protocolo de túnel de capa 2 (L2TP, Layer Two Tunneling Protocol) es un protocolo de túnel basado en RFC destinado a convertirse en el estándar del sector. Con el Protocolo de túnel de nivel dos (L2TP) se puede tener acceso a una red privada a través de Internet o de otra red pública mediante una conexión de red privada virtual (VPN).

L2TP es un protocolo estándar de túnel para Internet que tiene casi la misma funcionalidad que el Protocolo de túnel punto a punto. La implementación de L2TP

se ha diseñado para ejecutarse de forma nativa a través de redes IP. Esta implementación de L2TP no admite túneles nativos a través de redes X.25, Frame Relay o ATM.

Basándose en las especificaciones de Reenvío de capa dos (L2F) y del Protocolo de túnel punto a punto (PPTP), puede utilizar L2TP para configurar túneles a través de redes intermedias. Al igual que PPTP, L2TP encapsula las tramas del Protocolo punto a punto (PPP), que a su vez encapsulan los protocolos IP, IPX o NetBEUI, con lo que permiten que los usuarios ejecuten de forma remota aplicaciones que dependen de protocolos de red específicos **(Ver Figura 9)**.

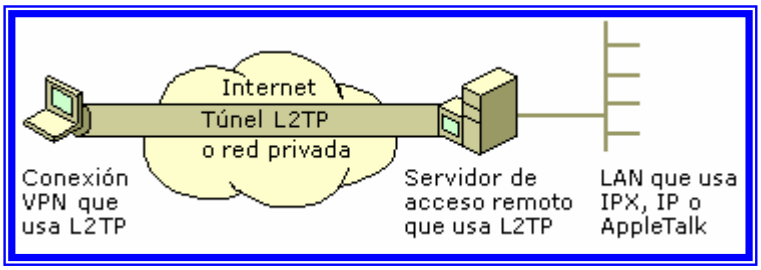

Figura 9
Protocolo de Túnel de Capa 2
Fuente: www.cisco.com

Con L2TP, el equipo que va a iniciar la sesión ejecuta todas las comprobaciones y validaciones de seguridad, y activa el cifrado de los datos, lo que hace mucho más seguro el envío de información a través de redes no seguras. Si se utiliza el nuevo protocolo de autenticación y cifrado Seguridad de protocolo Internet (IPSec), la transferencia de datos a través de una red privada virtual con L2TP es tan segura como en una red LAN de un sitio corporativo. La combinación de L2TP e IPSec se conoce como L2TP sobre IPSec.

Como resultado, las conexiones de red privada virtual basadas en L2TP son una combinación de L2TP y IPSec. L2TP e IPSec deben ser compatibles con el cliente VPN y el servidor VPN.

L2TP se instala con los Servicios de enrutamiento y acceso remoto. De forma predeterminada, L2TP se configura para cinco puertos L2TP. Puede habilitar los puertos L2TP para las conexiones de enrutamiento de marcado a petición y de acceso remoto entrante mediante el Asistente para enrutamiento y acceso remoto. L2TP sobre IPSec proporciona los servicios VPN principales de encapsulación y cifrado de datos privados.

Protocolos de Autenticación

La autentificación inicial en la llamada puede ser requerida por un ISP de servidor de acceso a la red. Un servidor PPTP es un gateway a tu red, y necesita la base estándar de "login" de Windows NT. Todos los clientes PPTP deben proporcionar un login y password. De todas formas, el login de acceso remoto usando un PC bajo NT Server o Workstation es tan seguro como hacer un login en un PC conectado a una LAN (teóricamente). La autentificación de los clientes remotos PPTP es hecha usando los mismos métodos de autentificación PPP usados para cualquier cliente RAS llamando directamente en un NT Server. Porque esto, soporta completamente MS-CHAP.

Protocolo de Autenticación de Contraseña (PAP)

El Protocolo de autenticación de contraseña (PAP, Password Authentication Protocol) utiliza contraseñas en texto simple (no cifradas) y es el protocolo de autenticación menos sofisticado. Se negocia, normalmente, si el cliente y el servidor de acceso remoto no pueden negociar una forma de validación más segura.

Al habilitar PAP como protocolo de autenticación, las contraseñas de usuario se envían en forma de texto simple. Cualquier persona que capture los paquetes del proceso de autenticación podrá leer fácilmente la contraseña y utilizarla para conseguir acceso no autorizado a la Intranet. El uso de PAP es poco aconsejable, especialmente en las conexiones de red privada virtual.

Si se deshabilita la compatibilidad con PAP en el servidor de acceso remoto, el cliente de acceso telefónico nunca envía las contraseñas en texto simple. Al deshabilitar la compatibilidad con PAP aumenta la seguridad de la autenticación, pero los clientes de acceso remoto que sólo admitan PAP no podrán conectarse.

Si la contraseña caduca, PAP no podrá cambiar las contraseñas durante el proceso de autenticación.

Para habilitar PAP en una directiva de acceso remoto de un servidor IAS, asegúrese de que el servidor de acceso a la red (NAS, Network Access Server) admite dicho protocolo.

En caso de que el servidor de acceso al que nos conectamos requiera PAP

como protocolo para realizar la autentificación de nuestra conexión, durante el establecimiento de la sesión LCP de PPP se negociará dicho protocolo, es decir, una vez establecida la conexión de Chat y lanzado el PPP, será este quien realice el envió del nombre de usuario y clave, buscando en el fichero /entre otros/ppp/pap-secrets los valores que debe usar. Este fichero tiene acceso de lectura y escritura solo para root, de modo que nadie que no sea el administrador vea su contenido con las claves.

Protocolo de Autenticación por Desafío Mutuo (CHAP)

El protocolo de autenticación por desafío mutuo CHAP (Challenge-Handshake Authentication Protocol) es usado para verificar periódicamente la identidad del otro extremo de la conexión, dicho protocolo negocia una forma protegida de autenticación cifrada que utiliza Message Digest 5 (MD5), un esquema de hash estándar. Un esquema de hash es un método de transformación de datos (por ejemplo, una contraseña) en el que el resultado es único y no se puede devolver a su forma original. CHAP utiliza un mecanismo de desafío y respuesta con un hash unidireccional de MD5 en la repuesta. De esta forma, puede probar al servidor que conoce la contraseña sin enviar realmente la contraseña a través de la red. Al aceptar CHAP y MD5, Conexiones de red y acceso telefónico puede conectar de forma segura con casi todos los servidores PPP.

La verificación se produce inmediatamente después de la fase de establecimiento de la conexión, y puede repetirse en cualquier momento, con el enlace ya establecido.

Los pasos a seguir son:

a. El extremo que quiere verificar la identidad de su par, le envía un mensaje de prueba.

b. El par responde con un valor calculado mediante un algoritmo.

c. El autenticador compara la respuesta de su par con su propio cálculo del valor correcto. Si los valores coinciden, el autenticador envía un asentimiento, indicando su conformidad. Si no se ha recibido el valor correcto, la conexión debe cerrarse.

d. A intervalos aleatorios, el autenticador envía un nuevo mensaje a su par, y se repiten los pasos 1 y 3.

Ventajas que proporciona

CHAP provee protección contra la repetición de intentos por parte del par que debe ser autenticado, mediante el uso de un identificador que se va incrementando en cada mensaje y un valor variable para la prueba. El tiempo que trascurre entre una autenticación y otra es el límite para un posible intento de violar la protección. El autenticador es el que decide la frecuencia de los mensajes de prueba.

Este método de autenticación depende de un secreto conocido únicamente por el autenticador y el par, este secreto no es enviado por el enlace. El protocolo CHAP funciona básicamente en un solo sentido, pero puede negociarse el uso el mismo secreto para ser usado en una autenticación mutua, en dos direcciones.

Desventajas

CHAP requiere que el secreto no esté encriptado. Cuando se desee autenticar todas las conexiones que se producen en instalaciones grandes, cada posible secreto debe estar presente en todos los posibles extremos. Para evitar esto, es recomendable que los mensajes de prueba y sus respuestas sean examinados en un servidor central. Si no es así, los secretos deben enviarse a cada posible extremo mediante alguna forma de encriptación.

El algoritmo de CHAP requiere que la longitud del secreto sea al menos de un octeto, aunque en la realidad se usan valores mayores. En la actualidad, el algoritmo usado es el MD5, que usa un valor de secreto de 16 octetos. El secreto debe ser lo suficientemente largo para que exista una protección fiable contra la repetición de intentos.

Cada valor para un mensaje de prueba debe ser único, de otra forma se podría violar la protección interceptando un mensaje de respuesta con el que responder a un mensaje de prueba.

Además, el valor del secreto debe ser totalmente impredecible, para evitar que pueda ser calculado, de otra forma podría enviarse un mensaje con un valor futuro, interceptar la respuesta y usarla para responder a un mensaje de prueba.

Telefonía sobre IP (VoIP)

El crecimiento y fuerte implantación de las redes IP, tanto en local como en

remoto, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y prioridad de tráfico, protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que permitan la calidad de servicio en redes IP, han creado un entorno donde es posible transmitir telefonía sobre IP lo que no significará en modo alguno la desaparición de las redes telefónicas modo circuito, sino que habrá, al menos temporalmente, una fase de coexistencia entre ambas, y por supuesto la necesaria interconexión mediante pasarelas (Gateways), denominadas genéricamente pasarelas VoIP. Este aspecto ha sido abordado tanto por ITU como por el IETF.

Si a todo lo anterior, se le suma el fenómeno Internet, junto con el potencial ahorro económico que este tipo de tecnologías puede llevar acarreado, la conclusión es clara: El VoIP (Protocolo de Voz Sobre Internet - Voice Over Internet Protocol) es un tema actual y estratégico para las empresas.

Hoy, desregulación mediante, la telefonía sobre IP empieza a ver su hora más gloriosa y es el fruto más legítimo de la convergencia tecnológica.

El concepto original es relativamente simple: se trata de transformar la voz en "paquetes de información" manejables por una red IP (protocolo Internet). Gracias a otros protocolos de comunicación, como el RSVP, es posible reservar cierto ancho de banda dentro de la red que garantice la calidad de la comunicación.

La voz puede ser obtenida desde un teléfono común: existen Gateways (dispositivos de interconexión) que permiten intercomunicar las redes de telefonía

tradicional con las redes de datos. De hecho, el sistema telefónico podría desviar sus llamadas a Internet para que, una vez alcanzado el servidor más próximo al destino, esa llamada vuelva a ser traducida como información analógica y sea transmitida hacia un teléfono común por la red telefónica tradicional. Vale decir, se pueden mantener conversaciones teléfono a teléfono.

Funcionamiento de la voz sobre IP

La voz sobre IP convierte las señales de voz estándar en paquetes de datos comprimidos que son transportados a través de redes de datos en lugar de líneas telefónicas tradicionales. La evolución de la transmisión conmutada por circuitos a la transmisión basada en paquetes toma el tráfico de la red pública telefónica y lo coloca en redes IP bien aprovisionadas. Las señales de voz se encapsulan en paquetes IP que pueden transportarse como IP nativo o como IP por Ethernet, Frame Relay, ATM o SONET.

Hoy, las arquitecturas ínter operables de voz sobre IP se basan en la especificación H.323 v2. La especificación H.323 define Gateways (interfaces de telefonía con la red) y Gatekeepers (componentes de conmutación Inter.-oficina) y sugiere la manera de establecer, enrutar y terminar llamadas telefónicas a través de Internet. En la actualidad, se están proponiendo otras especificaciones en los consorcios industriales tales como SIP, SGCP e IPDC, las cuales ofrecen ampliaciones en lo que respecta al control de llamadas y señalización dentro de arquitecturas de voz sobre IP.

El Estándar VoIP - Voz sobre IP

Realmente la integración de la voz y los datos en una misma red es una idea antigua, pues desde hace tiempo han surgido soluciones desde distintos fabricantes que, mediante el uso de multiplexores, permiten utilizar las redes WAN de datos de las empresas (típicamente conexiones punto a punto y Frame-Relay) para la transmisión del tráfico de voz. La falta de estándares, así como el largo plazo de amortización de este tipo de soluciones no había permitido una amplia implantación de las mismas **(Ver Figura 10)**.

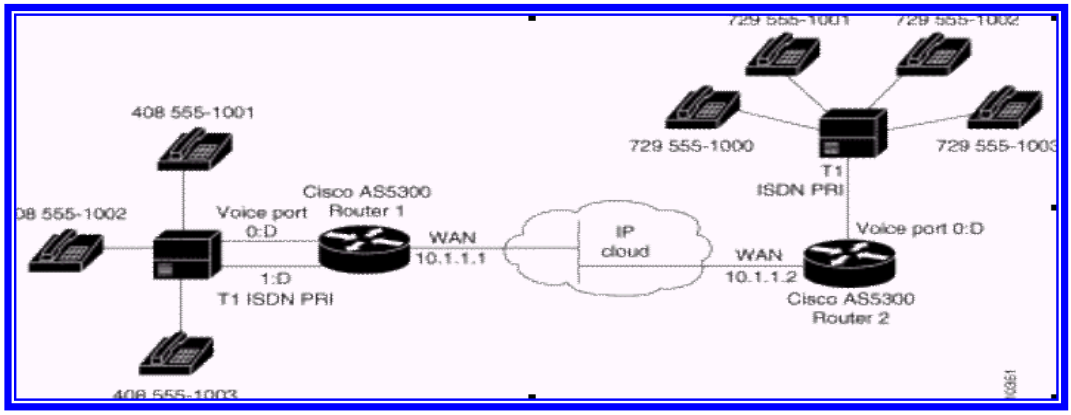

Figura 10
Ejemplo de Red con Conexión de Centralitas a Routers CISCO que Disponen de Soporte VoIP
Fuente: www.cisco.com

Es innegable la implantación definitiva del protocolo IP desde los ámbitos empresariales a los domésticos y la aparición de un estándar, el VoIP, no podía hacerse esperar. La aparición del VoIP junto con el abaratamiento de los DSP's (Procesador Digital de Señal), los cuales son claves en la compresión y descompresión de la voz, son los elementos que han hecho posible el despegue de

estas tecnologías. Para este auge existen otros factores, tales como la aparición de nuevas aplicaciones o la apuesta definitiva por VoIP de fabricantes como Cisco Systems o Nortel-Bay Networks. Por otro lado los operadores de telefonía están ofreciendo o piensan ofrecer en un futuro cercano, servicios IP de calidad a las empresas.

Actualmente podemos partir de una serie de elementos ya disponibles en el mercado y que, según diferentes diseños, nos permitirán construir las aplicaciones VoIP. Estos elementos son:

a. Teléfonos IP.

b. Adaptadores para PC.

c. Hubs Telefónicos.

d. Gateways (pasarelas RTC / IP).

e. Gatekeeper.

f. Unidades de audioconferencia múltiple. (MCU Voz).

g. Servicios de Directorio.

El Gatekeeper es un elemento opcional en la red, pero cuando está presente, todos los demás elementos que contacten dicha red deben hacer uso de aquel. Su función es la de gestión y control de los recursos de la red, de manera que no se produzcan situaciones de saturación de la misma.

El Gateway es un elemento esencial en la mayoría de las redes pues su misión

es la de enlazar la red VoIP con la red telefónica analógica o RDSI.

Los distintos elementos pueden residir en plataformas físicas separada, o nos podemos encontrar con varios elementos conviviendo en la misma plataforma. De este modo es bastante habitual encontrar juntos Gatekeeper y Gateway.

Ventajas de esta Tecnología

a. Integración sobre su Intranet de la voz como un servicio más de su red, tal como otros servicios informáticos.
b. Las redes IP son la red estándar universal para el Internet, Intranets y extranets.
c. Estándares efectivos
d. Interoperabilidad de diversos proveedores
e. Uso de las redes de datos existentes
f. Independencia de tecnologías de transporte (capa 2), asegurando la inversión.

