DESCRIPCIÓN DEL MONTAJE DE UNA RED WAN
PARA LA INTERCONEXIÓN DE SEDES EMPRESARIALES A NIVEL NACIONAL

MAURICIO ALEJANDRO SALCEDO DIAZ
WILFRIDO CONRADO HINCAPIE PINTO

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
MINOR EN COMUNICACIONES Y REDES
CARTAGENA DE INDIAS, D.T. Y C.
DICIEMBRE
2004

DESCRIPCIÓN DEL MONTAJE DE UNA RED WAN
PARA LA INTERCONEXIÓN DE SEDES EMPRESARIALES A NIVEL NACIONAL

MAURICIO ALEJANDRO SALCEDO DIAZ
WILFRIDO CONRADO HINCAPIE PINTO

Trabajo final de monografía presentado como requisito para aprobar el Minor de Comunicaciones y Redes

Director

GONZALO LOPEZ
Ingeniero Electrónico

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
MINOR EN COMUNICACIONES Y REDES
CARTAGENA DE INDIAS, D.T. Y C.
DICIEMBRE
2004

Cartagena de Indias, Diciembre de 2004

Señores:
UNIVERSIDAD TECNOLOGICA DE BOLIVAR
Comité de evaluación de proyectos
Ciudad

Estimados Señores:

De la manera más cordial nos permitimos presentar a ustedes para su estudio, consideración y aprobación el Trabajo Final Titulado “DESCRIPCIÓN DEL MONTAJE DE UNA RED WAN PARA LA INTERCONEXIÓN DE SEDES EMPRESARIALES A NIVEL NACIONAL”. Trabajo Final Presentado para aprobar el Minor de Comunicaciones y Redes.

Esperamos que este proyecto sea de su total agrado.
Cordialmente,

_____	_____
Mauricio Alejandro Salcedo Díaz	Wlifrido Conrado Hincapié Pinto
Cod. 9804504	Cod. 9804512

AUTORIZACIÓN

Cartagena de Indias, D.T. y C. Diciembre de 2004

Nosotros MAURICIO ALEJANDRO SALCEDO DIAZ Y WILFRIDO CONRADO HINCAPIE PINTO, autorizamos a la UNIVERSIDAD TECNOLOGICA DE BOLIVAR para hacer uso de nuestro trabajo de grado y publicarlo en el catalogo online de la biblioteca

Cordialmente,

_____ _____

Mauricio Alejandro Salcedo Díaz
Cod. 9804504

Wlifrido Conrado Hincapié Pinto
Cod. 9804512

Cartagena de Indias, Diciembre de 2004

Señores:
UNIVERSIDAD TECNOLOGICA DE BOLIVAR
Comité de Evaluación de Proyectos
Ciudad

Estimados Señores:

Con el mayor agrado me dirijo a ustedes para poner a consideración el Trabajo Final Titulado “DESCRIPCIÓN DEL MONTAJE DE UNA RED WAN PARA LA INTERCONEXIÓN DE SEDES EMPRESARIALES A NIVEL NACIONAL”. El cual fue llevado a cabo por los estudiantes MAURICIO ALEJANDRO SALCEDO DIAZ Y WILFRIDO CONRADO HINCAPIE PINTO, bajo mi orientación como asesor.

Agradeciendo su amable atención,
Cordialmente,

_____

GONZALO LOPEZ
Ingeniero Electrónico

Nota de aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Cartagena de Indias, Diciembre de 2004

DEDICATORIA

Dedico esta monografía a toda mi familia, en especial a mi madre Ludys Díaz Anaya por su apoyo moral y económico, a mi abuela Miguelina Anaya de Díaz por soportarme durante toda la vida y en especial durante estos cinco largos años de mi carrera. A mi novia Ana García Trespalacios por su cuidado y comprensión en la etapa final de este largo camino.

Finalmente a mi hermana y mi padre porque de alguna u otra forma me colaboraron en este proceso, también a todos los que olvide mencionar, gracias por todo.

DEDICATORIA

Yo Wilfrido Conrado Hincapié Pinto identificado con C.C # 9.174.834 de C/gena. Quiero dedicar esta monografía a mi Padre celestial que me ha dado las fuerzas y a derramado su bendición sobre mi para realizar este trabajo y culminar mi carrera de Ingeniería Electrónica, Dios mío sin ti no lo hubiese logrado. Mami Elia gracias por ese cariño y amor que me has brindado, reconozco todo tus esfuerzos y sacrificios para educarme y cuidarme eres súper importante para mi que linda eres, Harlon y Williams gracias por estar siempre a mi lado, no se imaginan lo mucho que los quiero, a la Familia Hincapié Taborda y La Familia Pinto Arrieta y en especial a mis abuelitos Esther y Julio, se me cumplió el sueño de que por lo menos ustedes dos estuviesen vivos, al momento de terminara mi carrera. Mi flaca preciosa Mauren y su familia, Mau tu apoyo es indescriptible gracias por tus consejos, este es un paso grande para la realización de nuestros sueños te amo "Chelito".Y no podía faltar la gente de Cántico Nuevo Producciones que me cubrieron en los momentos que mas los necesitaba Néstor, Jaime, Negrito, Elvis, La Red (Johnsi Moyano, Viviana, El Pavo, Omar, Julio, Laurita, Livinston y Elquin), Fabián Ballesteros, Williams Jr. Y Tal Iván Y a todo la gente que hace parte de este gran ministerio que es mi Familia, y Me despido no sin antes mandarles un saludo a toda mi fanaticada del Ministerio Juvenil del CFCI de Cartagena y mis pastores Ramón, Gloria, Fernando y Necid gracias por sus oraciones. Dios les bendiga a todos.

P.D: A mi Papá que (Q.E.P.D), este es el fruto de la semilla que tu sembraste en mi, te llevo en mi mente y en mi corazón. "Solo Dios ha podido sanarme el dolor de tu partida"

Att: PILO

AGRADECIMIENTOS

Agradecemos al Ingeniero Gonzalo López por su asesoría y colaboración, en este proyecto, al cuerpo de profesores de la Universidad Tecnológica, especialmente al profesor Isaac Zúñiga por su paciencia y colaboración, finalmente al Ingeniero Nicolás Milanes de la empresa DETEC S.A. por toda la colaboración prestada durante la realización de este proyecto.

TABLA DE CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

INTRODUCCIÓN

En esta monografía quisimos hacer una descripción de los elementos, protocolos y equipos necesarios para el montaje de una red WAN, teniendo en cuenta que esta será usada para la interconexión de sedes empresariales de cualquier empresa, tanto a nivel nacional como internacional.

Para realizar este trabajo se recopiló información de varias redes WAN, ya montadas por la empresa DETEC S.A. e INTERNEXA para tomarlas como referencia y así mostrar una monografía que se puede tomar como base en el momento de hacer una implementación de una red WAN real. También damos a conocer los distintos tipos de interconexión que existen para mostrar varias opciones en el momento de tomar una decisión.

JUSTIFICACION

Se escogió este tema debido a la acogida que tiene actualmente en las empresas, ya que la interconexión de redes brinda a las empresas la posibilidad de tener todo en un solo lugar, lo cual ayuda a la empresa a ser eficiente lo que se traduce como ahorro de tiempo y a su vez se representa en ahorro para esta. Al interconectar las sedes de una empresa por medio de una red WAN, se logra optimizar los recursos de red y a la vez esta nos brinda la perspectiva de usar aplicaciones de última generación, tales como VoIP que representa un gran ahorro en el costo llamadas ya que la empresa usa su propia red para transportar la voz. Además de esto contamos con el apoyo de la empresa DETEC S.A. para desarrollar el tema, mediante herramientas como catálogos, manipulación de equipos e información en general ya que esta lleva ya bastante tiempo haciendo este tipo de redes.

OBJETIVOS

- GENERAL: Describir el funcionamiento del montaje de interconexión de sedes empresariales a nivel nacional por medio de redes WAN teniendo en cuenta los elementos que se utilizan y sus aplicaciones**.**

- ESPECIFICOS:

  - Describir el funcionamiento de los equipos necesarios para el montaje de una red WAN
  - Presentar el esquema de montaje y la configuración de los equipos utilizados en la interconexión de redes.
  - Visitar las empresas prestadoras de servicio de transporte de datos a nivel nacional para presupuestar costos.
  - Analizar las ventajas que tienen las empresas al montar una red WAN y las aplicaciones que se pueden implementar
  - Comparar las diferentes posibilidades de interconexión y los diferentes protocolos en el mercado Colombiano con el fin de buscar la mejor alternativa para la interconexión de las sedes.

1. GENERALIDADES SOBRE LAS REDES WAN

1.1 DEFINICIÓN

Una red WAN, como su nombre lo indica, se define como una red de área extensa cuyo principal objetivo es el de integrar o unir varias redes LAN (redes de área local) que normalmente se encuentran separadas por grandes áreas geográficas, estas operan en la capa física y la capa de enlace de datos del modelo de referencia OSI.

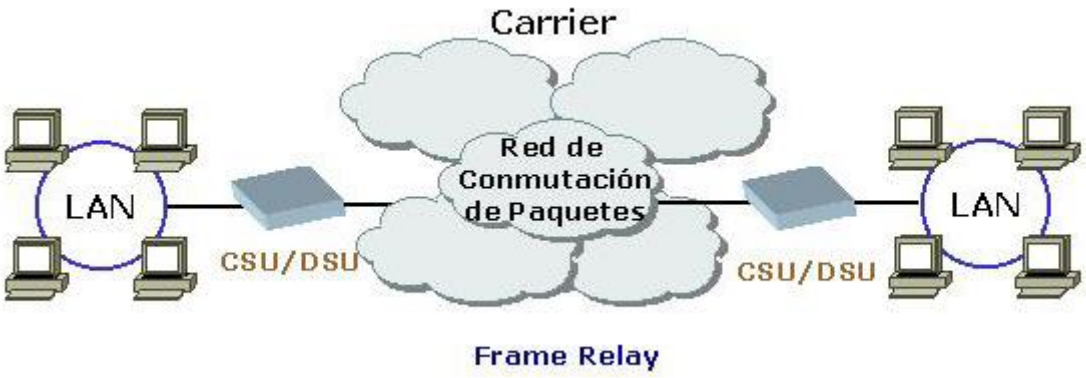
Las redes WAN, para cumplir su objetivo usan los servicios de los proveedores de servicios de telecomunicaciones públicos, tales como Telecom, Internexa, etc., los cuales usan conexiones seriales para ofrecer un ancho de banda determinado.

