ESCUELA POLITÉCNICA DEL EJÉRCITO

FACULTAD DE INGENIERÍA ELECTRÓNICA

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO EN INGENIERÍA ELECTRÓNICA

ESTUDIO Y DISEÑO DE LA RED WAN PARA EL CENTRO DE CAPACITACIÓN INFORMÁTICA "CECAI"

MAURICIO FERNANDO NAVAS GALLARDO

SANGOLQUI-ECUADOR

2006

CERTICACIÓN

Certificamos que el Señor Mauricio Fernando Navas Gallardo con el número de cédula 171705730-9 ha elaborado bajo nuestra Dirección y Codirección el proyecto de grado titulado *"Estudio y Diseño de la Red Wan para el Centro de Capacitación Informática CECAI"*

.

Sangolquí, 13 de Enero del 2006

Ing. Fabián Sáenz	**Ing. Carlos Romero**
DIRECTOR	**CODIRECTOR**

AGRADECIMIENTO

Deseo expresar mi agradecimiento a mis padres, profesores y amigos, ya que han sido de gran apoyo, ya que cada uno ha colaborado para la realización de este proyecto de una manera especial.

DEDICATORIA

Esta tesis va dedicada en especial a mi madre ya que sin su esfuerzo y apoyo no hubiera sido posible la realización de este proyecto, además a todas las personas que colaboraron en la culminación de mis estudios como profesores, amigos y familiares.

PROLOGO

El centro de Capacitación Informática “CECAI”, cuya principal dependencia se encuentra ubicada en la provincia de Pichincha (Sangolquí), ha decidido realizar una política de actualización tecnológica tendiente a optimizar sus procesos.

A fin de poder desarrollar esta propuesta, se va a realizar un estudio sobre la necesidad de alcanzar una mejor interconexión entre las distintas áreas del CECAI y sus clientes actuales y potenciales.

El mencionado estudio debe concluir con la necesidad de desarrollar un sistema de comunicaciones que permita integrar distintos servicios a las diferentes sedes del CECAI y al CECAI con el mundo exterior.

El Centro de Capacitación Informática CECAI, como proyecto de estudio de factibilidad y beneficios para la empresa, requiere desarrollar un sistema de comunicaciones antes mencionado.

Para lo cual se debe realizar distintos estudios como por ejemplo ancho de banda, topologías de red, posibles tecnologías a implementar, políticas de seguridad, para lo cual se debe tomar en cuenta también las necesidades comerciales de la Empresa.

Se presentará las posibles soluciones de una Red WAN (Red de Área Amplia), en la primera alternativa se conectarán 20 Centros del CECAI, mientras que en la segunda alternativa se enlazará a 8 centros, brindando acceso a los servicios y aplicaciones de la red desde un servidor central.

Se presentará dos alternativas de diseño de una red Wan para el Centro de Capacitación Informática, y al final del proyecto se establecerá cual diseño se adapta mejor a las necesidades económicas, sociales y estructurales del CECAI, valiéndonos para esto de herramientas fundamentales como son los análisis de rentabilidad, estableciendo cual propuesta es la más rentable

INDICE

CAPITULO I

INTRODUCCIÓN Y FUNDAMENTOS TEÓRICOS

1.1 DESCRIPCIÓN DEL CECAI

El Centro de Capacitación Informática, se creó en agosto de 1997, con la finalidad de brindar capacitación informática básica a la comunidad ecuatoriana y a los miembros de las Fuerzas Armadas.

La implementación de los Centros se realizó en convenio con la empresa privada y las unidades militares. En la actualidad se dispone de 40 centros asociados ubicados en 15 Provincias del Ecuador.

Los servicios que ofrece el Centro de Transferencia y Desarrollo Tecnológico de la ESPE-CECAI tienen alto grado de calidad y buscan fomentar mediante la transferencia de tecnología, que es uno de sus principales fines, la interactividad de las organizaciones con sus clientes, proveedores, funcionarios, entidades financieras, etc. Mediante la formulación de nuevas estrategias de modernización y de plena integración a la Sociedad de la Información y Comunicación.

1.1.1 Antecedentes.

El mundo está viviendo un proceso vertiginoso de cambios, marcados por el desarrollo acelerado de la tecnología, lo que ha producido profundas transformaciones estructurales en todos los países.

La globalización impone nuevos esquemas de negocios y ante esta realidad las empresas deben afinar sus procesos, mejorar sus productos y orientar sus actividades a la satisfacción del cliente, entregando valor agregado.

En este proceso de cambio el desarrollo del capital humano, constituye uno de los factores más importantes, ya que las personas son las que construyen y desarrollan las estrategias dentro de las instituciones.

Con este enfoque la Escuela Politécnica del Ejército creó el primer ***Centro de Transferencia y Desarrollo Tecnológico de la ESPE-CECAI*** como una entidad de soporte, con autonomía en la gestión y ejecución de proyectos de capacitación, consultoría, asesoría e investigación en beneficio de la comunidad.

1.1.2 Fines del CECAI.

- Promover la investigación científica y tecnológica.
- Propiciar la creación o el mejoramiento de laboratorios, gabinetes u otros medios idóneos para la investigación.
- Establecer y mantener la cooperación con las empresas privadas y públicas nacionales en el desarrollo de tecnologías.
- Colaborar con organismos, instituciones o empresas públicas y privadas extranjeras para la transferencia y adaptación de tecnologías a las necesidades del país.
- Buscar soluciones por parte de los establecimientos de educación superior a los requerimientos técnicos y tecnológicos que plantean los sectores productivos y sociales del país.
- Diseñar proyectos de desarrollo, participar en su ejecución y evaluarlos.
- Organizar programas de promoción y difusión de estrategias y de resultados.
- Desarrollar cursos de capacitación, asesorías y consultorías.

1.2 INTRODUCCIÓN A LAS REDES

1.2.1 Concepto De Red.

Una red consiste en dos o más computadoras unidas que comparten recursos como archivos, cd-roms o impresoras y que son capaces de realizar comunicaciones electrónicas, las redes están unidas por cable, líneas de teléfono, ondas de radio, satélite, etc.

1.2.2 Objetivos.

Su objetivo principal es lograr que todos sus programas, datos y equipos estén disponibles para cualquier usuario de la red que lo solicite, sin importar la localización física del recurso y del usuario.

Otro objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro, es decir que todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias.

1.2.3 Clasificación básica de redes

1.2.3.1 Red de Área Local.

Es una red que cubre una extensión reducida como una empresa, una universidad, un colegio, etc. No habrá por lo general dos ordenadores que disten entre si más de un kilómetro.

Una configuración típica en una red de área local es tener una computadora llamada servidor de ficheros en la que se almacena todo el software de control de la red, así como el software que se comparte con los demás ordenadores de la red.

Los ordenadores que no son servidores de ficheros reciben el nombre de estaciones de trabajo. Estos suelen ser menos potentes y tienen software personalizado por cada usuario. La mayoría de las redes LAN están conectadas por medio de cables y tarjetas de red, una en cada equipo.

1.2.3.2 Red de Área Metropolitana

Las redes de área metropolitana cubren extensiones mayores como pueden ser una ciudad o un distrito. Mediante la interconexión de redes LAN se distribuyen la información a los diferentes puntos del distrito, bibliotecas, universidades u organismos oficiales suelen interconectarse mediante este tipo de redes.

1.2.3.3 Redes de Área Extensa

Las redes de área extensa cubren grandes regiones geográficas como un país, un continente o incluso el mundo. Cable transoceánico o satélites se utilizan para enlazar puntos que distan grandes distancias entre si.

Con el uso de una WAN se puede conectar desde España con Japón sin tener que pagar enormes cantidades de teléfono. La implementación de una red de área extensa es muy complicada.

Se utilizan multiplexadores para conectar las redes metropolitanas a redes globales utilizando técnicas que permiten que redes de diferentes características puedan comunicarse sin problema. El mejor ejemplo de una red de área extensa es Internet.

1.3 REDES DE AREA AMPLIA (WAN)

Una WAN se extiende sobre un área geográfica amplia, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar programas de usuario (aplicaciones), estas maquinas se llaman Hosts.

Los hosts están conectados por una subred de comunicación. El trabajo de una subred es conducir mensajes de un host a otro. La separación entre los aspectos exclusivamente de comunicación de la red (la subred) y los aspectos de aplicación (hosts), simplifica enormemente el diseño total de la red.

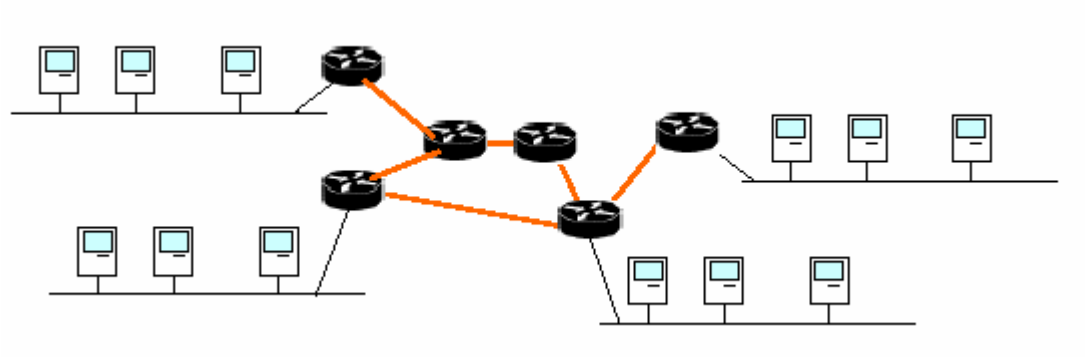


Figura. 1.1. Hosts conectados por una subred

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 de área amplia (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.

1.3.1 Constitución de una Red de Área Amplia (WAN)

La red consiste en ECD (computadores de conmutación) interconectados por canales alquilados de alta velocidad (por ejemplo, líneas de 56 kbit/s).

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 de soporte ETD (Terminales/computadores de usuario).

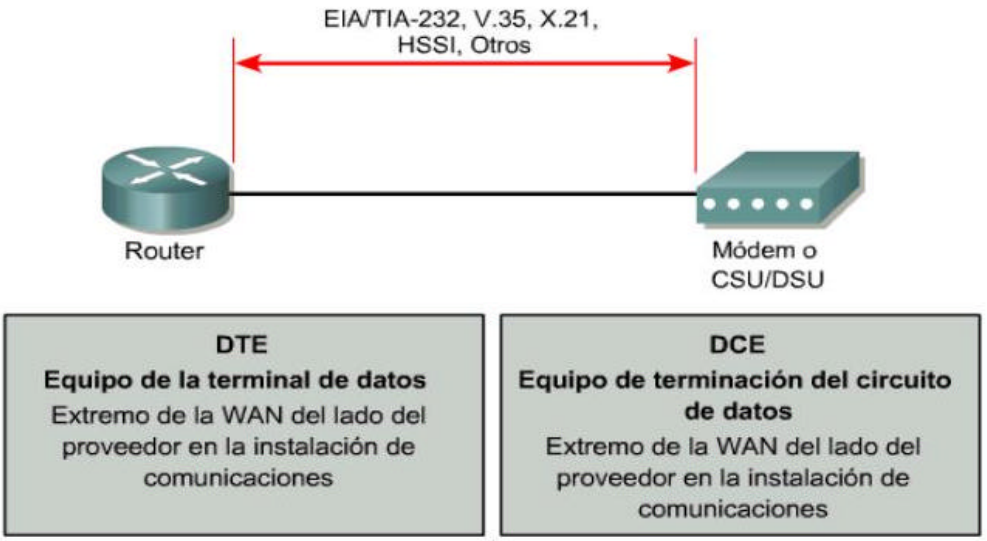


Figura. 1.2. Constitución de una red WAN

La función soporte del ETD se denomina a veces PAD (ensamblador / desensamblador 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.

1.3.2 Características de una Red de Cobertura Amplia

Los canales suelen proporcionarlos las compañías telefónicas, con un determinado costo mensual si las líneas son alquiladas, y un costo proporcional a la utilización si son líneas normales conmutadas

Los enlaces son relativamente lentos (de 1200 Kbit/s a 1.55Mbit/s), las conexiones de los ETD con los ECD son generalmente más lentas (150 bit/s a 19.2 kbit/s). Los ETD y los ECD están separados por distancias que varían desde algunos kilómetros hasta cientos de kilómetros.

Las líneas son relativamente propensas a errores (si se utilizan circuitos telefónicos convencionales). Las redes de área local (LAN) son significativamente diferentes de las redes de cobertura amplia. El sector de las LAN es uno de los de más rápido crecimiento en la industria de las comunicaciones.

La estructura de las WAN tiende a ser más irregular, debido a la necesidad de conectar múltiples terminales, computadores y centros de conmutación. Como los canales están

alquilados mensualmente, las empresas y organizaciones que los utilizan tienden a mantenerlos lo más ocupados posible.

Para ello, a menudo los canales "serpentean" por una determinada zona geográfica para conectarse a los ETD allí donde estén. Debido a eso la topología de las WAN suele ser más irregular.

1.3.3 Componentes Físicos

1.3.3.1 Línea de Comunicación

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

1.3.3.2 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.

1.3.4 Clasificación de Líneas de Conmutación

1.3.4.1 Líneas Conmutadas

Líneas que requieren de marcar un código para establecer comunicación con el otro extremo de la conexión.

1.3.4.2 Líneas Dedicadas

Líneas de comunicación que mantienen una permanente conexión entre dos o más puntos, estas pueden ser de dos o cuatro hilos.

El enlace está dedicado de forma permanente con un caudal reservado, se use o no.

- Es la solución más simple, máximo rendimiento
- Adecuada si hay mucho tráfico de forma continua
- Costo proporcional a la distancia y a la capacidad (tarifa plana)
- Velocidades: 64, 128, 256, 512 Kb/s, 2 Mb/s, 34 Mb/s (simétricos full-duplex)

1.3.4.3 Líneas Punto a Punto

Se encargan de enlazar dos DTE

1.3.4.4 Líneas Multipunto

Se encargan de enlazar tres o más DTE

1.3.4.5 Líneas Analógicas

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.

La máxima tasa de transferencia de tráfico digital posible sobre líneas analógicas está en 43,000 bps.

1.3.4.5 Líneas Digitales

Las líneas digitales 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 (CSU / DSU), el cual únicamente proporciona una interfaz a la línea digital.

Las líneas digitales pueden transmitir tráfico de datos a velocidades de hasta 45 Mbps y están disponibles tanto para servicios dedicados como conmutados.

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 en la cual los códigos más empleados son:

1.3.4.5.1 NRZ (No Retorno a Cero) Unipolar

La forma de onda binaria que utilizan normalmente las computadoras se llama *Unipola*r, es decir, que el voltaje que representa los bits varia entre 0 voltios y +5 voltios, se denomina NRZ porque el voltaje no vuelve a cero entre bits consecutivos de valor uno.

Este tipo de código es inadecuado en largas distancias debido a la presencia de niveles residuales de corriente continua y a la posible ausencia de suficientes números de transiciones de señal para permitir una recuperación fiable de una señal de temporización.

1.3.4.5.2 Código NRZ Polar

Este código desplaza el nivel de referencia de la señal al punto medio de la amplitud de la señal.

De este modo se reduce a la mitad la potencia requerida para transmitir la señal en comparación con el Unipolar.

1.3.4.5.3 Transmisión Bipolar o AMI (Alternate Marks Inverted)

Es uno de los códigos más empleados en la transmisión digital a través de redes WAN, este formato no tiene componente de corriente continua residual y su potencia a frecuencia cero es nula.

Se verifican estos requisitos transmitiendo pulsos con un ciclo de trabajo del 50% e invirtiendo alternativamente la polaridad de los bits 1 que se transmiten.

Dos valores positivos sin alternancia entre ellos serán interpretados como un error en la línea.

Los 0's son espacios sin presencia de voltaje. El formato Bipolar es en realidad una señal de tres estados (+V, 0, -V).

1.4 TIPOS DE REDES WAN

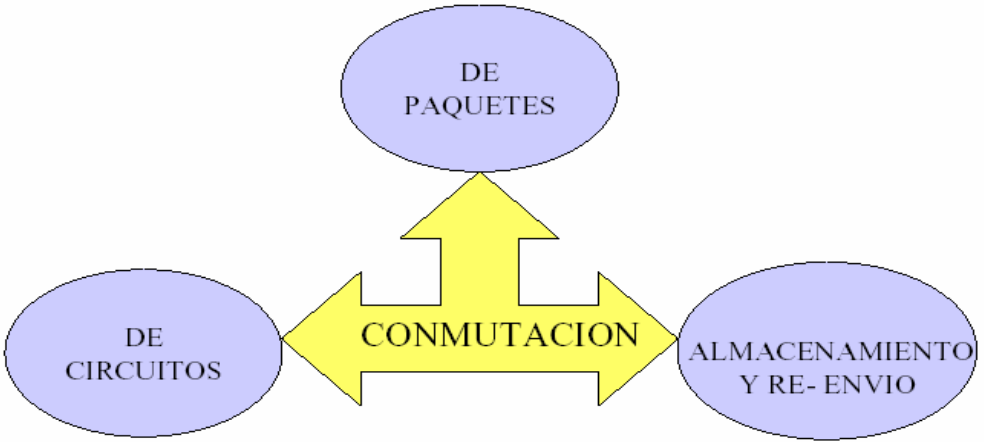


Figura. 1.3. Tipos de Redes WAN

1.4.1 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.

En una conexión de conmutación de circuitos se establece un canal dedicado, denominado circuito, entre dos puntos por el tiempo que dura la llamada.

El circuito proporciona una cantidad fija de ancho de banda durante la llamada y los usuarios sólo pagan por esa cantidad de ancho de banda el tiempo que dura la llamada.

Las conexiones de conmutación de circuitos tienen dos serios inconvenientes. El primero es que debido a que el ancho de banda en estas conexiones es fijo, no manejan adecuadamente las avalanchas de tráfico, requiriendo frecuentes retransmisiones.

El segundo inconveniente es que estos circuitos virtuales sólo tienen una ruta, sin caminos alternativos definidos.

Por esta razón cuando una línea se cae, es necesario que un usuario intervenga reencamine el tráfico manualmente o se detiene la transmisión.

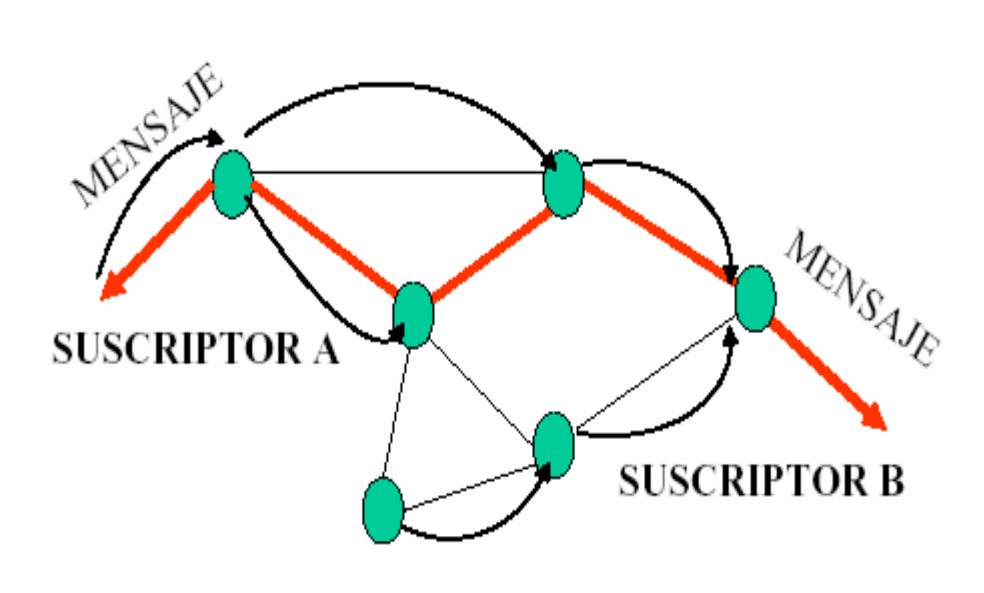


Figura. 1.4. Tipos de Redes WAN

1.4.2 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 DTE 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.

1.4.3 Conmutadas por Paquetes

En este tipo de red los datos de los usuarios se descomponen en trozos más pequeños, estos fragmentos o paquetes, están insertados dentro de informaciones del protocolo y recorren la red como entidades independientes.

Los servicios de conmutación de paquetes suprimen el concepto de circuito virtual fijo, los datos se transmiten paquete a paquete a través del entramado de la red o nube, de manera que cada paquete puede tomar un camino diferente a través de la red.

Como no existe un circuito virtual predefinido, la conmutación de paquetes puede aumentar o disminuir el ancho de banda según sea necesario, pudiendo manejar adecuadamente las avalanchas de paquetes de forma adecuada.

Los servicios de conmutación de paquetes son capaces de enrutar los paquetes, evitando las líneas caídas o congestionadas, debido a los múltiples caminos en la red.

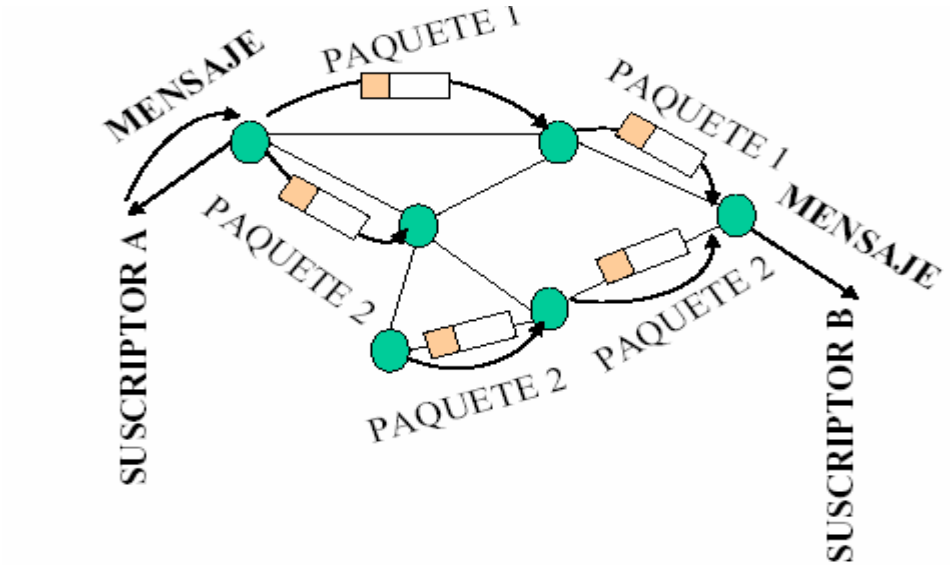


Figura. 1.5. Conmutación por Paquetes

1.4.4 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.

- Posibilidad de crear circuitos virtuales de dos tipos:

    1. Temporales: SVCs (Switched Virtual Circuits). Se crean y destruyen dinámicamente cuando se necesitan.

    2. Permanentes: PVCs (Permanent Virtual Circuits). Se configuran manualmente en los equipos para que estén siempre activos.