Desventajas de esta Tecnología

Entre las desventajas, cabe señalar es la falta de seriedad de algunos proveedores, solucionable con la prueba real de los equipos, a lo que debe añadirse la necesidad de adecuar los servicios de anchos de banda de Internet a la cantidad de conversaciones simultáneas, ya que, para evitar saturación y mantener la calidad de la

telefonía, es necesario contar con conexiones de Internet preferentemente simétricas y del ancho de banda que recomiende el proveedor.

Requerimientos de una Red para Soportar VoIP

A continuación se mencionan aspectos importantes que se deben tener en la red IP para implantar este servicio en tiempo real.

1. Manejar peticiones RSVP que es un protocolo de reservación de recursos.
2. El costo de servicio debe estar basado en el enrutamiento para las redes IP.
3. Donde se conecta con la red pública conmutada un interruptor de telefonía IP debe soportar el protocolo del Sistema de Señalización 7 (SS7). SS7 se usa eficazmente para fijar llamadas inalámbricas y con línea en la PSTN y para acceder a los servidores de bases de datos de la PSTN. El apoyo de SS7 en interruptores de telefonía IP representa un paso importante en la integración de las PSTN y las redes de datos IP.
4. Se debe trabajar con un comprensivo grupo de estándares de telefonía (SS7, Recomendación H.323) para que los ambientes de telefonía IP y PBX/PSTN y Gateway telefónica puedan operar en conjunto en todas sus características

DEFINICIÓN DE TÉRMINOS BÁSICOS

Arpanet: Red de datos desarrollada por DARPA, cuyo interés principal es haber sido el origen de la actual Internet.

Backbone: Segmento central de una red de área extendida, WAN, que soporta una gran capacidad de tráfico.

Bit: Cantidad de información más pequeña que puede transmitirse. Una combinación de bits puede indicar un carácter alfabético, un dígito, una señal, un modificador u otras funciones.

BPS (Bits por Segundo): Medida de velocidad de un módem.

Browser (Navegador): Programa en el ordenador o computadora del usuario que permite navegar por Internet; es decir, que permite visualizar las páginas Web en un formato legible. Los más conocidos son el Netscape Navigator y el Internet Explorer.

Cable Coaxial: Este es un tipo de cable muy utilizado en la transmisión de datos, este consta de un cable de cobre fino (o grueso) que es el portador de la información, recubierto de un plástico resistente. Su desventaja es que es muy susceptible a interferencias.

Cableado Estructurado: Es un sistema de disposición de los cables en una red, donde se debe seguir un patrón (topología) y una configuración específica, para la transmisión y recepción de datos a través de un medio físico (cable).

CGI = Common Gateway Interface (Interfaz de Gateway Común): Interfaz para programadores que crea archivos de comandos o aplicaciones que se ejecutan internamente en un servidor de Web. Estos archivos de comandos pueden generar texto y otros tipos de datos de forma inmediata, en respuesta a una entrada del

usuario, o bien tomando la información de una base de datos.

Colisión: Intento de transmisión simultanea de dos o más estaciones que están sobre una red. Concentrador (o Hub): Es un dispositivo que posee puertos a los cuales pueden llegar cables provenientes de varias estaciones de trabajo, permitiendo así la compartición de recursos entre dichas estaciones, generalmente se utiliza en redes con topología estrella.

Conectores BNC: estos son utilizados solo en las redes que utilizan cable coaxial (grueso o fino), ellos permiten la conexión entre el cable en sí y la tarjeta de red de la estación de trabajo.

Datagrama: En las redes de conmutación de paquetes es una forma de encaminamiento, en la cual un paquete se dirige hacia su destino final, independientemente del resto por los tramos de menor carga y retardo.

Digital: Dispositivo o método que utiliza variaciones discretas en voltaje, frecuencia, amplitud, ubicación, entre otros., para cifrar, procesar o transportar señales binarias (0 ó 1) para datos informáticos, sonido, vídeo u otra información.

DNS (Sistema de Nombres de Dominio): Sirve para designar un número de IP (Protocolo de Internet), facilitando su memorización.

Domain (Dominio): Nombre único que identifica a un sitio de Internet.

DTU: Unidad de transmisión digital.

E-mail (Correo Electrónico): Servicio telemático similar al sistema postal ordinario, pero sobre un sistema informático; es un eficaz y rápido medio de comunicación y transferencia de datos entre dos o más ordenadores conectados a una red. Usualmente son mensajes de texto, aunque se pueden enviar como anexo todo tipo de ficheros. Es posible enviar el mismo mensaje a un destinatario o a muchos a la vez, pero en el último caso se recomienda usar la opción de "copia oculta" para evitar que las direcciones de correo electrónico de los destinatarios queden visibles y puedan seguir circulando por la red.

FIREWALLS (Cortafuegos): Sistema de protección entre una red local e Internet que impide la entrada de "intrusos" y proporciona seguridad interna.

FTP = File Transfer Protocol (Protocolo de Transferencia de Ficheros): Método para enviar y recibir archivos a través de la red.

Gateway: Conversor de protocolos. Nodo específico de la aplicación que conecta redes que de otra forma serían incompatibles. Convierte códigos de datos y protocolos de transmisión que permiten la interoperatividad.

HTTP = Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto): Método mediante el cual se transfieren documentos desde el sistema "host" o servidor a los exploradores y usuarios individuales. El protocolo de transferencia hipertexto es el conjunto de reglas utilizadas por los ordenadores para transferir ficheros hipertexto, páginas Web, por Internet.

IEEE (Institute of Electrical and Electronics Engineers): Organismo internacional Interface: Nexo de interconexión, hardware o software, que facilita la comunicación entre dos dispositivos responsable de diversos estándares en el campo de las telecomunicaciones.

Internet: Red mundial de ordenadores o computadoras que conecta otras redes y también a empresas, instituciones educativas, fundaciones de investigación, individuos, entre otros. Todo el que se conecta puede compartir ficheros, comunicarse a través del correo electrónico, buscar información e, inclusive, manejar sus finanzas.

Intranet: Red privada para uso interno dentro de una empresa que utiliza el mismo "software" y protocolos empleados en el Internet global.

IP = Internet Protocol (Protocolo de Internet): Cualquier ordenador que se conecte a la red tiene una identificación que proporciona su servidor. Es una dirección numérica única que le identifica. Se compone del conjunto de cuatro números separados por puntos, cada uno de ellos entre 0 y 255. Las IP pueden ser asignadas por el servidor (variables) o fijas.

ISP = Internet Service Provider (Proveedor de Servicio de Internet): Compañías que proveen servicios de conexión a Internet; algunas proveen también otros servicios relacionados, tales como noticias de última hora, información del mercado de valores, entre otros. Puede ser una empresa pequeña o un servicio comercial grande (como Compuserve o América Online) al cual se conecta el ordenador personal del usuario, pero si se accede a Internet directamente a partir de una cuenta de empresa, entonces

el proveedor de acceso es la propia empresa.

LAN = Local Área Network: Red de ordenadores o computadoras ubicadas en el mismo ambiente, piso o edificio.

Modem (Modulador-Demodulador): Conexión del equipo del usuario final que permite transmitir datos digitales a través de dispositivos de transmisión analógicos, como las líneas telefónicas.

Network (Red): Grupo de ordenadores o computadoras conectados de forma tal que permiten compartir ficheros y recursos. La Internet es la red global de redes.

Nodo: Un nodo es un punto de la red que posee una tarjeta de Interface de red y que es capaz de compartir recursos, tales como, impresoras, archivos, escáneres, plotters, entre otros.

Par Trenzado: Se refiere al tipo de cable el cual posee internamente 8 hilos de cobre fino recubiertos de plástico, los cuales a su vez están enrollados en pares (4 pares), para hacerlos menos susceptibles a interferencias.

Password: (Contraseña). Palabra clave utilizada para evitar que cualquier extraño haga uso de nuestra cuenta de Internet o tenga acceso a nuestro correo electrónico.

Protocolo: Sistema utilizado entre dos o más ordenadores para comunicarse entre sí y entenderse. El Protocolo más utilizado en Internet es el TCP/IP.

PROXY: (Apoderado). Servidor encargado de centralizar el flujo entre Internet y una

red, para evitar que cada ordenador conectado a esa red necesite tener su propia conexión.

QoS: Calidad de servicio, garantía estándar de funcionamiento que en la actualidad es adoptada por los fabricantes.

Fuentes Vivas: Se define como las encuestas realizadas a un personal en específico, sobre un tema determinado.

Router: Aplicación que permite conexión entre varias redes La labor principal de un Router es disipar y coordinar la información perteneciente a las direcciones **lógicas** de Red en un sistema.

Servidor: En Internet, es un sistema conectado permanentemente a esta Red que proporciona al usuario la conexión con la misma, además de otros posibles servicios.

TCP/IP: (Protocolo de Control de Transmisiones/Protocolo Internet). Es el protocolo estándar de comunicaciones en red utilizado para conectar sistemas informáticos a través de Internet.

Topología: La topología de una red es la configuración y disposición de las estaciones de trabajo y el sistema de cableado, éstas pueden ser, de estrella, bus, árbol, entre otras.

CAPITULO III

MARCO METODOLOGICO

Este capítulo consta de los siguientes puntos: Naturaleza de la Investigación, Procedimientos de la Investigación y Técnica de Recolección de Información.

En naturaleza de la investigación se indica de qué clase es el estudio realizado. En los Procedimientos de la Investigación se indican cuales son los pasos a seguir para realizar la misma. En la Técnica de Recolección de Información se muestra la entrevista realizada en la presente investigación.

NATURALEZA DE LA INVESTIGACIÓN

El presente trabajo de grado, de acuerdo a su naturaleza, está orientado a la resolución de un problema de tipo práctico; es por esto, que se desarrolló dentro de la modalidad de proyecto factible, el cual consiste en el estudio de un modelo viable que proporciona soluciones y busca la satisfacción de las necesidades de comunicación de la empresa, en cuanto a incremento de ancho de Banda y seguridad de Red se refiere. Tomando en cuenta las normativas para la elaboración de trabajos de grado de la Universidad Centro Occidental Lisandro Alvarado (2002), este tipo de estudio "Consiste en el resultado de una actividad de adiestramiento o de investigación a través del cual el estudiante demuestra el dominio instrumental de los conocimientos adquiridos y debe constituir un aporte al estudio humanístico, científico o técnico de un problema preferiblemente vinculado a la realidad nacional", (p. 2).

Este trabajo trae beneficios de ahorro tanto en tiempo como en dinero, gracias a la integración de esta nueva tecnología con los equipos de computación existentes, lo que permite accesibilidad a los usuarios desde cualquier sitio y en cualquier momento.

Para llevar a cabo las diferentes etapas de investigación, se emplearon técnicas de investigación documental y bibliográfica para la recopilación de información.

TÉCNICAS DE RECOLECCIÓN DE DATOS

El proceso de obtención de datos para el propósito de esta investigación se realiza mediante las técnicas de la observación. La observación consiste en la recopilación mediante los sentidos **según Hurtado (1998)** "… se define la observación como la apertura integral de las personas (sentidos internos y sentidos externos, vivencias, percepción, intelecto…) con respecto a lo que circunda. La selección, registro sistemático y codificación de un conjunto de hechos, situaciones o conductas". (p.59)

Los instrumentos que le corresponden a la observación constituyen criterios al investigador para la medición de lo realmente importante en su estudio, según **Hurtado (1998)** "La ventaja de esta técnica es que permite obtener información independiente de la disposición que las personas estudiadas tengan que proporcionarla". (p.60)

En este estudio se emplea la observación no estructurada, la cual se

fundamenta según **Hurtado (1998)** "… en reconocer y anotar los hechos sin ayuda de medios técnicos especiales". El instrumento utilizado en este tipo de investigación es el de registro anecdótico, el cual se basa en observar y registrar los detalles que se consideran más relevantes para la investigación, en un tiempo previamente establecido. (p.60)

FASES DE ESTUDIO

FASE I. DIAGNÓSTICO

Durante esta fase de la investigación se realiza una inspección documental con el objeto de determinar la situación actual de la estructura de Red establecida en la empresa, y de esta manera conocer las necesidades de la misma.

A su vez también se utilizará el registro de fuentes vivas a través de entrevistas no estructuradas focalizadas, en formular preguntas de manera libre, el entrevistador ha elaborado previamente una lista de temas y puntos en los cuales se centra el interrogatorio (guía o pauta de preguntas).

De esta manera, se elaboraran visitas al departamento de Sistemas de la empresa VENEQUIP, S.A., donde se realizará la entrevista no estructurada al personal que labora en el área de Redes de este departamento, para obtener así, toda la información relacionada al entorno actual de las redes de comunicación que posee, en donde se desarrollará la interconexión de datos.

FASE II. ESTUDIO DE FACTIBILIDAD

Factibilidad Técnica

Para la sustitución del enlace existente en las sucursales de la empresa VENEQUIP S.A. manteniendo la capacidad de transmisión de Voz y Datos se requiere la adquisición de nuevos equipos así como también la reutilización de algunos de los equipos existentes actualmente en las sucursales en estudio y su cableado estructurado.

Cisco System es la empresa líder en equipos de comunicación que ofrecen tecnología de punta capaz de integrar voz y datos a través de un mismo canal, esto avalado por información reflejada en revistas de la rama tales como**: PC Magazine** y **PC World**, pagina Web del proveedor **http://www.cisco.com**, entre otros, junto con artículos y foros de discusión encontrados en la Internet. Se selecciona este proveedor ya que la empresa Venequip, S.A en los actuales momentos cuenta con equipos de esta marca, los cuales son recibidos por Cisco System como forma de pago por los próximos a adquirir, aunado a esto Cisco System proporciona mantenimiento y entrenamiento al personal el cual conoce la tecnología Cisco por un periodo de un (1) año. Estos nuevos equipos son capaces de satisfacer los requerimientos del diseño y garantizar una migración segura a la plataforma a implantar.

Venezuela se ha mostrado en los últimos años como un mercado demandante de tecnología de punta en comunicación e interconexión de equipos, lo que ha traído consigo el establecimiento de sedes en territorio nacional de las más grades empresas

que ofrecen estos servicios, como lo es en el caso de Cisco System. Esto es beneficioso para quien requiera de los equipos ofrecidos por estas empresas ya que de manera sencilla podrán adquirirlos sin tener que realizar trámites internacionales que generan pérdida de tiempo en la espera de los mismos y dichas sedes cuentan con un Stock capaz de satisfacer la demanda nacional.

Los equipos a adquirir son los siguientes:

1. Cinco (5) Routers Cisco de la serie 2600.
2. Cinco (5) Tarjetas VWIC-2MFT-E1-DI.
3. Cinco (5) Switches Cisco de la serie 3500.
4. Nueve (9) Switches Cisco de la serie 2900.

Se reutilizaran los Switches Cisco 2950, Servidores IBM, DELL y AS-400, Routers Cisco modelo 2600, Computadores de escritorio y portátiles, PBX Ericsson MD110, Teléfonos A/D, los equipos periféricos como Impresoras de red y de escritorio entre otros y el cableado estructurado de las mismas ya que estos son capaces de soportar la nueva tecnología a implantar.

Se conservaran los Sistemas Operativos actuales: Windows 2000 Professional, Windows 2003 Server, ya que se cuenta con las licencias necesarias para ello y cumplen los requerimientos básicos del proyecto.

Los proveedores de acceso a Internet banda ancha que se consideran para el presente trabajo son: CANTV, Movistar, IFX Networks, Intercable. Cada uno con sus respectivos planes, velocidades de ancho de banda, tiempos de instalación y costos mensuales asociados a cada servicio.