1.2 TIPOS DE REDES WAN

- Redes conmutadas por circuitos: El principio de funcionamiento es establecer un circuito para la comunicación entre los puntos que se desea intercambio de información. Este canal físico existe durante el diálogo entre ambos nodos, permaneciendo después en el caso de líneas dedicadas o desapareciendo en el caso de utilizar una red conmutada. El establecimiento de una conexión a través de una red telefónica conmutada se basa en el principio de conmutación de circuitos. Este tipo de redes no es usada actualmente debido a que usa línea telefónica lo que representa anchos de banda pequeños. Entre los protocolos usados en este tipo de red se encuentran el POTS y RDSI.

- Redes conmutadas por paquetes: El procedimiento de transferencia de los datos se hace mediante paquetes dotados de direcciones, en el que la vía de comunicación se ocupa solamente durante el tiempo de transmisión de un paquete, quedando a continuación la vía disponible para la transmisión de otros paquetes. En este tipo de sistemas, una comunicación entre dos equipos terminales de datos consiste en el intercambio de paquetes, los cuales viajan por la red a la que se le denominará también de transporte de paquetes a través de un canal lógico, utilizando medios físicos compartidos con otras comunicaciones. Este tipo de redes son muy usadas actualmente debido a las grandes velocidades con que viajan los paquetes y los protocolos que usa son X.25 y Frame Relay.

Figura 1. Esquema de Frame Relay



- Redes conmutadas por celdas: En los servicios de conmutación de celdas, la unidad mínima de datos conmutados es una "celda" de tamaño fijo (53 bytes), en vez de un paquete de longitud variable. La tecnología basada en celdas permite que la conmutación sea realizada en hardware sin la complejidad y el consumo de tiempo de cálculo trama por trama. Esto hace que la conmutación por medio de celdas sea más rápida. Los servicios más conocidos son ATM y SDMS con anchos de banda de hasta 622 Mbps.

- Redes digitales dedicadas: La serie T de servicios en los EE.UU. y la serie E1 de servicios en Europa son tecnologías WAN sumamente importantes. Usan la Multiplexación por división de tiempo para dividir y asignar ranuras de tiempo para la transmisión de datos. Los anchos de banda son muy altos y se dan en T1, T3, E1, E2, etc. y los principales protocolos de este tipo de redes son el xDSL y SONET.

Figura 2. Esquema de redes digitales dedicadas

2. TIPOS DE INTERCONEXION Y EQUIPOS USADOS EN REDES WAN

En este capitulo hablaremos sobre las diferente formas de interconexión mas usadas que para conformar redes WAN además de esto también se mencionaran los equipos necesario para la conformación de estas.

2.1 OPCIONES DE INTERCONEXION

Actualmente existen diversas formas de hacer redes WAN, pero nosotros solo mencionaremos dos, que son las VPN´s y los Canales Dedicados de Comunicación, ya que son los mas usados en Colombia por las empresas tanto generales como las prestadoras de servicios de telecomunicaciones.

2.1.1 VPN´s

Una VPN es una red privada, fue construida sobre la infraestructura de una red pública, la cual normalmente es Internet. Es decir, en vez de utilizar enlaces dedicados (como el X.25 ó Frame Relay) para conectar redes remotas, se utiliza la infraestructura de Internet, una vez que las redes están conectadas es transparente para los usuarios.

La principal motivación para la implementación de las VPN´s es la financiera. Ya que los enlaces dedicados son demasiados costosos, principalmente cuando las distancias son demasiado largas. Por otro lado existe Internet, que por ser una red de alcance mundial, tiene puntos de presencia diseminados por el mundo. Las conexiones con Internet tienen un coste mas bajo que los enlaces dedicados, principalmente cuando las distancias son largas.

Internet es una red pública, donde los datos en transito pueden ser leídos por cualquier equipo. La seguridad en la comunicación entre las redes privadas es imprescindible, se hace necesaria una forma de cambiar los datos codificados, de forma que si fuesen capturados durante la transmisión, no puedan ser descifrados. Los datos transitan codificados por Internet en "Túneles Virtuales" creados por dispositivos VPN´s que utilizan criptografía y encapsulación; y esos dispositivos que son capaces de entender los datos codificados forman, una red virtual sobre la red pública.

2.1.2 CANALES DEDICADOS DE COMUNICACIÓN

Los canales dedicados de comunicación son aquellos en los cuales el usuario esta conectado de forma permanente a través de medios de comunicación inalámbricos o por fibra óptica. Estos canales son suministrados por empresas prestadoras de servicio de telecomunicaciones públicas y privadas.

Las empresas prestadoras de servicios de telecomunicaciones públicas tales como Telecom e Internexa se utilizan para el transporte de datos a nivel nacional, estas hacen la interconexión, a través de microondas y fibra óptica usando la tecnología SDH, con la cual se limita el ancho de banda para el usuario por medio de los time-slots.

Las compañías de telecomunicaciones privadas tales como DETEC S.A., Promitel, ETB, Ductel y Telefónica Data se encargan de suministrar la última milla, a través de fibra óptica, microondas y par dedicado de cobre usando las diferentes tecnologías disponibles para estos tipos de medios.

Hay que tener en cuenta que la mayoría de las empresas que tienen necesidad de interconexión nacional lo hacen a través de las empresas privadas de telecomunicaciones y estas a su vez subcontratan los servicios de las empresas de telecomunicaciones públicas para los enlaces nacionales. Esto es transparente al usuario ya que para este es mas practico contratar los servicios de una sola empresa privada que haga los dos servicios de interconexión que contratar dos empresas, una publica y una privada para hacer la interconexión nacional.

2.2 EQUIPOS USADOS EN INTERCONEXIÓN DE REDES

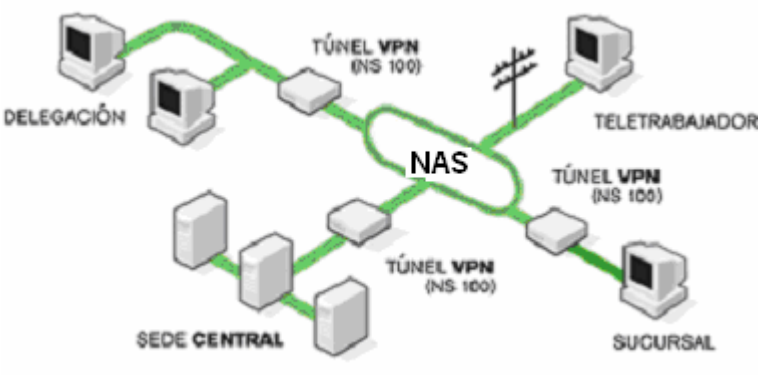
A continuación se describirán los diferentes equipos utilizados en la interconexión de redes WAN tanto para la conformación de VPN´s como para la de los Canales Dedicados De Comunicación.

2.2.1 EQUIPOS USADOS EN VPN´S

Dependiendo del protocolo a utilizar, así mismo existen diferentes equipos de hacer VPN.

Si usamos el protocolo PPTP se usan servidores de acceso de red (NAS), los cuales pueden estar configurados bajo Linux o Windows y en el momento de accesar al equipo NAS este pide automáticamente un nombre de usuario y una contraseña para autenticarse al equipo VPN y cuando termina la autenticación el NAS entrega automáticamente una dirección IP al equipo remoto, lo que quiere decir que el equipo que se conecta a la VPN queda con una IP asignada del mismo rango de la red privada.

Figura 3. Esquema de red VPN usando PPTP



Cuando usamos el protocolo IPsec, el esquema es completamente distinto, ya que se pueden usar tanto equipos PC programados para hacer VPN sobre IPsec como también una gran cantidad de appliances disponibles en el mercado, los cuales se programan de tal manera que cualquier red privada pueda ser vista a través de una dirección publica en Internet, como ejemplo de estos appliances tenemos:

- La VPN RF550VPN de Multitech la cual tiene 4 puertos LAN y un puerto WAN, el cual se conecta directamente a Internet, cuenta con IKE (Internet Key Exchange) y diversos protocolos de encripción como 3DES, un ejemplo del entorno Web usado para configurar la VPN se muestra en la figura 4.

- La Trendnet BW100-BRV204 la cual cuenta con más algoritmos de encripción que la anterior lo que la hace más segura para trabajar sobre redes publicas basadas en IP y un ejemplo de este tipo de VPN se muestra a continuación en la figura 5.