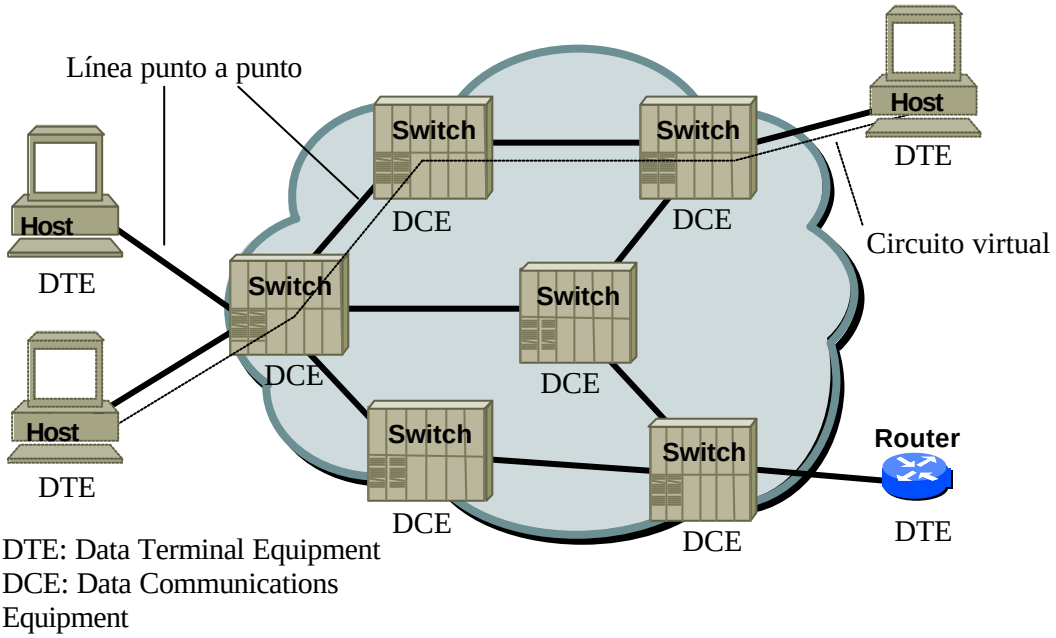


Figura. 1.6. Red Orientado a la Conexión

1.4.5 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.

1.4.6 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.

1.5 TOPOLOGIAS

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 del método de acceso que se usa.

Las redes WAN típicamente tienen topologías irregulares.

1.5.1 Configuración de Estrella

En este esquema, todas las estaciones están conectadas por un cable a un módulo central (Central hub), y como es una conexión de punto a punto, necesita un cable desde cada PC al módulo central.

Una ventaja de usar una red de estrella es que ningún punto de falla inhabilita a ninguna parte de la red, sólo a la porción en donde ocurre la falla, y la red se puede manejar de manera eficiente. Un problema que sí puede surgir, es cuando a un módulo le ocurre un error, y entonces todas las estaciones se ven afectadas.

1.5.2 Configuración de anillo

En esta configuración, todas las estaciones repiten la misma señal que fue mandada por la terminal transmisora, y lo hacen en un solo sentido en la red. El mensaje se transmite de terminal a terminal y se repite, bit por bit, por el repetidor que se encuentra conectado al controlador de red en cada terminal.

Una desventaja con esta topología es que si algún repetidor falla, podría hacer que toda la red se caiga, aunque el controlador puede sacar el repetidor defectuoso de la red, así evitando algún desastre. Un buen ejemplo de este tipo de topología es el de Anillo de señal, que pasa una señal, o token a las terminales en la red.

Si la terminal quiere transmitir alguna información, pide el token, o la señal, y hasta que la tiene, puede transmitir. Claro, si la terminal no está utilizando el token, la pasa a la

siguiente terminal que sigue en el anillo, y sigue circulando hasta que alguna terminal pide permiso para transmitir.

1.5.3 Topología de bus

También conocida como topología lineal de bus, es un diseño simple que utiliza un solo cable al cual todas las estaciones se conectan. La topología usa un medio de transmisión de amplia cobertura (broadcast medium), ya que todas las estaciones pueden recibir las transmisiones emitidas por cualquier estación. Como es bastante simple la configuración, se puede implementar de manera barata.

El problema inherente de este esquema es que si el cable se daña en cualquier punto, ninguna estación podrá transmitir.

1.5.4 Topología de árbol

Esta topología es un ejemplo generalizado del esquema de bus. El árbol tiene su primer nodo en la raíz, y se expande para afuera utilizando ramas, en donde se encuentran conectadas las demás terminales.

Ésta topología permite que la red se expanda, y al mismo tiempo asegura que nada más existe una "ruta de datos" (data path) entre 2 terminales cualesquiera.

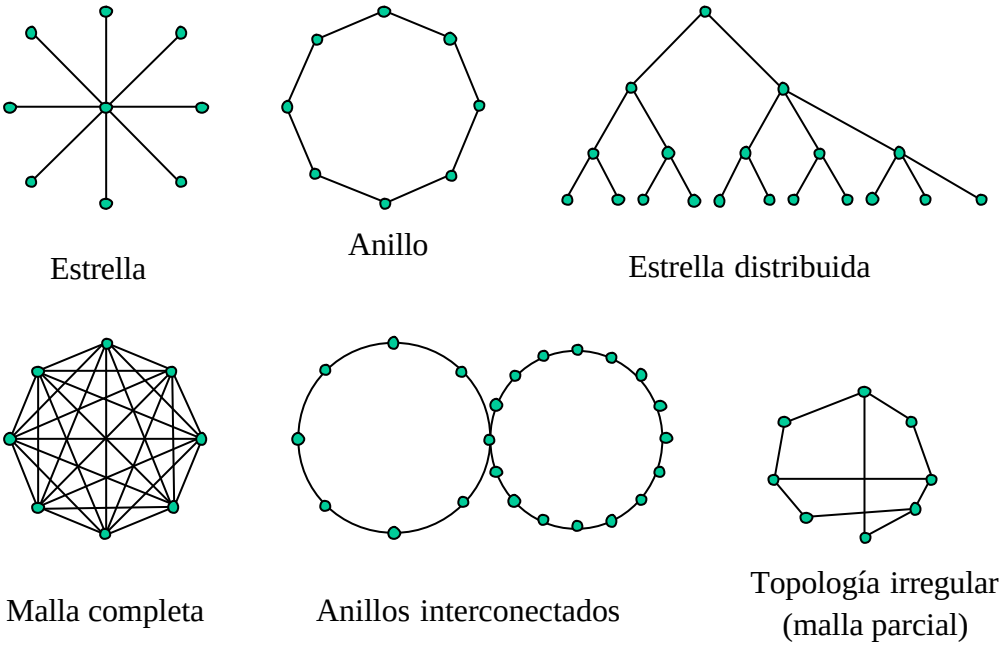


Figura. 1.7. Topologías de una Red

1.6 ROUTER

Un router es un conmutador de paquetes que opera en el nivel de red del modelo OSI. Sus principales características son:

Permiten interconectar tanto redes de área local como redes de área extensa. Proporcionan un control del tráfico y funciones de filtrado a nivel de red, es decir, trabajan con direcciones de nivel de red, como por ejemplo, con direcciones IP. Son capaces de rutear dinámicamente, es decir, son capaces de seleccionar el camino que debe seguir un paquete en el momento en el que les llega, teniendo en cuenta factores como líneas más rápidas, líneas más baratas, líneas menos saturadas, etc.

Los routers son más "inteligentes" que los switches, pues operan a un nivel mayor lo que los hace ser capaces de procesar una mayor cantidad de información. Esta mayor inteligencia, sin embargo, requiere más procesador, lo que también los hará más caros. A diferencia de los switches y bridges, que sólo leen la dirección MAC, los routers analizan la información contenida en un paquete de red leyendo la dirección de red.

Los routers leen cada paquete y lo envían a través del camino más eficiente posible al destino apropiado, según una serie de reglas recogidas en sus tablas. Los routers se utilizan a menudo para conectar redes geográficamente separadas usando tecnologías WAN de relativa baja velocidad, como ISDN, una línea T1, Frame Relay, etc. El router es entonces la conexión vital entre una red y el resto de las redes.

Un router también sabe cuándo mantener el tráfico de la red local dentro de ésta y cuándo conectarlo con otras LANs, es decir, permite filtrar los broadcasts de nivel de enlace. Esto es bueno, por ejemplo, si un router realiza una conexión WAN, así el tráfico de broadcast de nivel dos no es ruteado por el enlace WAN y se mantiene sólo en la red local.

Eso es especialmente importante en conexiones conmutadas como RDSI. Un router dispondrá de una o más interfases de red local, las que le servirán para conectar múltiples redes locales usando protocolos de nivel de red.

Eventualmente, también podrá tener una o más interfases para soportar cualquier conexión WAN.

1.6.1 Especificaciones Técnicas

Figura. 1.8. Router

Características Hardware:

- Número de Slots (slots para cable, interfaces WAN, comunicación)
- Tarjetas que soporta
- Capacidad (en bps)
- Tipo de Procesador
- Tipos y capacidad de Memoria
- Software que soporta

Características Físicas

- Tipo d Alimentación (dc, ac)
- Potencia
- Dimensiones
- Temperatura
- Humedad
- Peso

1.7 RED DE TELECOMUNICACIONES

Establecer una conexión (comunicación de voz, datos, vídeo, audio) entre dos usuarios (terminales de voz, datos, audio, vídeo, de servicios integrados, etc.) En este proceso intervienen 4 eventos:

- **Señalización de usuario:** Señales analógicas (tonos, timbres, corrientes eléctricas, frecuencias) o digitales (mensajes) intercambiados entre la red y el usuario para establecer, mantener, supervisar y liberar una llamada.

- **Conexión de usuarios:** Proporcionar temporalmente el soporte y organismos de red necesarios que permita a los usuarios comunicarse.

- **Señalización de red:** Conjunto de señales y/o mensajes entre nodos de la red que garantizan la selección y reserva de recursos de la misma para establecer rutas, enlaces y circuitos entre usuarios.

- **Gestión de la red:** Comandos y mensajes de red que permiten administrar la red, efectuar un diagnóstico de la misma, de su desempeño y calidad del servicio.

1.7.1 Red de Acceso

Porción de la red que conecta los nodos de acceso a suscriptores Individuales, normalmente está conformada por pares trenzados, fibra óptica o sistemas de radio y el equipo electrónico asociado que une una red troncal a los Puntos Terminales.

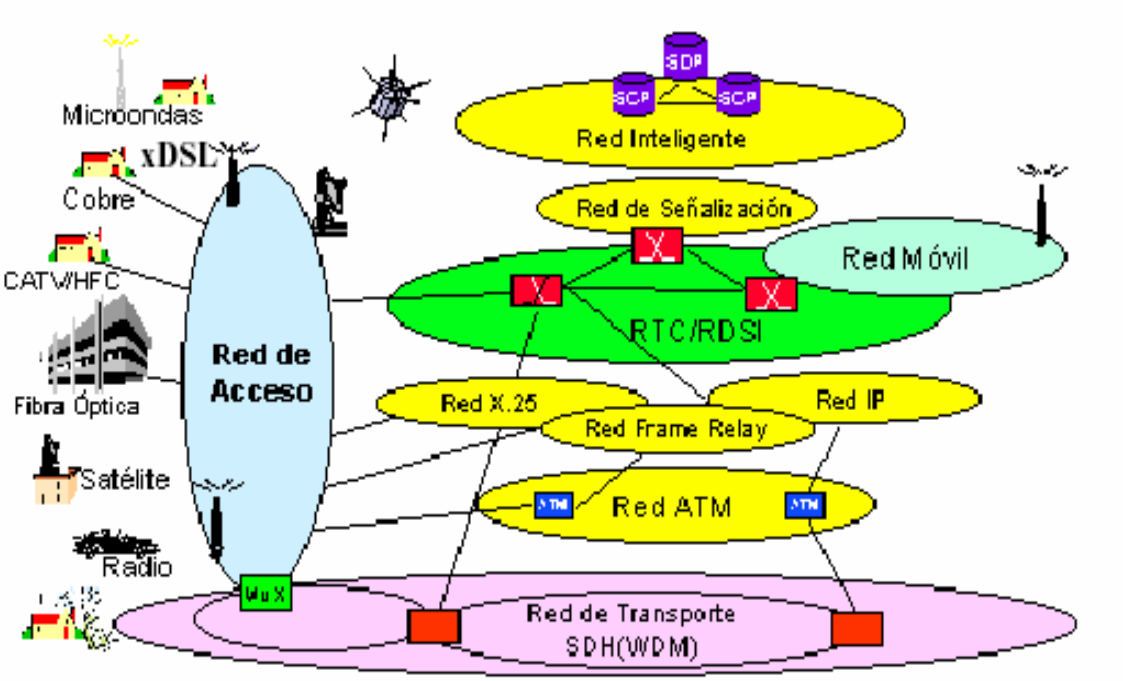


Figura. 1.9. Red de telecomunicaciones

1.7.2 Nodos de Acceso

Puntos en el borde de una red que proporcionan un medio para permitir acceso de los suscriptores a una red. En este nodo, el tráfico de los suscriptores se concentra en un número más pequeño de redes, que lo entregan posteriormente a la red troncal. Los nodos

de acceso pueden realizar diferentes conversiones o adaptación de protocolos (ej., X.25, Frame Relay y ATM)

CAPITULO II

ENLACES Y SERVICIOS

2.1 ESTABLECIMIENTO DE ENLACES PUNTO A PUNTO

Los enlaces a larga distancia necesarios para comunicaciones punto a punto o para crear la estructura de una red de área extensa, se pueden conseguir de diferentes formas (y con costos diferentes) en función de las necesidades del usuario u organización que las precise.

Este capítulo se va a centrar en cómo resolver las necesidades de un usuario para establecer una conexión entre dos dispositivos de su propiedad situados en puntos más o menos distantes geográficamente.

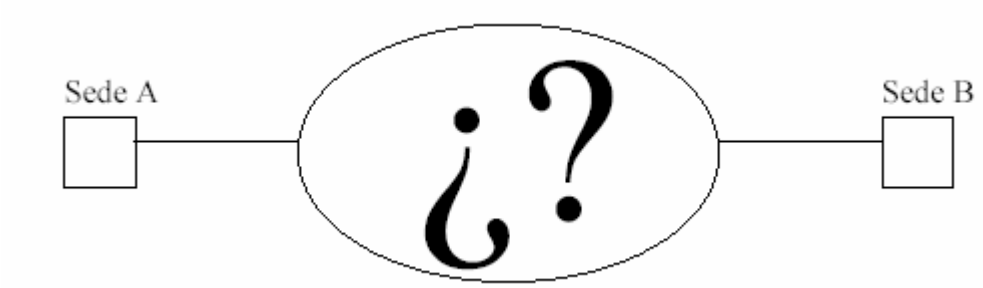


Figura. 2.1. Enlace Punto a Punto

2.1.1 Conexiones temporales a través de RTB o RDSI

Cuando los intercambios de datos se realizan de forma muy esporádica, no resulta rentable mantener una comunicación permanente entre los sistemas informáticos. La alternativa es el establecimiento de una conexión temporal por medio de una línea telefónica convencional de la Red Telefónica Básica (RTB) o de una línea digital de la Red Digital de Servicios Integrados (RDSI).

En el primer caso es necesario el uso de un módem telefónico en ambos extremos de la línea, pudiendo alcanzar velocidades de transmisión de la información de hasta 33,6 kbps. o 56 kbps dependiendo de la calidad de las líneas telefónicas.

La facturación se realiza en función de la duración de la llamada telefónica que se establece con la marcación del número de abonado telefónico del destinatario, del horario

en que se realiza y del tipo de esta (local, provincial, nacional, etc.), a parte de los costos fijos mensuales o bimestrales por disposición y mantenimiento de la línea.

Actualmente las compañías telefónicas ofertan la posibilidad del uso de "bonos" o sistemas de "tarifa plana" sobre todo para el acceso a Internet (siempre a través de un proveedor de acceso a Internet, ISP, Internet Service Provider).

RDSI se presenta para el usuario en dos modalidades de acceso: básico y primario. La primera se suele utilizar para establecer conexiones temporales de voz o de datos. Los costos para una llamada a través de la RDSI son similares, la forma de tarifación es la misma y solo varía la cuantía de los costos fijos.

Mediante un "módem RDSI", que no es un módem analógico, si no que simplemente codifica los datos para su transmisión a través de la línea digital, el usuario dispone en la modalidad más económica de uno o dos canales digitales full-duplex a 64 kbps.

La velocidad de transmisión de la información se puede incrementar a veces mediante la modificación del contrato con la compañía suministradora a múltiplos de 64 kbps con el aumento de costos correspondientes.

El establecimiento de la comunicación se realiza de la misma forma que con una línea telefónica convencional ya que el disponer de una línea RDSI permite sustituir a la anterior si se dispone de un teléfono digital RDSI, de tal manera que el usuario utiliza igualmente un número de abonado telefónico convencional.

Además, a través de la línea RDSI se pueden utilizar simultáneamente el teléfono y la conexión de datos.

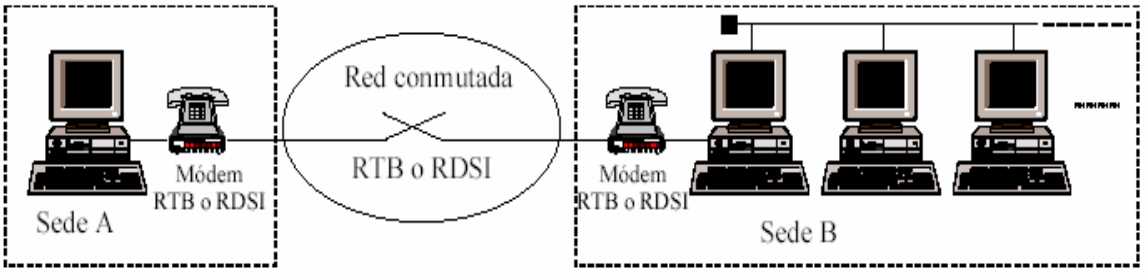


Figura. 2.2. Conexiones Temporales

El acceso RDSI primario no permite conexiones temporales, si no que se trata de un acceso punto a punto permanente a 2 Mbps. hacia otro usuario o hacia un servicio de red de área extensa.

En cualquiera de los casos, el uso de la RTB o la RDSI es para el usuario un simple medio de transmisión, con distintas velocidades posibles, que le permiten la conexión a otros usuarios o redes públicas utilizando el protocolo que en cada caso sea preciso.

2.1.2 Accesos permanentes con ADSL o con Cable módem

Para el acceso a una red de datos como Internet, muchos usuarios desean poder disponer de una conexión permanente, barata, con un ancho de banda aceptable y que no impida el uso independiente del teléfono.

Este tipo de acceso es posible mediante un Módem ADSL a través de una línea telefónica convencional o mediante un Cable módem a través de una red de televisión por cable. Se utilizan fundamentalmente para acceder a los servicios de los proveedores de acceso a Internet (1SP).

Sin embargo, estos accesos no se suelen utilizar para el establecimiento de enlaces punto a punto a larga distancia o de redes de área extensa privadas, salvo que se establezca un sistema de Red Privada Virtual.

El acceso por ADSL proporciona al usuario un canal privado con el ISP independiente en velocidad y uso del acceso del resto de usuarios del ISP. En cambio, con el módem de cable todos los usuarios de una zona geográfica comparten el medio de transmisión hacia el ISP (constituido de un sistema de cableado coaxial con amplificadores de señal).

La velocidad de acceso de cada usuario depende del número de usuarios de la zona conectados en cada momento y el uso que estén haciendo de la red. Además la privacidad de cada conexión podría verse comprometida.

El acceso ADSL puede ser conducido hacia otros servicios, a parte del de un ISP. Por ejemplo, hacia la red de la empresa en la que trabaja el usuario (habitualmente esto se hace combinando la tecnología ATM), proporcionando así al usuario un acceso punto a punto con la red de su empresa.

2.1.3 Alquiler de líneas de transmisión para uso exclusivo

Cuando la frecuencia del intercambio de datos aconseja al usuario mantener una conexión permanente punto a punto, una de las opciones es el alquiler de una línea de transmisión a una compañía que disponga de ellas.

No sólo las compañías telefónicas disponen de estas líneas, sino que otros tipos de compañías que tienen facilidades para el tendido de ellas. Este es el caso de empresas eléctricas, de distribución de gas, ferrocarriles, radiodifusión, etc., que normalmente realizan tendidos para la transmisión de datos paralelos a sus instalaciones para su propio uso o el alquiler a terceros.

Las velocidades de transmisión de la información y los dispositivos de interfaz para la conexión a esas líneas dependen de la tecnología y características de las mismas. La facturación suele ser fija e independiente del volumen de datos transmitidos. Permite al usuario el disponer de un canal de capacidad fija para su uso exclusivo, por lo que se ha de valorar bien su necesidad.

Si su uso no es muy intensivo, puede dar lugar a un desaprovechamiento del canal en periodos de baja actividad y no justificar el costo del mismo.

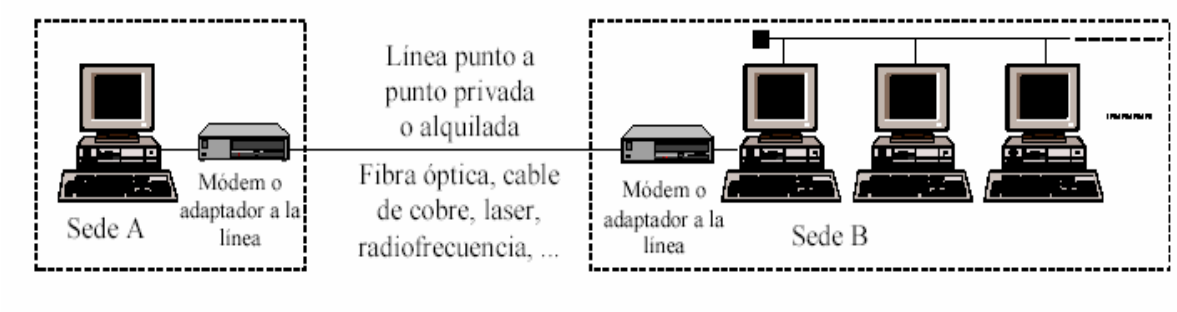


Figura. 2.3. Líneas de Transmisión de uso Exclusivo

2.1.4 Líneas de transmisión en propiedad

Cuando el usuario puede realizar el tendido de sus propias líneas de transmisión ha de tener en cuenta la inversión inicial y los costos de mantenimiento de esas líneas que estará en función de su capacidad y tecnología.

Estos costes son justificables si la frecuencia y volumen de datos es grande. Generalmente se trata de compañías como las mencionadas anteriormente, que en muchas ocasiones, a parte del uso propio, alquilan esas líneas a terceros.

2.1.5 Alquiler de circuitos virtuales permanentes o temporales

Los operadores de transmisión de datos suelen ofrecer servicios avanzados de red mediante sus redes de conmutación X.25, Frame-Relay, ATM, etc.

Esto permite ofrecer al usuario un ancho de banda mínimo para sus conexiones temporales o permanentes y la posibilidad de aumentar ese ancho de banda si lo necesita y la carga de la red en esos momentos lo permite.

El aprovechamiento de las líneas de transmisión es mayor, ya que al ser compartidas por múltiples usuarios, los periodos de inactividad se reducen al mínimo.

La velocidad de la línea de transmisión que une al usuario a la red suele ser bastante superior al ancho de banda contratado, ya que este suele tener un mayor peso en el costo de la conexión.

Los parámetros de facturación pueden ser tremendamente complejos, añadiendo en general a los costos fijos (conexión, velocidad de la línea de transmisión y ancho de banda contratado), costos variables en función del volumen de tráfico, horario de acceso, exceso sobre el ancho de banda contratado, etc.