Factibilidad Operativa

La empresa cuenta con un Departamento de Sistema Central el cual tiene a cargo personal altamente calificado en cada una de las sucursales de estudio de la empresa y de igual manera en las restantes sucursales de la misma, el cual es capaz de desenvolverse en el ámbito del manejo, configuración y administración de la tecnología a implementar. Todo el personal del área de operaciones y redes de la empresa Venequip, S.A. son analistas de sistemas con muchos años de experiencia en dicha área y con cursos y certificaciones avanzadas en las herramientas que allí se usan tales como AS400, Windows Server 2000 y 2003, instalación y configuración de equipos cisco de todas las series y configuración de la seguridad de las redes con el Cisco Pix Firewal modelos 515. En este sentido se afirma con propiedad que a nivel operativo de los equipos a usar se pueden instalar y configurar sin ninguna dificultad operativa.

En cuanto a los equipos a instalar Cisco System ofrece un servicio de atención al cliente completamente gratuito durante el primer año de operación de sus equipos, a manera tal de adecuar al personal que administra la red de la empresa a operar de la manera más óptima los equipos requeridos y por ende la red. Este servicio de

atención al cliente es considerado el mejor del mundo, esto debido a que no se permiten por políticas de Cisco System tener un equipo fuera de servicio por mas de 24 horas en casos extremos ya que la respuesta debe ser inmediata.

A nivel de usuario final quienes son una de las razones del porque una interconexión entre las sucursales de la empresa en general, los cambios serán totalmente transparentes para ellos, por lo que no se requiere de un adiestramiento adicional a estos.

Factibilidad Económica

La factibilidad económica de la sustitución del enlace existente en las sucursales de la empresa VENEQUIP S.A., está dada por la relación costo-beneficio que representa el desarrollo de la misma, la cual se establece haciendo un análisis de los costos en cuanto a los equipos a adquirir, gastos operativos generados por el tipo de conexión y una estimación del tiempo en el cual la inversión será recuperada basándose en los gastos que se reducen con la puesta en marcha de esta tecnología.

En primer lugar se calculó el costo total de los equipos a adquirir, desglosado cada uno en el costo del activo, gastos capitalizados, siendo estos los gastos por traslado, como se observa a continuación **(Ver Cuadro 1)**.

Cuadro 1. Equipos a Adquirir

Cant	Descripción	Costo Activo	Gastos Capitalizados	Costo Unidad	Sub-total
5	Tarjetas VWIC-2MFT-E1-DI	1.569 US$	50 US$	1.619 US$	8.095 US$
1	Switch 3508 -24	5.000 US$	50 US$	5050 US$	5050 US$
4	Switches 3508 -12	2.900 US$	50 US$	2950 US$	11.800 US$
8	Switches C2950T-24	919 US$	50 US$	969 US$	7.752 US$
1	Switch C2950T-12	469 US$	50 US$	519 US$	519 US$
				TOTAL	32.216 US$

Fuente: Cisco, CANTV (2006)
Elaborado: Falcón (2006)

El segundo paso consiste en estimar el costo total en cuanto al cambio de los equipos activos (Routers), adicionando los gastos capitalizados de los mismos, menos las ganancias provenientes de la venta de los equipos activos antiguos a desincorporar (Ver Cuadro 2).

Cuadro 2. Costo de Equipos por Sustitución.

Cant	Descripción	Costo Activo	Gastos Capitalizados	Ganancia Ventas	Costo Unidad	Total
5	Routers 2651	5.195 US$	500 US$	900 US$	4.795 US$	23.975 US$

Fuente: Cisco, CANTV (2006)
Elaborado: Falcón (2006)

Como tercer paso se estipularon los gastos operativos por conexión, dichos servicios son provistos por diversas empresas a precios muy variados dependiendo de la capacidad de conexión que se requiera.

Los costos de los diferentes paquetes y empresas que ofrecen servicios de

conexión en nuestro mercado nacional se muestran en el Cuadro 3.

Cuadro 3. Proveedores de Banda Ancha

Proveedor	Velocidad y nombre del plan	Renta mensual	Costo por instalación	Disponibilidad y tiempo de instalación
CANTV ABA	Plan 768 768/256 Kbps.	96,81 US$	Gratis	Si. 21 días
CANTV ABA	Plan 1536 1536/512 Kbps.	186,87 US$	Gratis	Si. 21 días
TELCEL	Corporativo 1024/512 Kbps.	374,37 US$	148,75 US$	Si. Máximo de 2 meses
IFX Networks	Corporativo 512/256 Kbps.	211,25 US$	187,50 US$	Si. 21 días
Intercable	Corporativo 16 1280/384 Kbps.	288.25 US$	84,37 US$	Si. 21 días
Intercable	Corporativo 8 1024/512 Kbps.	201,75 US$	84,37 US$	Si. 21 días

Fuente: CANTV, MOVISTAR, INTERCABLE (2006)
Elaborado: Falcón (2006)

De las tablas anteriores y tomando en cuenta la disponibilidad económica de la empresa se seleccionan los paquetes de conexión que más se adaptan a los requerimientos establecidos en el estudio del problema, los criterios en que se fundamentó la selección fueron: la velocidad, la renta mensual, el costo por instalación, y la asignación de direcciones IP fijas.

El proveedor que tiene los mejores costos y velocidad es CANTV debido a que además de tener los costos más bajos, proveen de cuatro (4) direcciones IP fijas para Barquisimeto y dos (2) para el resto de las sucursales en estudio, que son necesarias para la configuración de la VPN propietaria. **(Ver Cuadro 4)**.

Cuadro 4. Proveedor y Servicios Seleccionados

Características Sucursal	Velocidad	Costo ABA CANTV
Barquisimeto	1536/512 Kbps.	186,87 US$
Caracas	768/256 Kbps.	96,81 US$
Maracaibo	768/256 Kbps.	96,81 US$
Puerto La Cruz	768/256 Kbps.	96,81 US$
Puerto Ordaz	768/256 Kbps.	96,81 US$
	Total	574,11 US$

Fuente: VENEQUIP S.A, CANTV (2006)
Elaborado: Falcón (2006)

Debido a la existencia de estos dos (2) tipos de conexión y teniendo los costos de los equipos a utilizar se realiza el cálculo del costo total de la implantación y una estimación del tiempo en el cual se generará el retorno de dicha inversión.

Las redes LAN de las sucursales de la empresa VENEQUIP S.A., que están implícitas en el estudio se interconectaran través de la tecnología de conexión Banda Ancha. Los costos generados son los siguientes **(Ver Cuadro 5)**.

Cuadro 5. Costo Total de Equipos a Adquirir

Descripción	Costo
Equipos a Adquirir	32.216 US$
Costo de Equipos por Sustitución	23.975 US$
Total	56.191 US$

Fuente: VENEQUIP S.A, CANTV (2006)
Elaborado: Falcón (2006)

El costo fijo mensual por concepto de conexión de todas las sucursales en estudio con el servicio Banda Ancha ABA del proveedor seleccionado (CANTV) es

de 574,11 US$ mensual.

En el siguiente cuadro se observa el costo actual detallado por sucursal de conexión Frame Relay y el costo por sucursal de la conexión seleccionada Banda Ancha **(Ver Cuadro 6)**.

Cuadro 6. Diferencia de costos entre Conexión

Sucursal	Costo Conexión Frame Relay	Costo Conexión Banda Ancha	Diferencia
BARQUISIMETO	**1816.14 US$**	186,87 US$	1629.27 US$
MARACAIBO	**813.54 US$**	96,81 US$	716.73 US$
CARACAS	**813.54 US$**	96,81 US$	716.73 US$
PUERTO LA CRUZ	**813.54 US$**	96,81 US$	716.73 US$
PUERTO ORDAZ	**813.54 US$**	96,81 US$	716.73 US$
TOTAL:	**5068.70 US$**	574.11 US$	4494.59 US$

Fuente: VENEQUIP S.A, CANTV (2006)

Elaborado: Falcón (2006)

Con la puesta en marcha de esta propuesta la Gerencia General de la compañía estima generar una notable reducción en los gastos operativos de la empresa en cuanto al enlace de conexión de las sucursales en estudio, el cual es para la fecha de 5.068,70 US$ mensual.

Este último valor, menos el costo mensual del nuevo enlace viene a representar la ganancia generada por la sustitución del enlace en la sucursales de la empresa VENEQUIP S.A.

Ganancia = Costo Mensual Enlace Actual – Costo Mensual Nuevo Enlace
Ganancia = 5.068,70 US$ – 574,11 US$
Ganancia = 4.494,59 US$ Mensual.

Con la información suministrada por la empresa (por políticas de la compañía los valores son estimados) y la información arrojada del estudio, el tiempo de retorno de la inversión se estima de la siguiente manera.

$$\text{Retorno Inversión} = \frac{\text{Costo Total de Equipos a Adquirir} = 56.191\ US\$}{\text{Ganancia} = 4.494{,}59\ US\$} = 12{,}5\ \text{Meses}$$

Arrojando como respuesta que la inversión para esta propuesta será recuperada al cabo de un (1) año y seis (6) meses aproximadamente.

Comparación entre Frame Relay y enlace VPN:

Frame Relay

1. Funciona con circuitos virtuales privados dedicados
2. Altos costos de operación y mantenimiento
3. Son monitoreados constantemente por el proveedor
4. Mayores niveles de servicio y disponibilidad

VPN

1. Funciona a través de túneles encriptados a través de Internet
2. Los costos de mantenimiento y operación son mínimos.
3. Se tienen que monitorear diversos proveedores de Internet
4. La disponibilidad del servicio puede verse afectada por fallas en los proveedores de acceso a Internet.

FASE III. DISEÑO

La empresa VENEQUIP S.A., cuenta en los actuales momentos con una red WAN conformada por sus sucursales como lo son: Barquisimeto, Maracaibo, Caracas, Puerto La Cruz, Puerto Ordaz, Valencia, Guasare, San Cristóbal, Punto Fijo, El Tigre, entre otras, existentes en el territorio nacional. Estando toda la información centralizada en la sede de Barquisimeto por encontrarse en ella la Gerencia Nacional de Sistemas, esta red utiliza enlaces de conexión FRAME RELAY dedicados para la transmisión de datos y voz **(Ver Figura 11)**.

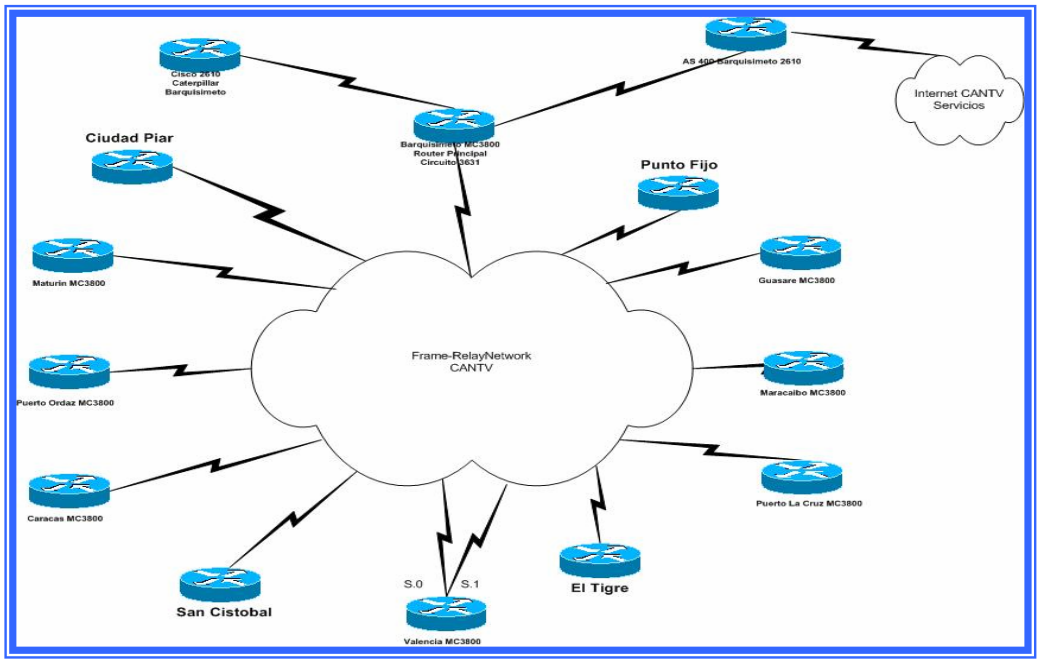

Figura 11
Red WAN Actual Venequip S.A.
Fuente: Venequip, S.A
Elaborado: Falcón (2006)

En este caso de estudio se toman cinco (5) sucursales (Barquisimeto, Caracas,

Maracaibo, Puerto La Cruz y Puerto Ordaz) como piloto para la migración progresiva de esta red WAN a un enlace de conexión Banda Ancha (ABA) ofrecido por CANTV, además de poder transmitir voz y datos a través de un mismo canal (canal de datos) una vez realizado el cambio de enlace.

Para lograr lo anteriormente expuesto se requiere de la adquisición de nuevos equipos Cisco que actualicen parcialmente las LAN en estudio. Para brindar seguridad a la información (datos) transmitida mediante la nueva plataforma se aplicará una VPN propietaria entre las cinco (5) sucursales pilotos.

Por último y no menos importante, se establecerá la comunicación entre las sucursales en estudio y las restantes que conforman la WAN actual de la empresa VENEQUIP S.A., **(Ver Figura 12)**.

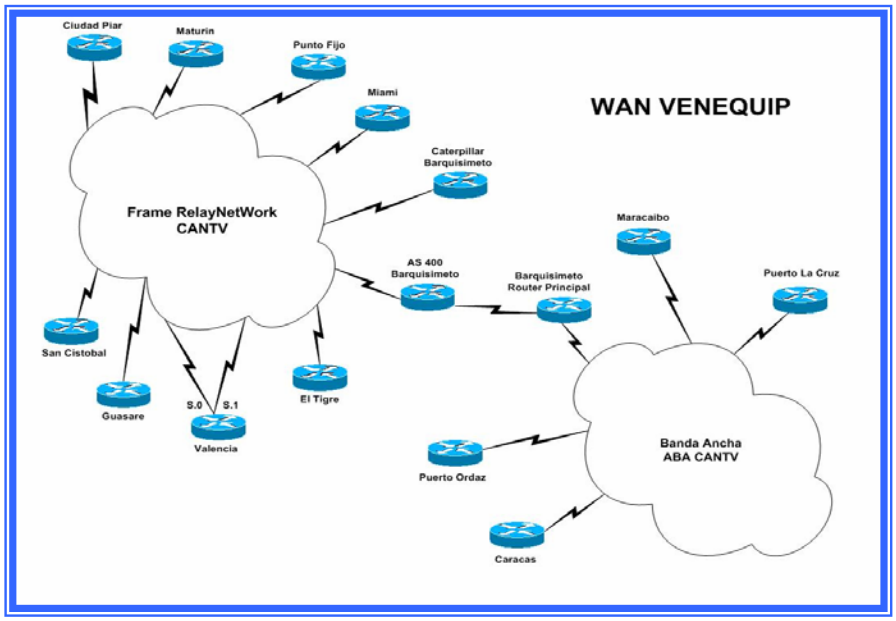

Figura 12
Red WAN propuesta para Venequip S.A.
Fuente: Venequip, S.A
Elaborado: Falcón (2006)

CAPÍTULO IV

ANÁLISIS DE RESULTADOS

RESULTADOS DEL DIAGNÓSTICO

Mediante la inspección documental se encontró que la empresa VENEQUIP S.A. cuenta con una variedad de sucursales en el territorio nacional distribuidas en Barquisimeto, Caracas, Guasare, Maracaibo, Maturín, Punto Fijo, Puerto La Cruz, Puerto Ordaz, San Cristóbal y Valencia. Para el presente estudio se tomaran en cuenta solo las sucursales de Barquisimeto, Caracas, Maracaibo, Puerto La Cruz y Puerto Ordaz ya que según el departamento de sistemas de la empresa estas son tomadas como la primera fase de migración hacia un nuevo enlace debido a su importancia dentro de la empresa y los costos generados por la conexión actual de las mismas.