Figura 4. Pantalla Web de configuración de la VPN Multitech

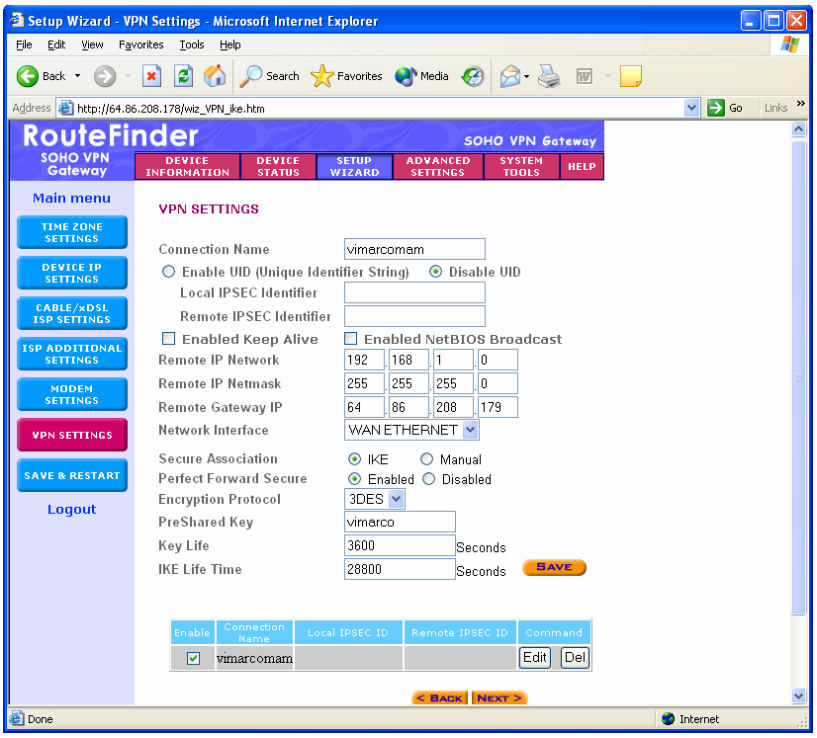
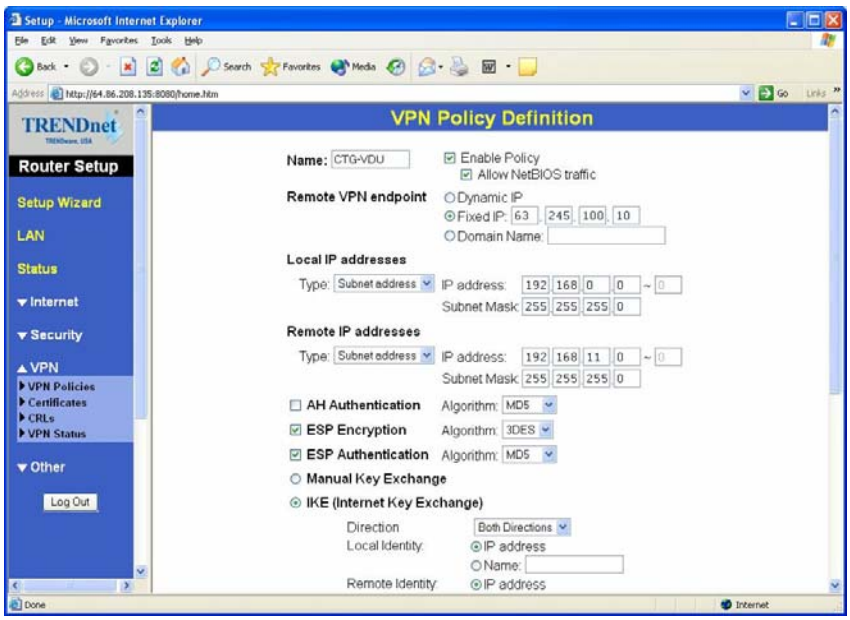


Figura 5. Pantalla Web de configuración de la VPN Trendnet



2.2.2 EQUIPOS USADOS EN CANALES DEDICADOS DE COMUNICACIÓN

El esquema básico de una red WAN para un Canal Dedicado consta de lado y lado de la red de una ultima milla, la cual va conectada a un enrutador, cuya interfaz WAN es serial V.35, pero como los datos a través de esta interfaz viajan sobre redes SDH hay que colocar un equipo intermedio llamado CSU/DSU (fraccionador), el cual convierte la interfaz V.35 en G.703 que son un par de cables coaxiales sobre los cuales viaja el E1.

Figura 6. Esquema básico de una red WAN usando canales dedicados

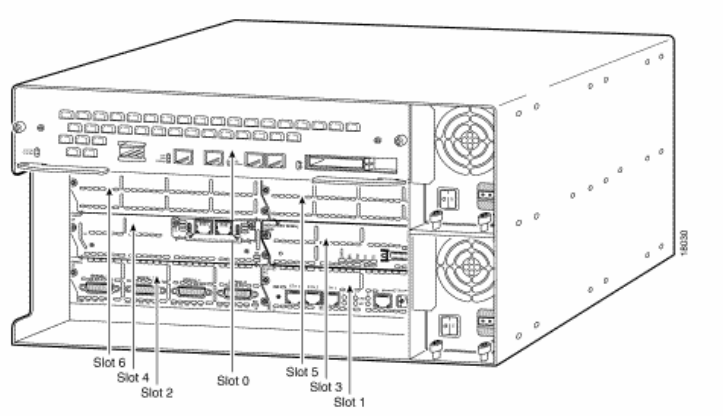
A continuación mostraremos una breve descripción con sus respectivas marcas de los equipos mostrados anteriormente.

- Equipos de Ultima Milla: Dependiendo del tipo de ultima milla, ya sea inalámbrico, por fibra óptica o por par dedicado de cobre, así serán los equipos a usar, por ejemplo si usamos tecnología inalámbrica necesitaremos radios de microondas que trabajen bajo los estándares 802.11b, 802.11a u 802.11g, los cuales cuentan con una interfaz ethernet que va conectada directamente a un switch o a un servidor de alguna aplicación especifica. En la figura 7, vemos un radio Wavecon OR-4200, que trabaja bajo 802.11b

Figura 7. Radio Wavecon OR-4200

- ☑ Enrutadores: Dispositivo que opera en la capa de red del modelo OSI, estos usan una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Envía paquetes de una red a otra basándose en la información de la capa de red, la marca mas usada en el mercado de enrutadores son los Cisco aunque existen otros fabricantes como 3com, IBM y Planet. Como muestra tenemos el cisco 3660

Figura 8. Router Cisco 3660



- ☑ CSU/DSU: También conocidos como fraccionadores, son dispositivos utilizados en la transmisión digital, y sirve para adaptar la interfaz física en un dispositivo DTE/DCE a una instalación de transmisión como T1 o E1. La CSU/DSU también está a cargo de funciones tales como la temporización de las señales para el control del ancho de banda por medio de los time slots que van en la trama SDH.

Figura 9. Fraccionador ADTRAN ESU LT

3. TECNOLOGIAS USADAS EN REDES WAN

En este capitulo se describirán los distintos protocolos mas usados en la conformación de VPN´s, Como los de los Canales Dedicados De Comunicación.

3.1 TECNOLOGIAS USADAS EN VPN´S

3.1.1 PROTOCOLO PPTP

PPTP (Point to Point Tunneling Protocol), es un protocolo que permite el intercambio seguro de datos de un cliente a un servidor, formando una red privada virtual a través de redes basadas en TCP/IP. El punto fuerte de PPTP es la habilidad de proveer soporte multiprotocolo sobre infraestructura de redes ya existentes, tales como el Internet. Esto permite a las empresas establecer redes privadas virtuales sin necesidad de contratar Canales Privados de Comunicación.

La tecnología que hace posible PPTP es una extensión del protocolo de acceso remoto PPP, esta encapsula los paquetes PPP en datagramas IP para la transmisión sobre redes basadas en TCP/IP, las compañías que hicieron posible PPTP y que estuvieron involucradas en el foro PPTP fueron Microsoft, Ascend Communications, 3Com/Primary Access, ECI Telematics y US Robotics.

El funcionamiento básico del protocolo PPTP involucra tres elementos principales que son: Un cliente PPTP, un servidor PPTP y una ISP (Proveedor de Servicio de Internet). El cliente PPTP se conecta a Internet usando la ISP y adquiere la habilidad de intercambiar datos IP sobre esta red y después que el cliente ha hecho la conexión PPP se establece una segunda conexión que es la que permite

establecer una red privada virtual con el servidor PPTP hacia la red privada de la empresa.

El tunneling es el proceso mediante el cual se intercambian datos entre computadores de redes privadas enrutandolos hacia otra red que en este caso es el Internet, cuando el servidor PPTP recibe el paquete de Internet lo envía hacia el computador destino de la red privada procesando la información del paquete PPP que esta encapsulada en el paquete PPTP.

3.1.2 PROTOCOLO IPSEC

IPsec es un protocolo de seguridad de extremo a extremo. Toda la funcionalidad e inteligencia de la conexión VPN reside en los puntos extremos; es decir, gateway o en la computadora central terminal.

Hasta hace poco tiempo se estaban poniendo en servicio diversos protocolos de tunelado IP. En los últimos tres años, sin embargo, IPsec ha sido el protocolo de tunelado IP predominante, y es actualmente la tecnología preferida a la hora de establecer conectividad de sitio a sitio por una red pública. En un principio, IPsec fue desarrollado para establecer comunicaciones privadas por redes IP públicas. El protocolo IPsec permite establecer dos funciones de seguridad principales:

- Autentificación, que permite asegurar la autenticidad e integridad del paquete IP completo.

- Encriptación, que permite asegurar la confidencialidad de los datos transportados.

El protocolo IPsec permite definir un túnel entre dos gateways. Un gateway IPsec consistiría normalmente en un router de acceso o un firewall en el que esté implementado el protocolo IPsec. Los gateways IPsec están situados entre la red privada del usuario y la red pública de Internet.

Los túneles IPsec se establecen dinámicamente y se liberan cuando no están en uso. Para establecer un túnel IPsec, dos gateways deben autentificarse y definir los algoritmos de seguridad y las claves que utilizarán para el túnel. El paquete IP original es encriptado en su totalidad e incorporado en encabezamientos de autentificación y encriptación IPsec. Se obtiene así la carga útil de un nuevo

Paquete IP cuyas direcciones IP de origen y destino son las direcciones IP de red pública de los gateways IPsec. Se establece así la separación lógica entre los flujos de tráfico de la VPN en una red IP compartida. Seguidamente, se utiliza un encaminamiento IP tradicional entre los extremos del túnel.