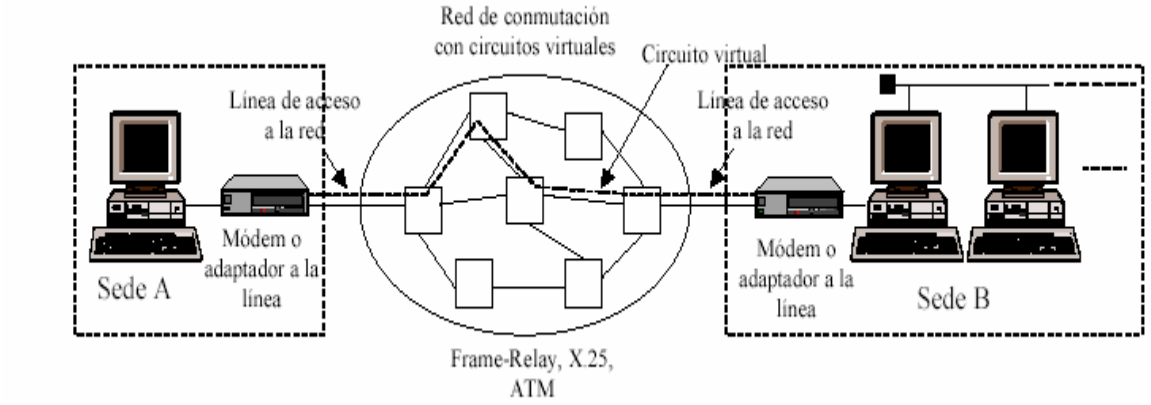


Figura. 2.4. Circuitos Virtuales

2.1.6 Red Privada Virtual (VPN)

Una alternativa más económica que la contratación de circuitos virtuales, es la utilización de una red publica de conmutación de paquetes, como Internet, para establecer las conexiones punto a punto de larga distancia de la empresa.

En el transporte de los datos pueden intervenir múltiples nodos pertenecientes a diferentes empresas y organizaciones públicas o privadas. Por ello, hay que poner especial interés en mantener su privacidad en su viaje a través la red mediante el uso técnicas de cifrado.

Estas técnicas son también recomendables en el caso de los ejemplos descritos en los casos anteriores, especialmente, cuando no exista confianza en el medio de transmisión o las compañías que le dan soporte.

El acceso de cada extremo a la red Internet se hará a través de un proveedor de servicio (ISP), hasta el que se llega mediante alguno de los métodos habituales: RTB, RDSI, ADSL, Cable módem, Frame-Relay, etc.

Desde el ISP el acceso a la red Internet se realiza a través de alguna organización conectada a la misma normalmente mediante conexiones Frame-Relay o ATM. Es responsabilidad del ISP que estas últimas tengan el ancho de banda adecuado para dar un servicio de calidad a todos sus clientes, conectados temporal o permanentemente a la red Internet.

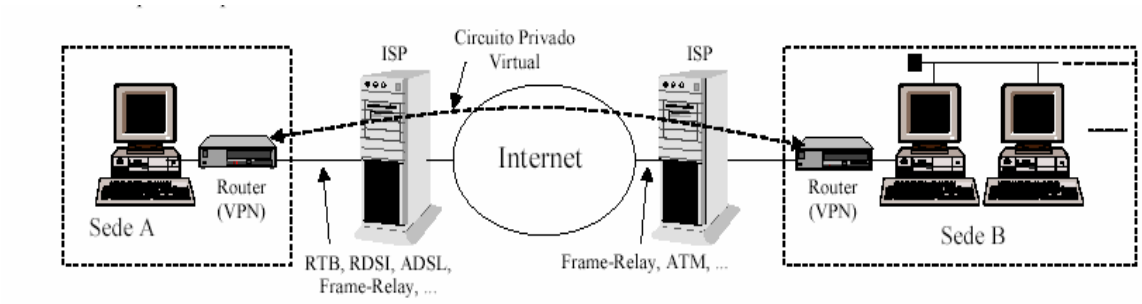


Figura. 2.5. Red Privada Virtual

El elemento final que conecta cada sede a la línea de transmisión que va hacia el ISP, suele ser un encaminador (router) con capacidad para establecer una Red Privada Virtual (VPN, Virtual Prívate Nefwork).

Esto consiste en crear un Circuito Privado Virtual, es decir, una conexión punto a punto con el encaminador del otro extremo, a través del que viajan todos los datos que se intercambian entre ambas sedes. Los datos viajan normalmente codificados y obviamente se pueden conectar más de dos sedes, manteniendo varias conexiones punto a punto.

De esta manera, los nodos de ambos extremos del enlace tienen la sensación de pertenecer a la misma red, a la vez que esta resulta prácticamente invisible para el resto del mundo. Los inconvenientes son la imposibilidad de garantizar un ancho de banda mínimo e incluso el servicio de los enlaces punto a punto, sometidos a los avalares del estado de las conexiones y el tráfico de la red Internet.

2.2 CIRCUITOS DE TRANSMISIÓN PARA REDES DE ÁREA EXTENSA

Como se ve existen distintas tecnologías para la transmisión física de los datos que permiten el establecimiento temporal o permanente de enlaces punto a punto. Con estos enlaces se pueden establecer conexiones simples entre dos sistemas o crear múltiples conexiones punto a punto entre sistemas para la organización de una estructura de red de área extensa.

En este caso se describen las características técnicas (medio físico, codificación de la señal, etc.) de los medios de transmisión más habitualmente utilizados para establecer los enlaces punto a punto, descritos anteriormente.

2.2.1 Líneas de telefonía analógica

El modo más elemental para establecer un enlace temporal a larga distancia es utilizando una línea telefónica de la RTB.

Originalmente se trataba del establecimiento de un enlace por conmutación de circuitos mediante la marcación del número del abonado de destino, pero en la actualidad las tecnologías de conmutación, sobre todo entre centrales de la RTB han cambiado mucho.

Sin embargo, no ha cambiado tanto la línea que une al abonado con la central más próxima de la RTB. Se trata de un par de cables trenzados que debido a los sistemas de repetidores analógicos (amplificadores de banda) que se emplean para amplificar la señal que porta la voz del usuario, apenas tiene un ancho de banda de 4 KHz en el mejor de los casos, estando generalmente limitado entre 300 y 3000 Hz.

El no poder bajar de 300 Hz impide que seriales digitales en banda base, que establecen generalmente valores de tensión continua en la codificación, puedan viajar por estas líneas. Por lo tanto se ha de utilizar un equipo modulador-demodulador, módem, para enviar y recibir señales a través de ellas.

La mejora en la tecnología de estos equipos con la utilización de varias frecuencias portadoras sobre las que se modula la información digital combinando la modulación de fase y de amplitud, permite la transmisión de información full-duplex a velocidades de hasta 33,6 y 56 kbps según la calidad de la línea, en un medio que apenas permite transmitir 600 elementos de señal por segundo (baudios) sobre cada frecuencia portadora.

Si la distancia del abonado a la central telefónica más próxima no es muy grande (unos 5 Km. sino se limita más por otras circunstancias) y la central telefónica está suficientemente modernizada, el usuario podrá optar por soluciones RDSI o ADSL, ya que para esas distancias no son necesarios los amplificadores de banda en la línea de cobre.

Para distancias mayores, se precisará algún sistema de amplificación específico que normalmente no es rentable para las compañías que ofertan el servicio.

ADSL (Asymmetric Digital Subscriber Line o Línea de Abonado Digital Asimétrica) consiste en transmitir conjuntamente voz y datos modulados a distintas frecuencias sobre la línea telefónica convencional.

Ambas transmisiones se separan en la recepción por medio de un filtro (o splitter) colocado en ambos extremos de la línea telefónica.

El filtro separa las frecuencias correspondientes a la voz (o telefonía convencional) de las frecuencias sobre las que se modulan los datos digitales.

Así, cuando se está utilizando el módem ADSL (un módem especial para este tipo de tecnología), se tiene la línea de teléfono disponible para realizar simultáneamente llamadas de voz. Además la conexión del usuario a través del módem ADSL puede mantenerse las 24 h del día.

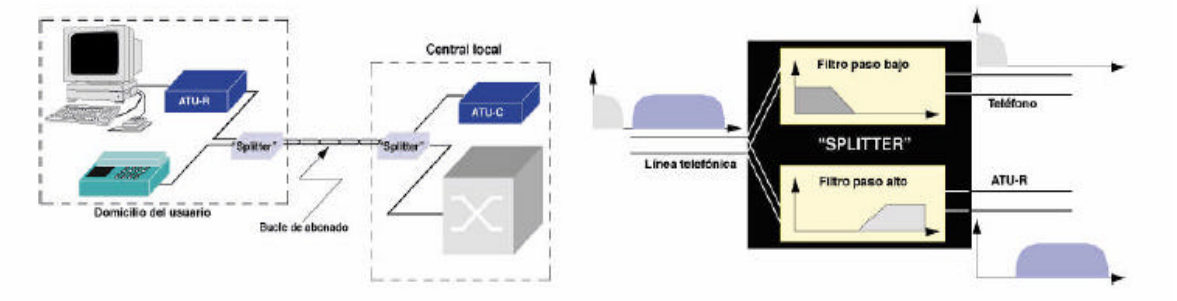


Figura. 2.6. Comunicación ADSL

La comunicación que se establece mediante ADSL es asimétrica, ya que la velocidad en bits por segundo a la que se transmite la información hacia el usuario es mucho mayor que la que se utiliza en sentido contrario.

2.2.2 Cable módem

La tecnología Cable módem es ofertada por las compañías de televisión por cable como alternativa al acceso a la red Internet y, por lo tanto, puede permitir el establecimiento de conexiones punto a punto a través de enlaces privados virtuales (VPN) u otras estrategias.

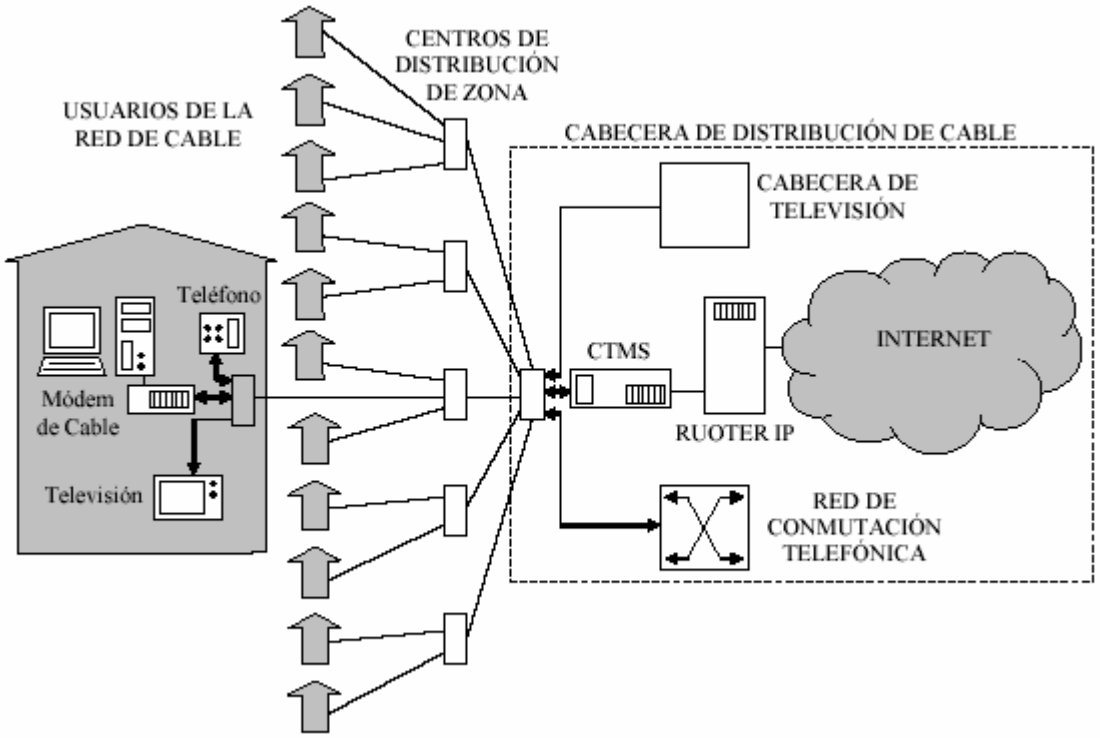


Figura. 2.7. Conexión por Cable Modem

A través de una red de cable se difunden habitualmente las señales desde la cabecera de distribución de los canales de televisión hacia los clientes, utilizando tantos canales de frecuencia como canales se distribuyen.

Los medios de transmisión son fundamentalmente la fibra óptica y el cable coaxial. La primera se utiliza para conectar las centrales de transmisión con los distribuidores de zona y el segundo para llegar desde estos hasta los domicilios de los clientes finales.

El resto de ancho de banda de estos cables (el que no se utiliza para la distribución de televisión) se puede utilizar para otros servicios con flujos de información tanto de bajada hacia el usuario como de subida desde el domicilio del usuario hacia la cabecera, fundamentalmente telefonía y acceso a redes de datos.

El servicio es asimétrico, con una mayor velocidad de datos en la bajada que en la subida. La bajada de datos puede superar los 50 Mbps usando un único canal de frecuencia de 8 MHz (equivalente a un canal de televisión) en la banda comprendida entre los 65 y los 850 MHz con modulación 64-QAM ó 256-QAM.

Este flujo de bajada es enviado desde el CMTS (Cable Modem Termination System) y recibido por todos los módem de cable que filtran el tráfico que corresponde a su sesión, por lo que comparten el ancho de banda total. Por lo general, un CMTS tiene capacidad para dar servicio hasta unos 1000 usuarios.

La subida de datos se realiza en un canal de 2 MHz en la banda de frecuencias entre 5 y 65 MHz. con modulación QPSK ó 16-QAM, que proporciona hasta 3 Mbps. Los módem de cable transmiten en ranuras de tiempo reservadas en unos casos o por las que compiten mediante un sistema de contienda en otros, en cuyo caso se pueden producir colisiones.

Sin embargo, la transmisión de un módem de cable hacia el CMTS no puede ser escuchada por los demás.

2.2.3 Acceso a través de la red Eléctrica

Las compañías de suministro eléctrico empiezan a ofrecer a sus clientes acceso de banda ancha a Internet a través de la propia red eléctrica. El sistema es comparable al proporcionado por un módem de cable: se utiliza un módem PLC (Power Line Communication) que se conecta a cualquier enchufe de la vivienda o local del usuario, y se

comparte el ancho de banda de la red eléctrica de baja tensión a la que se está conectado con el resto de los usuarios.

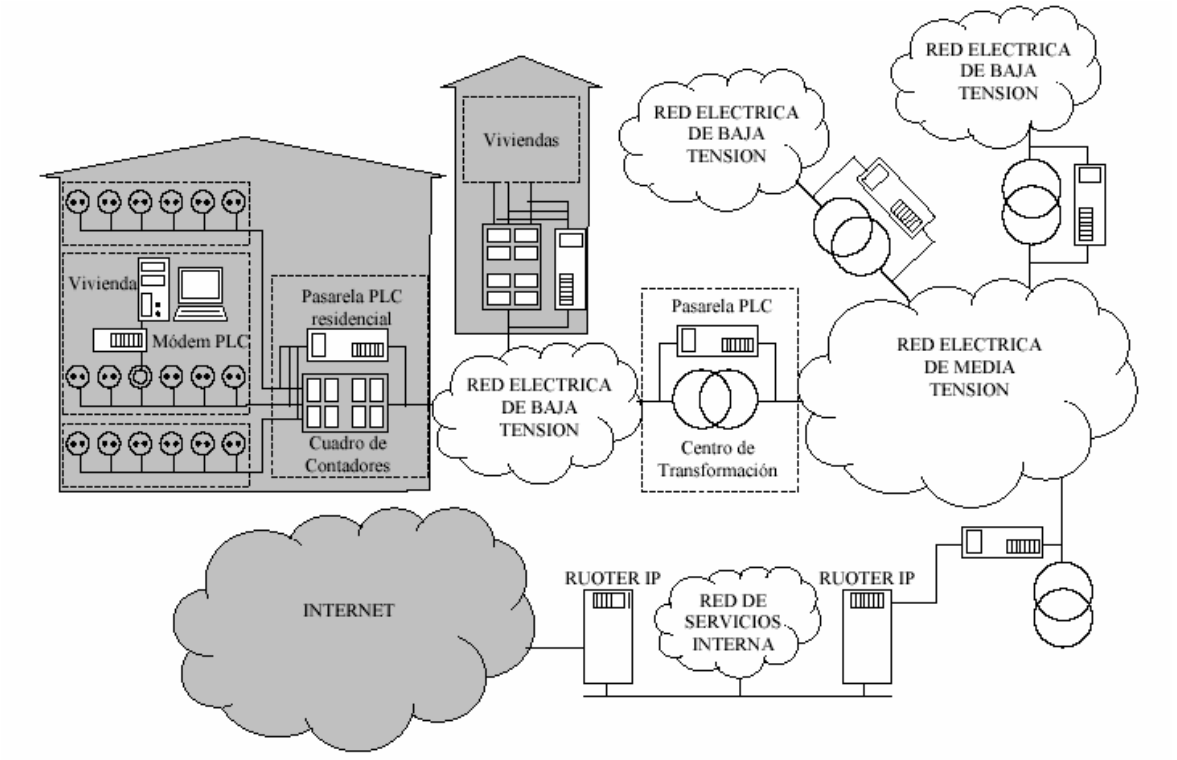


Figura. 2.8. Acceso por Red Eléctrica

La tecnología más desarrollada se denomina Powerline. La transmisión se realiza mediante modulación OFDM empleando múltiples bandas de frecuencia entre los 4 y los 21 MHz.

No todas esas frecuencias sufren la misma atenuación en los cables eléctricos de una instalación, e incluso las características de la instalación varían de unos edificios a otros y se ven afectadas por los dispositivos conectados, la longitud de los cables, el número de puntos de conexión, etc.

Para superar estos inconvenientes, el sistema Powerline monitoriza constantemente la línea de transmisión y suprime o utiliza el envío de señales en determinadas frecuencias según se propaguen o no adecuadamente.

Los mismos principios de la tecnología Powerline pueden aplicarse para establecer una red local de dispositivos a través de los enchufes de la vivienda, pero utilizando frecuencias y modulaciones diferentes.

2.2.4 Bucle de Abonado Vía Radio (WLL)

El bucle de abonado vía radio, cuya denominación en inglés es Wireless Local Loop (WLL), es el término que se refiere a la distribución del servicio telefónico y de datos por un sistema que utiliza señales de radio para conectar a los abonados a su central telefónica más cercana, en lugar de utilizar los métodos cableados convencionales.

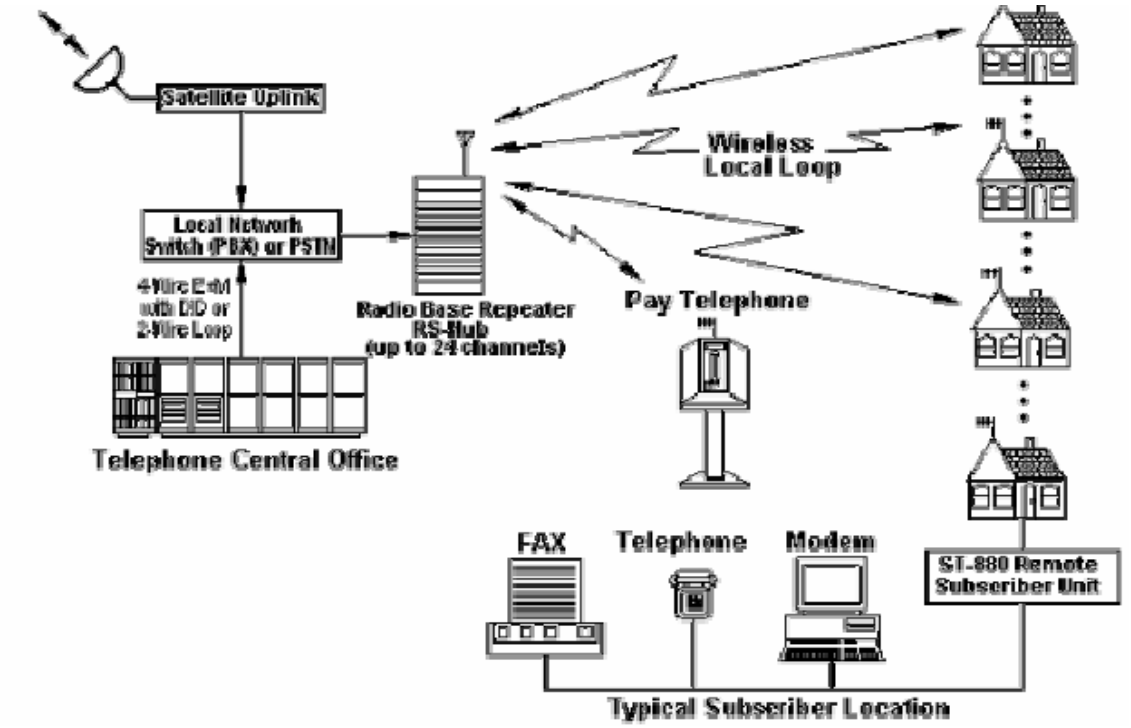


Figura. 2.9. Acceso por WLL

Estos sistemas utilizan ondas radioeléctricas de alta frecuencia permitiendo ofrecer velocidades de transmisión entorno a los 2 Mbps. Tienen un costo de instalación y mantenimiento relativamente bajo y no deben producir interferencias con otros sistemas de comunicación ya existentes como las comunicaciones por microondas o de señales broadcast (TV y Radiodifusión).

Las tecnologías a utilizar para establecer el WLL pueden ser analógicas o digitales, entre las que están las tecnologías tradicionales de telefonía móvil o sistemas inalámbricos como DECT (Digital European Cordiess Telecommunication). Actualmente son preferibles las tecnologías digitales y en este campo aún existen muchos sistemas propietarios, sin que se haya impuesto un estándar abierto.

Algunas tecnologías como SkyLink, PHS o CDMA se muestran en la figura.