Las sucursales seleccionadas cuentan en general con una red LAN de interconexión establecida bajo topología estrella. En ellas se encuentran los diferentes equipos activos y pasivos que las componen tales como: Switches Cisco 2950 y Dell Power Connect marcas Dell, Servidores IBM, Dell e IBM AS-400, Routers Cisco modelos 3800 y 2600, Computadores de escritorio y portátiles, PBX Ericsson MD110, Teléfonos, múltiples equipos periféricos como Impresoras de red y de escritorio, al igual cableado estructurado en las mismas. Estas redes LAN están interconectadas mediante una red WAN a través de enlaces privados de comunicación FRAME RELAY para voz y datos ofrecido por la empresa CANTV (Compañía Anónima Nacional de Telefonía de Venezuela), utilizado para centralizar toda la

información manejada por la empresa y establecer comunicación telefónica entre todas sus sucursales utilizando la técnica de Voz sobre FRAME RELAY.

La Gerencia General de la empresa en conjunto con el departamento de sistemas de la misma manifestó que en los actuales momentos, mantener los enlaces de conexión privada FRAME RELAY a través de los cuales está conformada su WAN resulta en muchos casos insostenible, queriendo así la empresa migrar hacia nuevas tendencias de conexión mas económicas como en el caso de enlaces de Banda Ancha específicamente.

Así también, dio a conocer que la relación de negocios existente entre VENEQUIP S.A. y CANTV ha sido excelente y desean en lo posible seguir adquiriendo los servicios de la misma para la conexión Banda Ancha tomando en consideración que no todas las sucursales van a migrar inmediatamente a esta tendencia, debiendo ellos seguir manteniendo la conexión privada de FRAME RELAY con la misma compañía en las restantes sucursales, además CANTV es el único proveedor que proporciona IP fijas para el enlace de la VPN propietaria. Por último y no menos importante realizar las actualizaciones necesarias (Hardware y Software) al momento de adoptar este cambio.

Las redes LAN de las sucursales en estudio se encuentran estructuradas de la siguiente manera.

Red LAN Barquisimeto:

Se encuentra ubicada en la zona Industria I de la ciudad y cuenta con una Red LAN basada en topología estrella la cual está conformada por lo siguientes equipos activos como se observa en la Figura 13:

a. Seis (6) Servidores de aplicaciones varias, con sistema operativo Windows 2003 Server.

b. Dos (2) Servidores AS400, aplicación de negocio Base de Datos.

c. Sesenta (60) estaciones de trabajo las cuales operan en su mayoría con el Sistema Operativo Windows XP Professional y Windows 2000 Profesional.

d. Una (1) Central telefónica ERICCSON MD-110 que da servicios de llamadas internas sin restricciones y salientes solo a personal autorizado.

e. Tres (3) Switch Catalyst C2950T Cisco 24 puertos.

f. Un (1) Hub Fasthub IBM 24 puertos.

g. Tres (3) Routers 2600.

h. Un (1) Routers 3810V.

i. Un (1) DTU (Unidad de Transmisión Digital).

j. Una (1) antena de comunicaciones.

k. Un (1) Multiplexor.

l. Un Ancho de Banda de 256 Kbps.

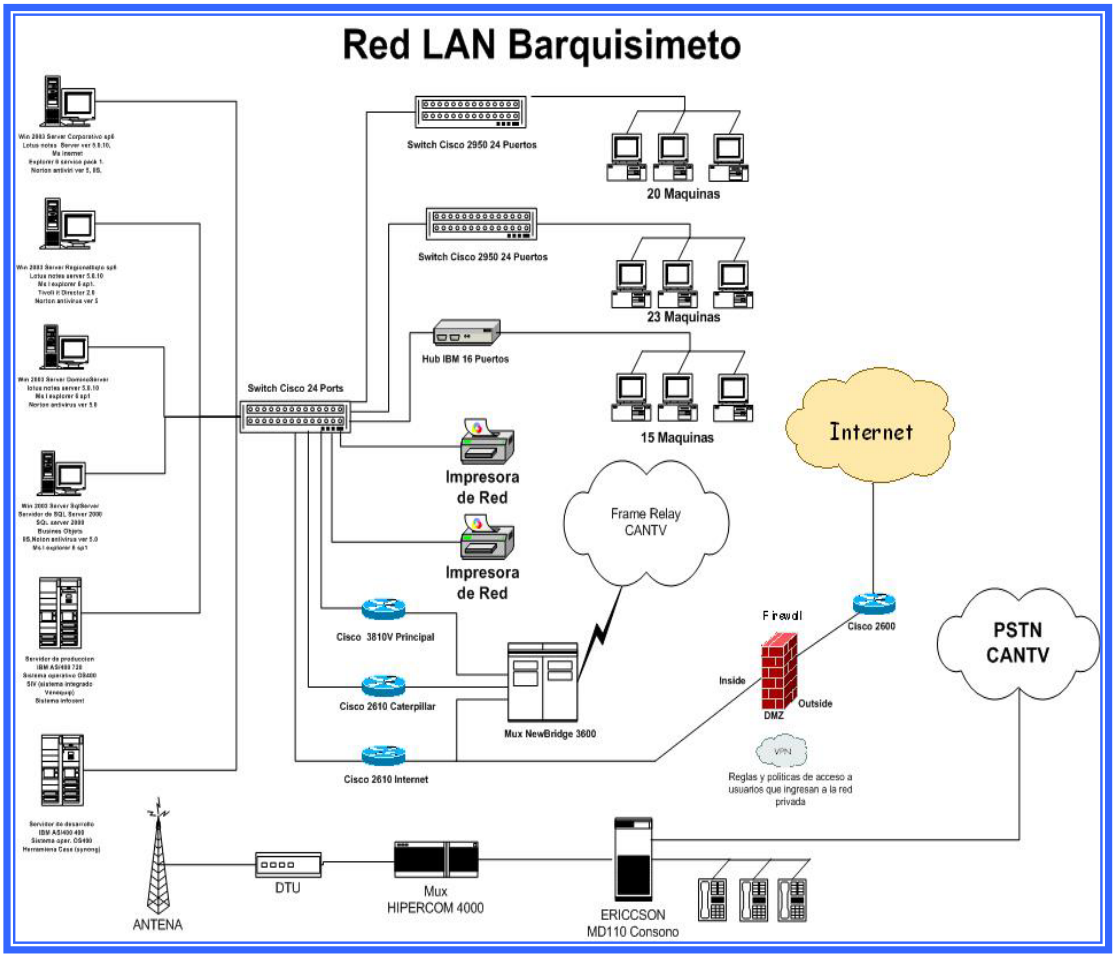

Figura 13
Red LAN Actual de Barquisimeto
Fuente: Venequip, S.A.
Elaborado: Falcón (2006)

Red LAN Maracaibo:

Esta cuenta con una Red LAN basada en topología estrella la cual esta conformada por lo siguientes equipos activos como se observa en la Figura 14:

a. Un (1) Servidor de aplicaciones varias, con sistema operativo Windows

2003 Server.

b. Setenta (70) estaciones de trabajo las cuales operan en su mayoría con los Sistemas Operativos Windows 2000 Professional y Windows XP Professional.

c. Una (1) Central telefónica ERICCSON MD-110 que da servicios de llamadas internas sin restricciones y salientes solo a personal autorizado.

d. Un (1) Switch IBM 8257 24 puertos.

e. Un (1) Switch D–LINK 16 puertos.

f. Un (1) Hub 3COM de 16 puertos.

g. Un (1) Router Cisco 3810V

h. Un (1) DTU (Unidad de Transmisión Digital).

i. Un Ancho de Banda de 64 Kbps

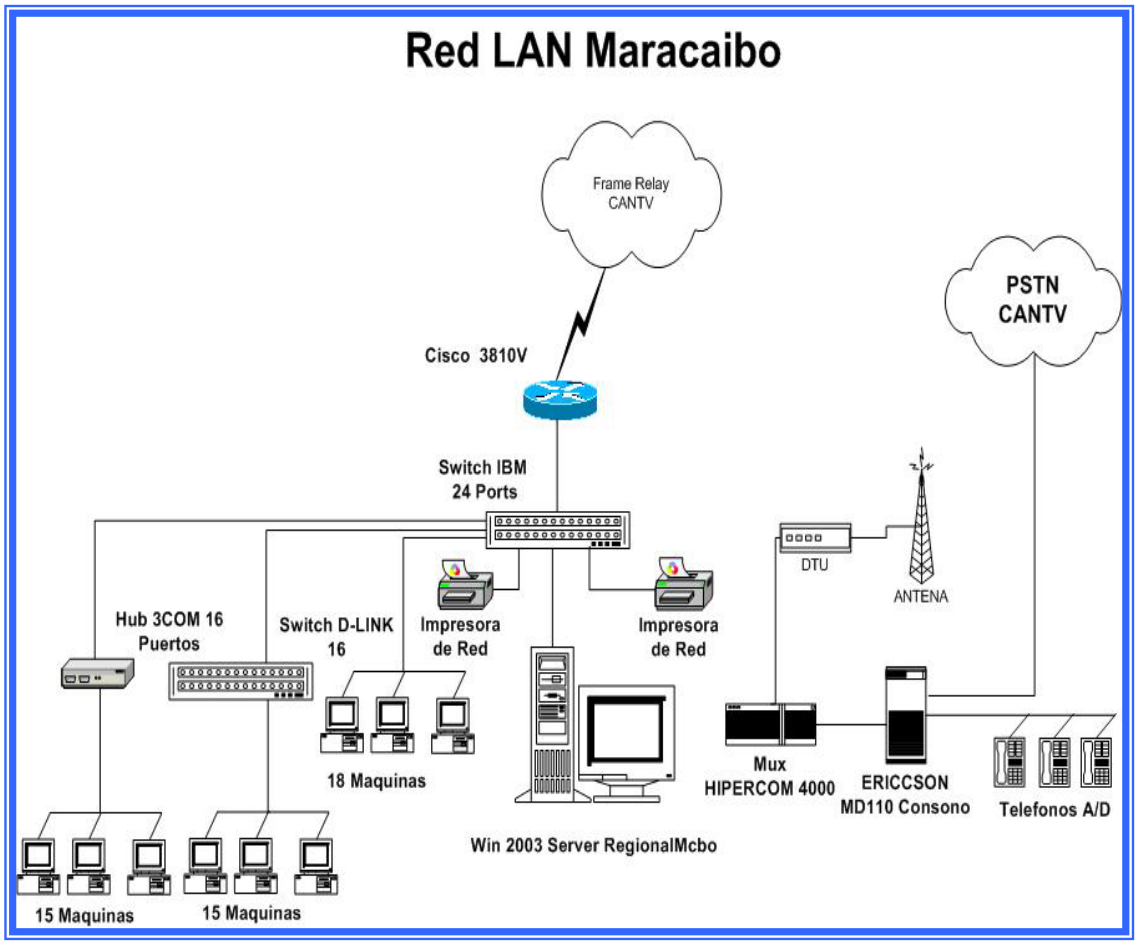

Figura 14
Red LAN Actual Maracaibo
Fuente: Venequip, S.A.
Elaborado: Falcón (2006)

Red LAN Caracas:

Esta cuenta con una Red LAN basada en topología estrella la cual esta conformada por lo siguientes equipos activos como se observa en la Figura 15:

a. Un (1) Servidor de aplicaciones varias, con sistema operativo Windows 2003 Server.

b. Cuarenta y cinco (45) estaciones de trabajo las cuales operan en su mayoría

con el Sistema Operativo Windows 2000 Professional.

c. Una (1) Central telefónica ERICCSON MD-110 que da servicios de llamadas internas sin restricciones y salientes solo a personal autorizado.

d. Un (1) Switch IBM 8257 24 puertos.

e. Un (1) Hub 3COM de 16 puertos.

f. Un (1) Router Cisco 3810V

g. Un (1) DTU (Unidad de Transmisión Digital).

h. Un Ancho de Banda de 64 Kbps.

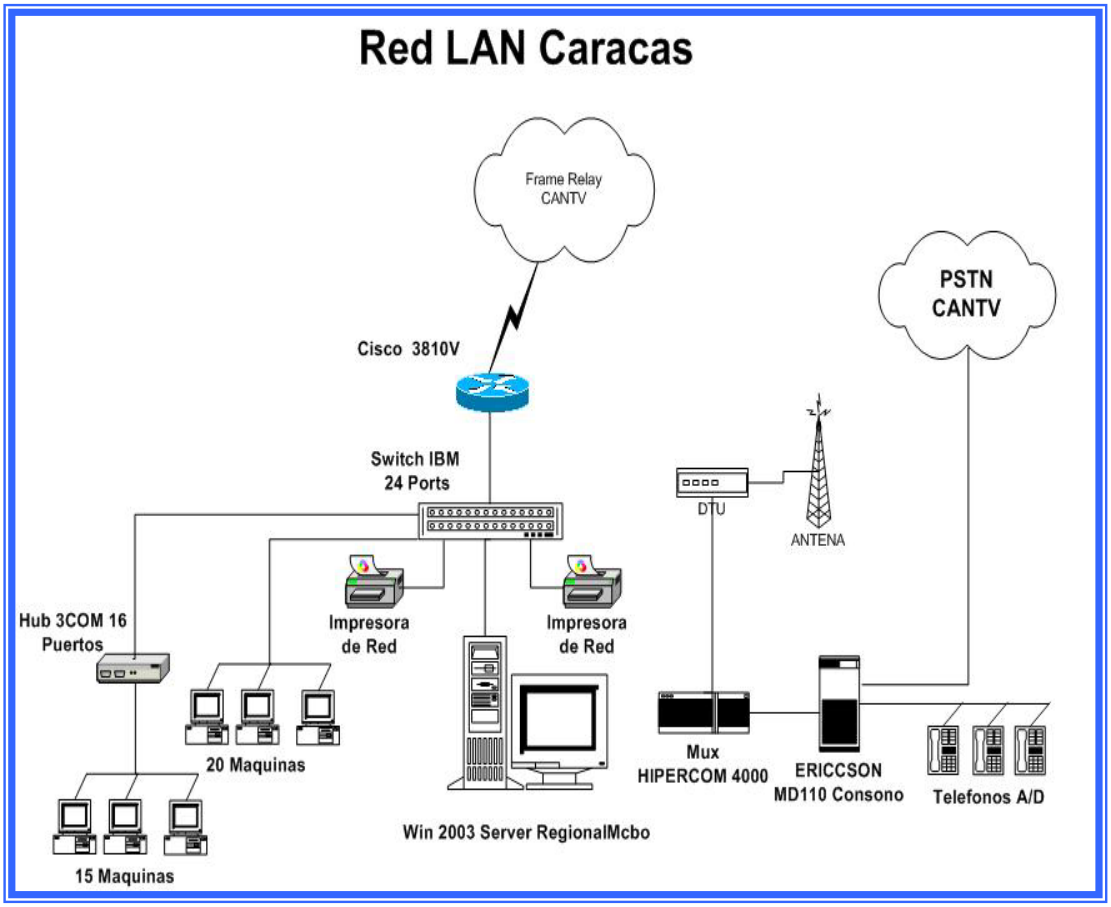

Figura 15
Red LAN Actual Caracas
Fuente: Venequip, S.A.
Elaborado: Falcón (2006)

Red LAN Puerto La Cruz:

Esta cuenta con una Red LAN basada en topología estrella la cual esta conformada por lo siguientes equipos activos como se observa en la Figura 16:

a. Un (1) Servidor de aplicaciones varias, con sistema operativo Windows 2003 Server.

b. Cuarenta y Tres (43) estaciones de trabajo las cuales operan en su mayoría

con los Sistemas Operativos Windows XP Professional y Windows 2000 Professional.

c. Una (1) Central telefónica ERICCSON MD-110 que da servicios de llamadas internas sin restricciones y salientes solo a personal autorizado.

d. Un (1) Switch Cisco Catalyst C2950T 24 puertos.

e. Dos (2) Hub 3COM de 16 puertos.

f. Un (1) Router Cisco 3810V

g. Un (1) DTU (Unidad de Transmisión Digital).

h. Un Ancho de Banda de 64 Kbps.