IPsec consigue estos objetivos mediante:

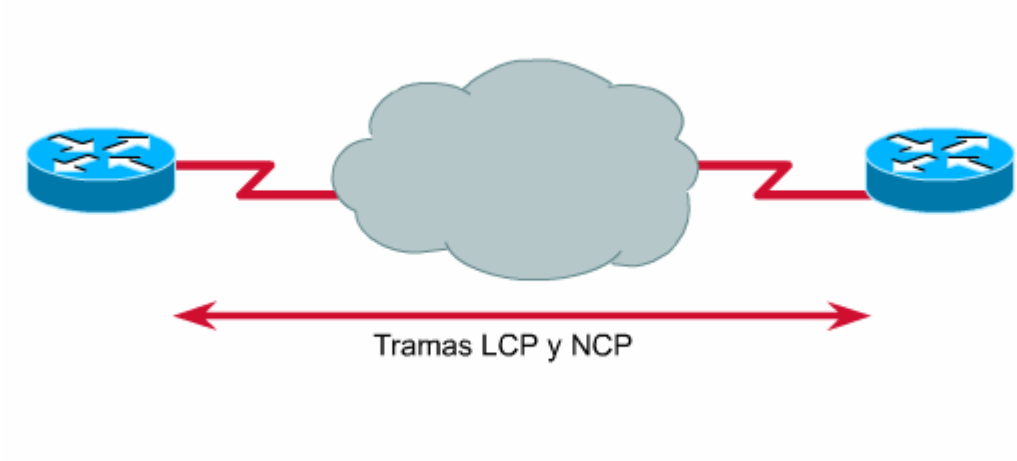
- Dos protocolos de seguridad de tráfico: el encabezamiento de autentificación (AH), que confiere integridad de los datos, y la carga útil de seguridad de encapsulación (ESP), que confiere integridad y confidencialidad de los datos.

- Un protocolo de gestión de clave criptográfica: el denominado ‘intercambio de claves por Internet’ (IKE), que se utiliza para negociar las conexiones IPsec.

3.2 TECNOLOGIAS USADAS EN CANALES DEDICADOS DE COMUNICACIÓN

3.2.1 PPP

Figura 10. Esquema de red usando PPP



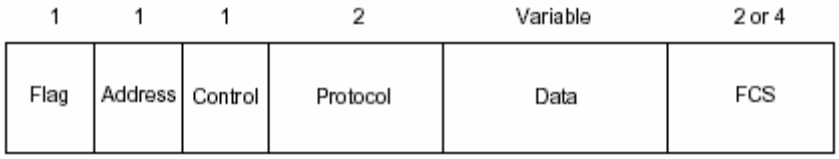
El Protocolo Punto a punto (PPP) originalmente surgió como un protocolo de encapsulación para transportar trafico IP sobre enlaces punto a punto. PPP también estableció una norma para la asignación y manejo de direcciones IP, encapsulación asíncrona (start/stop) y sincrona orientada a bits, configuración de enlace, testeo de calidad del enlace y detección de errores. PPP soporta un Protocolo de Control de Enlace extensible (LCP) y una familia de Protocolos de Control de Red (NCP), para negociar parámetros de configuración opcionales y mejoras.

PPP brinda un método para transmitir datagramas sobre enlaces seriales punto a punto y consta de tres componentes principales:

- Un método para encapsular datagramas sobre enlaces seriales como HDLC.
- Un LCP para establecer, configurar y testear la conexión de enlace de datos
- Una familia de NCP´s para establecer y configurar diferentes protocolos de la capa de red de manera que pueda ser usado para transmitir diferentes protocolos simultáneamente.

El extremo PPP que empieza la comunicación originalmente envía tramas LCP para configurar y testear el enlace y después que el enlace ha sido establecido se envían tramas NCP para escoger y configurar uno o mas protocolos de red y después que han sido configurados los protocolos escogidos pueden ser transmitidos a través del enlace y la comunicación permanece hasta que el LCP o el NCP termine la comunicación o hasta que algún evento externo ocurra.
La trama de PPP se forma de la siguiente manera:

Figura 11. Estructura de la trama PPP



- Flag (Bandera): Es un byte que indica el principio y fin de la trama.

- Address (Dirección): Byte que contiene la dirección de broadcast 11111111 ya que PPP no asigna direcciones a estaciones individuales.

- Control: Es un byte que avisa al otro extremo cuando debe iniciar la transmisión de los datos.

- Protocol: 2 Bytes que identifican el protocolo o los protocolos encapsulados en el campo de datos de la trama.

- Data: Cero o mas bytes que contienen el datagrama con el protocolo especificado en el campo de protocolo.

- FCS (Secuencia de Chequeo de Trama): De 16 hasta 32 bits para mejorar la corrección de errores.

3.2.2 FRAME RELAY

Frame Relay es una nueva técnica de conmutación de paquetes que requiere menos proceso que el antigua protocolo X.25, lo que se traduce en velocidades de acceso mayores 2 a 1,5 Mbps frente a las de X.25 64 a 56 kbps y además permite unos costos de implementación menor.

Esta técnica se describe en las recomendaciones UIT-T.430/31 y Q.922, que añaden funciones de *relay* (repetición) y *routing* (enrutamiento) al nivel de la capa de enlace de datos del modela OSI. El objetivo de diseño fue conseguir un servicio multiplexado que transportara tramas, minimizando los tiempos muertos y el *overhead* (sobrecarga) normalmente asociados a X.25, para lo cual, funcionalidades del tipo control de errores, de flujo, etc., se eliminan.

Frame Relay nació en los comités encargados de la formulación RDSI con el objetivo de sacar el mayor provecho posible de los accesos primarios de 2 Mbps

para servicios portadores de paquetes. Actualmente la especificación permite alcanzar hasta 45 Mbps. Frame Relay no incluye corrección de errores cada vez que un paquete es enviado de un nodo a otro, este era un aspecto que retrasaba la transmisión de datos, y en su lugar, el control de errores se realiza solamente entre el equipo del cliente y el nodo de conmutación. Con esta técnica, la detección de posibles errores descansa más en el protocolo de transmisión que utilizan las aplicaciones que se ejecutan en los equipos terminales.
Frame Relay opera sobre la dirección de las tramas sin analizar el contenido de los datos, delegando a la capa de red del modelo OSI las facilidades de conmutación.

Este opera sobre dos tipos de circuitos virtuales:

- Circuitos virtuales permanentes (CVP): Funcionan esencialmente igual que un canal dedicado donde se establece una ruta fija a través de la red hacia Nodos finales prefijados.

- Circuitos virtuales conmutados (CVC): Similares a las llamadas telefónicas, donde las decisiones de los nodos destino se crean según se necesite.

Para cada circuito virtual se debe definir un CIR (Caudal Mínimo Comprometido) en cada sentido de la comunicación. Este CIR representa el ancho de banda que garantiza la red en caso de congestión o saturación de la misma, sin embargo, debido a que Frame Relay se basa en el concepto de *Multiplexación estadística,* se podrá superar esta velocidad de transmisión comprometida hasta la *velocidad de acceso* al servicio (ancho de banda de la conexión entre el equipo terminal de comunicaciones y el nodo de red Frame Relay). La diferencia entre el ancho de banda de conexión a la red y el CIR se denomina EIR (Ráfaga en Exceso).

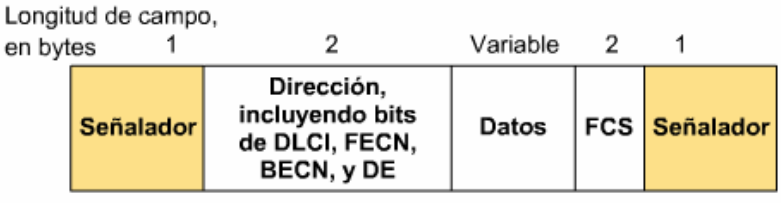
Para un mismo acceso Frame Relay será necesario definir tantos circuitos virtuales (caso de CVPs) como puntos de red con los que se desee conexión, siempre que la suma de los CIRs de cada uno de estos circuitos no supere en dos veces (teóricamente) la velocidad de acceso a la red, en otro caso será necesario aumentar el ancho de banda de conexión. (Para asegurar la concurrencia de comunicaciones por todos los CVPs la suma de los CIRs deberá ser como máximo equivalente a la velocidad de acceso a la red Frame Relay). Mediante sus métodos de notificación de congestión explícita hacia adelante/hacia atrás, esta tecnología permite supervisar las condiciones de congestión en las redes con el fin de evitar la pérdida de datos.

La técnica Frame Relay presenta un conjunto de ventajas que la hacen idónea para la definición de redes de área Amplia, no representa cambios sustanciales a nivel de equipamiento físico, las modificaciones en el equipamiento lógico a nivel de enlace son mínimas, presenta una eficiencia óptima para tráfico de datos y un Comportamiento excelente hasta 45 Mbps, lo que se considera suficiente para la interconexión de redes locales a medio y largo plazo.

Frame Relay no conoce las redes de área local que interconecta, por ello es un protocolo transparente y adecuado en aplicaciones que intercambian grandes volúmenes de datos a grandes velocidades.

A continuación describiremos como esta compuesta la trama Frame Relay

Figura 12. Estructura de la trama Frame Relay



- Señaladotes: Indica el principio y el final de la trama Frame Relay

- Dirección: Indica la longitud del campo de dirección Aunque las direcciones Frame Relay son actualmente todas de 2 bytes de largo, los bits de Dirección ofrecen la posibilidad de extender las longitudes de las direcciones en el futuro. El octavo bit de cada byte de campo Dirección se utiliza para indicar la dirección. La Dirección contiene la siguiente información:

    - Valor DLCI: Indica el valor de DLCI. Consiste en los 10 primeros bits del campo Dirección.