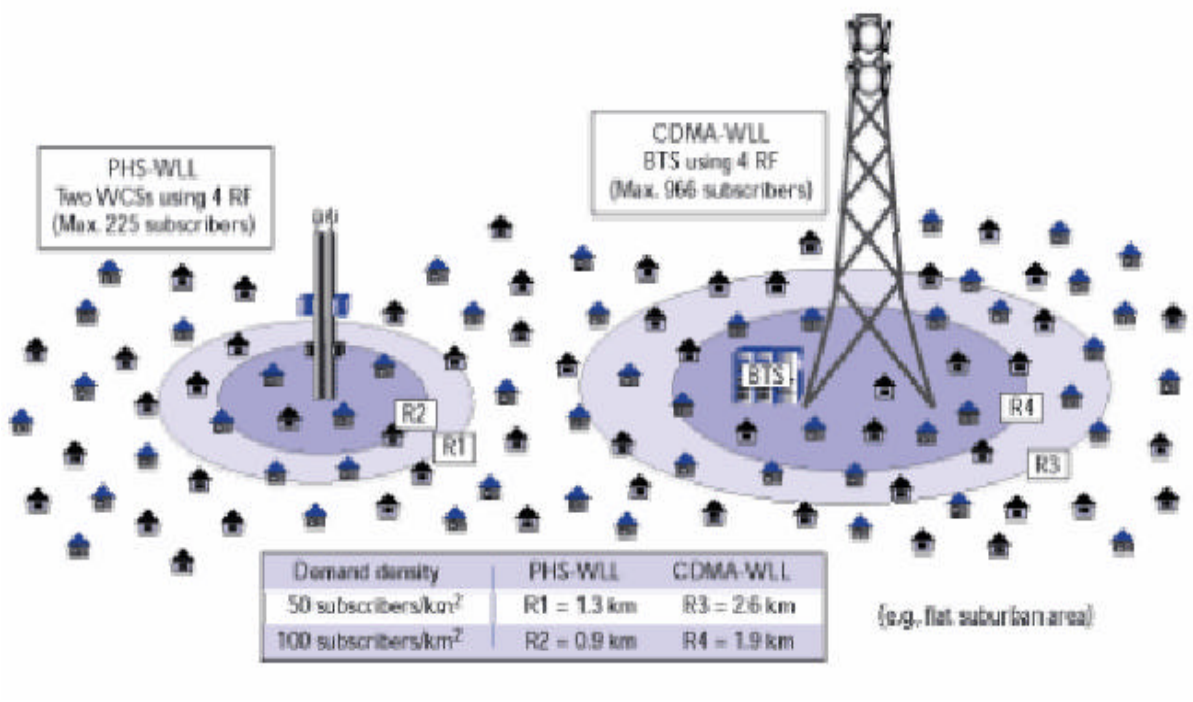


Figura. 2.10. Tecnología CDMA

2.2.5 Circuitos con Modulación por Codificación de Pulsos (PCM)

Las compañías telefónicas han optado por las ventajas de la comunicación digital y han ido cambiando sus tradicionales circuitos analógicos para la interconexión de centrales telefónicas por sistemas digitales en los que las señales analógicas se digitalizan para su posterior transmisión.

Esto facilita en alguna manera la transmisión de datos digitales, que ya no necesitan ser modulados sobre portadoras analógicas.

La modulación por codificación de pulsos (PCM) consiste en muestrear una señal analógica cada 125 us. Esta frecuencia de muestreo se considera suficiente para reproducir sin problemas la voz humana en una línea telefónica.

El valor de cada muestra se codifica en 7 u 8 bits (es decir, en valores de 0 a 127 ó de 0 a 255) que se envían con esa misma cadencia por la línea en banda base. Esto quiere decir que la velocidad de transmisión de información necesaria para un canal de voz en PCM será 8 bits / 125 us = 64 kbps.

Precisamente los canales B de las líneas RDSI están diseñados para ser el soporte de conexiones telefónicas de voz con la ayuda de teléfonos digitales que muestrean y reconstruyen la voz de los interlocutores.

Aparentemente utilizar un canal digital de voz parece una desventaja, ya que una línea analógica con un ancho de banda de 4 kHz es más que suficiente frente a los 28 kHz que se necesitan al menos para transmitir una señal digital a 56 kbps (suponiendo que cada muestra se codifica con 7 bits en lugar de con 8). Sin embargo hay otras ventajas que compensan esta opción:

- Al usar repetidores de señales digitales en lugar de amplificadores de señales analógicas no hay ruido aditivo.
- Las señales digitales se multiplexan en el tiempo (Time división multiplexing, TDM) en lugar de en frecuencia {Frecuency-division multiplexing, FDM) por lo que no hay ruido de intermodulación.
- La conversión a señales digitales permite el uso de técnicas más eficaces de conmutación.

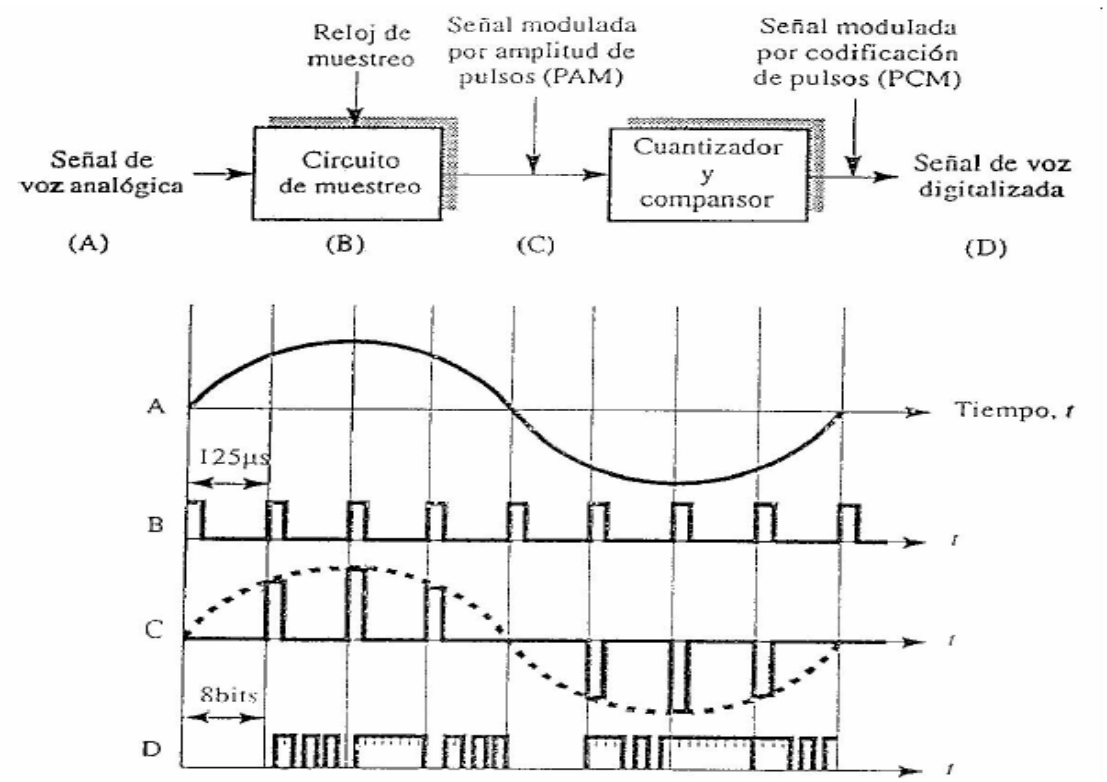


Figura. 2.10.a. Modulación PCM

2.2.6 Líneas RDSI

La forma más básica en la que se suelen utilizar los canales PCM es la que presentan las líneas RDSI. Las modalidades de acceso RDSI son en principio dos: el acceso básico y el acceso primario.

El acceso básico consiste en dos canales full-duplex a 64 kbps, denominados de tipo B, y uno a 16 kbps, denominado de tipo D, que suman en total 144 kbps. De todas formas, el usuario puede optar por un uso restringido del acceso básico a un costo más económico. Aún siendo tres canales independientes, se multiplexan sobre uno o dos pares de hilos.

Si es un único par se establece un sistema con un transformador híbrido y cancelación de eco para permitir la transmisión en ambos sentidos simultáneamente. En ambos casos las líneas trabajan en realidad a 192 kbps full-duplex, debido a la necesidad de añadir bits para la sincronización y la compensación de niveles de continua en la señal.

El acceso primario requiere normalmente que la conexión desde el usuario al proveedor de la línea se realice mediante fibra óptica, aunque existen soluciones mediante cable de cobre.

2.2.7 Multiplexación de canales PCM

Como se ha mencionado anteriormente las señales digitales se suelen multiplexar en el tiempo (TDM). Tanto en Norte América como en Europa se han desarrollado sistemas TDM sincrónicos y jerárquicos, pero con diferentes capacidades.

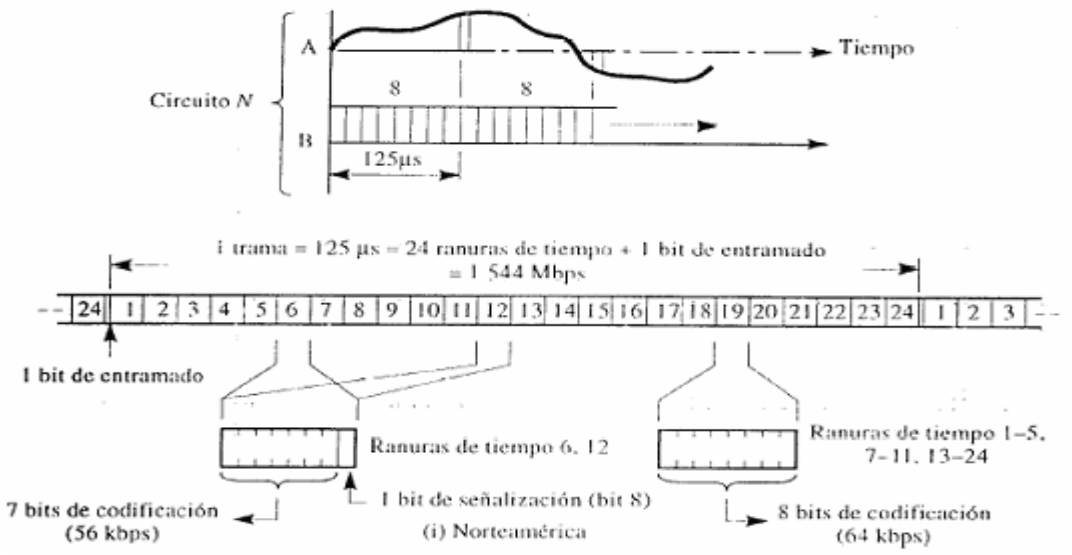


Figura. 2.11. Multiplexación de Canales PCM

La multiplexación básica de canales PCM en Norte América se denomina T1 o DS1 y consiste en tramas de 193 bits que se transmiten cada 125 µs, lo que significa 1,544 Mbps.

En esa trama se transportan los 8 bits de 24 canales de voz correspondientes a una muestra de la señal analógica que codifica cada canal (8x24=192 bits) más un bit adicional que sirve para la delimitación y sincronización de la trama.

En Europa la presentación básica es la agregación de 30 canales de voz con un total 2,048 Mbps. En ambos casos, la capacidad de transmisión de información coincide con la del acceso primario de una línea RDSI.

El resto de capacidades que se reflejan en la tabla siguiente se consiguen mediante la multiplexación de más canales PCM o de canales básicos en otros de velocidad superior. Por ejemplo, cuatro canales T1 se pueden multiplexar en un canal T2. En Europa se ha adoptado la recomendación internacional U1T-T (Unión Internacional de Telecomunicaciones-Sector Telecomunicaciones) que se refleja en la misma tabla.

Los valores en Mbps no se corresponden con múltiplos exactos de los canales de voz soportados, ya que en las distintas tramas se insertan bits o se utilizan los 8 de algún canal para la sincronización y otras funciones de señalización (como establecimiento de llamadas).

Norte América			UIT-T		
Identificación	Nº canales de voz	Mbps	Identificación	Nº canales de voz	Mbps
T1 o DS1	24	1,544	E1	30	2,048
T1C o DS1C	48	3,152	E2	120	8,448
T2 o DS2	96	6,312	E3	480	34,368
T3 o DS3	672	44,736	E4	1920	139,264
T4 o DS4	4032	274,176	E5	7680	565,148

Figura. 2.12. Capacidad de Transmisión

En las líneas TDM las diferencias en la sincronización de los relojes de los canales que se multiplexan dan lugar a que las tasas de las líneas de salida tengan que ser un poco

superiores a la suma de las tasas de los canales de entrada, y rellenadas con los llamados bits de justificación. A esta técnica se la conoce como Jerarquía Digital Plexocrónica

Estas líneas se establecen como enlaces punto a punto, lo que puede dar a la red la topología que se quiera. Lo habitual, sobre todo para velocidades altas, es elegir una topología de anillo bidireccional (a veces doble para tener redundancia por si se produjera la rotura de uno de ellos) sobre fibra óptica.

En la aplicación telefónica, este anillo une centralitas donde se conmutan los canales de voz de los abonados conectados a cada una de ellas hacia otros abonados de la centralita o hacia el canal correspondiente de la línea multiplexada si el interlocutor está conectado a otra centralita del anillo.

Si un usuario necesita una portadora para transmitir datos entre 2 o más oficinas de su empresa, se le pueden reservar en la portadora que circula por cada segmento del anillo el espacio correspondiente en canales PCM que necesita para la velocidad solicitada.

La forma de insertar los datos del usuario en la portadora no es sencilla y la suele llevar a cabo un ADM (Add-Drop Multíplexer) situado en la centralita más próxima al o los puntos de acceso correspondientes.

Este dispositivo ha de demultíplexar la portadora general hasta el nivel de la portadora del cliente para extraer o introducir en ella los datos de sus comunicaciones.

Desde el punto de vista del usuario e independientemente de como estén configuradas las líneas TDM, se dispondrá de una línea de comunicación punto a punto de la velocidad que se haya establecido.

2.2.8 Jerarquía Digital Sincrónica (SDH)

La Jerarquía Digital es una recomendación estándar del CCITT (Comité Consultivo Internacional para la Telefonía y la Telegrafía) basado y prácticamente idéntico al estándar que desarrolló la compañía Bellcore bajo la denominación de SONET {Synchronous Optical NETwork).

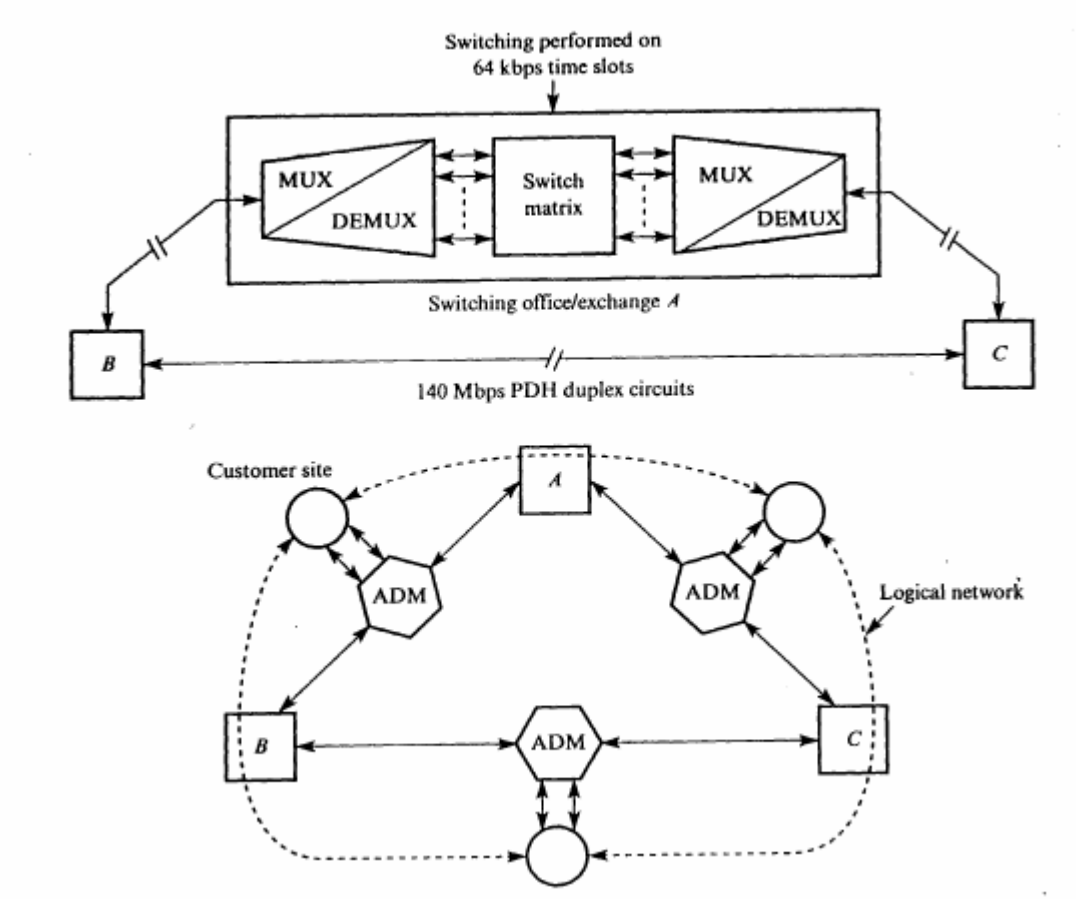


Figura. 2.13. Jerarquía Digital Sincrónica

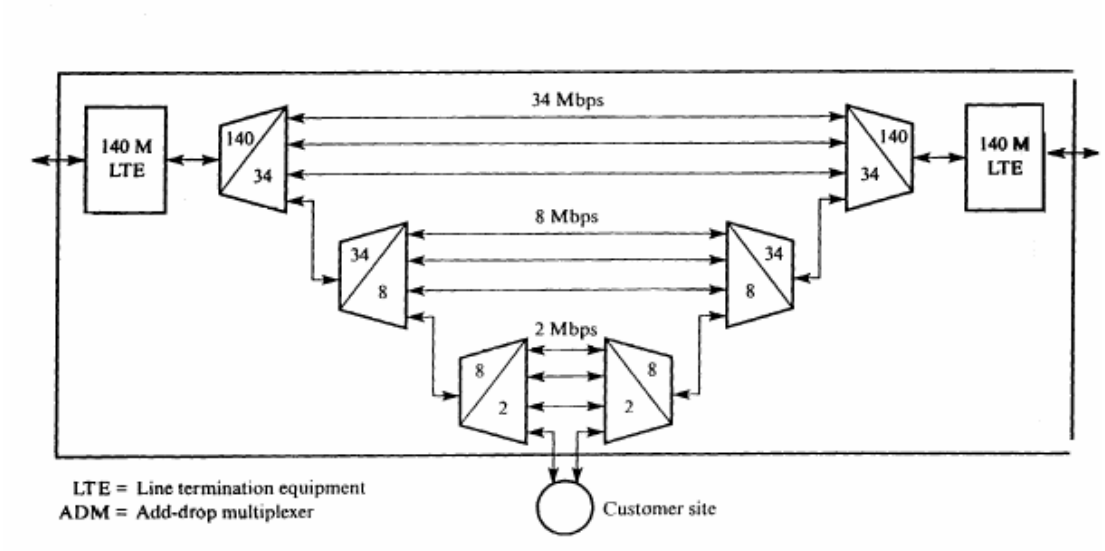


Figura. 2.14. SDH

El objetivo de SONET era superar las barreras de velocidad definidas para T4 con un esquema sincrónico gobernado por un reloj maestro para evitar los inconvenientes del esquema PDH.

SONET	STS-1	STS-3	STS-9	STS-12	STS-18	STS-24	STS-36	STS-48
JDS		STM-1	STM-3	STM-4	STM-6	STM-8	STM-12	STM-16
Mbps	51,84	155,52	466,56	622,08	933,12	1244,16	1866,24	2488,32

Figura. 2.15. Capacidad de Transmisión SONET

La velocidad básica definida para SONET es de 51,84 Mbps y se denomina STS-1 u OC-1, habiéndose definido también tasas más altas. En JDS el módulo básico es 155,52 Mbps, denominado STM-1. La correspondencia entre ambas especificaciones se refleja en la figura.2.15.

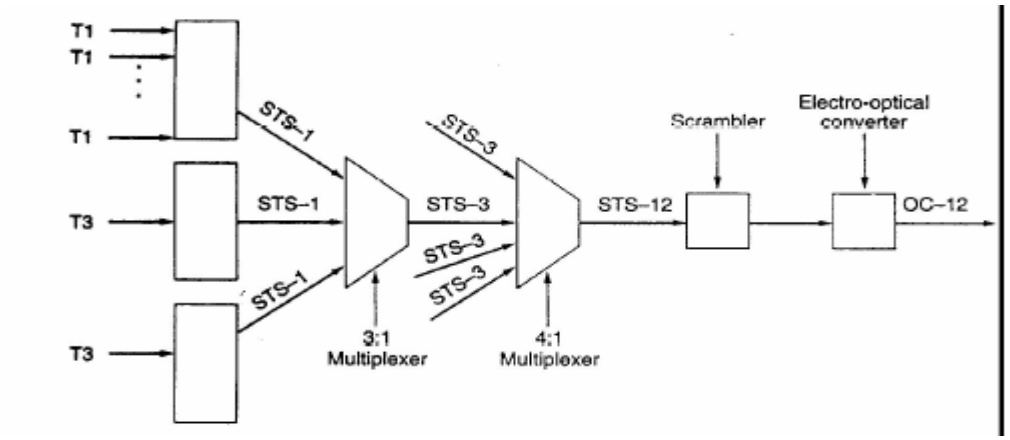


Figura. 2.16. Diagrama STM-1

Al igual que en la TDM de la PDH, la señal portadora en SONET o JDS se compone de un conjunto repetitivo de tramas que se transmiten cada 125 µs. Para STS-1 la trama está constituida por 810 octetos. La trama se suele representar como una matriz de 9 filas de 90 octetos que se transmiten fila a fila de izquierda a derecha y de arriba abajo.

Los tres primeros octetos de cada fila (3x9=27) llevan información suplementaria para las líneas y secciones por las que circula la trama. El resto es carga útil que incluye también una columna de información suplementaria relacionada con la ruta. Esta columna no tiene por que ser la primera, sino que su posición se determina mediante un puntero de la información suplementaria.

Cuando se multiplexan tramas, por ejemplo tres STS-1 en una STS-3, se hace octeto a octeto, es decir, el primer octeto en STS-3 es el primero del primer canal STS-1, el

segundo es el primero del segundo canal STS-1, el tercero es el primero del tercer canal STS-1, el cuarto es el segundo del primer canal STS-1 y así sucesivamente.

En las figuras se muestra la estructura de una trama STS-1 de SONET y de tramas multiplexadas según la nomenclatura de JDS.

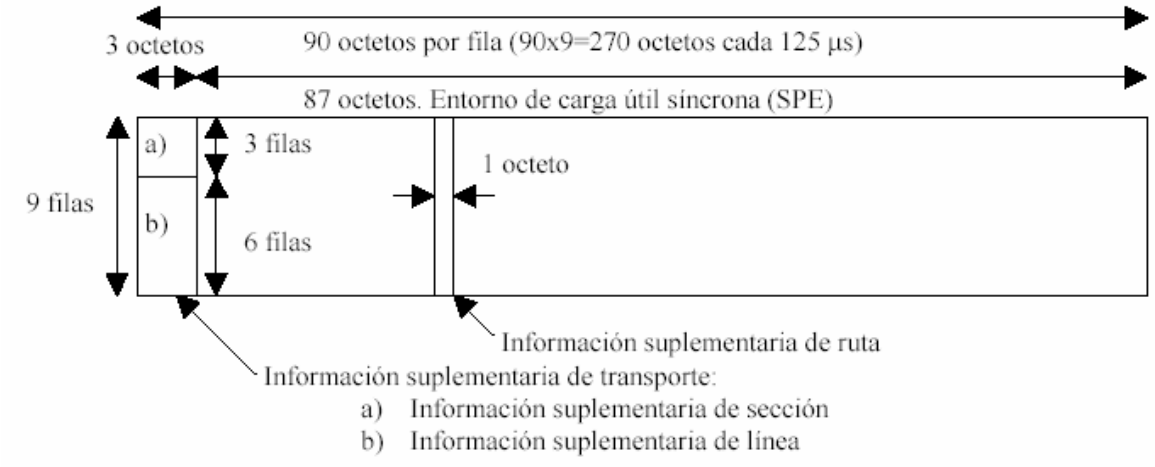


Figura. 2.17. Formato de la Trama STS-1

El contenido de información de cada trama puede servir para transportar múltiples flujos de PDH tributarios entre 1,5 y 140 Mbps u otros de distinta naturaleza procedentes por ejemplo de un conmutador ATM.