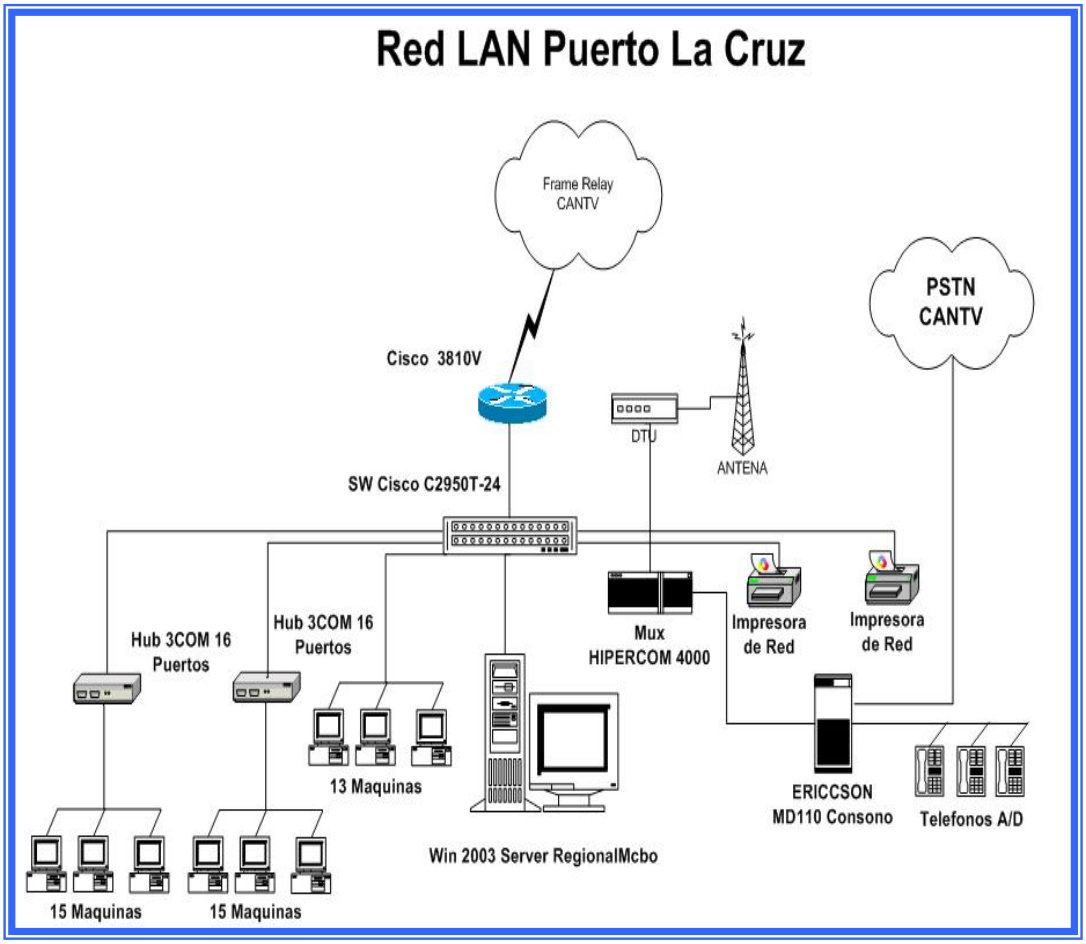

Figura 16
Red LAN Actual Puerto La Cruz
Fuente: Venequip, S.A.
Elaborado: Falcón (2006)

Red LAN Puerto Ordaz:

Esta cuenta con una Red LAN basada en topología estrella la cual esta conformada por lo siguientes equipos activos como se observa en la Figura 17:

a. Un (1) Servidor de aplicaciones varias, con sistema operativo Windows 2003 Server.

b. Cuarenta y Cinco (45) estaciones de trabajo las cuales operan en su mayoría

con el Sistema Operativo Windows 2000 Professional.

c. Una (1) Central telefónica ERICCSON MD-110 que da servicios de llamadas internas sin restricciones y salientes solo a personal autorizado.

d. Un (1) Switch IBM 8257 24 puertos.

e. Dos (2) Hub 3COM de 16 puertos.

f. Un (1) Router Cisco 3810V

g. Un (1) DTU (Unidad de Transmisión Digital).

h. Un Ancho de Banda de 64 Kbps.

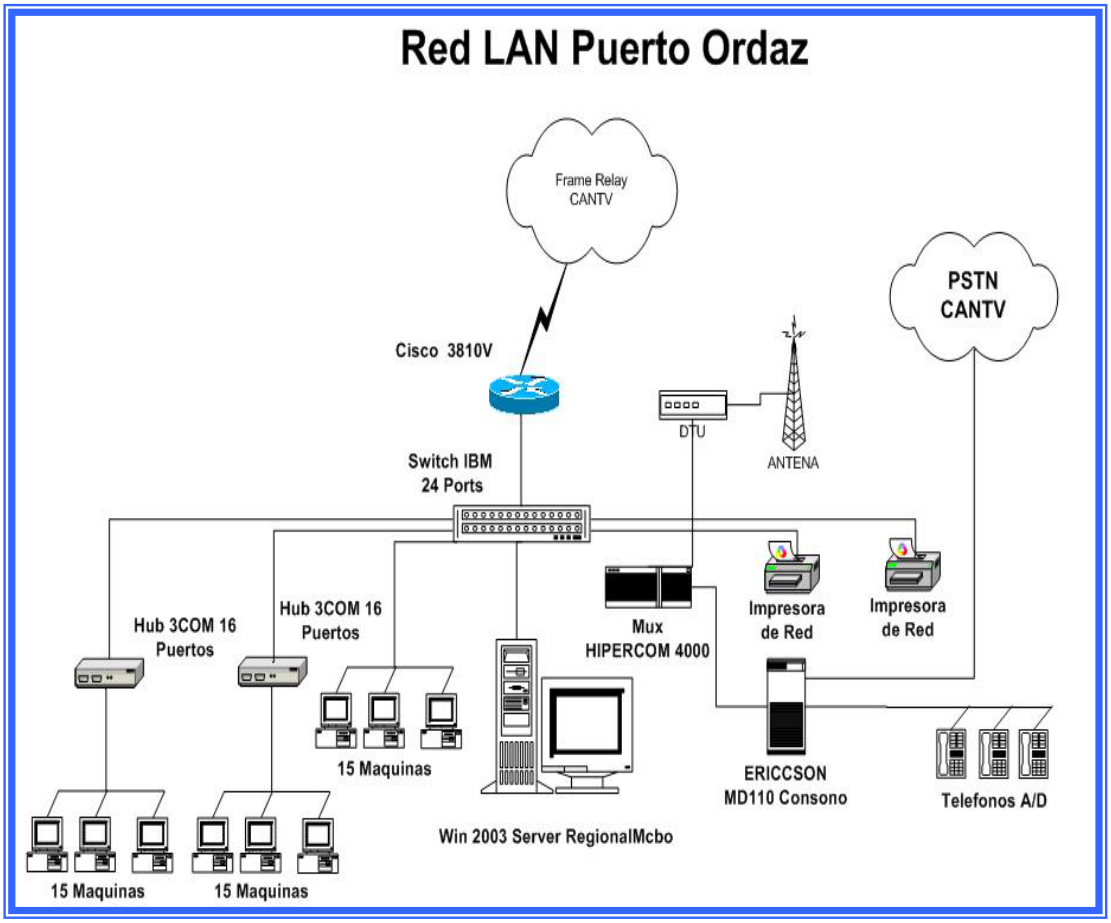

Figura 17
Red LAN Actual Puerto Ordaz
Fuente: Venequip, S.A.
Elaborado: Falcón (2006)

ESPECIFICACIONES DE LA PROPUESTA:

DESCRIPCIÓN DE EQUIPOS PARA LA SUSTITUCIÓN DEL ENLACE EXISTENTE EN LAS SUCURSALES DE LA EMPRESA VENEQUIP S.A., UTILIZANDO VPN PROPIETARIA.

A continuación se procederá a la descripción detalla del diseño propuesto en el capitulo anterior así como también de los equipos seleccionados y su

funcionamiento dentro de las LAN y la WAN. De igual manera se explicaran las técnicas utilizadas para la implementación de la VPN; finalizando con una breve explicación del funcionamiento del diseño.

En primer lugar se realiza la actualización parcial de las redes LAN utilizando los equipos Cisco seleccionados, estos equipos brindan mayor velocidad de distribución de paquetes de información (datos).

REDES LAN

Core Switch (Switch Principal)

Para la distribución interna de las LAN se utilizará un Switch Cisco 3508 por cada sucursal. Este Switch se encargará de dar conexión de alta velocidad a todos los equipos activos que integran estas redes como en el caso de los Switches Cisco C2950T, Servidores de aplicaciones (Windows 2003 y AS-400), y en algunos casos impresoras de red. A su vez estos estarán conectados a los Routers de cada sucursal. Entre las características más relevantes de este Switch tenemos:

a. Soporta un Ancho de Banda de 5.4 Gbps

b. Permite el acoplamiento de los rangos de los Transceivers GBIC

c. Incluye los Cisco GigaStack GBIC, 1000BASE-T, 1000BASE-SX y 1000BASE-LX/LH GBICs, y 1000BASE-ZX.

d. Soporta la Tecnología IEEE 802.1 para tareas de voz y tráfico de telefonía en la red.

Switches

Para el reemplazo de los Switches y Hub existentes en la redes LAN que dan servicio de conexión a los computadores de escritorio y portátiles y a las impresoras de red se seleccionaron los Switch Cisco C2950T de 12 y 24 puertos dependiendo de la segmentación existente en cada una de las LAN. Esto proveerá mayor velocidad de interconexión entre los dispositivos anteriormente señalados. Entre sus características principales tenemos:

a. Con diversidad de capacidad de conexión, esto dependiendo de la capacidad de los equipos que anteriormente cumplían con esta función, para así, reutilizar el cableado estructurado existente.

b. Maneja Velocidades de 10/100/1000 BASET.

c. Comunicación Full-duplex.

d. Soporta el estándar IEE 802.3.

e. Maneja VLAN.

f. 2 Módulos de conexión GBIC (no incluidos).

g. Ofrece QoS.

Servidores

Seguirán activos los servidores existentes en las LAN actualmente. Estos conservaran sus Sistemas Operativos (Windows 2003 Server y AS-400) y mantendrán las funciones que cumplen individualmente cada uno de ellos en cada

LAN de la siguiente manera:

Se utilizará un (1) Servidor de Impresión y Archivos en las sucursales de Caracas, Maracaibo, Puerto La Cruz y Puerto Ordaz. Adicionalmente estos servidores prestaran servicios de autenticación y dominio para la validación de usuario, DNS, DHCP y el establecimiento de políticas de seguridad a través del Active Directory.

En Barquisimeto existe la mayor cantidad servidores por ser esta la sucursal principal de la empresa y donde se encuentra centralizada toda la información pertinente a las actividades desempeñadas par la misma. Esto servidores son:

a. Servidor de Desarrollo (AS-400 400): En este se realizan todas la aplicaciones y pruebas de las mismas que luego serán puestas en funcionamiento en el servidor de Aplicaciones y Base de Datos como en el caso de SIV (Sistema Integrado VENEQUIP)

b. Servidor de Aplicación y Base de Datos (AS-400 720): Este se encarga de almacenar toda la información obtenida mediante la utilización del SIV. El SIV es un software desarrollado por la misma empresa y se encarga de administrar actividades relacionadas a la misma.

c. Servidor SQL (DELL): Este almacena de manera centralizada todas las bases de datos SQL de los diversos Software de la empresa que lo requieren.

d. Servidor de Fax y Correo (IBM): Se encarga de recibir vía MODEM los Fax de la empresa. Adicionalmente se encarga de la mensajería interna de la empresa mediante Lotus Note.

e. Servidor Corporativo de Dominio y Aplicaciones (IBM): Este ofrece servicios de autenticación y dominio para la validación de usuario, DNS, DHCP y establecer políticas de seguridad a través del Active Directory. Adicionalmente están instaladas diversas aplicaciones empleadas para la realización de las actividades de la empresa.

f. Servidor Web (DELL): En el están instalados los servicios de aplicaciones de Internet y ofrece alojamiento a su pagina Web (http://www.venequip.com).

g. Servidor Regional Barquisimeto (IBM): En el corren las Aplicaciones de Antivirus y Tivoli para acceso remoto al resto de los servidores.

h. Servidor de Monitoreo (IBM): Se encarga monitorear el estado de la WAN mediante el software What´s Up.

Impresoras de Red

Existen en cada una de las LAN dos (2) impresoras de red modelos: HP *LaserJet* 4000N, IBM 4312 las cuales en algunos casos estarán conectadas al los Switches C2950T y en otros casos en los Switches 3508, esto dependiendo de la segmentación de la red.

Computadores de Escritorio y Portátiles

En cada una de las LAN existen diversas cantidades de estos computadores los cuales operan en su mayoría con el sistema operativo Windows 2000 Professional.

Todos estos estarán configurados dentro de las LAN, esta configuración dependerá de la LAN a la que pertenezca. Los portátiles estarán configurados para operar dentro de las diferentes LAN así como para poder acceder a la red remotamente una vez establecida la VPN. La configuración de los portátiles para el acceso remoto a los servicios y recursos compartidos se realizara instalando en cada equipo el software vpn client de Cisco y colocando allí los parámetros de conexión necesarios para abrir el túnel tales como la dirección IP del equipo, el usuario de autenticación y el password adecuado.

Telefonía

Los teléfonos que prestan servicio a través de las PBX seguirán operativos, puesto que este seguirá siendo el medio empleado para la comunicación de voz en cada una de las LAN (Sucursales). En Barquisimeto se conservaran el Multiplexor, el DTU y la antena de comunicación con el enlace FRAME RELAY, por ser esta sucursal el puente o enlace entre las dos tecnologías que serán utilizadas para la interconexión general de todas las sucursales de las empresa VENEQUIP S.A.,

PBX

Los equipos Ericsson MD 110 que se encuentran funcionando actualmente en cada una de las LAN seguirán operativos. Estos equipos son capaces de soportar (migrar) la sustitución del enlace y la nueva tecnología a implementar. Estos equipos estarán conectados a las Tarjetas Cisco VWIC-2MFT-E1-DI a través de un enlace E1 Las características más relevantes de estos equipos son:

1. Poseen un sistema SPC-PBX (Stored Program Controlled - Private Branch Exchange), el cual emplea tecnología completamente digital de Conmutación y Transmisión.

2. Su modularidad y flexibilidad, les permiten cubrir una amplia variedad de necesidades en las conexiones de la red, entre las cuales cabe a destacar:

a. Crecimiento en forma progresiva (se pueden conectarse dos sistemas formando un único sistema, pudiendo duplicar sus líneas de conexión y por ende sus extensiones), implementación de nuevas aplicaciones, ampliaciones en capacidad de tráfico, y dispersión geográfica.

b. Mantener sincronizado todo el sistema.

c. Distribución uniforme de llamadas.

d. Capacidad para ISDN.

e. Mantenimiento remoto.

f. Puerto de dispositivo extra.

g. Registro de llamadas.

h. Anuncio de llamada en teléfono descolgado.

i. Integración a correo de voz.

j. Acceso directo al sistema (DISA).

k. Mensaje en ausencia.