    - Control de congestión: Los últimos 3 bits del campo de dirección, que controlan los mecanismos de notificación de congestión Frame Relay. Estos son FECN, BECN y bits posibles para descarte (DE)

- Datos: Campo de longitud variable que contiene datos de la capa superior encapsulados.

- FCS: Secuencia de verificación de trama (FCS), utilizada para asegurar la integridad de los datos transmitidos.

3.2.3 ATM

ATM *(Asynchronous Transfer Mode,* Modo de Transferencia Asíncrono) surgió como parte de un conjunto de investigaciones realizadas por los operadores públicos de telecomunicaciones para desarrollar la Red Digital de Servicios Integrados de banda ancha (RDSI-BA). En 1991, los trabajos de la UIT-T en el campo RDSI-BA dieron lugar a la definición de un estándar global de interfaces de usuario para redes ATM (recomendación ÜIT-T.I.121), con una capacidad de transferencia de información de 155,52 Mbps y 622,08 Mbps, Un año después, la ÜIT-T había desarrollado más extensamente protocolos e interfaces estándares para redes ATM. A principios de 1992 se formó el ATM Forum, que publicó su primera especificación en Junio de ese mismo año. ATM fue diseñada para el transporte de datos sobre fibra óptica, de forma que el ancho de banda se reparte en bloques de tamaño idéntico denominados células *(cells).* Es una técnica del tipo *Cell Relay* orientada a la conmutación de células de tamaño constante de53 bytes a alta velocidad. El objetivo de ATM es realizar el *routing* y la Multiplexación de las células. Es similar a Frame Relay diferenciándose, fundamentalmente, en que en esta última el tamaño de la célula *(oframe)* es variable. Las redes ATM son transparentes a todos los tipos de información de usuario transportados mediante los servicios proporcionados por la red: voz, datos y vídeo. Soporta la transmisión de tráfico de diferente naturaleza de forma integrada. La flexibilidad del ancho de banda es prácticamente ilimitada, se puede establecer cualquier ancho de banda hasta la capacidad máxima del enlace de transmisión utilizado, es una técnica eficiente para el tráfico de datos interactivo. Parra aplicaciones del tipo de transferencia masiva de información o conexión entre redes de alta velocidad es la técnica idónea.

Una red ATM está formada por un conjunto de elementos de conmutación ATM interconectados entre sí por enlaces o interfaces punto a punto. Los conmutadores ATM soportan dos tipos de interfaces distintas: interfaz de red de usuario e interfaz de red de nodo. Las interfaces de red de usuario conectan dispositivos ATM

finales como host, router, PBX, vídeo entre otros a un conmutador ATM. Las interfaces de red de nodo conectan dos conmutadores ATM entre sí.
Las redes ATM están orientadas a conexión, es decir se requiere el establecimiento de un circuito virtual antes de la transferencia de información entre dos extremos. Los circuitos que establece ATM son de dos tipos:

- Caminos virtuales
- Circuitos virtuales: que son la agnación de un conjunto de caminos virtuales.

El funcionamiento básico de un conmutador ATM es el siguiente: una vez recibida una celda a través de un camino o circuito virtual asigna un puerto de salida y un número de camino o circuito a la celda en función del valor almacenado en una tabla dinámica interna. Posteriormente retransmite la celda por el enlace de salida y con el identifícador de camino o circuito correspondiente.
Existen principalmente dos tipos de conexiones en ATM:

- **Conexiones virtuales permanentes:** La conexión se efectúa por mecanismos externos, principalmente a través del gestor de red, por medio del cual se programan los elementos de conmutación entre fuente y destino.
- **Conexiones virtuales conmutadas:** La conexión se efectúa por medio de un protocolo de señalización de manera automática. Este tipo de conexión es la utilizada habitualmente por los protocolos de nivel superior cuando operan con ATM.

Dentro de estas conexiones se pueden establecer dos configuraciones distintas:

- Conexión punto a punto: Se conectan dos sistemas finales ATM entre sí, con una comunicación uni- o bidireccional.

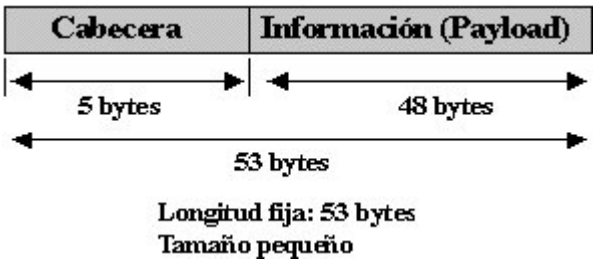
- Conexión punto multipunto: Conecta un dispositivo final como fuente con múltiples destinos finales, en una comunicación unidireccional.

Los conmutadores ATM intercambian cada cierto número de celdas de información otras denominadas RM (Resource Management). Estas viajan en un sentido y en el conmutador final son rescritas y devueltas al origen con la indicación de retransmitir más despacio o de que todo va bien y que se puede continuar la transmisión del mismo modo. Este es un mecanismo de control de congestión.
Otra ventaja de la tecnología ATM es la utilización eficiente del ancho de banda, por el mismo "canal" circulan celdas que pueden llevar información de voz, datos o imagen y todas reciben el mismo tratamiento en los conmutadores. Cuando una comunicación finaliza, el ancho de banda que ocupaba queda liberado para otra comunicación. Para establecer una comunicación, se negocia el ancho de banda y la calidad de servicio con el conmutador ATM, que puede aceptar la petición o limitar sus pretensiones de acuerdo con el ancho de banda disponible (este proceso de negociación forma parte de las especificaciones UNÍ (User-Network Interface).

En la actualidad el servicio ATM ofrecido por los operadores dominantes está disponible en todo el territorio nacional ofreciendo servicios de transporte de datos, conmutación de voz, etc. interoperando con otras redes de comunicaciones como Frame Relay de mayor penetración en el mercado. ATM pretende ser una solución

multimedia totalmente integrada para la interconexión de edificios ofreciéndose por parte de los operadores de comunicaciones la posibilidad de alquiler o compra del equipamiento de acceso al servicio, e infraestructura de líneas en caso de establecimiento de redes privadas. ATM es la apuesta de las empresas de equipos de comunicaciones condicionada por la demanda de servicios multimedia y la liberalización del mercado de las comunicaciones, ya que es una tecnología que permite a los nuevos operadores de comunicaciones ser rápidamente competitivos. Un ejemplo de esta tendencia la presentan los operadores de cable que ofrecen multiservicios por una única infraestructura (televisión de alta Definición, transporte de datos de gran ancho de banda, telefonía, etc.)

Figura 13. Estructura de la celda ATM



La celda ATM se compone de dos partes que son:

- LA Cabecera: Esta tiene un tamaño de 5 bytes, y contiene los bits de control de flujo y el VCI que es el Identificador de Conexión Virtual.

- Información o Payload: Es donde viaja la información sea de video, voz o datos y tiene un tamaño de 48 bytes

La Celda ATM, debe transportar la identificación de la conexión a la que pertenece, de esta forma no existirán Celdas vacías ya que serán utilizadas por conexiones pendientes. La cabecera presente en cada celda, consume aproximadamente un 9.5% del ancho de banda, siendo este el precio que hay que pagar por la capacidad para disponer de ancho de banda bajo demanda, en lugar de tenerlo permanentemente reservado y eventualmente desperdiciado.

3.3 TECNOLOGIAS USADAS EN COLOMBIA

Como mencionamos anteriormente, las empresas prestadoras de servicios de comunicaciones publicas mas grandes que existen en la actualidad en Colombia son Telecom e Internexa, las cuales manejan redes basadas en SDH y estas a su vez usan Multiplexación TDM, Internexa hace mas o menos 1 año empezó a incluir en sus redes la Multiplexación por División de Longitud de Onda WDM la cual usa las diferentes longitudes de onda que poseen los colores para hacer la Multiplexación.

A pesar que Internexa se ha consolidado como una gran empresa de telecomunicaciones, no ha cubrir la totalidad del territorio Colombiano caso contrario a Telecom que como brinda comunicación de voz a toda Colombia es fácil llegar prácticamente a cualquier parte del país usando la red de este proveedor.

La gran mayoría de las redes WAN hechas en Colombia usan Frame Relay debido a su alta velocidad y a la posibilidad que brinda de reuso del canal por medio de los circuitos virtuales, ya que se establece un CIR mínimo para cada circuito virtual y este se expande cuando los demás circuitos virtuales no están establecidos. Aun los proveedores de últimas millas están asumiendo a Frame Relay como su estándar para transporte de datos precisamente por su capacidad de reuso.

El protocolo PPP también es muy usado en enlaces que no necesiten más de un canal, es decir que si un cliente solicita un canal nacional único, el protocolo mas apto para este tipo de conexiones es el PPP, ya que es muy sencillo de usar y los equipos utilizados no requieren grandes características.

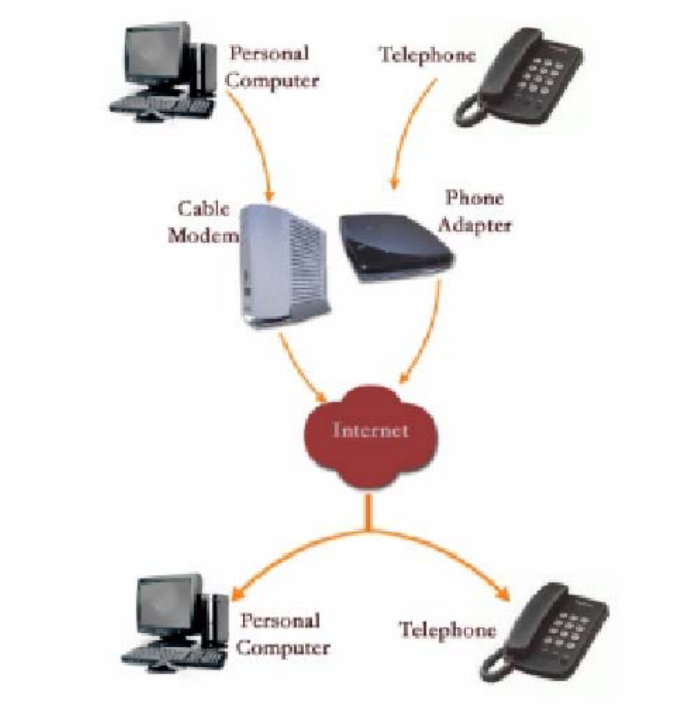
4. APLICACIONES ACTUALES PARA REDES WAN

4.1 VoIP

Como su nombre lo indica, VoIP (Voz sobre IP) es el proceso mediante el cual la voz es transportada sobre redes IP, las cuales son usadas en Internet y debido a que el Internet es mas económico que el proceso de telefonía convencional, el trafico de voz se esta migrando hacia IP, dejando atrás los viejos circuitos TDM.