Cada uno de esos flujos se transporta en un contenedor virtual cuyo inicio no tiene por que coincidir con el inicio de la trama STS o STM, ni tampoco su tamaño pudiendo ser mayor o menor que ella y, por lo tanto, puede no estar contenido en una sola trama.

Es decir, el contenedor virtual puede empezar en cualquier punto de una trama y terminar en cualquier punto de la misma o de alguna de las siguientes.

En la estructura de la red SONET/JDS intervienen tres elementos principales: los conmutadores, multiplexores, y repetidores todos ellos conectados por fibra óptica.

A los conmutadores y multiplexores se les denomina Equipos Terminales de Línea (LTE).

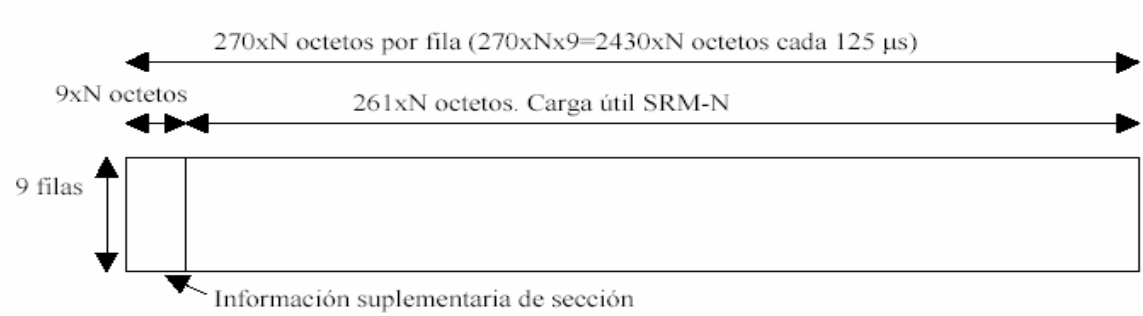


Figura. 2.18. Formato de la Trama STM-N

Al tramo de fibra que une dos repetidores, se le denomina sección. Al conjunto que une dos LTEs, posiblemente a través de varios repetidores intermedios, se le denomina línea.

Y finalmente, al recorrido a través de varios repetidores y/o LTEs intermedios, entre el LTE a través del que accede el tributario del usuario en un extremo y aquel por el que accede el tributario conectado con él en el otro extremo, se le denomina ruta.

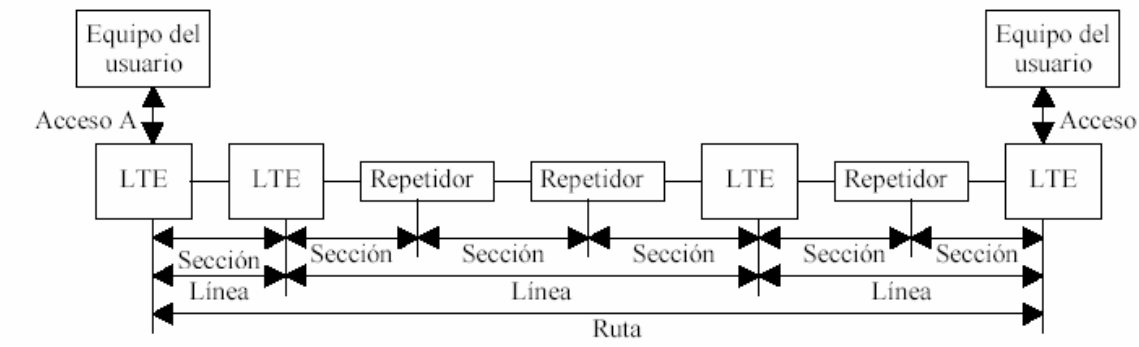


Figura. 2.19. Topología de Red SONET

La topología de la red SONET/JDS podría ser la que se quisiera, aunque lo habitual suele ser una topología en anillo bidireccional sobre fibra óptica, como la descrita anteriormente para PDH, donde los nodos que forman el anillo son conmutadores o multiplexores (LTEs).

Por lo tanto, para el usuario del transporte de datos de la red, esta será un enlace punto a punto transparente para él, al que accederá en cada extremo a través de un ADM adecuado para esta red.

2.3 SERVICIOS DE RED DE ÁREA EXTENSA

Los protocolos de capa física WAN describen cómo proporcionar conexiones eléctricas, mecánicas, operacionales, y funcionales para los servicios de una red de área amplia.

Con el objeto de mejorar el servicio que da al cliente una red de transmisión de datos, se han desarrollado distintos servicios de red para redes de área extensa.

Uno de los más utilizados ha sido la red X.25. Se trata de una red de conmutación de paquetes que ofrece un servicio de red fiable con conexión sobre enlaces, en principio, poco fiables.

La mejora de las tecnologías de transmisión, ha hecho que muchas de las funciones de protocolo de X.25 orientadas a mejorar la fiabilidad del enlace resulten innecesarias, e incluso perjudiciales por hacer más lentas las comunicaciones.

Por ello aparece un sistema de conmutación de tramas denominado Frame Relay cuyo protocolo más simplificado se basa en la mejor calidad de las nuevas líneas digitales y, además, realiza la conmutación a nivel de enlace en lugar de a nivel de red como ocurre con X.25. Frame Relay consigue superar la velocidad de X.25 en al menos un orden de magnitud.

Posteriormente se ha desarrollado el Modo de Transferencia Asincrono (ATM, Asinchronous Transfer Mode) donde se realiza conmutación de celdas. Conceptualmente es similar a Frame Relay ya que las celdas ATM son básicamente tramas de pequeño tamaño. La ventaja de ATM está en su funcionalidad que permite alcanzar velocidades varios ordenes de magnitud superiores a 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 International Telegraph and Telephone (CCITT).
- International Organization for Standardization (ISO).
- Internet 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.

2.3.1 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 (CSU / DSU).

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 sincrónico de banda ancha (analógico) que operara en el intervalo de 48 a 168 kbps.
- 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 Interface (HSSI): Estándar de red para las conexiones seriales de alta velocidad (hasta 52 Mbps) sobre conexiones WAN.

2.3.2 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.

2.3.3 ATM

El Modo de Transferencia Asincrono (ATM) es un sistema en muchos aspectos similar a las técnicas de conmutación de X.25 y de Frame Relay, aunque en este caso se habla de retransmisión de celdas. La unidad de datos con la que funcionan los conmutadores ATM tiene sólo 53 octetos y es de longitud fija.

Estos dispositivos tienen un número de puertos fijo entre los que conmutan las celdas a velocidades del orden de Gbits por segundo. Las transmisiones de las celdas a través de los puertos son a 155,52 y 622,08 Mbps en la mayoría de los casos, aunque se admiten otras velocidades, lo que implica el uso de tecnologías ópticas aplicándose en muchos casos JDS.

A un puerto de un conmutador ATM se puede encontrar conectado otro conmutador, una estación de trabajo o un concentrador para varias estaciones, un conmutador de una red local, un dispositivo de captura y digitalización de voz y/o vídeo, etc.

Toda la información que proceda de esos dispositivos estará encapsulada en celdas que viajarán a través de circuitos virtuales temporales o permanentes de la red ATM desde su fuente hacia su destino atravesando uno o varios conmutadores ATM.

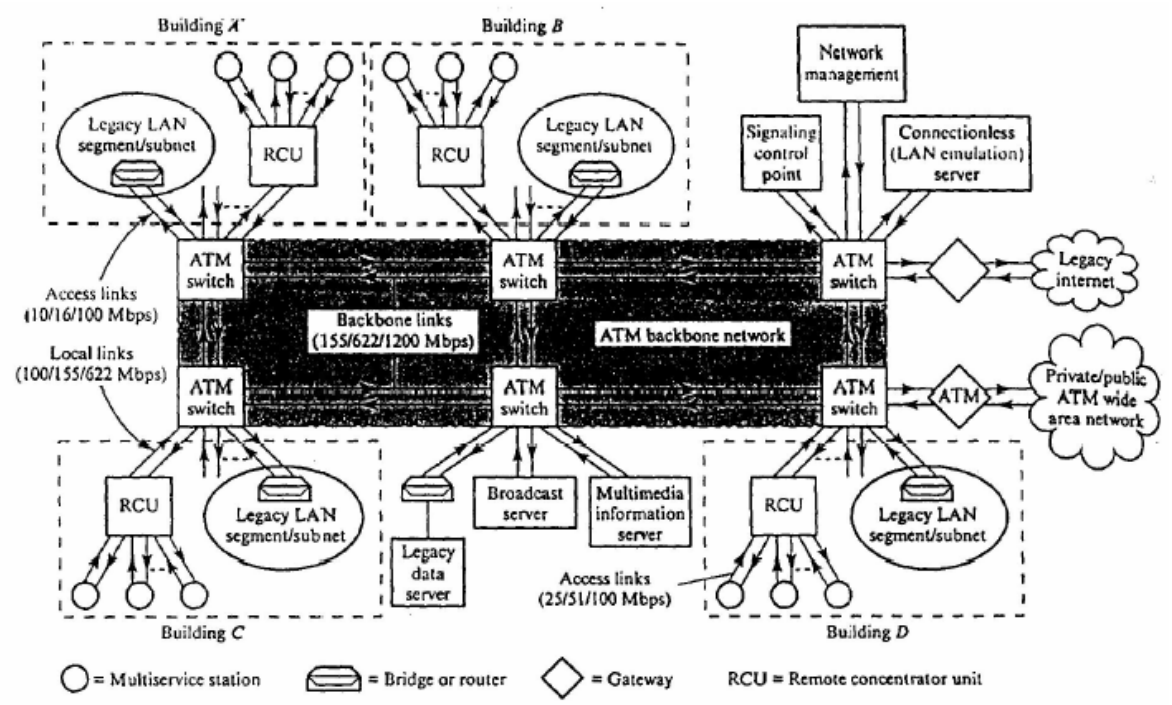


Figura. 2.20. Red ATM

Aún siendo un servicio basado en circuitos virtuales, la red ATM sólo asegura la correcta secuencia de las celdas (nunca llegarán fuera de orden) y existe una pequeña probabilidad de que se pierdan celdas al no tener implementados los mecanismos de recuperación de errores necesarios.

La red ATM debe poder adaptarse a tipos de tráfico muy diferentes: de tasa fija, como la voz y en ocasiones el vídeo, o variable como los datos. En las celdas ATM pueden ir fragmentadas y encapsuladas unidades de datos de diferentes protocolos de red o incluso tramas de redes locales.

En este último caso, ATM junto con los conmutadores de red local que actúan como puentes, permite la construcción de las denominas LAN virtuales. Básicamente se trata de redes locales muy separadas geográficamente pero que funcionan como una sola al existir un medio de interconexión (la red ATM) que permite propagar las tramas de unas redes locales en las otras cuando es necesario.

2.3.3.1 Arquitectura ATM

En la arquitectura de ATM se definen tres capas. La inferior es la capa física que podría corresponder con la capa física del modelo de referencia OSI de ISO y en principio ATM no la define ya que puede tratarse de cualquier medio físico adecuado a los requisitos de ATM.

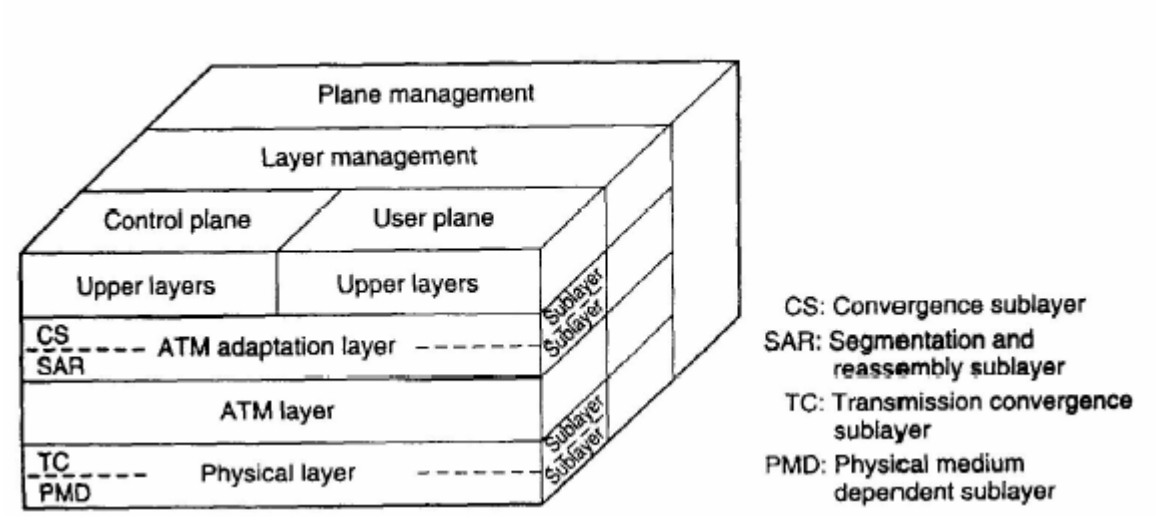


Figura. 2.21. Arquitectura de la Red ATM

Las otras dos capas están relacionadas con las funciones ATM, y podrían constituir la capa de enlace de OSI aunque se discute que dada la capacidad de encaminamiento de la información a través de circuitos virtuales, se trate de una capa de red.

La capa inferior de estas dos se denomina capa ATM y define la transmisión de datos en celdas de tamaño fijo utilizando conexiones lógicas. La superior se denomina capa de adaptación ATM (AAL). Permite la adaptación de protocolos no basados en ATM para su transmisión a través de la red ATM. Agrupa información de las capas superiores en celdas para su transmisión y la extrae de las celdas recibidas para entregarla a las capas superiores.

En el modelo de ATM se hace también mención a tres planos separados: plano de usuario que permite la transferencia de información de usuario, plano de control que realiza el control de llamadas y de conexión y plano de gestión que proporciona coordinación entre todos los planos, gestión de plano, y todas las capas, gestión de capa.

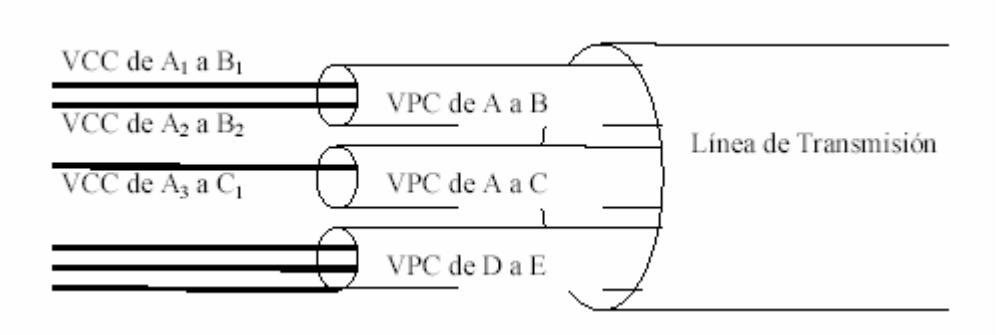


Figura. 2.22. Línea de Transmisión ATM

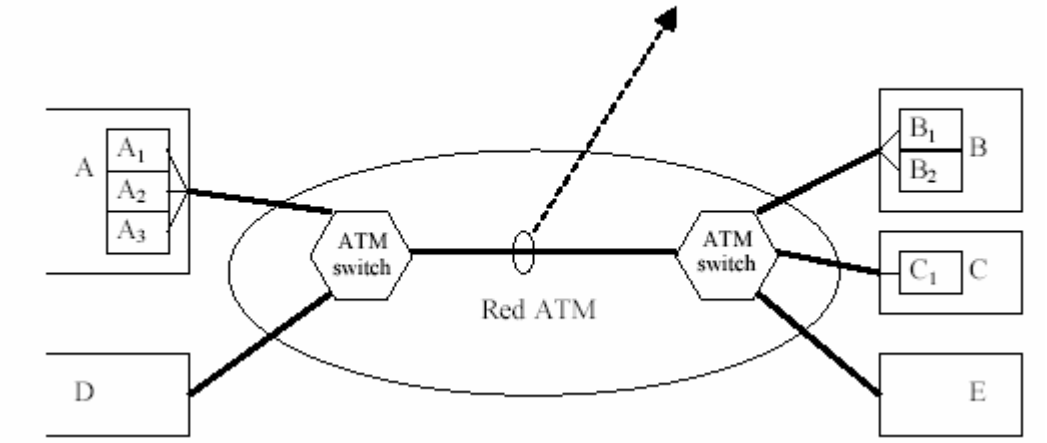


Figura. 2.23. Nodos ATM

2.3.3.2 Conexiones ATM

En las conexiones lógicas ATM se distinguen Conexiones de Canales Virtuales (VCC, Virtual Channel Connection) y Conexiones de Caminos Virtuales (VPC, Virtual Path Connection).

Un VPC es una conexión virtual extremo a extremo entre dos dispositivos, A y B, que intercambian información a través de una red ATM y contiene un haz de VCC independientes que tienen el mismo origen y destino que el VPC. Esto permite reducir el costo de encaminamiento en los nodos de conmutación, ya que todos los VCC de un mismo VPC se conmutan conjuntamente por el mismo camino.

Si se tiene que establecer un nuevo circuito virtual entre A y B se generará un nuevo VCC dentro del VPC ya establecido, lo que agiliza el proceso de establecimiento, control y liberación de la conexión. Las líneas de transmisión que unen conmutadores de la red ATM entre sí y con los dispositivos terminales de usuario contendrán a su vez múltiples VPC.

2.3.3.3 Celdas ATM

En ATM se utilizan celdas de tamaño fijo, 53 octetos, de los cuales 5 son de cabecera y los 48 restantes forman el campo de información. Las razones que justifican celdas tan pequeñas y de tamaño fijo son que pueden ser conmutadas más eficientemente y que se reduce el retardo en cola para celdas de alta prioridad.

Las cabeceras varían ligeramente si se trata de una celda de la interfaz entre el usuario y el primer nodo de conmutación de la red o de una celda que viaja entre dos nodos de conmutación de la red.

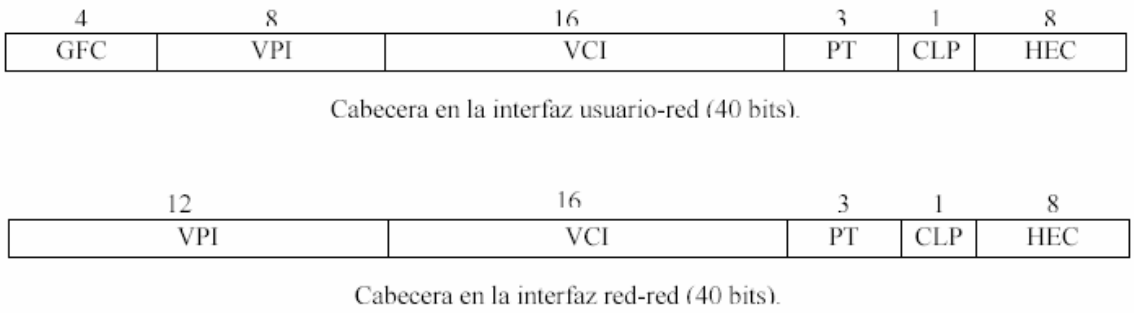


Figura. 2.24. Celdas ATM

VPI y VCI son respectivamente los identificadores de camino y canal virtual. El campo GFC sólo se usa en la interfaz usuario-red para realizar un control de flujo o calidad de

servicio (QOS, Quality Of Service) en esta interfaz que ayuda también a la aparición de sobrecarga en la red.

El campo PT indica el tipo de carga útil que lleva la celda, de usuario o de gestión y mantenimiento de la red. Este campo además puede señalizar si se ha producido congestión en la transmisión de una celda con información de usuario.

El bit CLP indica si la celda es de una categoría de baja o alta prioridad para que en el caso de tener que rechazar celdas por congestión de la red, empezar por las de baja prioridad. Este bit puede ser activado por un conmutador de la interfaz usuario-red si está en desacuerdo con los parámetros de tráfico o calidad de servicio fijados para el usuario.

Finalmente, el campo HEC es un control de errores para la cabecera que, en caso de que el dispositivo que recibe la celda errónea implemente el algoritmo adecuado, permite además la recuperación de aquellos errores en la cabecera que sean solamente de un bit.

2.3.3.4 Conmutadores ATM

Un conmutador de celdas ATM está formado por un número limitado de líneas de entrada y generalmente el mismo número de líneas de salida, ya que normalmente las líneas son bidireccionales. En el interior del conmutador se produce la conmutación a alta velocidad de las celdas que llegan por las líneas de entrada hacia su correspondiente línea de salida.

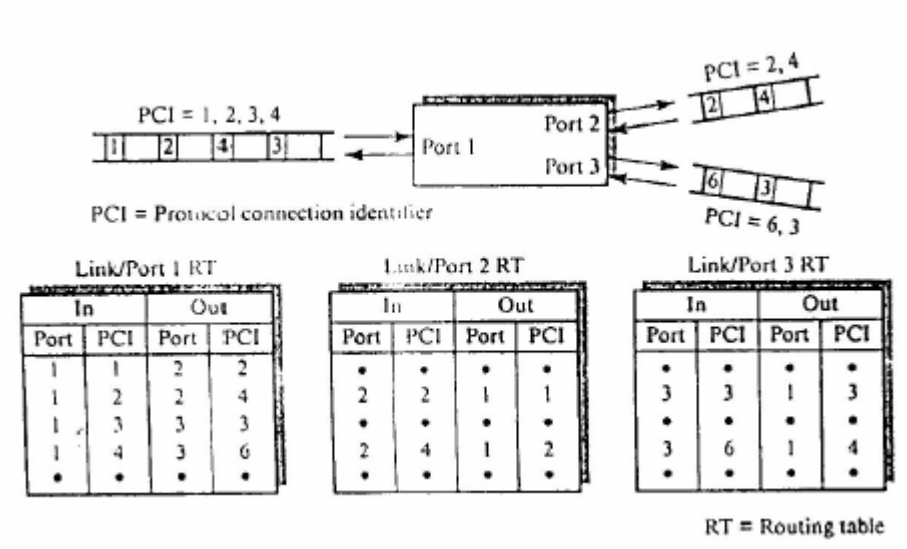


Figura. 2.25. Conmutadores ATM

Aunque las celdas llegan de forma asincrónica a las líneas de entrada el procesamiento interno del conmutador es sincrónica. Se basa en un reloj maestro que marca el comienzo de cada ciclo de conmutación.

En general, durante un ciclo las celdas que hayan llegado completamente a las líneas de entrada al comienzo del mismo son recogidas, se comprueba su HEC y, si no son descartadas por este o por otros motivos (congestión, colisiones, etc.), pasan por el conmutador y se ponen para su transmisión en las líneas de salida.

En otros casos la secuencia de operaciones necesaria permite realizar el proceso en varios ciclos de reloj. Por una línea a 150 Mbps podrían llegar 360000 celdas por segundo lo que indica que el tiempo de cielo máximo debería estar entorno a 2,7 µs. Para 622 Mbps debería ser inferior a 700 ?s. Los conmutadores comerciales suelen tener entre 16 y 1024 líneas de entrada-salida, por lo que deberían ser capaces de conmutar de 16 a 1024 celdas, según el caso, en los tiempos de ciclo indicados.

Esto supone, por ejemplo, para un conmutador con 16 puertos a 155 Mbps una velocidad de conmutación de 2,5 Gbps.

Todos los conmutadores ATM tienen dos objetivos comunes y fundamentales:

a) Conmutar las celdas con la tasa de rechazo más baja posible.

b) No cambiar nunca el orden de las celdas de un circuito virtual.