Tarjetas Cisco VWIC-2MFT-E1-DI

Estas tarjetas serán las encargadas de transformar los la voz de los teléfonos en datos para poder utilizar la voz sobre IP, es decir, las tarjetas son módulos conectadas a las PBX. Sus principales características son las siguientes:

a. Posee dos (2) puertos RJ 45.

b. Son Drop and Insert.

Routers

Se utilizaran cinco (5) Routers Cisco 2651para sustituir los 3810V existentes en las LAN en estudio. Estos Routers 3810V son funcionales bajo la plataforma actual, pero no soportan la nueva tecnología a implantar. Los Routers 2651 proporcionan integración, potencia y versatilidad, además de ser una solución rentable para satisfacer las necesidades actuales y futuras de las sucursales en lo referente a:

a. Integración de voz y datos.

b. Acceso a redes privadas y virtuales (VPN) con opciones de Firewall.

c. Enrutamiento con gestión de Ancho de Banda.

d. Enrutamiento entre VLAN.

La arquitectura modular de estas series permite ajustarlas a expansiones o cambios tecnológicos de la red cuando se producen por la instalación de nuevos

servicios u aplicaciones. Estos Routers proporcionan un envío de hasta 37000 pps (paquetes por segundo), las características más relevantes de estos Routers son:

a. Permiten el Acceso a redes WAN, incluyendo servicios ATM.

b. Las interfaces de red pueden actualizarse en las instalaciones y permiten instalar nuevas tecnologías

c. Pueden añadirse interfaces a medida que aumentan las necesidades de ampliación de la red para ajustar los costos al crecimiento.

Estos equipos serán instalados en las redes LAN de las cinco (5) sucursales en estudio. El objetivo de estos equipos (Routers) es el de establecer las rutas (enrutar) a seguir por los paquetes de información dependiendo del origen y destino de los mismos. Internamente en estos equipos estarán predefinidas dos tablas de direcciones IP. La primera tabla contendrá todas las direcciones IP de cada uno de los distintos Routers de las sucursales en estudio así como las del resto de sucursales que componen la red total de VENEQUIP S.A. La segunda contendrá las direcciones IP de los equipos que conforman individualmente cada sucursal.

Modularmente a estos equipos les será adicionado las tarjetas Cisco VWIC-2MFT-E1-DI las cuales estarán conectadas por medio de un enlace E1 a la PBX de la LAN. Aunado a todo lo anteriormente descrito, dentro de estos equipos estará en funcionamiento el protocolo de autenticación CHAP.

REDES WAN

Una vez instalados y configurados los Routers con las tablas de direcciones IP correspondientes para cada uno en especifico y habiendo realizado las configuraciones necesarias para el funcionamiento de los mismos se debe establecer el medio por el cual se accesarán a dichas direcciones entre ellos, esto es, el nuevo enlace de comunicación que establecerá la WAN. Para la sustitución del enlace de la empresa se utilizará el enlace de Banda Ancha ABA ofrecido por CANTV ya que es la única en proporcionar direcciones IP fijas, a velocidades de 1536/512 Kbps para la sucursal de Barquisimeto la cual a su vez mantendrá en enlace de voz FRAME RELAY ofrecido por la misma empresa y 768/256 Kbps en el resto de las diferentes sucursales en estudio.

Para brindar mayor seguridad al momento de la transmisión de los paquetes de información a través del enlace de Banda Ancha se creará una Red Privada Virtual (VPN). Por medio de esta VPN se logra el establecimiento de una conexión de las redes locales (LAN), de la red WAN o de alguna conexión remota a través de Internet (esta última dota a la red de portabilidad) mediante un túnel cifrado de conexión bajo protocolo PPTP para proteger los paquetes de datos que viajan de una a otra LAN de la empresa a través de Internet. Esta VPN estará siempre apuntando a cada uno de los Routers de las sucursales pues estos son las puertas de salidas de las mismas. Para dar mayor seguridad a los datos que viajan a través de esta VPN se utilizara el protocolo IPsec para la encriptación de estos.

REDES LAN DE LA NUEVA PLATAFORMA

Una vez que los equipos adquiridos, aquellos que se reutilizaran y el enlace a utilizar estén configurados en cada uno de las redes LAN de las sucursales de la empresa VENEQUIP quedaran de la siguiente manera.

Red LAN Barquisimeto:

a. Seis (6) Servidores de aplicaciones varias, con sistema operativo Windows 2003 Server.
b. Dos (2) Servidores AS400, aplicación de negocio Base de Datos.
c. Sesenta (60) estaciones de trabajo las cuales operan en su mayoría con el Sistema Operativo Windows 2000 Professional.
d. Una (1) Central telefónica ERICCSON MD-110 que da servicios de llamadas internas sin restricciones y salientes solo a personal autorizado.
e. Tres (3) Switch Catalyst C2950T Cisco 24 puertos.
f. Un (1) Switch Cisco 3508 24 puertos.
g. Cuatro (4) Routers 2651.
h. Una (1) Tarjeta Cisco VWIC-2MFT-E1-DI
i. Un (1) Multiplexor.
j. Un (1) DTU (Unidad de Transmisión Digital).
k. Una (1) antena para comunicación.

Como se observa en la Figura 18.

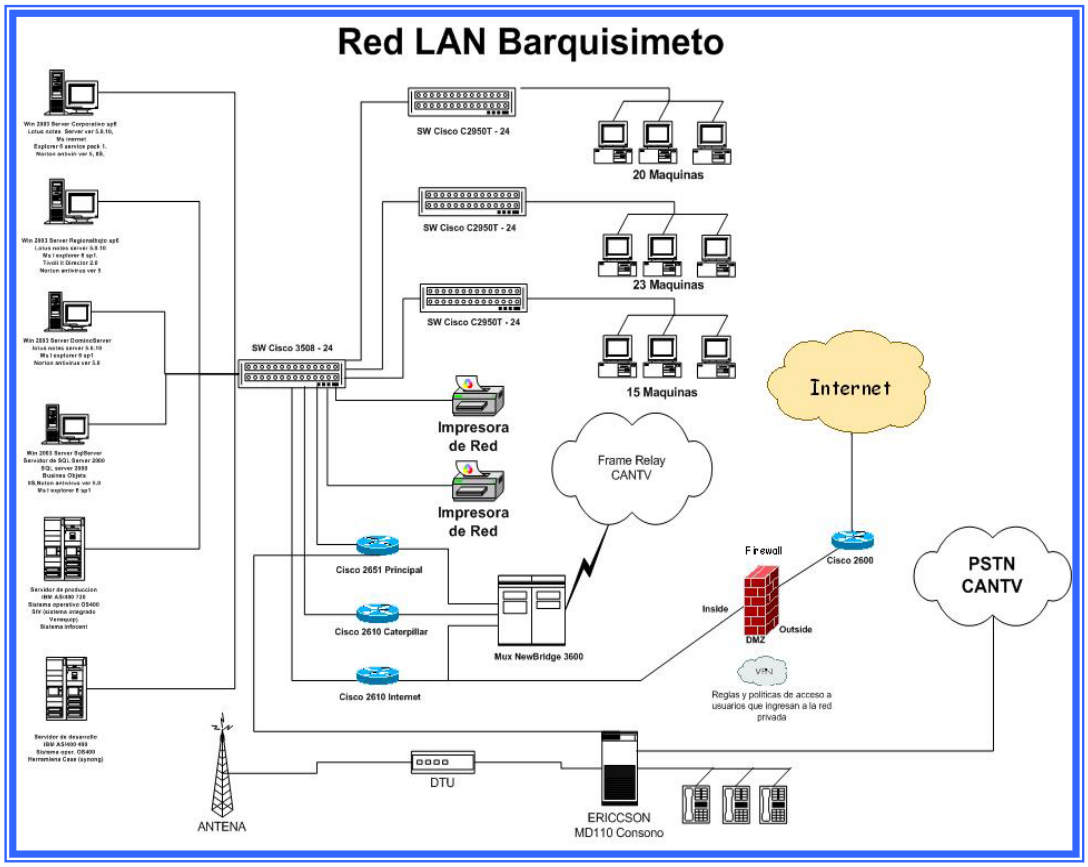

Figura 18
Red LAN Propuesta Barquisimeto
Fuente: Venequip, S.A.
Elaborado: Falcón (2006)

Red LAN Maracaibo:

a. Un (1) Servidor de aplicaciones varias, con sistema operativo Windows 2003 Server.

b. Cuarenta y ocho (48) estaciones de trabajo las cuales operan en su mayoría con el Sistema Operativo Windows 2000 Professional.

c. Una (1) Central telefónica ERICCSON MD-110 que da servicios de llamadas internas sin restricciones y salientes solo a personal autorizado.

d. Dos (2) Switch Catalyst C2950T Cisco 24 puertos.

e. Un (1) Switch Catalyst C2950T Cisco 12 puertos.

f. Un (1) Switch Cisco 3508-12 puertos.

g. Un (1) Router Cisco 2651.

h. Una (1) Tarjeta Cisco VWIC-2MFT-E1-DI.

Como se observa en la Figura 19.

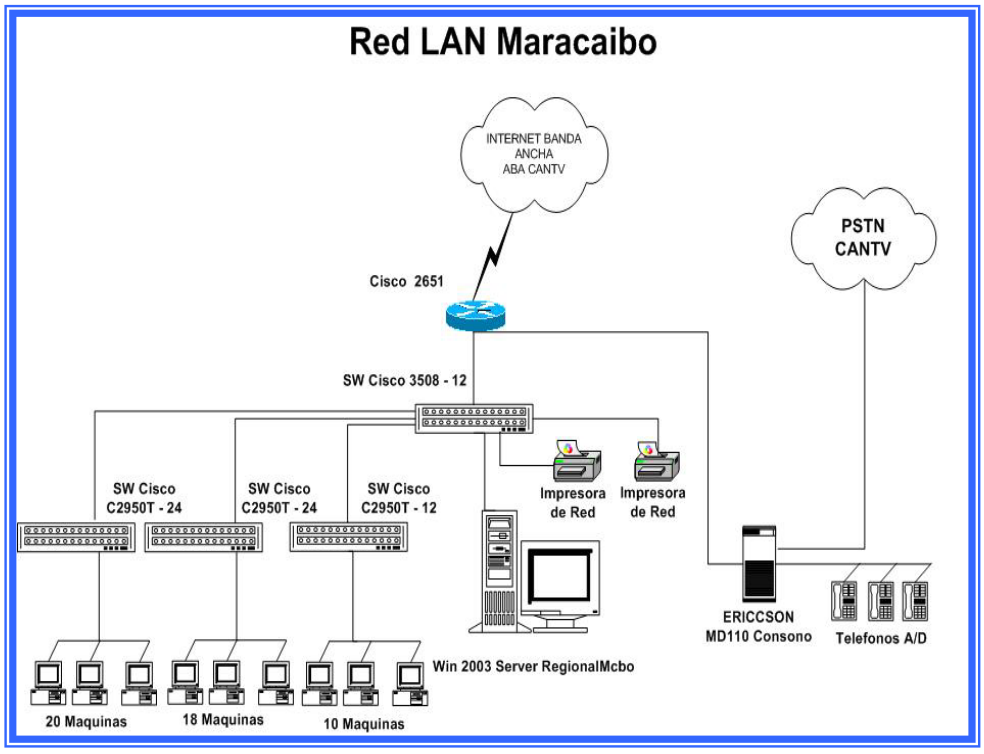

Figura 19
Red LAN Propuesta Maracaibo
Fuente: Venequip, S.A.
Elaborado: Falcón (2006)

Red LAN Caracas:

a. Un (1) Servidor de aplicaciones varias, con sistema operativo Windows 2003 Server.

b. Treinta y cinco (35) estaciones de trabajo las cuales operan en su mayoría con el Sistema Operativo Windows 2000 Professional.

c. Una (1) Central telefónica ERICCSON MD-110 que da servicios de llamadas internas sin restricciones y salientes solo a personal autorizado.

d. Dos (2) Switch Catalyst C2950T Cisco 24 puertos.

e. Un (1) Switch Cisco 3508 12 puertos.

f. Un (1) Router Cisco 2651.

g. Una (1) Tarjeta Cisco VWIC-2MFT-E1-DI.

Como se observa en la Figura 20.

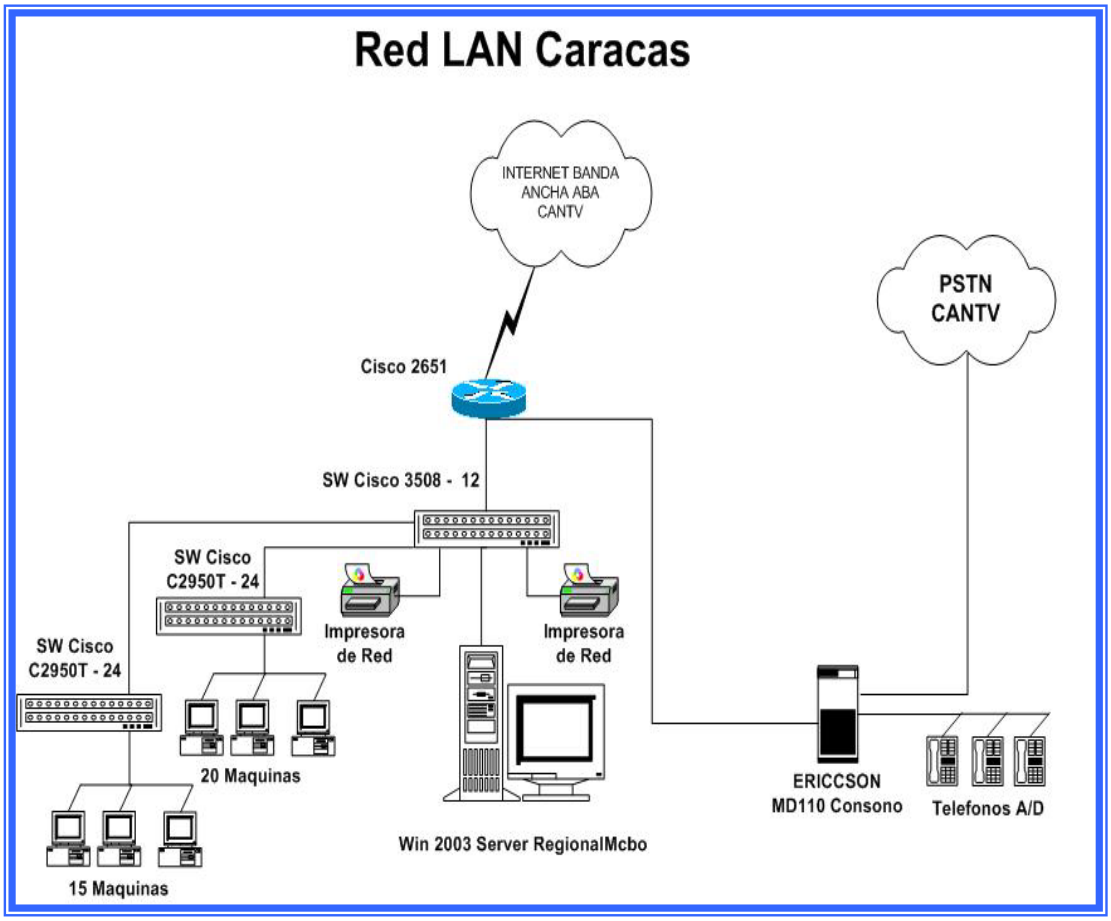

Figura 20
Red LAN Propuesta Caracas
Fuente: Venequip, S.A.
Elaborado: Falcón (2006)

Red LAN Puerto La Cruz:

a. Un (1) Servidor de aplicaciones varias, con sistema operativo Windows 2003 Server.

b. Cuarenta y Tres (43) estaciones de trabajo las cuales operan en su mayoría con el Sistema Operativo Windows 2000 Professional.

c. Una (1) Central telefónica ERICCSON MD-110 que da servicios de llamadas internas sin restricciones y salientes solo a personal autorizado.

d. Dos (2) Switch Catalyst C2950T Cisco 24 puertos.

e. Un (1) Switch Cisco 3508 12 puertos.

f. Un (1) Router Cisco 2651.

g. Una (1) Tarjeta Cisco VWIC-2MFT-E1-DI.