Una llamada de VoIP es realizada entre dos puntos, los cuales pueden ser líneas telefónicas comunes (PSTN) o PC´s.

Figura 14. Esquema básico de VoIP



Cuando ambas partes involucradas en la comunicación son teléfonos se denomina llamada teléfono a teléfono, pero si alguno de los dos es un PC, esta se conoce como llamada PC a teléfono, como ejemplo a estos servicios tenemos a Net2phone y DialPad.

Si ambas de las partes son teléfonos se requiere de un Gateway de voz para convertir las llamadas de Internet a líneas PSTN o viceversa, y en el momento de realizar la llamada, ambas partes conectadas a Internet deben estar de acuerdo en un protocolo de señalización y de intercambio de voz.
Los protocolos mas comunes para la señalización son el H.323 y el SIP y para el intercambio de voz se usan unos protocolos llamados **codec** entre los cuales se encuentra el G.729A y el G.723.1 los cuales son llamados protocolos de compresión, aunque existe uno que no usa compresión de voz y se denomina G.711.

Cuando la llamada es hecha desde un PC, se requiere un software como el de la figura 15, el cual tiene tanto el protocolo de señalización como el codec.

Los codec usados normalmente requieren un ancho de banda específico, así que como G.711 no tiene compresión necesita un mínimo de 64Kbps para establecer una llamada, diferente a G.729A y G.723.1 que solo requieren de 16Kbps incluido el overhead para establecer una llamada

Figura 15. Pantalla de software usado en VoIP

4.2 CÁMARAS DE SEGURIDAD

La seguridad informática va adquiriendo una importancia creciente con el aumento del volumen de información importante que se halla distribuida en las computadoras. La norma Data Encryption System (DES) para protección de datos informáticos, implantada a finales de los años setenta, se ha visto complementada recientemente por los sistemas de clave pública que permiten a los usuarios codificar y decodificar con facilidad los mensajes sin intervención de terceras personas.

Actualmente las Cámaras IP juegan un papel importante para el monitoreo de la seguridad de las empresas, a continuación describiremos una aplicación con estas y las facilidades que brinda al sector de la seguridad

Una aplicación importante es la de programar un servidor para que controle las cámaras IP, este servidor se configura para detectar el movimiento dentro del campo visual de la cámara, si ocurre algún evento se registra y envían mensajes de alarma a aquellas personas responsables de monitorear estos lugares.

Los eventos no tienen que ser el resultado de movimiento en el campo visual, También pueden ser un evento de tiempo por ejemplo, cada 15 minutos, cuando se abre una puerta o un torniquete es cambiado de lugar, cuando la temperatura supera un rango normal definido, o cuando el sensor infrarrojo incorporado en la cámara IP detecta la actividad relacionada con calor o el micrófono interno o externo detecta el sonido por encima o por debajo de unos decibeles aceptables.

El servidor tiene incorporadas capacidades de almacenamiento, y las imágenes fotográficas pueden ser guardadas en el mismo tiempo en que se produce el evento, y para varias imágenes antes de que el evento tenga lugar o después de que ocurrido, o ambos casos. Así que no solamente podemos documentar el evento mismo, sino también la escena anterior al evento ocurrido después del mismo. Estas imágenes tienen detector de huellas, por lo cual los organismos legales pueden determinar fácilmente si la imagen ha sido modificada de alguna manera.

Con estos sistemas, se pueden monitorear casas, oficinas u otros intereses, para poder verlos en cualquier momento y desde cualquier lugar, y ser notificado automáticamente si un intruso está en los alrededores.

Este tipo de sistemas puede monitorear una línea de producción y notificar a la persona apropiada no solamente cuando haya demasiada actividad, sino también cuando no haya suficiente. Así que, por ejemplo, si se esperan que 10 cajas se desplacen abajo por una banda transportadora cada 15 segundos, usted puede ser notificado si el recuento verdadero es demasiado o muy poco.

En las siguientes figuras podemos ver una secuencia cuadro a cuadro de una persona tratando de volarse la valla de seguridad de una empresa y la imagen emitida por una cámara IP vía Web.

Figura 16. Secuencia cuadro a cuadro emitida por una cámara IP

Figura 17. Imagen fija producida por una cámara IP

4.3 TRANSFERENCIA DE ARCHIVOS

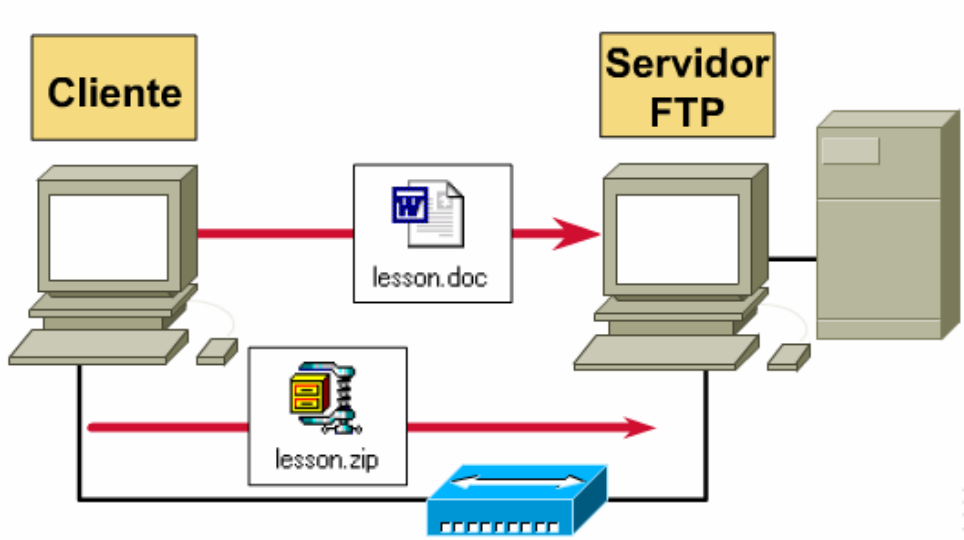
Actualmente manejan un alto volumen de información y necesitan hacer intercambio de archivos para lo cual se usa el protocolo de transferencia de archivos (FTP). Este está diseñado para descargar archivos por ejemplo de Internet o cargarlos. La capacidad para cargar y descargar archivos en este protocolo es una de las características más valiosas de Internet. Esto resulta sumamente útil para aquellas personas que utilizan los computadores para varios propósitos y que pueden necesitar controladores de software y actualizaciones de forma inmediata. Los administradores de red rara vez pueden esperar ni siquiera unos pocos días para obtener los controladores necesarios para que los servidores de red puedan volver a funcionar. A través de Internet pueden obtener estos archivos inmediatamente mediante FTP.

FTP es una aplicación cliente/servidor al igual que el correo electrónico y Telnet. Requiere software de servidor que se ejecuta en un host al que se puede acceder a través del software de cliente.

Una sesión FTP se establece de la misma forma que una sesión Telnet. Al igual que lo que ocurre con Telnet, la sesión FTP se mantiene hasta que el cliente la termina o hasta que se produce algún tipo de error de comunicación. Una vez que se establece una conexión con un daemon FTP, debe proporcionar un identificador de conexión y una contraseña. Normalmente, se usa "anonymous (anónimo)" como identificador de conexión y su dirección de correo electrónico como contraseña. Este tipo de conexión se denomina FTP anónimo. Una vez que establece su identidad, se abre un vínculo de comandos entre la máquina cliente y el servidor FTP. Esto es similar a la sesión Telnet donde los comandos se envían y se ejecutan en el servidor y los resultados se devuelven al cliente. Esta función le permite cambiar y crear carpetas, borrar y renombrar archivos y ejecutar muchas otras funciones relacionadas con la administración de archivos.

El propósito principal de FTP es transferir archivos desde un computador hacia otro copiando y moviendo archivos desde los servidores hacia los clientes, y desde los clientes hacia los servidores. Cuando los archivos se copian de un servidor, FTP establece una segunda conexión, un enlace de datos entre los computadores, a través del cual se transfieren los datos. La transferencia de datos se puede realizar en modo ASCII o en modo binario. Estos dos modos determinan la forma de transferencia de los archivos de datos entre las estaciones. Cuando termina la transferencia de archivos, la conexión de datos se termina automáticamente. Después de completar toda la sesión de copiado y desplazamiento de archivos, puede desconectarse, cerrando de esta manera el vínculo de instrucciones y finalizando la sesión. Otro de los protocolos que tiene la capacidad de descargar archivos es el Protocolo para la transferencia de hipertexto (HTTP), una de las limitaciones de HTTP es que sólo se puede utilizar para descargar archivos y no para cargarlos.

Figura 18. Proceso de obtención de archivos sobre FTP



5. EJEMPLO DE INTERCONEXION DE SEDES EMPRESARIALES

A continuación daremos en ejemplo concreto de interconexión de sedes empresariales a través de una red WAN, teniendo en cuenta todos los equipos, protocolos y esquemas de interconexión descritos anteriormente, buscando siempre la opción mas optima para la empresa que solicita el servicio. Tomaremos como ejemplo una empresa con sedes a nivel nacional, la cual llamaremos Lecheros de Colombia S.A.