Una tasa aceptable de rechazo seria del orden de 1 celda entre cada 10. En un conmutador grande esto puede suponer 1 ó 2 celdas rechazadas por hora. Las limitaciones que imponen estas dos reglas se aprecian al observar detenidamente el funcionamiento de un conmutador. Si a más de una celda de las que están en las líneas de entrada en un ciclo de reloj le corresponde salir por una determinada línea de salida, se podría optar por dos soluciones inmediatas:

a) Enviar una de las celdas a la línea de salida y descartar las demás, lo cual incumpliría el primer objetivo.

b) Hacer recircular por un bus las celdas descartadas de nuevo hacia las líneas de entrada, lo que si no se implementa la lógica necesaria puede incumplir el segundo objetivo.

La solución, más adecuada es establecer colas en las líneas de entrada o de salida de manera que las celdas que no puedan ser despachadas en un determinado ciclo, lo sean en el siguiente. Es más eficiente el que las colas estén en las líneas de salida, ya que en el otro caso, celdas que no son capaces de ser conmutadas hacia una determinada línea de salida saturada, pueden bloquear otras celdas que están detrás en la misma cola de la línea de entrada destinadas a salidas que se encuentran libres.

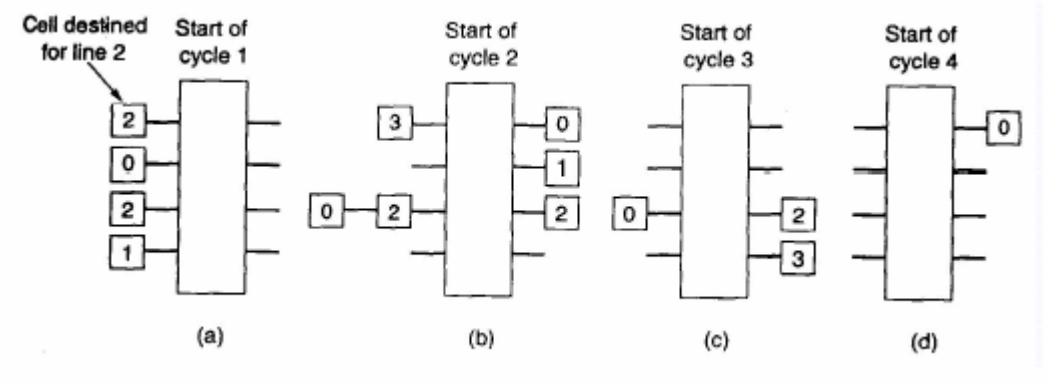


Figura. 2.26. Líneas de Entrada y Salida

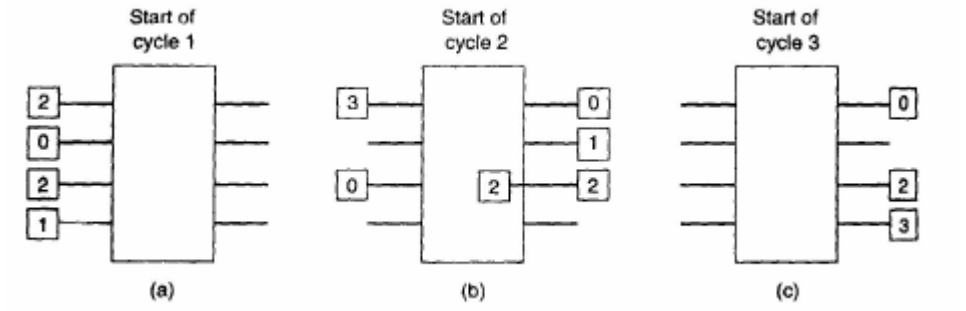


Figura. 2.27. Líneas de Entrada y Salida

2.3.3.4.1 Conmutador por división de tiempo

Una de las posibilidades de realizar la conmutación es disponer de una placa base con un bus de alta velocidad capaz de transferir N celdas en el tiempo de ciclo, siendo N igual al número de puertos de entrada.

Las celdas son así multiplexadas en el tiempo sobre el bus de transferencia, que las deja a su salida en las colas de las líneas de salida correspondiente.

Este diseño sólo permite un número reducido de puertos, ya que está limitado por la velocidad del bus de la placa base. Por ejemplo, un bus a 2,5 Gbps puede manejar 16 puertos de entrada/salida de 155 Mbps o 4 de 622 Mbps.

2.3.3.4.2 Conmutador por división de espacio

En este caso la matriz de conmutación está formada por un conjunto de elementos de conmutación que proporcionan caminos alternativos por el interior del conmutador.

2.3.3.4.2.1 Conmutador de matriz totalmente conectada

En este tipo de arquitectura todas las líneas de entrada están conectadas con todas las líneas de salida mediante un elemento de conmutación en cada conexión. Lógicamente en un mismo ciclo puede aparece más de una celda dirigida a la misma salida, lo que implica la necesidad de disponer de una cola en la salida que permita mediante un elemento concentrador colocar en ella todas las celdas que llegan en un ciclo.

A veces en lugar de una única cola por cada salida se implementan varias en paralelo que son utilizadas por un registro de desplazamiento que las rellena de forma uniforme. El sistema de colas en paralelo permite dar servicio a celdas que llegan simultáneamente a la línea de salida de una forma más rápida y eficaz.

Según como se implemento el concentrador este podrá dar servicio a todas las celdas o sólo a una parte de las que en un ciclo van simultáneamente hacia una misma salida, otras serán descartadas. Esta última es la implementación conocida como conmutador Knockout en el que las celdas dirigidas a una misma salida en un mismo ciclo compiten como en un torneo de cuartos de final, semifinales, etc. para ver cuales alcanzan la salida.

Se consigue así simplificar la estructura electrónica del conmutador a costa de elevar ligeramente la tasa de pérdida de celdas. El otro motivo que puede suponer que se descarten celdas es que la cola de una determinada salida esté llena y ya no pueda aceptar más celdas.

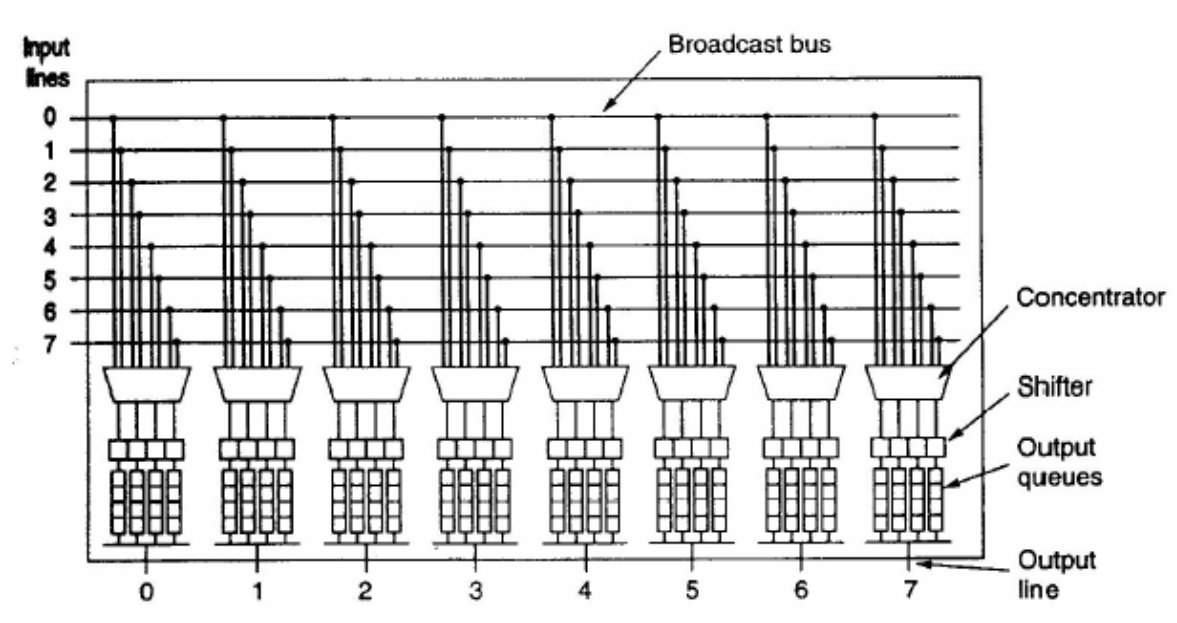


Figura. 2.28. Conmutador de Matriz

El mayor problema de este tipo de conmutador es que el número de elementos de conmutación es el cuadrado del número de entradas/salidas que tiene, N^2, lo que limita su tamaño máximo.

2.3.3.4.2.2 Conmutador Batcher-Banyan

En un conmutador Batcher-Banyan la conmutación se hace en varios ciclos al tener que pasar las celdas por varias etapas de conmutación. La matriz de conmutación Banyan, también conocida como matriz delta, se encarga en la conmutación propiamente dicha pero, por las siguientes razones, suele ir precedida por una matriz de ordenamiento Batcher.

El elemento de conmutación básico del conmutador Banyan tiene dos entradas y dos salidas. Se basa en un bit de la salida de destino de la celda en cuestión para decidir por cual de las dos salidas la conmuta.

En un conmutador para cuatro entradas/salidas se necesitan dos etapas de conmutación con dos elementos básicos de conmutación cada una, en total 4, frente a los 16 (N^2) que requiere una matriz totalmente conectada. En general para N entrada/salidas se precisan $\log_2 N$ etapas con N/2 elementos de conmutación cada una, es decir, $(N/2)\cdot\log_2 N$ elementos básicos de conmutación.

El primer problema que aparece, es que si a la entrada de un elemento de conmutación hay dos celdas con el bit que se utiliza para conmutación igual, una de las dos ha de ser descartada. En segundo lugar, esto supone también que varias celdas dirigidas a la misma salida en el mismo ciclo, acabarán encontrándose y sólo una de ellas llegará a la salida.

El primero de los dos problemas se puede solventar con una matriz de ordenamiento Batcher que se encarga de ordenar las celdas en función de la dirección (de menor a mayor) de la línea de salida hacia la que van. Se puede comprobar que si las celdas llegan a las entradas de la matriz Banyan ordenadas, no se producirán colisiones en los elementos de conmutación.

El segundo problema es más complejo de resolver, ya que hay que encolar celdas en alguna parte del proceso cuando simultáneamente llegan celdas dirigidas hacia la misma salida. La matriz Banyan por su forma de funcionamiento no permite las colas en las líneas de salida.

Las soluciones aplicadas se basan en sistemas de colas internas, en las matrices de ordenamiento o conmutación, o la recirculación de celdas tras su ordenamiento de nuevo hacia la entrada de la matriz de ordenamiento.

Esto último implica una elevada complejidad en la lógica del conmutador ya que se debe cumplir el precepto de mantener el orden de las celdas de cada conexión lógica.

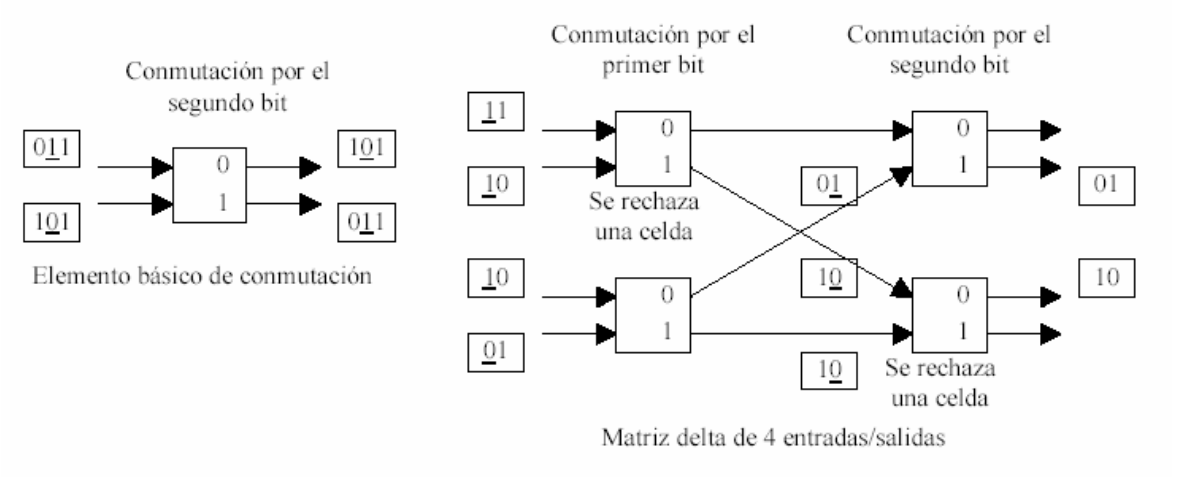


Figura. 2.29. Conmutación Batcher

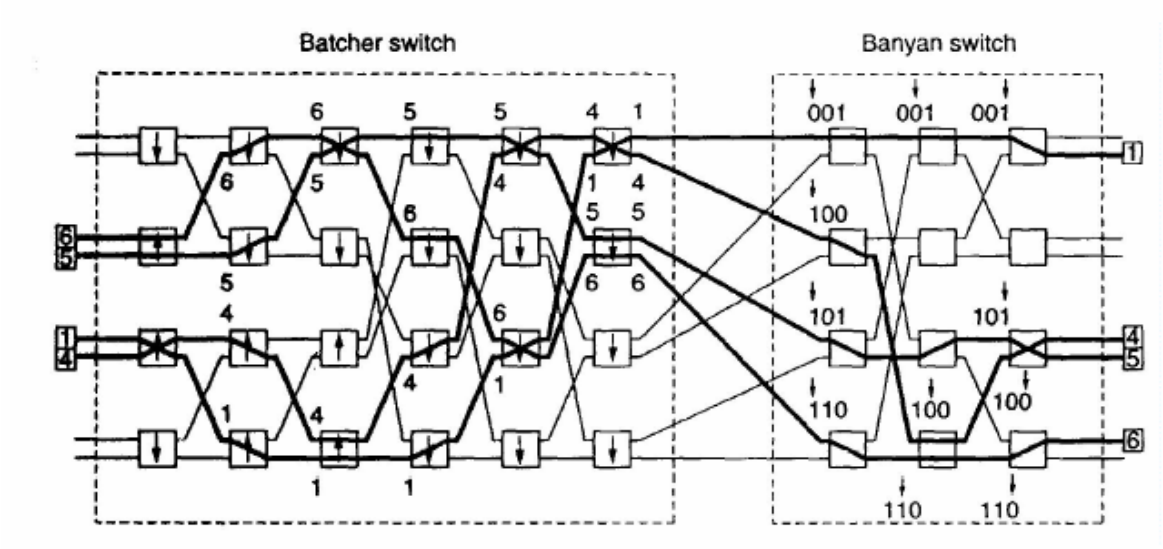


Figura. 2.30. Swi tch Batcher

2.3.4 RADIOENLACES FIJOS TERRESTRES

2.3.4.1 Banda Base Digital

Aquí se hace referencia a los equipos para redes de micro-ondas desde un punto de vista genérico abarcando las 3 etapas reconocidas: Banda-Base, Frecuencia Intermedia y Radio Frecuencia.

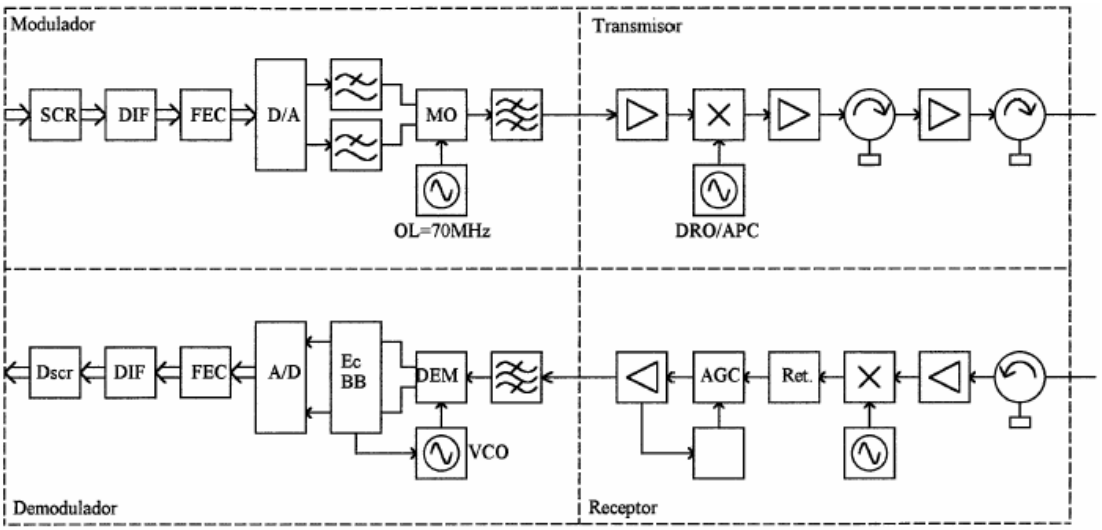


Figura. 2.31. Diagrama de Bloques de un Radio Enlace Típico

2.3.4.1.1 Funciones

Las funciones de la etapa de banda-base son:

- Formación de un trama de datos
  - Permite efectuar el alineamiento de trama.
  - Ofrece suficiente capacidad de tráfico adicional para canales de servicio para hablar **EOW** (*Orderwire*).
  - Transporta canales de datos para supervisión y gestión;
  - Adiciona bits de paridad para el control de errores y emisión de alarmas.

- Permitir la protección del tipo N+1
  - Esta operación se realiza mediante la conmutación *hit-less* entre dos señales de recepción.
  - Los comandos de conmutación son seleccionados en base a las alarmas de tasa de error **BER**.

- Temporización del aparato.
  - La temporización de un equipo de radio es en forma independiente a la red (*Free Runnig*) para sistemas PDH.
  - En sistema SDH el sincronismo se toma desde la red.

2.3.4.2 Protección mediante Conmutación

La conmutación de canales con la misma banda base digital se requiere como mecanismo de protección para contrarrestar las fallas de equipos y la mala propagación. Existen 2 grandes tipos de mecanismos de conmutación:

- En una conexión de radio enlaces **hot stand by** se transmite una sola frecuencia, por lo tanto existe una conmutación de transmisores a nivel de radiofrecuencia. En recepción se tiene una conmutación en banda base con un circuito separador para los dos receptores en radiofrecuencia. La conmutación es efectuada en base a una lógica de alarmas del equipo de recepción, que toma en cuenta entre otras la alarma de tasa de error BER.

- En una conexión de **diversidad de frecuencia o de espacio** se transmiten dos frecuencias o caminos distintos desde el transmisor y la conmutación se realiza en la banda base de recepción. Como las frecuencias sufren distinto retardo en el vínculo, la relación de fase entre los bits antes de la conmutación es variables y por ello se requiere de un circuito desfasador, también variable, que ponga en fase los dos trenes de datos antes de la conmutación.

El tipo de conmutación que pone en fase los trenes de datos previamente a la operación de conmutar se denomina **hitless** (sin deslizamientos). De esta forma, se asegura la conmutación en el mismo bit y se elimina el deslizamiento (*slip*), consistente en la eliminación o la repetición de bits.

2.3.4.2.1 Temporización

La sincronización de los equipos permite ser configurada mediante la entrada tributarias; el sincronismo externo o sincronismo desde demodulador. La prioridad entre las distintas fuentes de sincronismo se programa mediante software, cada equipo selecciona en forma automática la fuente de sincronismo en caso de falla.

En general los equipos de radio enlace son dependientes del reloj del multiplexor. El enlace de radio es entonces transparente al sincronismo.

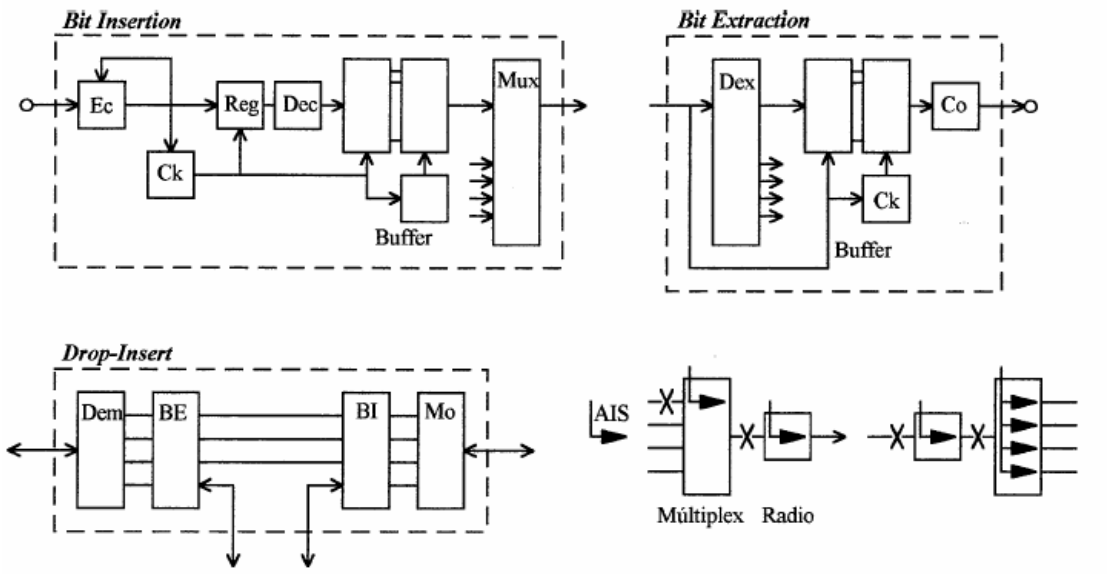


Figura. 2.32. Etapa de Banda Base de un Radioenlace

2.3.4.3 Etapa Modulador-Demodulador

La etapa modulador-demodulador continua luego de la etapa de Banda-Base y tiene como objetivo la codificación y la modulación de la señal digital.. Las funciones principales son:

- Codificación y decodificación de la señal digital.
- Filtrado del canal antes del modulador.
- Ecualización en recepción de la señal demodulada.
- Generación del oscilador local para el modulador.
- Modulación y demodulación de la señal digital filtrada para obtener la frecuencia intermedia.
- Filtrado de la frecuencia intermedia.

2.3.4.3.1 Etapa Transmisor-Receptor

La estructura básica usada en los equipos de radioenlaces digitales de la primera generación no difiere substancialmente en la etapa de radiofrecuencia con los equipos para señales analógicas, las cuales tienen las siguientes funciones generales

- Entrada de la frecuencia intermedia.
- Generador del oscilador local de RF.
- Conversión Up y Down desde IF hacia RF en transmisión y recepción.
- Control automático de ganancia a nivel de IF en recepción.
- Amplificación de potencia en transmisión y bajo ruido en recepción.
- Control de potencia ATPC y linealizador de RF.
- Ecualización del retardo de grupo y la linealidad de amplitud.
- Circuito de branching: filtros, circuladores y guía de onda o cable coaxial de salida.