Como se observa en la Figura 21.

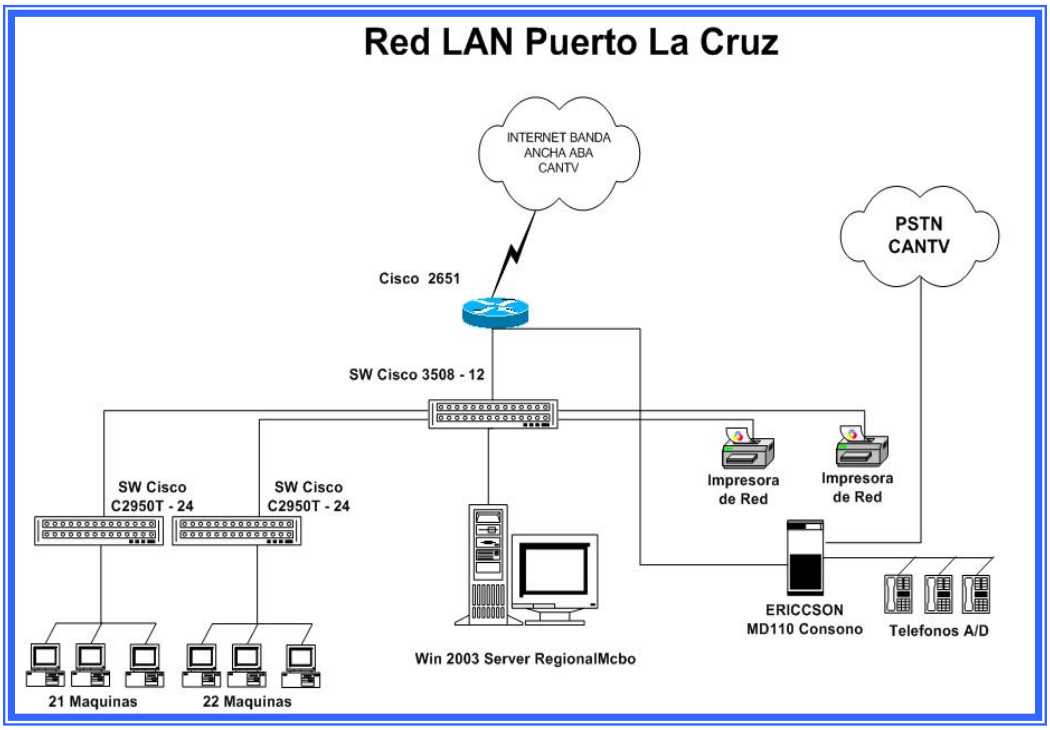

Figura 21
Red LAN Propuesta Puerto La Cruz
Fuente: Venequip, S.A.
Elaborado: Falcón (2006)

Red LAN Puerto Ordaz:

a. Un (1) Servidor de aplicaciones varias, con sistema operativo Windows 2003 Server.

b. Cuarenta y Cinco (45) estaciones de trabajo las cuales operan en su mayoría con el Sistema Operativo Windows 2000 Professional.

c. Una (1) Central telefónica ERICCSON MD-110 que da servicios de llamadas internas sin restricciones y salientes solo a personal autorizado.

d. Dos (2) Switch Catalyst C2950T Cisco 24 puertos.

e. Un (1) Switch Cisco 3508 12 puertos.

f. Un (1) Router Cisco 2651.

g. Una (1) Tarjeta Cisco VWIC-2MFT-E1-DI.

Como se observa en la Figura 22.

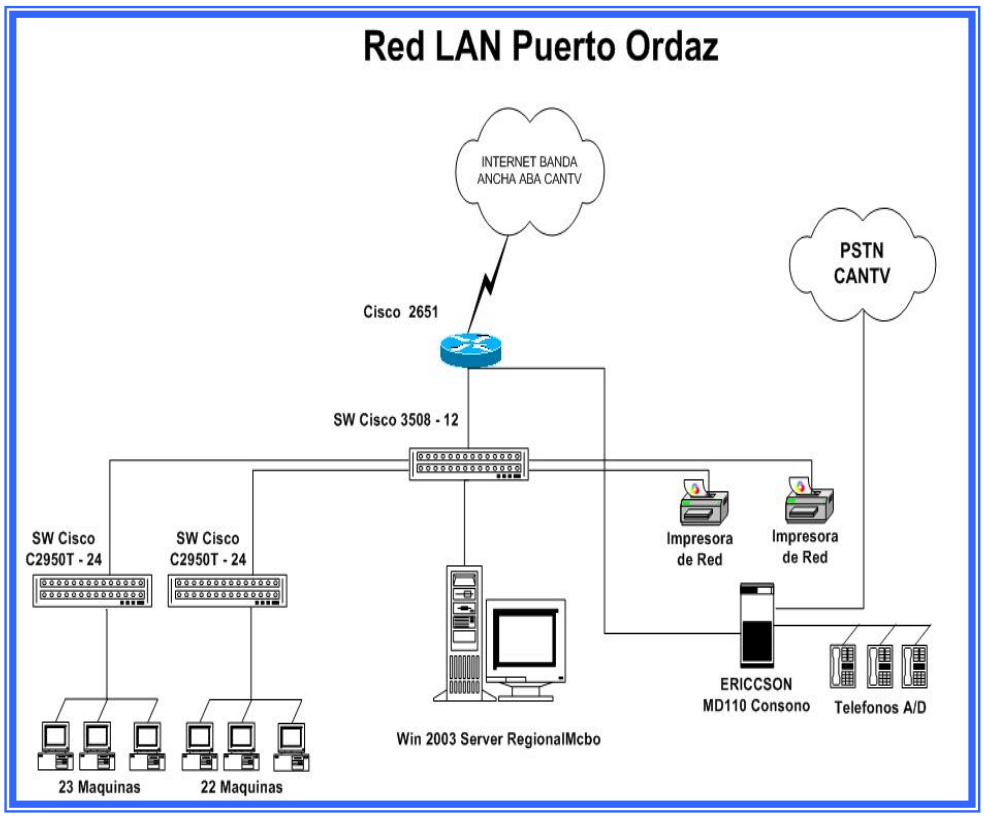

Figura 22
Red LAN Propuesta Puerto Ordaz
Fuente: Venequip, S.A.
Elaborado: Falcón (2006)

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Después de haber analizado los resultados arrojados en el diagnóstico de la situación actual de los enlaces existentes en la empresa Venequip y los resultados de la propuesta de diseño de una red VPN se puede afirmar que con la sustitución del enlace existente se lograra el aumento del ancho de banda entre las sucursales de la empresa Venequip S.A., a un costo menor al actual lo que traería como consecuencia que los usuarios de la red tendrían una mayor velocidad para realizar sus transacciones entre las diferentes sucursales disminuyéndoles considerablemente los costos fijos mensuales que cancela la empresa por concepto de comunicación.

Con la puesta en marcha de la propuesta para la migración a una VPN propietaria la empresa Venequip S.A. lograra una disminución de más del 50 % de lo que paga actualmente por el servicio Frame Relay: En el análisis de costos se demostró que:

1. Se obtendrá un ahorro mensual de **4494,59 $**

2. El retorno de la inversión se lograra en aproximadamente un año y 6 meses.

3. Se obtendrán altos niveles de seguridad en las redes

Lo que se traduce en ahorros para la empresa y propicia el ambiente para que se hagan inversiones importantes en el área de tecnologías de información y

comunicaciones. En el mismo orden de ideas se pretende que esta propuesta aporte grandes beneficios económicos y de seguridad a la empresa Venequip, S.A., así como también a otras empresas locales y nacionales que estén interesadas en mantener una infraestructura de comunicaciones acorde a los cambios tecnológicos actuales que aporten mayor valor agregado a sus transacciones y a sus operaciones, tanto a nivel económico, como a nivel operativo y de seguridad.

Los clientes pueden utilizar este servicio VPN para crear sus extranets, intranets y proveer acceso remoto a sus redes locales. Permite que la empresa extiendan sus comunicaciones dentro y fuera de su organización, lo cual les brinda mayor productividad en sus procesos al conectar sus oficinas, sucursales y/o empleados remotos a la red corporativa principal, e incluso conectarse con sus clientes, proveedores, distribuidores y socios.

De igual manera se concluye que con la sustitución de los equipos existentes las sucursales seleccionadas como piloto estarán actualizados en cuanto a tecnología se refiere, además que tendrían mayor control sobre la seguridad de sus plataformas ya que la configuración de los túneles y filtrado de personas que tendrían acceso a la red estarían en manos de la gerencia nacional de sistemas de la empresa VENEQUIP S.A., la cual está conformada por personal altamente capacitado, lo que les garantizará el funcionamiento, mantenimiento y seguridad del enlace.

Se demostró la factibilidad técnica, operativa y económica de la sustitución del enlace existente entre las sucursales de la empresa VENEQUIP S.A. por una VPN propietaria por lo que se puede afirmar que es totalmente factible la implantación y

puesta en marcha de la misma, logrando una disminución significativa en cuanto a gastos de conexión y de soporte se refiere ya que será la misma empresa quien administre su red y ancho de banda para cada sucursal recuperando la inversión en un lapso de un año y seis meses aproximadamente.

RECOMENDACIONES

Se le recomienda a la gerencia nacional de sistemas realizar la implantación y puesta en marcha de la VPN para las sucursales de Barquisimeto, Maracaibo, Caracas, Puerto La Cruz y Puerto Ordaz.

Además se sugiere que la administración de los servicios de red sea realizada de una manera equitativa para evitar congestionamiento en alguna de las sucursales.

Ir incorporando poco a poco el resto de las sucursales de la Empresa VENEQUIP S.A., para de ésta forma mantener todo la empresa bajo una misma plataforma.

Contratar los servicios de otros proveedores de Internet banda ancha como respaldo en caso de que el enlace de Internet que se tenga presente fallas técnicas.

BIBLIOGRAFÍA

Alan A., Freier P. Kocher P. C. (2001). **The SSL Protocol Versión 3.0.** Internet Draft.

Arévalo J. (2003), **"Como escoger e implementar una vpn conceptos teóricos y prácticos"**, trabajo de grado para optar al titulo de Ingeniero electrónico en la Universidad del Valle en Colombia. Sitio Web disponible: http:\\eiee.univalle.edu.co

Black, U. (2000). **Redes de Computadoras, Protocolos, Normas e Interfaces.** México: Prentice Hall – Hispanoamericana.

Camacaro, D. (2002). **Propuesta de Redes LAN y MAN de la Empresa ENELBAR.** Trabajo de Grado para optar al título de Ing. en Computación. Facultad de Ingeniería. Universidad Fermín Toro. Cabudare, Venezuela.

Carballar, M. (2002). **Funciones de las Redes de Computadoras.** México: Prentice-Hall Hispanoamericana S.A.

Cisco System [Página Web] Disponible http://www.ciscosystem.com

Diffie, W., Hellman, M. (1976). **New directions in Cryptography. IEEE Transactions on information Theory**.

Douskalis, B. (2000). **IP telephony: the integration of robust VoIP services**. New Jersey: Prentice Hall

Hamdi, M., Verscheure, O., Hubaux, J-P., Dalgic, I. y Wang. P. (Mayo. 1999).**Voice Service Interworking for PSTN and IP Networks**.

Huidobro, J. (2000). **Todo Sobre Comunicaciones.** Tercera Edición, España: Paraninfo.

Hurtado, J. (1998). **Metodología de la Investigación Holística**. Caracas: SYPAL Servicio y Proyecciones para América Latina.

Jeanton, H. (2002). **Proponer una Red de Área Extensa (WAN), para Interconectar las Redes Locales (LAN) de las Plantas Embotelladoras del Grupo Terepaima.** Trabajo de Grado para optar al título de Ing. en Computación. Facultad de Ingeniería. Universidad Fermín Toro. Cabudare, Venezuela.

Mason, Andrew. (2002) **Cisco Secure Virtual Private Networks**. Editorial Prentice Hall. Primera Edición

Mendoza, M. (2002). **Propuesta de Instalación de una Red Privada Virtual (VPN) Empleando la Red Híbrida Nodal de Fibra Óptica y Cable Coaxial (HFC) de la Empresa InterCable.** Trabajo de Grado para optar al título de Ing. en Computación. Facultad de Ingeniería. Universidad Fermín Toro. Cabudare, Venezuela.

Minoli, D. y Minoli. E. (1998). **Delivering Voice over IP Networks**. New York: John Wiley & Sons. Inc.

Monografias.Com [Página Web] Disponible http://www.monografias.com

Naranjo, A. (2001). **Redes de Computadoras y Procesamiento de Datos.** España: Mc Graw Hill.

Networks. **IEEE Communications**. 32(9):33-38. September 1994.

Redes de Area Local (2000). [Página Web en Línea]. Disponible http://www.geocities.com/Athens/Olympus/7428/red1.com.[Consulta 2006 marzo 14]

Rodríguez, J. (Agosto, 1999). El papel de la Información. **Global Communications.**

Rodríguez, P. (2.003), en su trabajo titulado **"Interconexión de Voz, Datos y Video para la empresa Inversiones Tecnológicas C.A."** Trabajo de Grado para optar al título de Ing. en Computación. Facultad de Ingeniería. Universidad Fermín Toro. Cabudare, Venezuela.

Stallings, W. (1999). **Cryptography and Network Security.** Prentice Hall.

Tanenbaun, A. (2000). **Redes de Ordenadores**. México: Prentice - Hall Hispanoamericana S.A.

Tecnologías de Comunicación (2001). [Página Web en Línea]. Disponible http://www.geocities.com/siliconvalley/hardware/8840/nuevo3 [Consulta 2006 Marzo 14].

Universidad Centroccidental Lisandro Alvarado (2002). **Manual para la presentación del trabajo conducente al grado académico de: Especialización, Maestría, Doctorado.** Universidad Centroccidental Lisandro Alvarado, Decanato de Ciencias y Tecnología. Barquisimeto (Venezuela).

Vela, E. (2001). **Redes de Computadoras en la Actualidad**. México: Prentice - Hall Hispanoamericana S.A.

ANEXOS

ESPECIFICACIONES TECNICAS DE EQUIPOS A USAR Y DE LOS EQUIPOS A SUSTITUIR

Cisco Router 3810 V

Cisco 3810 Router

This Cisco MC3810 is a compact, cost-efficient multiservice access device which integrates voice, data and video traffic over a variety of services.

The Cisco MC3810 product utilizes Cisco IOS routing to provide superior performance and unmatched interface handling. Cisco's proven switching and routing technologies allow you to design networks that integrate legacy data, Ethernet, analog or digital voice, fax, and video into a common communications network that significantly reduces network costs.

The Cisco MC3810 series is designed to scale from low-speed leased-line environments up to 56 Kbps to 2.048 Mbps Frame Relay and T1/E1 ATM networks with a simple software change. The Cisco MC3810 will also work with a full range of Cisco routers and switches, so you can enjoy the benefits of a single end-to-end networking solution. Benefits such as reduced equipment costs, improved performance, and centralized management make the combined Cisco backbone and Cisco MC3810 solution unique.