5.1 DEFINICION DEL PROBLEMA

La empresa Lecheros de Colombia S.A. cuenta con sedes a nivel nacional en las ciudades de Cartagena, Valledupar y Bogota. Esta empresa cuenta con redes LAN en cada una de sus sedes, en este momento desea centralizar la información referente a las ventas y al control de inventarios, actualmente lo hacen vía telefónica por medio de Fax y llamadas, lo cual hace este proceso muy lento, representándose en altos costos tanto por perdida de tiempo como en llamadas telefónicas. Por lo cual nos han solicitado que encontremos la opción mas adecuada de interconexión para enlazar sus tres sedes a nivel nacional, teniendo en cuenta sus necesidades y que además les ofrezcamos los diferentes servicios que se puedan implementar sobre la red WAN.

5.2 DISEÑO DE LA RED WAN

Después de haber visitado las sedes nacionales de Lecheros de Colombia S.A. nos dimos cuenta que el control de pedidos e inventarios debe hacerse de forma muy rápida, también se puede implementar VoIP para la comunicación entre las tres sedes ya que esto es de vital importancia y nos percatamos que existen algunos huecos de seguridad que pueden ser eliminados por medio de cámaras IP.

5.2.1 ELECCION DEL TIPO DE INTERCONEXION

Teniendo en cuenta las necesidades de la empresa y los servicios que se van a implementar, se necesitan tiempos de respuestas cortos y un ancho de banda lo suficientemente grande para transportar datos, voz y video. La VoIP usando como codec el G.723.1 necesita un ancho de banda mínimo de 16 Kbps, el ancho de banda mínimo de las cámaras IP usando solo el video es de 64 Kbps y finalmente la empresa necesita transportar los datos de forma rápida, así que podemos pensar en un ancho de bando total de mínimo 256 Kbps.

Si miramos la opción de VPN nos damos cuenta que esta solo serviría si fuéramos a transportar solamente datos, ya que las VPN funcionan a través de Internet lo cual implica tiempos de respuesta muy altos (200 a 600 ms en promedio), por la gran cantidad de saltos que hace un paquete para llegar de un lugar a otro y por estadística se conoce que el ancho de banda de Internet es muy valioso por lo que un 256 Kbps que se encuentra alrededor de los US$600.oo en cada una de las sedes resulta un tanto costoso y muy poco productivo al momento de usar las tres aplicaciones (datos, voz y video) simultáneamente.

Por tal motivo escogimos como forma de interconexión un canal dedicado para cada una de las sedes, ya que este tipo de conexiones a pesar de ser un poco mas costosas brinda tiempos de respuesta muy cortos (45 a 60 ms en promedio) lo cual hace posible la implementación de llamadas sobre VoIP de muy buena calidad auditiva, imágenes provenientes de las cámaras con muy buena resolución y hasta se puede afirmar que se dan en tiempo real, así como también velocidades de transferencia de archivos muy altas.

Otra razón que nos lleva a escoger un canal dedicado es la seguridad que brinda en le transporte de los paquetes de un lugar a otro, ya que no se usa una red publica para transportar los datos, diferente a las VPN que aunque cuentan con algoritmos de encripción y encapsulamiento los paquetes de este tipo de red viajan a través de una red publica como lo es Internet, lo que la hace insegura respecto a los datos confidenciales del empresa.

5.2.2 TECNOLOGIA A UTILIZAR

Después de haber escogido un canal dedicado como nuestra forma de interconexión a seguir, debemos pensar ahora en que tipo de tecnologia de red WAN es el más adecuado para nuestro canal.

Las empresas dedicadas a transportar datos a nivel nacional lo hacen sobre redes SDH, por las cuales puede circular trafico ATM, Frame Relay y PPP, la desventaja de ATM para nuestro caso es que esta transfiere datos a muy alta velocidad, por lo que es demasiado costosa y estaríamos subutilizando un ancho de banda tan grande como el que brinda ATM.

Estas empresas que brindan servicios de interconexión nacional dedicada proveen como mínimo un E1 para transportar datos de un lugar a otro, debido a que

nuestra empresa va a contratar 256 Kbps se debe buscar una empresa que ya tenga contratados canales nacionales entre las ciudades donde se ubican nuestras sedes, ya que si contratamos el E1 completo saldría muy costoso y estaríamos comprando mas canal del que necesitamos. Como vamos a compartir el E1 con otros usuarios la mejor opción seria escoger a Frame Relay como nuestra tecnología a usar, ya que esta nos brinda la capacidad de establecer un circuito virtual privado para nuestros datos a pesar que el E1 este compartido con otros usuarios y además de esto nos ofrece reuso del canal cuando los demás usuarios no estén usando los canales. No se escogió el protocolo PPP como nuestra tecnología ya que este es muy básico y no brinda el reuso y las ventajas de Frame Relay.

5.2.3 EQUIPOS ESCOGIDOS

Debido a que nuestras sedes quedan ubicadas en fincas en las afueras de las ciudades se requieren ultimas millas vía microondas y en nuestro caso se utilizaran radios que cuenten con una interfaz ethernet como los bridges OR-4200 de Wavecon mostrado en la figura 7, que son usados regularmente para efectos de ultima milla. Se usarán 6 radios, 2 por ciudad para hacer los 3 punto a punto de ultima milla

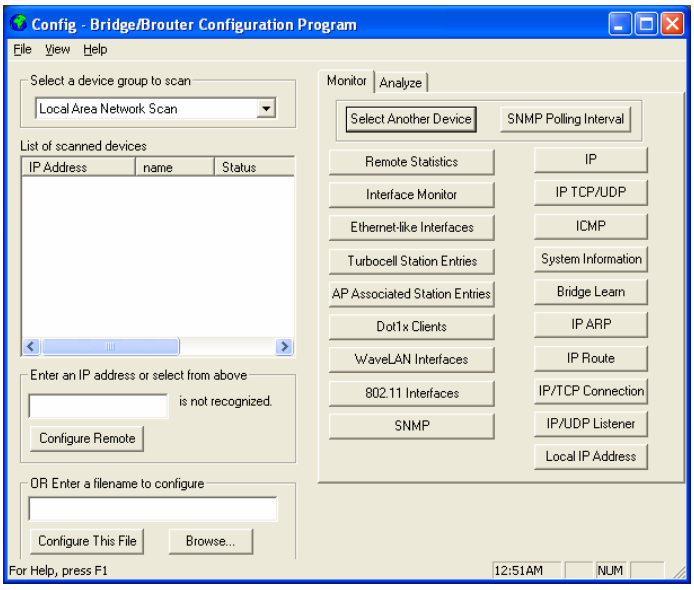
Por calidad y experiencia se escogieron enrutadores Cisco de la serie 3600, ya que estos poseen gran capacidad de procesamiento y tiene la ventaja de colocar varias interfaces seriales V.35 para ubicar diferentes enlaces WAN en la ciudad central y en las ciudades satélites se usarán routers mas sencillos, como el cisco de la serie 2600, en total son 2 routers cisco 2600 y un 3600.

Dependiendo la empresa con la cual se establezca el enlace nacional se necesitarán, fraccionadotes o CSU/DSU para enlazar la interfaz V.35 del enrutador a la interfaz G.703 por la cual viaja el E1. Telecom suministra el fraccionador para todos sus enlaces diferente de Internexa que entrega G.703 en el nodo final, pero debido a que los precios de E1 de una y otra compañía son tan diferentes escogimos Internexa que es el más económico, para lo cual debemos contar con cuatro fraccionadores.

5.2.3.1 CONFIGURACION DE LOS EQUIPOS

Los radios microondas se configuran mediante un software llamado configurator, el cual viene con los radios y permite configurarle frecuencias, velocidades de transferencia de datos, dirección IP y hasta un firewall para bloquear puertos indeseables y en la figura 19 se muestra una imagen del software de configuración.

Figura 19. Configurator



Debido a que Cartagena es la ciudad central aquí se colocara el router 3600 de gran capacidad para que maneje los routers 2600 de las otras dos ciudades y la configuración del router se muestra a continuación.

Configuración de Router 3600 ubicado en Cartagena

```
hostname 4700-DIST-LECHECOL-CGENA
enable secret 5 $1$KGpL$m42Wo24ZXWae0SKrQKX0m/
username nico privilege 15 password 7 15345B5F550C1A1C7C62657041
frame-relay switching
clock timezone SKCG -5
interface Ethernet0
 description ETH-01-DETECSA-CGENA
 ip address 192.168.0.1 255.255.255.0
 no ip directed-broadcast
 media-type 10BaseT
interface Ethernet1
 no ip address
 no ip directed-broadcast
 shutdown
 media-type 10BaseT
nterface Serial0
 description E1-01-LECHECOL-CGENA_VDUPAR
 bandwidth 1280
 no ip address
 encapsulation frame-relay IETF
 no ip mroute-cache
```

```
 no fair-queue
 frame-relay intf-type dce
interface Serial0.1 point-to-point
 description CANAL INTERNET
 bandwidth 1024
 ip address 192.168.248.25 255.255.255.252
 frame-relay interface-dlci 17
interface Serial0.2 point-to-point
 description Datos LECHECOL
 bandwidth 256
 ip address 10.10.10.1 255.255.255.252
 frame-relay interface-dlci 18
interface Serial1
 description E1-01-LECHECOL-CGENA_BOGOTA
 bandwidth 1280
 no ip address
 encapsulation frame-relay IETF
 no ip mroute-cache
 no fair-queue
 frame-relay intf-type dce
interface Serial0.1 point-to-point
 description CANAL INTERNET
 bandwidth 1024
 ip address 192.168.208.25 255.255.255.252
 frame-relay interface-dlci 19
interface Serial0.2 point-to-point
 description Datos LECHECOL
```

```
 bandwidth 256
 ip address 10.10.20.1 255.255.255.252
 frame-relay interface-dlci 20
ip classless
ip route 192.168.1.1 255.255.255.0 Serial 0
ip route 192.168.2.1 255.255.255.0 Serial 1
line con 0
 exec-timeout 0 0
 password 7 096A1E5A4823262A5F5D547879
 login
 transport input none
line aux 0
 password 7 03220B58572910741A58495745
 login
line vty 0
 access-class 20 in
 password 7 132347415A2A35127F75786167
 login local
 length 25
line vty 1 4
 access-class 20 in
 password 7 06205F721D683821514642595E
 login local
end
```

Los enrutadores 2600 se configuran de igual forma teniendo en cuenta el DLCI de cada circuito virtual establecidos en el router 3600, así como también las direcciones IP establecidas en el esquema de red.