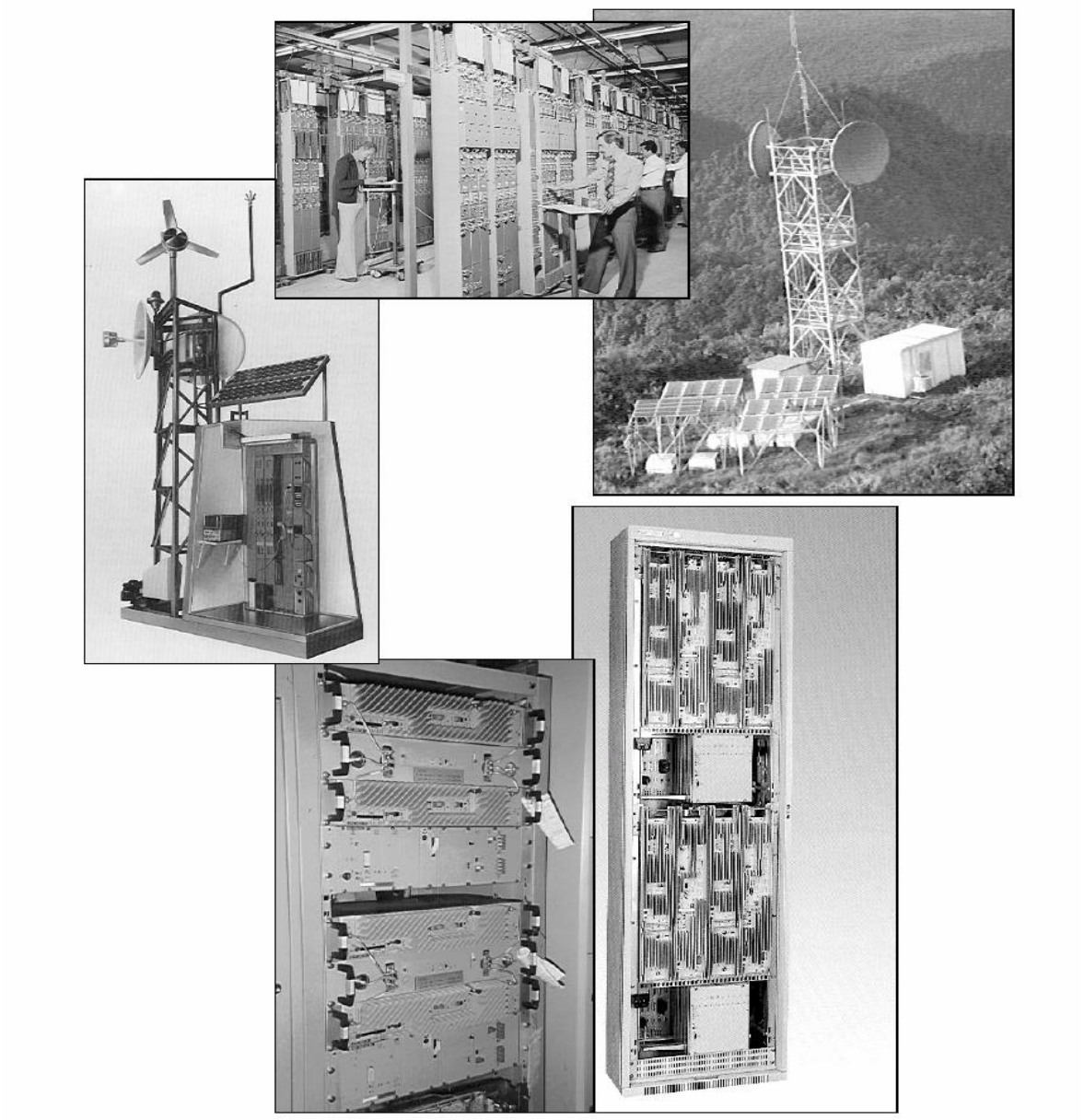


Figura. 2.33. Ilustración de equipos de Comunicaciones

2.3.4.4 Comunicación Vía Microondas

Se denomina así la porción del espectro electromagnético que cubre las frecuencias entre aproximadamente 3 Ghz y 300 Ghz, que corresponde a la longitud de onda en vacío entre 10 cm. y 1mm.

Básicamente un enlace vía microondas consiste en tres componentes fundamentales: El Transmisor, El receptor y El Canal Aéreo. El Transmisor es el responsable de modular una señal digital a la frecuencia utilizada para transmitir, El Canal Aéreo representa un camino

abierto entre el transmisor y el receptor, y como es de esperarse el receptor es el encargado de capturar la señal transmitida y llevarla de nuevo a señal digital.

El factor limitante de la propagación de la señal en enlaces microondas es la distancia que se debe cubrir entre el transmisor y el receptor, además esta distancia debe ser libre de obstáculos. Otro aspecto que se debe señalar es que en estos enlaces, el camino entre el receptor y el transmisor debe tener una altura mínima sobre los obstáculos en la vía, para compensar este efecto se utilizan torres para ajustar dichas alturas.

2.3.4.5 Antenas y Torres de Microondas

La distancia cubierta por enlaces microondas puede ser incrementada por el uso de repetidoras, las cuales amplifican y redireccionan la señal, es importante destacar que los obstáculos de la señal pueden ser salvados a través de reflectores pasivos.

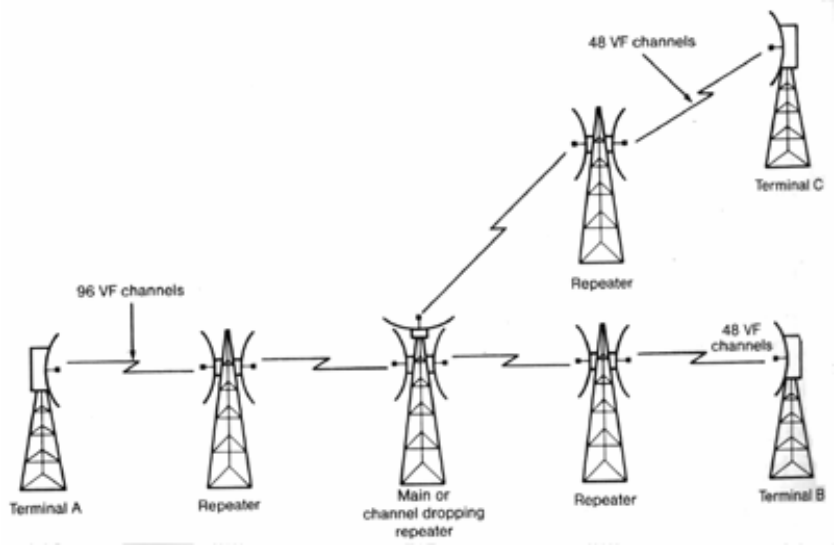


Figura. 2.34. Antenas y Torres Microonda

La señal de microondas transmitidas es distorsionada y atenuada mientras viaja desde el transmisor hasta el receptor, estas atenuaciones y distorsiones son causadas por una perdida de poder dependiente a la distancia, reflexión y refracción debido a obstáculos y superficies reflectoras, y a pérdidas atmosféricas.

El correcto uso de las frecuencias permite obtener algunas ventajas:

- Antenas relativamente pequeñas son efectivas.

- A estas frecuencias las ondas de radio se comportan como ondas de luz, por ello la señal puede ser enfocada utilizando antenas parabólicas y antenas de embudo, además pueden ser reflejadas con reflectores pasivos.

2.3.4.6 Ventajas de los radio Enlaces de Microondas

- Volumen de inversión generalmente más reducido.
- Instalación más rápida y sencilla.
- Conservación generalmente más económica y de actuación rápida.
- Puede superarse las irregularidades del terreno.
- La regulación solo debe aplicarse al equipo, puesto que las características del medio de transmisión son esencialmente constantes en el ancho de banda de trabajo.
- Puede aumentarse la separación entre repetidores, incrementando la altura de las torres.

2.3.4.7 Desventajas de los radio Enlaces de Microondas

- Explotación restringida a tramos con visibilidad directa para los enlaces.
- Necesidad de acceso adecuado a las estaciones repetidoras en las que hay que disponer de energía y acondicionamiento para los equipos y servicios de conservación.
- Las condiciones atmosféricas pueden ocasionar desvanecimientos intensos y desviaciones del haz, lo que implica utilizar sistemas de diversidad y equipo auxiliar.

2.3.4.8 Estructuran General de un Radio Enlace por Microondas

Un radioenlace esta constituido por equipos terminales y repetidores intermedios. La función de los repetidores es salvar la falta de visibilidad impuesta por la curvatura terrestre y conseguir así enlaces superiores al horizonte óptico.

Los repetidores pueden ser:

- Activos
- Pasivos

En los repetidores pasivos o reflectores.

- No hay ganancia
- Se limitan a cambiar la dirección del haz radielectrónico.

Los enlaces se hacen básicamente entre puntos visibles es decir, puntos altos de la topografía.

Cualquiera que sea la magnitud del sistema de microondas, para funcionamiento correcto es necesario que los recorridos entre enlaces tengan una altura libre adecuada para la propagación en toda época del año, tomando en cuenta las variaciones de las condiciones atmosféricas de la región.

Para poder calcular las alturas libres debe conocerse la topografía del terreno, así como la altura y ubicación de los obstáculos que puedan existir en el trayecto.

2.3.4.9 Desvanecimiento

El desvanecimiento se debe normalmente a los cambios atmosféricos y a las reflexiones del trayecto de propagación al encontrar superficies terrestres o acuáticas.

La intensidad del desvanecimiento aumenta en general con la frecuencia y la longitud de trayecto.

En el caso de transmisión sobre terreno accidentado, el desvanecimiento debido a propagación multi-trayecto es relativamente independiente del desvanecimiento por obstáculo.

Existe el desvanecimiento total que es relativamente raro, pero cuando se presenta, sus efectos suelen ser catastróficos, pues anulan por completo las señales. En este caso, los métodos tradicionales usados para mejorar la confiabilidad de los radioenlaces, tales como: el aumento del margen de desvanecimiento o la aplicación de diversidad resultan prácticamente ineficaces.

Se considera como desvanecimiento total a cualquier atenuación excesivamente larga de las señales de microondas. El desvanecimiento total se da por algunos factores como:

- Formación de ductos
- Atrapamiento del haz.
- Bloqueo o desaparición de las señales.
- Desacople de antena.

El desvanecimiento total se caracteriza por una aguda disminución de densidad atmosférica a medida que aumenta la altura, que es la causante del verdadero desvanecimiento.

2.3.4.10 Confiabilidad de los Sistemas de Microonda

Las normas de seguridad de funcionamiento de los sistemas de microondas han alcanzado gran rigidez. Por ejemplo, se utiliza un 99.98% de confiabilidad general en un sistema patrón de 6000 Km. de longitud, lo que equivale a permitir solo un máximo de 25 segundos de interrupción del año por cada enlace.

Por enlace se entiende el tramo de transmisión directa entre dos estaciones adyacentes, ya sean terminales o repetidoras, de un sistema de microondas. El enlace comprende los equipos correspondientes de las dos estaciones, como así mismo las antenas y el trayecto de propagación entre ambas. De acuerdo con las recomendaciones del CCIR, los enlaces, deben tener una longitud media de 50 Km.

La confiabilidad de los enlaces de microondas puede darse según fallas de equipo, aplicándose cálculos de probabilidad.

2.3.4.11 Disponibilidad de Enlaces Digitales

La Confiabilidad puede definirse como la capacidad de un componente, equipo o sistema de no fallar durante un periodo determinado de tiempo. Existe una relación matemática entre la confiabilidad de cada una de las partes, y el sistema completo.

Esta Relación matemática es uno de los métodos conocidos para obtener en forma anticipada la confiabilidad de un equipo aún no instalado.

La Confiabilidad distingue tres tipos de falla que puede presentar un sistema:

- Fallas que ocurren al iniciarse el periodo de vida operativo y que suceden generalmente por defectos en la producción en el control de calidad o en la instalación

- Fallas debidas al desgaste y que dependen del mantenimiento preventivo

- Fallas aleatorias distribuidas al azar y que no dependen de pruebas ni del mantenimiento.

CAPITULO III

PARÁMETROS DE CALIDAD Y SEGURIDAD

3.1 SEGURIDAD EN LAS COMUNICACIONES

La seguridad en las computadoras implica tres exigencias que se extienden al sistema de comunicaciones cuando aquellos se integran en este:

a) Secreto: Acceso a la información y recursos sólo a los entes autorizados.
b) Integridad: Modificación de la información y recursos sólo por entes autorizados.
c) Disponibilidad: La información y recursos deben estar disponibles para los entes autorizados.

La incorporación de un computador en una red informática u otro sistema de comunicaciones añade nuevos aspectos a la seguridad relacionados básicamente con la identificación de los interlocutores (denominada también autentificación o autenticación). Es decir, que cada una de las dos o más partes que intervienen en una comunicación esté segura de quien o quienes son las otras partes. Algunos de estos aspectos son:

a) Control de acceso: Autorizar el acceso a través de una comunicación a la información y recursos sólo a los entes autorizados y negándolo a los demás.
b) Prueba de origen: Asegurar al receptor que un dato recibido proviene en realidad de quien dice ser su emisor.
c) Prueba de recepción: Asegurar al emisor que un dato transmitido ha sido recibido realmente por quien debe ser su receptor.
d) No rechazo: Pruebas más fuertes que las anteriores que impidan que un extremo niegue haber enviado un dato habiéndolo hecho o que el otro niegue haberlo recibido.

Generalmente los ataques a la seguridad se dividen en pasivos y activos. Los ataques pasivos son la escucha y divulgación de la información (snooping) y el análisis de tráfico (packet sniffing). Este último no implica que se conozca el contenido de la información

que fluye en una comunicación, pero el conocimiento de ese flujo, volumen, horarios o naturaleza, puede ser información útil.

Los ataques activos comprenden el enmascaramiento (spoofing), que es la suplantación de un ente autorizado para acceder a información o recursos, la modificación (tampering o data diddling), que incluye también la posible destrucción y creación no autorizada de datos o recursos, y la interrupción (jamming o flooding y otros), que supone el impedir a entes autorizados su acceso a la información o recursos a los que tienen derecho de acceso (denegación de servicio, DoS).

Las contramedidas se suelen aplicar cuando se ha detectado un ataque, lo cual no suele ser una política adecuada. Los ataque pasivos son difíciles de detectar pero suelen existir contramedidas para prevenirlos. Por el contrario, los ataque activos son más fáciles de detectar pero bastante más complejos de prevenir. Las contramedidas se suelen concretar en los siguientes aspectos:

- Minimizar la probabilidad de intromisión con la implantación de elementos de protección.
- Detectar cualquier intrusión lo antes posible.
- Identificar la información objeto del ataque y su estado para recuperarla tras el ataque.

Sería prácticamente interminable el enumerar las posibles formas de ataque que puede sufrir un computador conectado a una red de comunicaciones, bien por intervención física sobre los mismos o vía software. Las medidas de prevención son múltiples también desde la vigilancia física del sistema, por ejemplo, el estado de las líneas de comunicación para detectar posibles perdidas de potencia en la señal o interferencias atribuibles a intervenciones sobre ellas, hasta el registro de los eventos que se producen en el sistema y la vigilancia de modificaciones en aquellos archivos o procesos que son críticos para la seguridad del mismo.

Todo ello involucra la responsabilidad de los usuarios y del administrador del sistema encargado de establecer las políticas de cuentas de usuario adecuadas y mantener actualizados los dispositivos y el software que puedan tener agujeros que comprometan la seguridad.

3.2 TIPOS DE ATAQUE MÁS COMUNES

En los primeros años, los ataques involucraban poca sofisticación técnica. Los "insiders" (empleados disconformes o personas externas con acceso a sistemas dentro de la empresa) utilizaban sus permisos para alterar archivos o registros. Los "outsiders" (personas que atacan desde afuera de la ubicación física de la organización) se introducían en la red simplemente averiguando una contraseña válida.

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas. Esto permitió a los nuevos atacantes tomar control de sistemas completos, produciendo verdaderos desastres que en muchos casos llevo a la desaparición de aquellas organizaciones o empresas con altísimo grado de dependencia tecnológica (bancos, servicios automatizados, etc.).

Estos nuevos métodos de ataque han sido automatizados, por lo que en muchos casos sólo se necesita conocimiento técnico básico para realizarlos. El aprendiz de intruso tiene acceso ahora a numerosos programas y scripts de numerosos "hackers", BBSs y sitios web, donde además encuentra todas las instrucciones para ejecutar ataques con las herramientas disponibles.

Los métodos de ataque están divididos en categorías generales que pueden estar relacionadas entre sí, ya que el uso de un método en una categoría permite el uso de otros métodos en otras. Por ejemplo: después de "crackear" una contraseña, un intruso realiza un "login" como usuario legitimo para navegar entre los archivos y explotar vulnerabilidades del sistema.

Eventualmente el atacante puede también adquirir derechos de acceso a lugares que le permitan dejar un virus u otras bombas lógicas para paralizar todo un sistema antes de huir.

3.2.1 Eavesdropping y Packet Sniffing (husmeo de paquetes)

Muchas redes son vulnerables al eavesdropping, o la pasiva intercepción (sin modificación) del tráfico de red. En Internet esto es realizado por packet sniffers, que son programas que monitorizan los paquetes que circulan por la de red. El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un router o a un gateway

de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

Este método es muy utilizado para capturar nombres de usuario y contraseñas, que generalmente viajan claros (sin cifrar) al conectarse a sistemas de acceso remoto (RAS). También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mail entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones o individuos.

3.2.2 Snooping

Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante captura los documentos, mensajes de e-mail y otra información guardada, descargando en la mayoría de los casos esa información a su propia computadora.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos mas sonados de este tipo de ataques fueron el robo de un archivo con más de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de informes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

3.2.3 Tampering o Data Diddling

Esta categoría se refiere a la modificación desautorizada de los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de ejecutar cualquier comando y alterar o borrar cualquier información que puede incluso terminar en la destrucción total del sistema en forma deliberada.

Esto puede ser realizado por insiders o outsiders, generalmente con el propósito de fraude o dejar fuera de servicio un competidor.

Son innumerables los casos de este tipo, como empleados bancarios que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes.

La utilización de programas troyanos esta dentro de esta categoría, y refiere a falsas versiones de un software con el objetivo de averiguar información, borrar archivos y hasta tomar control remoto de una computadora a través de Internet como el caso de Back Orifice y NetBus.

3.2.4 Spoofing

Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de sniffing o tampering. Una forma común de spoofing, es conseguir el nombre y contraseña de un usuario legítimo para, una vez en el sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e-mails.

El intruso usualmente utiliza un sistema para obtener información y conectarse a otro, y luego utiliza éste para entrar en otro, y en otro. Este proceso, llamado "Looping", tiene la finalidad de imposibilitar la identificación y la ubicación del atacante.

El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del looping es que una compañía pueden suponer que están siendo atacados por un competidor, cuando en realidad están seguramente siendo atacado por un insider, o por un estudiante a miles de Km. de distancia, pero que ha tomado la identidad de otros.

El looping hace su investigación casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta, que pueden ser de distintas jurisdicciones.

Los protocolos de red también son vulnerables al spoofing. Con el IP spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo Origen, pero que es aceptada por el destinatario del paquete.

El envío de falsos e-mails es otra forma de spoofing permitida por las redes. Aquí el atacante envía e-mails a nombre de otra persona.

Muchos ataques de este tipo comienzan con ingeniería social, y la falta de cultura por parte de los usuarios para facilitar a extraños sus identificaciones dentro del sistema. Esta primera información es usualmente conseguida a través de una simple llamada telefónica.

3.2.5 Jamming o Flooding

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla.

Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión.

Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP. El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

Muchos nodos de Internet han sido dados de baja por el "ping de la muerte", una versión-trampa del comando ping. Mientras que el ping normal simplemente verifica si un sistema esta activo en la red, el ping de la muerte causa el reinicio o el apagado instantáneo del equipo.

Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los distintos servidores destino.

3.2.6 Bombas Lógicas

Este suele ser el procedimiento de sabotaje mas comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá, modificará la información o provocará el cuelgue del sistema.

3.2.7 Ingeniería Social

Básicamente convencer a la gente de que haga lo que en realidad no debería. Por ejemplo llamar a un usuario haciéndose pasar por administrador del sistema y requerirle la contraseña con alguna excusa convincente. Nunca se deben de subestimar este tipo de ataques.

3.2.8 Difusión de Virus

Si bien es un ataque de tipo tampering, difiere de éste porque puede ser introducido en el sistema por un dispositivo externo (disquetes) o través de la red (e-mails u otros protocolos) sin intervención directa del atacante.

Dado que el virus tiene como característica propia su autoreproducción, no necesita de mucha ayuda para propagarse a través de una LAN o WAN rápidamente, si es que no esta instalada una protección antivirus en los servidores, estaciones de trabajo, y los servidores de e-mail.

Cientos de virus son descubiertos mes a mes, y técnicas más complejas se desarrollan a una velocidad muy importante a medida que el avance tecnológico permite la creación de nuevas puertas de entrada. Por eso es indispensable contar con una herramienta antivirus actualizada y que pueda responder rápidamente ante cada nueva amenaza.

3.2.9 Explotación de errores de diseño, implementación u operación

Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje.

Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" han sido descubiertas en aplicaciones de software, sistemas operativos, protocolos de red, navegadores de Internet, correo electrónico y toda clase de servicios en LANs o WANs.

Hay multitud de ataques basados en explotar las vulnerabilidades del protocolo TCP/IP, entre ellos la Predicción de Números de Secuencia TCP ("ISN prediction / IP spoofing"), sistemas operativos abiertos como Unix tienen agujeros mas conocidos y controlados que aquellos que existen en sistemas operativos cerrados, como Windows.

Constantemente encontramos en Internet avisos de nuevos descubrimientos de problemas de seguridad (y herramientas de hacking que los explotan), por lo que hoy también se hace indispensable contar con productos que conocen esas debilidades y pueden diagnosticar un servidor, actualizando su base de dalos de tests periódicamente, además de normas y procedimientos de seguridad en los procesos de diseño e implementación de proyectos de informática.

3.2.10 Obtención de Contraseñas

Este método usualmente denominado cracking, comprende la obtención "por fuerza bruta" u otros métodos más inteligentes, de aquellas contraseñas que permiten ingresar a servidores, aplicaciones, cuentas, etc.

Muchas contraseñas de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario, que además nunca la cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles contraseñas hasta encontrar la correcta.

Es muy frecuente crackear una contraseña explotando agujeros en los algoritmos de cifrado utilizados, o en la administración de las contraseñas por parte la empresa.

Por ser el uso de contraseñas la herramienta de seguridad más cercana a los usuarios, es aquí donde hay que poner énfasis en la parte "humana" con políticas claras (¿cómo se define una contraseña?, ¿a quién se esta autorizado a revelarla?) y una administración eficiente (¿cada cuanto deben de cambiarse?)

No muchas organizaciones están exentas de mostrar contraseñas escritas y pegadas en la base del monitor de sus usuarios, u obtenerlas simplemente preguntando al responsable de cualquier PC cual es su contraseña.

3.2.11 Otras formas de "colgar" un equipo

Otro método para colgar un equipo es el denominado "Land attack", en el que se genera un paquete con direcciones IP y puertos de origen y destino idénticos. Existen diferentes variantes para este ataque. Una de ellas usa idénticas direcciones IP de origen y destino, pero no números de puertos.

Un ataque característico de los equipos con Windows es el Supernuke (llamado también a veces Winnuke), que hace que los equipos que escuchan por el puerto UDP 139 se cuelguen. NetBIOS es un protocolo integral para todas las versiones en red de Windows. Para transportar NetBIOS por IP, Microsoft ideó el Windows Networking (Wins), un esquema que enlaza el tráfico NetBIOS a puertos TCP y UDP 137, 138 y 139.

Al enviar a estos puertos fragmentos UDP, se pueden arruinar equipos Windows que no estén arreglados o disminuir la velocidad del equipo durante un largo tiempo.