The Cisco MC3810 supports either analog or digital voice connections. The analog configuration allows 1 to 6 ports of analog voice. When configured for digital operation, the Cisco MC3810 will support up to 24 channels of compressed voice.

The Cisco MC3810 flexibility enables it to be deployed within public and private networks and supports a variety of network services and applications.

Tarjeta conversora de voz VWIC-E1-D1

Data Features
• T1/E1 or fractional T1/E1 network interface
• N X 64 Kbps or N X 56 Kbps, nonchannelized data rates (T1:N=1 to 24, E1:n=1 to 31)
• Standards based, including ANSI T1.403 and AT&T Publication 62411

T1 Network Interface

Transmit Bit Rate	1.544 Mbps +/- 50 bps/32 PPM
Receive Bit Rate	1.544 Mbps +/- 50 bps/32 PPM
Line Code	AMI, B8ZS
AMI Ones Density	Enforced for N x 56 Kbps channels
Framing Format	D4 (SF) and ESF
Output level (LBO)	0, -7.5, or -15 dB
Input Level	+1dB0 down to -24 dB0
DTE Interface (WIC mode)	Fractional Service
DTE Interface (VIC mode)	G.704/structured
DCE Interface	G.704/structured

E1 Network Interface

Transmit Bit Rate	2.048 Mbps +/- 100 bps/50 PPM
Receive Bit Rate	2.048 Mbps +/- 100 bps/50 PPM
Data Rate	1.984 Mbps (framed mode) Per E1 Port
Clocking	Internal and Loop (recovered from network)
E1 National Bits	Fixed (non-configurable)
Encoding	HDB3
DTE Interface (WIC mode)	Fractional Service
DTE Interface (VIC mode)	G.704/structured
DCE Interface	G.704/structured

Dimensions and Weight (H x W x D)
• 0.8 in. x 3.1 in. x 4.8 in.
• (2.1 x 7.9 x 12.2 cm)
Weight
• .12 lb (56 g) (minimum)
• .18 lb (81 g) (maximum)

Diagnostics

• ANSI T1.403 Annex B/V.54 loopup/down code recognition, network loopback, and user initiated loopbacks, network payload loopback, local data terminal equipment (DTE) loopback, remote line (codes: V.54, loop up, and loop down)
• BERT patterns all 0's, all 1's, 1:2, 1:8, 3:24, QRW, QRSS, 63, 511, 2047 and V.54/T1.403 annex B bit patterns, two user-programmable 24-bit patterns
• Alarm detection: alarm indication signal (AIS), time slot 16 AIS, remote alarm, far-end block error (FEBE), out of frame (OOF), cyclic redundancy check (CRC) multiframe OOF, signaling multiframe OOF, frame errors, cycle redundancy checks (CRC) errors, Loss of network signal (red alarm), loss of network frame, receive (blue alarm) (AIS) from network, receive (yellow) from network Performance Reports / Error Counters CRC, errored seconds, burst errored seconds, severely errored seconds, Ft and Fs framing errors for SF framing, FPS framing errors for ESF framing, 24-hour history stored in 15-minute increments
• Onboard processor for real-time facility data link (FDL) messaging, in-band code detection and insertion, alarm integration, and performance monitoring
• Full FDL support and FDL performance monitoring, according to configurable standard: ANSI T1.403 or AT&T TR 54016
DSU/CSU
• Selectable DSX-1 cable length in increments from 0 to 655 feet in DSU mode)
• Selectable DS1 CSU line build-out: 0, -7.5, -15, and -22.5 dB
• Selectable DS1 CSU receiver gain: 26 or 36 dB
Packet Voice Support
On the voice network modules, the basic voice connectivity is as follows:
• The 1-port T1 Multiflex VWIC connects 1 to 24 DS0 channels (voice calls) to the network module
• The 2-port T1 Multiflex VWIC or 2-port Drop and Insert T1 Multiflex VWIC connect 1 to 48 DS0 channels (voice calls) to the network module
• The 1-port E1 Multiflex VWIC connects 1 to 30 DS0 channels (voice calls) to the network module
• The 2-port E1 Multiflex VWIC or 2-port Drop and Insert E1 Multiflex VWIC connect 1 to 60 DS0 channels (voice calls) to the network module
See the data sheet of each network module (NM-HDV, NM-HD-2VE, and NM-HDV2) for further details.
LEDs
• CD (Data Carrier Detect)
• LP (loopback)
• AL (Alarm)

Management

Telnet/Console Remote and local configuration, monitoring, and troubleshooting from Cisco IOS Command Line Interface
SNMP Router and DSU/CSU managed by single SNMP agent; router/DSU/CSU appear as single network entity to user
Standard MIB (MIB II)
Cisco integrated DSU/CSU MIB

RFC 1406 T1 MIB, including alarm detection and reporting
SNMP Traps Generated in response to alarms

Environmental

• Operating Temperature: 0 to 40º C (32 to 104° F)
• Storage Temperature: -25 to +70º C (-13 to 158° F)
• Relative Humidity
–5 to 85% noncondensing operating
–5 to 95% noncondensing, nonoperating

T1 Compliance (Partial List)

• ANSI T1.403
• US (UL 1950, T1)
• FCC Part 68
• CS-03
• Canada (CSA 950, T1)
• US (FCC Part 15 Class B, T1)
• U.K. (BS6301, EN60950, EN41003)
• Canada (CSA C108.8 Class A, T1)
• Bellcore-AT&T Accunet (62411)
• ATT 54016
• Japan (VCCI Class 2, VCCI:V-3/97.04, T1, JATE Green Book, IEC950)

E1 Compliance (Partial List)

• Australia (TS 016, AS/NZS 3548:1995)
• Germany (TUV GS, EN60950)
• Germany (VDE 0878 part 3 and 30)
• France (NFC98020, EN60950, EN41003)
• Sweden (SS447-2-22, SS636334, EN60950)
• UK (NTR4)
• Europe (EN55022 Class B, EN55102-1, EN55102-2, CTR12, EN60950, EN50082-1:1992, EN55022:1994)
• CCITT/ITU G.704, I.431
• ETSI NET5, ETS300156
• TBR4
• CTR-13
• ETS 300011
• ITU I.431

Cisco Router 2651

The Security Policy document is part of the complete FIPS 140-1 Submission Package. In addition to this document, the complete Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Module Software Listing
- Other supporting documentation as additional references

This document provides an overview of the Cisco 2651 router and explains the secure configuration and operation of the module. This introduction section is followed by the "Cisco 2651 Modular Access Routers" section, which details the general features and functionality of the Cisco 2651 router. The "Secure Operation of the Cisco 2651 Router" section specifically addresses the required configuration for the FIPS-mode of operation.

This Security Policy and other Certification Submission Documentation was produced by Corsec Security, Inc. under contract to Cisco Systems. With the exception of this Non-Proprietary Security Policy, the FIPS 140-1 Certification Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

Cisco 2651 Modular Access Routers

Branch office networking requirements are dramatically evolving, driven by web and e-commerce applications to enhance productivity and converging the voice and data infrastructure to reduce costs. The Cisco 2651 modular multi-service router offers versatility, integration, and security to branch offices. With over 70 network modules and interfaces, the modular architecture of the Cisco router easily allows interfaces to be upgraded to accommodate network expansion. The Cisco 2651 provides a scalable, secure, manageable remote access server that meets FIPS 140-1 Level 2 requirements. This section describes the general features and functionality provided by the Cisco 2651 router. "Secure Operation of the Cisco 2651 Router" section provides further details on how the router addresses FIPS 140-1 requirements.

The Cisco 2651 Cryptographic Module

The metal casing that fully encloses the module establishes the cryptographic boundary for the router, all the functionality discussed in this document is provided by components within the casing. Cisco IOS features such as tunneling, data encryption, and termination of Remote Access WANs via IPSec, Layer 2 Forwarding (L2F) and Layer 2 Tunneling Protocols (L2TP) make the Cisco 2600 an ideal platform for building virtual private networks or outsourced dial solutions. Cisco 2600\Qs RISC-based processor provides the power needed for the dynamic requirements of the remote branch office, achieving wire speed Ethernet to Ethernet routing with up to 25 thousand packets per second (Kpps) throughput capacity.

The Cisco 2600 series features single or dual fixed LAN interfaces, a network module slot, two Cisco WAN interface card (WIC) slots, and a new Advanced Integration Module (AIM) slot. LAN support includes single and dual Ethernet options; 10/100 Mbps auto-sensing Ethernet; mixed Token-Ring and Ethernet; and single Token Ring chassis versions. WAN interface cards support a variety of serial, ISDN BRI, and integrated CSU/DSU options for primary and backup WAN connectivity, while available network modules support multi-service voice/data/fax integration, departmental dial concentration, and high-density serial options. The AIM slot supports integration of advanced services such as hardware-assisted data compression and encryption. All Cisco 2600 series routers include an auxiliary port supporting 115Kbps Dial On Demand Routing, ideal for back-up WAN connectivity.

The physical interfaces include power plug for the power supply and a power switch. The router has two Fast Ethernet (10/100 RJ-45) connectors for data transfers in and out. The module also has two other RJ-45 connectors on the back panel for a console terminal for local system access and an auxiliary port for remote system access or dial backup using a modem. The 10/100Base-T LAN ports have Link/Activity, 10/100Mbps, and half/full duplex LEDs.

Switch C2950 T

Technical Specifications

Environmental Ranges

Operating temperature	32 to 113°F (0 to 45°C)
Storage temperature	-13 to 158°F (-25 to 70°C)
Operating humidity	10 to 85% (noncondensing)
Operating altitude	Up to 10,000 ft (3000 m)
Storage altitude	Up to 15,000 ft (4570 m)
Shock	84 in. per sec (2.13 m per sec)1

Power Requirements

AC input voltage 100 to 127/200 to 240 VAC
(autoranging) 50 to 60 Hz
DC input voltages for the Cisco RPS2 300 Redundant Power System
+12 V @4.5 A

DC input voltages for the Cisco RPS 675 +12 V @4.5 A

Power consumption 30 W (maximum)
102 Btus per hour
Power rating 0.05 kVA

Physical Dimensions

Weight 6.5 lb (3 kg)
Dimensions
(H x W x D) 1.72 x 17.5 x 9.52 in.
(4.36 x 44.45 x 24.18 cm)

1 This switch meets ASTM D3332.
2 RPS = redundant power system

Operating temperature
32 to 113°F
(0 to 45°C) 32 to 113°F
(0 to 45°C)

Storage temperature
-13 to 158°F
(-25 to 70°C) -13 to 158°F
(-25 to 70°C)

Operating humidity
10 to 85% (noncondensing) 10 to 85% (noncondensing)

Operating altitude	Up to 10,000 ft (3000 m)	Up to 10,000 ft (3000 m)
Storage altitude	Up to 15,000 ft (4570 m)	Up to 15,000 ft (4570 m)

Shock 84 in. per sec
(2.13 m per sec)1
84 in. per sec
(2.13 m per sec)

Power Requirements

AC input voltage 100 to 127/200
to 240 VAC (autoranging)
50 to 60 Hz 100 to 127/200
to 240 VAC (autoranging)
50 to 60 Hz

DC input voltage for the Cisco RPS2 300
+12 V @4.5 A
+12 V @4.5 A

DC input voltage for the Cisco RPS 675 +12 V @4.5 A
+12 V @4.5 A

Power consumption 30 W (maximum)
102 Btus per hour 45 W (maximum)
154 Btus per hour

Power rating 0.05 kVA 0.075 kVA

Physical Dimensions

Weight 6.5 lb (3 kg) 10.5 lb (4.8 kg)

Dimensions
(H x W x D) 1.72 x 17.5 x 9.52 in.
(4.36 x 44.45 x 24.18 cm) 1.72 x 17.5 x 13 in.
(4.36 x 44.45 x 33.02 cm)

1 This switch meets ASTM D3332.
2 RPS = redundant power system

Switch 3508

Technical Specifications

Environmental Ranges

Operating temperature	32 to 113°F (0 to 45°C)
Storage temperature	-4 to 149°F (-10 to 65°C)
Operating humidity	10 to 85% (noncondensing)
Operating altitude	Up to 10,000 ft (3000 m)
Storage altitude	Up to 15,000 ft (4570 m)

Power Requirements

AC input voltage	100 to 127/200 to 240 VAC (autoranging) 50 to 60 Hz
DC input voltages	+3.3V @14A, +12V @3A
Power consumption	82.2W 280 Btus per hour

Physical Dimensions

Weight	12 lb (5.45 kg)
Dimensions (H x W x D)	1.75 x 16 x 17.5 in. (4.45 x 40.46 x 44.45 cm)

Environmental Ranges			
Operating temperature	32 to 113°F (0 to 45°C)	32 to 113°F (0 to 45°C)	32 to 113°F (0 to 45°C)
Storage temperature	-4 to 149°F (-10 to 65°C)	-4 to 149°F (-10 to 65°C)	-4 to 149°F (-10 to 65°C)
Relative humidity	10 to 85% (noncondensing)	10 to 85% (noncondensing)	10 to 85% (noncondensing)
Operating altitude	Up to 10,000 ft (3000 m)	Up to 10,000 ft (3000 m)	Up to 10,000 ft (3000 m)
Storage altitude	15,000 ft (4570 m)	15,000 ft (4570 m)	15,000 ft (4570 m)
Power Requirements			
AC input voltage	100 to 127/200 to 240 VAC (autoranging) 50 to 60 Hz	100 to 127/200 to 240 VAC	

(autoranging) 50 to 60 Hz 100 to 127/200 to 240 VAC
(autoranging) 50 to 60 Hz
DC input voltages +5V

Power consumption 50W
171 Btus per hour 75W
256 Btus per hour 100W
600 Btus per hour
Physical Dimensions
Weight10.25 lb (4.65 kg) 8.5 lb (3.86 kg) 12 lb (5.45 kg)
Dimensions (H x D x W) 1.75 x 11.82 x 17.5 in.
(4.45 x 30.02 x 44.45 cm) 1.75 x 11.82 x 17.5 in.
(4.45 x 30.02 x 44.45 cm) 1.73 x 15.34 x 17.5 in
(4.39 x 39.0 x 44.45 cm)

Environmental Ranges

Operating temperature	32 to 113°F (0 to 45°C)
Storage temperature	-4 to 149°F (-10 to 65°C)
Operating humidity	10 to 85% (noncondensing)
Operating altitude	Up to 10,000 ft (3000 m)
Storage altitude	Up to 15,000 ft (4570 m)

Power Requirements
AC input voltage 100 to 127/200 to 240 VAC
(autoranging) 50 to 60 Hz
DC input voltages -48V

@3A,
+12V

@6A
Power consumption 325W1
1100 Btus per hour
Physical Dimensions
Weight10.25 lb (4.65 kg)
Dimensions (H x W x D) 1.75 x 11.82 x 17.5 in.
(4.45 x 30.02 x 44.45 cm)
1The actual power consumption depends on the number of IP phones connected. 325W represents 24 IP phones connected.

Safety EMC
UL to UL 1950, Third Edition FCC Part 15 Class A

c-UL to CAN/CSA 22.2 No. 950-95, Third Edition EN 55022 Class A (CISPR 22 Class A)
TUV/GS to EN 60950 with Amendment A1-A4 and A11 VCCI Class A
ACA/A2LA to AS/NZS 3260 and TS001-1997 AS/NZS 3548 Class A
CB to IEC 60950 with all country deviations BSMI
NOM to NOM-019-SCFI CE Marking
CE Marking

Switch 3508

Tarjeta Conversora de voz VWIC

Switch ws-c2950-24

Router Cisco 3800 Series

Router Cisco 2651