Los fraccionadotes Adtran constan de una pantalla LCD la cual indica los modos de configuración, aunque existen otros de marca RAD que se configuran por medio del puerto de comunicación serial, en fin a estos fraccionadores solo hay que indicarles cuantos time-slots van a llevar datos con el fin de establecer un ancho de banda determinado.

5.2.4 APLICACIONES MONTADAS SOBRE LA RED WAN

5.2.4.1 VoIP

Para la implementación de Voz sobre IP en nuestro canal utilizaremos Gateway AdvancedVOIP como las mostradas en la figura 19, la cual soporta 4 líneas analógicas, las cuales tienen un valor aproximado de US$ 100 a 500. Estos estarán ubicados en cada una de las sedes y ya que soportan 4 líneas análogas cada teléfono tendrá la oportunidad de comunicarse con 11 extensiones diferentes, por vía IP y sin usar la red telefónica convencional es decir que se esta invirtiendo en el canal dedicado pero se esta ahorrando en llamadas telefónicas de larga distancia nacional por la red convencional. Si lo vemos desde cierto punto de vista, es como si la empresa tuviera montada su propia telefónica.

Figura 20. Gateway AdvancedVOIP

5.2.4.2 CAMARAS DE SEGURIDAD

Las cámaras que recomendamos son cámaras marca Mobotix, cuyas imágenes pudimos ver en el capitulo anterior en las figuras 15 y 16, ya que estas cámaras son capaces de detectar movimientos y también cuentan con vista infrarroja, por lo cual se pueden usar en los diferentes procesos de la empresa y para situaciones de vigilancia. Estas cámaras dependiendo de sus funciones están entre US$300 y US$1000.

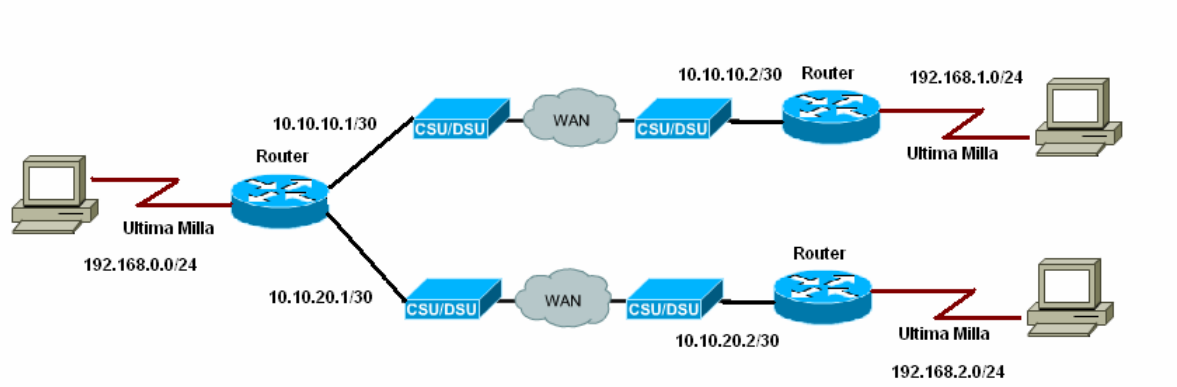
5.2.4.3 TRANSFERENCIA DE ARCHIVOS

Para efectos de transferencia de archivos, ya sean documentos de inventario o pedidos, archivos de imágenes o de videos se puede montar un servidor FTP, el cual se debe ubicar en la sede principal para así recoger información de todas las sedes satélite. Recomendamos el uso de un servidor FTP bajo Linux, ya que es un sistema operativo más estable que Windows, a pesar que el servidor Windows es mas fácil de manejar, este es mas susceptible a virus y lo que menos se quiere

es que se pierda la información grabada en este servidor. Un servidor FTP bajo Linux esta costando alrededor de los US$2000.oo

5.3 ESQUEMA GRAFICO DE LA RED WAN

Figura 21. Esquema grafico de la red WAN



Para este esquema usamos direcciones IP privadas clase C y para las interfaces seriales se establecieron direcciones IP con mascara de red grande para no abarcar una red en donde estuvieran comprometidos mas host de lo necesario.

5.4 EVALUACION DE LOS COSTOS DE INTERCONEXION

Como mencionamos anteriormente los dos únicos grandes proveedores de canales nacionales en Colombia son Telecom e Internexa, los cuales solo venden E1´s a los mayoristas, en Telecom el E1 tiene un costo de $4.500.000 y en Internexa cuesta $3.500.000, la razón que vemos a esta diferencia de precios es que Telecom puede llegar a casi toda Colombia, en cambio la red de Internexa esta limitada a las principales ciudades y también que internexa cuenta con

equipos y tecnologías mas avanzadas que le permiten transportar mayor ancho de banda que Telecom.

En cuanto a últimas milla nos encontramos con el panorama que dependiendo la ciudad así son los costos de últimas millas.

En las ciudades de Barranquilla, Cartagena y Bucaramanga las últimas millas las proveen; Promitel, Metrotel, Ductel y Detec y los precios de estas dependen del ancho de banda contratado. Los siguientes precios son aproximados a los valores de cada una de las empresas

Tabla 1. Precios de última milla en Barranquilla, Cartagena y Bucaramanga

Ancho de Banda	Costo US$
64 Kbps	120
128 Kbps	160
256 Kbps	200
512 Kbps	300
E1 2.048 Kbps	600

En las ciudades de Bogota, Medellín y Cali se encuentran ETB, EPM y Emcali, las cuales ofrecen los siguientes costos.

Tabla 2. Precios de última milla en Bogota, Medellín y Cali

Ancho de Banda	Costo US$
64 Kbps	280
128 Kbps	290
256 Kbps	450
512 Kbps	600
E1 2.048 Kbps	700

En las demás ciudades no existen proveedores de servicios de ultimas millas, la única opción es comprar la ultima milla a Telecom, la cual ofrece precios en otras ciudades de.

Tabla 3. Precios de Ultima Milla en otras ciudades

Ancho de Banda	Costo US$
64 Kbps	100
128 Kbps	150
256 Kbps	200
512 Kbps	300
E1 2.048 Kbps	500

Tomando en cuenta los datos anteriores y la premisa que se recomienda un canal de 256 Kbps, la interconexión dedicada por este medio tiene un costo total que se encuentra alrededor de los US$1200 mensuales.

CONCLUSIONES

- ☑ Si se analiza la relación costo beneficio de montar un enlace nacional dedicado es mucho más económico que seguir trabajando con los antiguos sistemas de comunicación, como son el teléfono y las conexiones de red vía telefónica.

- ☑ Gracias a los canales dedicados se pueden reducir los tiempos de comunicación ya que se tiene todo a la mano en el momento de solicitar informes y archivos a oficinas geográficamente distantes.

- ☑ Las VPN son una muy buena opción cuando se requiere trabajar con aplicaciones que no requieran grandes anchos de banda y que si es el caso contrario la mejor opción son los canales dedicados.

- ☑ Al momento de contratar servicios de canales nacionales dedicados, lo mejor es contratar una sola empresa para que haga todo el trabajo, normalmente la proveedora de ultima milla, evitando así costos y tiempos de solicitud de servicios de mantenimiento.

- ☑ La tecnología ATM es poco usada en Colombia, por lo cual normalmente se usa Frame Relay y PPP por las ventajas que presta cada uno.

GLOSARIO

- ☑ Appliance VPN: Equipo de VPN diferente a un PC que usa protocolos de encripcion IPsec y PPTP

- ☑ CSU/DSU: Unidad de servicio de datos, dispositivo utilizado en la transmisión digital que adapta la interfaz física en un dispositivo DTE a una instalación de transmisión como T1 o E1. La DSU también está a cargo de funciones tales como la temporización de las señales. Frecuentemente denominado, conjuntamente con CSU, como *CSU/DSU*.

- ☑ IKE: Intercambio de llaves (claves) por Internet

- ☑ LCP: Protocolo de Control de Enlace

- ☑ NCP: Protocolo de control de Red

- ☑ POTS: Servicio telefónico analógico convencional

- ☑ PSTN: Red Publica de Servicios de Telefonía

- ☑ RDSI: Red digital de servicios integrados

- ☑ SDH: Jerarquía Digital Sincronía

- ☑ SONET: Red Óptica Sincronía

BIBLIOGRAFIA

Tanebaum Andrew. Computer Networks, third edit, Prentice Hall.

Black Uyless. Tecnologías Emergentes para Redes de Computadores, segunda edición, Prentice Hall.

Black Uyless. Redes De Computadores, Protocolos, Normas e Interpretes, Alfa Omega Grupo Editor.

Cisco Systems. Software Configuration Guide for Cisco 3600 Series and Cisco 2600 Series routers, 1998

http://www.advancedvoip.com

http://www.cisco.com/univercd/cc/td/doc/product/software/

http://www.timestep.com

http://www.adtran.com