3.3 LAS TRES ÁREAS DE LA SEGURIDAD

Actualmente, cuando las empresas disponen ya de sus propias redes internas a las que dan acceso a usuarios desde el exterior, los problemas de seguridad se plantean en tres áreas principales:

1. La seguridad de perímetro: protección frente ataques del exterior generalmente basada en cortafuegos (firewalls).

2. La seguridad en el canal: donde hay que proteger los datos frente a escuchas mediante criptografía

3. La seguridad de acceso: donde se contemplan tres aspectos, la identificación del usuario, la autorización del acceso y la auditoria de las operaciones realizadas por el usuario.

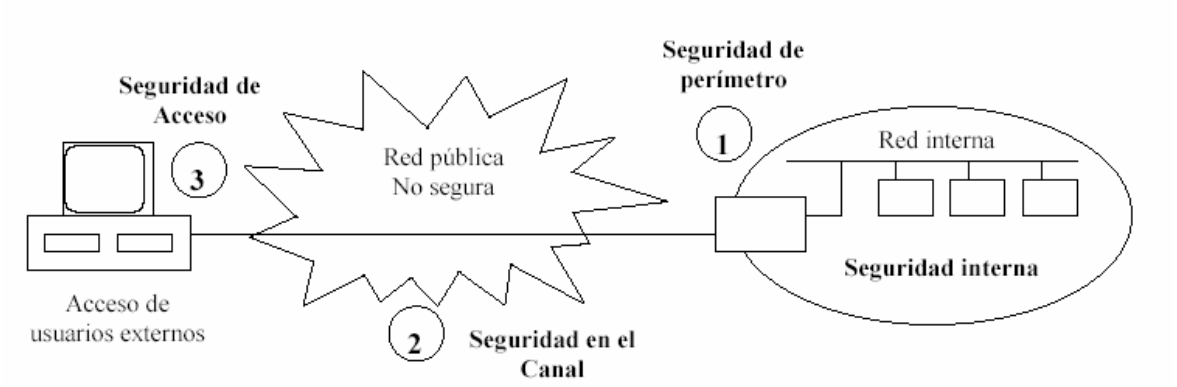


Figura. 3.1. Áreas de Seguridad

Sin embargo, se olvida a veces la seguridad interna. El problema de seguridad puede aparecer dentro de la propia empresa, en su red interna, provocado bien por empleados de la empresa, o porque la barrera del cortafuegos ha sido insuficiente y el enemigo ya está dentro.

En este caso cobran importancia el uso de técnicas como la compartimentalización de la red mediante el uso de conmutadores (switches) y repetidores (hubs) con características de seguridad, los sistemas de monitorización de la red y la seguridad en servidores.

3.4 POLÍTICAS DE SEGURIDAD

A la hora de implantar una política de seguridad en la empresa hay que partir de la base de que el sistema o la red 100% segura no existen. Se ha de hacer una valoración de los recursos a proteger, de tal manera que el esfuerzo y costo de la implementación del sistema de seguridad sea proporcional a su valor. Incluso se pueden definir áreas de la red interna de la empresa con información más valiosa o confidencial que deberán ser protegidas con mayor cuidado que otras.

Una técnica que empieza a implantarse en la política de seguridad es la realización de Auditorias de Seguridad. Estas pueden ser llevadas a cabo por personal de la propia empresa o por consultorías externas. Una Auditoria de Seguridad comprende entre otras las siguientes actividades:

- Evaluación de los recursos y la información a proteger.
- Evaluación de los sistemas de seguridad implementados y de aquellos que se podrían implementar.
- Prueba del estado de la seguridad de la red informática en general y de cada uno de los sistemas conectados a ella en particular, mediante la ejecución de programas o el empleo de técnicas que traten de explotar y pongan de manifiesto los posibles agujeros de seguridad. En este último aspecto existen ya aplicaciones informáticas comerciales que permiten detectar la mayoría de los agujeros de seguridad más evidentes de los sistemas operativos y aplicaciones más extendidas.
- Elaborar planes de contingencia y seguridad.

La seguridad de una red informática pasa por involucrar o concienciar a todos los usuarios y administradores de sistemas en los lemas de seguridad y las implicaciones legales del uso de una red informática

Algunas prácticas habituales de usuarios y administradores comprometen gravemente la seguridad como es el caso de:

- El uso de contraseñas de acceso personales demasiado evidentes.

- La cesión de cuentas de usuarios a terceros.

- El mantenimiento de cuentas de usuario de acceso libre, a grupos o sin contraseña de acceso.

- La instalación de programas poco conocidos o mal mantenidos que pueden aceptar peticiones de la red.

- La ejecución de programas desconocidos que llegan por correo electrónico, a través de la red o cualquier otro medio.

Cualquier sistema, sobre todo si está conectado a cualquier tipo de red informática, debe de tener asignado un administrador. Se ha de tener especial cuidado si además el sistema es un servidor dentro de la red informática (y téngase en cuenta que cualquier PC que comparta tan siquiera una impresora o parte de un disco con otros ya es un servidor dentro de la red). Son obligaciones del administrador del sistema las siguientes tareas:

- Instalar el S.O. y el software de aplicaciones del servidor manteniéndolos convenientemente actualizados e instalando los parches que los fabricantes elaboren para corregir los eventuales problemas que tanto de seguridad como de funcionamiento puedan surgir.

- Modificar las contraseñas de acceso tanto del usuario administrador del sistema como de los demás usuarios, según sea necesario para mantener la seguridad del sistema.

- Administrar la seguridad del sistema mediante la instalación de programas que realicen trazas del funcionamiento del servidor o del uso que los usuarios hacen de él, o cualquier otra labor que beneficie la seguridad del sistema.

- Crear estructuras de directorios para programas y datos administrando correctamente los privilegios de acceso de cada usuario o proceso a los directorios o datos.

- Definir y borrar cuentas de usuarios.

- Designar usuarios con privilegios especiales.

- Controlar el rendimiento del sistema.

- Asegurarse de que los datos están convenientemente salvaguardados con políticas de copia de seguridad adecuadas y otros sistemas.

- Arbitrar algún tipo de mecanismo para que en caso de su ausencia temporal o permanente otra u otras personas de confianza puedan acceder a la contraseña de la cuenta del usuario administrador del sistema en caso de necesidad.

3.4.1 Auditoria aplicada a la seguridad en redes de computadores

No importa lo que haga la empresa, siempre va a haber un punto de fallo, para adelantarse a intrusos, entonces se han ideado algunas herramientas para probar la eficacia de las políticas de seguridad en red de la empresa, algunas de tales herramientas, son: SAFEsuite y COPS.

Estas empiezan probando la fiabilidad de las contraseñas de usuario usando algunas técnicas de indagación como es el leer el tráfico de la red buscando en tal información sobre nombres de usuarios y contraseñas respectivas.

3.4.1.1 Auditoria de comunicaciones

Se debe tener en cuenta:

- La gestión de red = los equipos y su conectividad.
- La monitorización de las comunicaciones.
- La revisión de costos y la asignación formal de proveedores.
- Creación y aplicabilidad de estándares.

Objetivos de control:

- Tener una gerencia de comunicaciones con plena autoridad de voto y acción.
- Llevar un registro actualizado de módems, controladores, terminales, líneas y todo equipo relacionado con las comunicaciones.
- Mantener una vigilancia constante sobre cualquier acción en la red.
- Registrar un costo de comunicaciones y reparto a encargados.
- Mejorar el rendimiento y la resolución de problemas presentados en la red.

Han de existir normas de comunicación en:

- Tipos de equipamiento como adaptadores LAN.
- Autorización de nuevo equipamiento, tanto dentro, como fuera de las horas laborales.
- Uso de conexión digital con el exterior como Internet.
- Instalación de equipos de escucha como Sniffers (exploradores físicos) o Traceadores (exploradores lógicos).

3.4.1.2 Auditoria De La Red Física

Se debe garantizar que exista:

- Áreas de equipo de comunicación con control de acceso.
- Protección y tendido adecuado de cables y líneas de comunicación para evitar accesos físicos.
- Control de utilización de equipos de prueba de comunicaciones para monitorizar la red y el tráfico en ella.
- Prioridad de recuperación del sistema.
- Control de las líneas telefónicas.

3.4.1.3 Auditoria De La Red Lógica

En ésta, debe evitarse un daño interno, como por ejemplo, inhabilitar un equipo que empieza a enviar mensajes hasta que satura por completo la red. Para éste tipo de situaciones:

- Se deben dar contraseñas de acceso.
- Controlar los errores.
- Garantizar que en una transmisión, ésta solo sea recibida por el destinatario. Para esto, regularmente se cambia la ruta de acceso de la información a la red.
- Registrar las actividades de los usuarios en la red.
- Encriptar la información pertinente.
- Evitar la importación y exportación de datos.
- Generar estadísticas de las tasas de errores y transmisión.
- Crear protocolos con detección de errores.
- Los mensajes lógicos de transmisión han de llevar origen, fecha, hora y receptor.
- El software de comunicación, ha de tener procedimientos correctivos y de control ante mensajes duplicados, fuera de orden, perdidos o retrasados.

- Los datos sensibles, solo pueden ser impresos en una impresora especificada y ser vistos desde una terminal debidamente autorizada.
- Se debe hacer un análisis del riesgo de aplicaciones en los procesos.
- Se debe hacer un análisis de la conveniencia de cifrar los canales de transmisión entre diferentes organizaciones.
- Asegurar que los datos que viajan por Internet vayan cifrados.

3.5 SEGURIDAD DE PERÍMETRO. CORTAFUEGOS

3.5.1 Introducción

Un cortafuego es una de las varias formas de proteger una red de otra red no fiable desde el punto de vista de la seguridad. Los mecanismos reales mediante los cuales se implementan las funciones del cortafuego son muy variados, pero en general, el cortafuegos puede verse como la unión de un mecanismo para bloquear tráfico y otro para permitirlo. Algunos cortafuegos hacen especial hincapié en el primero, mientras que otros se basan fundamentalmente en el segundo.

La razón para la instalación de cortafuegos es proteger una red privada de intrusos, pero permitiendo a su vez el acceso autorizado desde y hacia el exterior. Otra razón importante es que pueden proporcionar un bastión en el que centrar los esfuerzos de administración y auditoria. Por último, un cortafuegos puede actuar como representante de la empresa en Internet ya que muchas compañías usan sus cortafuegos para almacenar información pública sobre los servicios y/o productos que ofrece.

Hay muchas formas en las que la seguridad de un cortafuegos puede verse comprometida. Aunque ninguna de estas situaciones es buena, hay algunas que son claramente más peligrosas que otras. Dado que el propósito de muchos cortafuegos es bloquear el acceso externo a mía red privada, un claro fallo del sistema es la existencia de algún lazo que permita alcanzar máquinas que se encuentran dentro de la red protegida.

Una situación más peligrosa se produce si alguien es capaz de entrar en la máquina cortafuegos y reconfigurarla de modo que toda la red protegida quede accesible. Este tipo de ataque se suele denominar destrucción del cortafuego. Los daños derivados de este tipo de ataque resultan muy difíciles de evaluar. Una medida importante de cómo un cortafuegos es capaz de soportar un ataque, es la información que almacena para ayudar a

determinar cómo se produjo. La peor situación posible es la que resulta de la destrucción de un cortafuegos sin que queden trazas de cómo se perpetró el ataque.

Una forma de ver el efecto del fallo de un cortafuego es en términos de la zona de riesgo que crea su fallo. Si una red se encuentra conectada a Internet directamente, toda la red es susceptible de ser atacada (toda es una zona de riesgo).

Eso no significa que la red sea necesariamente vulnerable, sino que es necesario reforzar las medidas de seguridad en todas y cada una de las máquinas que forman la red. Esto es extremadamente difícil a medida que aumenta el número de máquinas y el tipo de servicios de red que estas ofrecen a sus usuarios.

Aplicaciones como rlogin o telnet representan un peligro potencial, usado habitualmente por los hackers para ir ganando acceso a diferentes máquinas y usarlas como plataformas para nuevos ataques.

Un cortafuego típico reduce la zona de riesgo al propio cortafuego o a un reducido grupo de nodos de la red, simplificando notablemente el trabajo del administrador.

Si el cortafuegos falla, la zona de riesgo puede expandirse hasta alcanzar a toda la red protegida. Si un hacker gana acceso al cortafuego, puede utilizarlo como plataforma para lanzar ataques contra las máquinas de la red interna.

Se debe tener claro que un cortafuegos no puede proteger de ataques que no se produzcan a través del mismo. Si una compañía posee información reservada en los ordenadores de su red interna, el cortafuego no podrá protegerla contra un ataque desde dentro.

Por ello, esa parte de la red interna debería estar aislada, o bien contar con medidas extras de protección.

Un cortafuego tampoco puede proteger contra virus o contra ataques debidos a los datos que se transfieren salvo que se combine con algún tipo de software antivirus. Es responsabilidad final de los usuarios y de los responsables de cada máquina particular, la protección contra este tipo de riesgos. Se debe prestar especial atención a los troyanos, a fin de evitar ataques desde el interior.

3.5.2 Tipos de cortafuegos

En la configuración de un cortafuego, la principal decisión consiste en elegir entre seguridad o facilidad de uso. Este tipo de decisión es tomado en general por las direcciones de las compañías. Algunos cortafuegos sólo permiten tráfico de correo electrónico a través de ellos, y por lo tanto protegen a la red contra cualquier ataque que no sea a través del servicio de correo. Otros son menos estrictos y sólo bloquean aquellos servicios que se sabe que presentan problemas de seguridad.

Existen dos aproximaciones básicas:

- Todo lo que no es expresamente permitido está prohibido.
- Todo lo que no es expresamente prohibido está permitido.

En el primer caso, el cortafuegos se diseña para bloquear todo el tráfico, y los distintos servicios deben ser activados de forma individual tras el análisis del riesgo que representa su activación y la necesidad de su uso. Esta política incide directamente sobre los usuarios de las comunicaciones, que pueden ver el cortafuego como un estorbo.

En el segundo caso, el administrador del sistema debe predecir que tipo de acciones pueden realizar los usuarios que pongan en entredicho la seguridad del sistema, y preparar defensas contra ellas. Esta estrategia penaliza al administrador frente a los usuarios. Los usuarios pueden comprometer inadvertidamente la seguridad del sistema si no conocen y cumplen unas consideraciones de seguridad mínimas.

El problema se magnifica si existen usuarios que tengan cuenta en la propia máquina que hace de cortafuegos. En este tipo de estrategia hay un segundo peligro latente, y es que el administrador debe conocer todos los posibles agujeros de seguridad existentes en los protocolos y las aplicaciones que estén ejecutando los usuarios.

3.5.3 Capa de trabajo del Cortafuego.

También podemos clasificar los cortafuegos por la capa de la pila de protocolos en la que trabajen.

3.5.3.1 Cortafuegos a nivel de Red

Por lo general se trata de un enrutador (router) o una computadora especial que examina las características de los paquetes IP para decidir cuáles deben pasar y cuáles no. Por

ejemplo se podría configurar el enrutador para que bloquease todos los mensajes que provengan del sitio de un determinado competidor, así como todos los mensajes destinados al servidor de ese competidor.

Normalmente se suele configurar un router para que tenga en cuenta la siguiente información para cada paquete antes de decidir si debe enviarlo;

- Dirección IP de origen y destino (cabecera IP, nivel 3)
- Puerto origen y destino (campo de datos IP, cabecera nivel 4)
- Protocolo de los datos (TCP, UDP o ICMP) (cabecera IP. nivel 3)
- Si el paquete es inicio de una petición de conexión (campo de datos IP, cabecera nivel 4)

Si se instala y se configura correctamente un cortafuego a nivel de red, éste será muy rápido y casi totalmente transparente para los usuarios.

3.5.3.2 Cortafuegos a nivel de circuito

Se trata de una versión avanzada de los cortafuegos vistos en el punto anterior que trabajan en la capa de transporte. La seguridad en este caso está basada en el establecimiento, seguimiento y liberación de las conexiones que se realizan entre las máquinas internas y externas.

Observan la conveniencia o no de la existencia de esas conexiones en función del tipo de aplicación que realiza la conexión y la procedencia de la petición. Además, realizan seguimiento en los números de secuencia de la conexión buscando aquellos paquetes que no corresponden con conexiones establecidas. Durante este seguimiento, se establece un circuito virtual entre el cliente y el servidor a través del cortafuegos, que hace transparente la existencia de dicho cortafuegos.

3.5.3.3 Cortafuegos a nivel de aplicación

Suele ser un ordenador que ejecuta software de servidor Proxy. La palabra "proxy" significa "actuar por poderes" o "en nombre de otro". Los servidores proxy hacen

precisamente esto, se comunican con otros servidores del exterior de la red en nombre de los usuarios.

En otras palabras un servidor proxy controla el tráfico entre dos redes estableciendo la comunicación entre el usuario y él mismo y entre él mismo y el ordenador destino. De este modo la red local queda oculta para el resto de Internet.

Un usuario que acceda a Internet a través de un servidor proxy aparecerá para los otros ordenadores como si en realidad fuera el servidor proxy. Esto combinado con un servicio NAT, puede hacer completamente invisibles las direcciones IP de los ordenadores de la red interna hacia el exterior.

Como trabaja a nivel de aplicación, este tipo de cortafuegos es más seguro y potente, pero también menos transparente y rápido que un router. Existen servidores proxy disponibles para diferentes servicios como HTTP, FTP, Gopher, SMTP y Telnet. Es necesario configurar un servidor proxy diferente para cada servicio que se desee proporcionar.

Al implementar un servidor proxy a nivel de aplicación, los usuarios de la red deberán utilizar programas clientes que puedan trabajar con un proxy. Se han creado muchos protocolos TCP/IP, como HTTP, FTP y otros, pensando en la posibilidad de utilizar un proxy. En la mayoría de los navegadores web, los usuarios pueden establecer fácilmente sus preferencias de configuración para seleccionar el servidor proxy a utilizar.

3.5.4 Topologías de cortafuegos

Aunque el propósito de todos los cortafuegos es el mismo, existen diferencias en sus topologías y prestaciones. Los siguientes son algunos ejemplos de las múltiples posibilidades existentes:

- Bastión Host
- Encaminador con filtrado (Screening Router)
- Host con doble conexión (Dual-Homed Host)
- Cortafuegos mediante filtrado de host (Screened Host)
- Cortafuegos mediante filtrado de subred(Screened Subnet)

3.5.4.1 Bastión Host

Son sistemas identificados por el administrador de la red como puntos clave en la seguridad de la red. Son auditados regularmente y pueden tener software modificado para filtrar y bloquear determinados intentos de conexión, trazar las comunicaciones y reparar fallos de seguridad del sistema.

Un ejemplo simple es el caso de la instalación de un software de cortafuegos personal en el equipo del usuario. Mediante este tipo de software el usuario puede controlar, bloquear y filtrar el tráfico de datos que entra y sale por cada uno de los puertos de comunicación de su ordenador personal, tanto si utiliza aplicaciones cliente, como si ofrece servicios a equipos remotos.

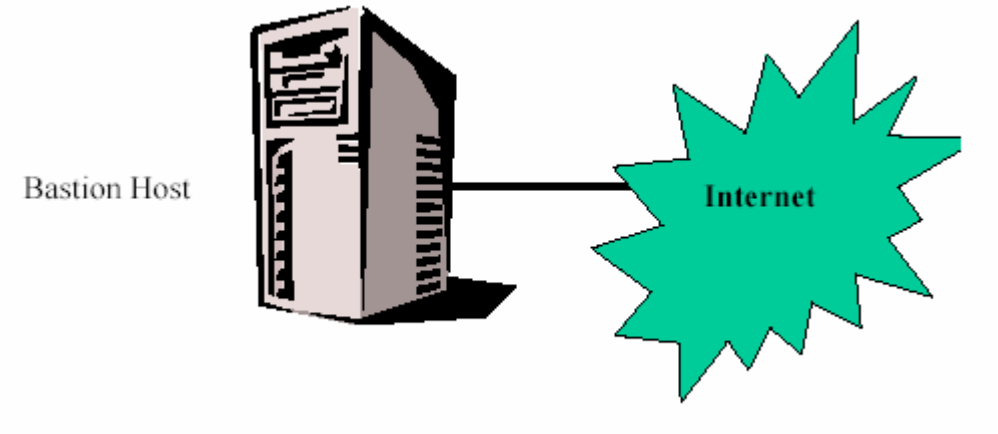


Figura. 3.2. Bastión Host

3.5.4.2 Encaminador con Filtrado (Screening Router)

Son un componente básico de la mayor parte de los cortafuegos. Pueden ser un router comercial o basado en un ordenador convencional, con capacidad para filtrar paquetes. Tienen la capacidad para bloquear el tráfico entre redes o nodos específicos basándose en direcciones y puertos TCP/IP (trabajan a nivel de red). Algunos cortafuegos sólo consisten en un "screening router" entre la red privada e Internet.

En general permite la comunicación entre múltiples nodos de la red protegida y de Internet. La zona de riesgo es igual al número de nodos de la red protegida y el número y tipo de servicios para los que se permite el tráfico. Es difícil controlar los daños que pueden producirse dado que el administrador de la red debe examinar regularmente cada host para buscar trazas de ataques.

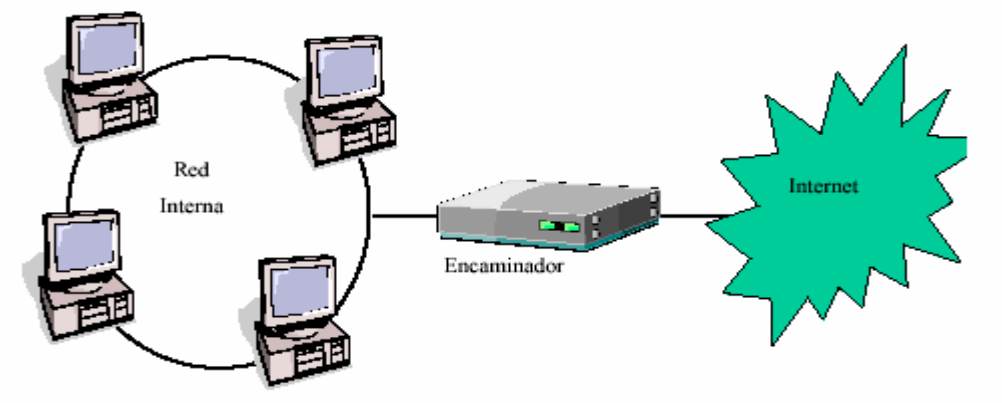


Figura. 3.3. Filtrado mediante Router

Es casi imposible reconstruir un ataque que haya llevado a la destrucción del cortafuegos, e incluso puede ser difícil detectar la propia destrucción, aunque algunos poseen capacidades de registro de eventos para aplacar esta situación. En general responden a configuraciones en las que lo que no está expresamente prohibido, está permitido. No son la solución más segura, pero son muy populares dado que permiten un acceso a Internet bastante libre desde cualquier punto de la red privada.

3.5.4.3 Host con doble conexión (Dual-Homed Host)

Algunos cortafuegos son implementados sin necesidad de un screening router. Para ello se conecta un servidor mediante dos tarjetas independientes a la red que se quiere proteger y a Internet, desactivando las funciones de reenvío TCP/IP. Este dispositivo puede ser un bastión host y funcionar como servidor (Web, FTF, ...) tanto para la red interna como para la red externa. Los hosts de la red privada pueden comunicarse con el bastión host, al igual que los nodos de Internet, pero el tráfico directo entre ambos tipos de nodos está bloqueado.

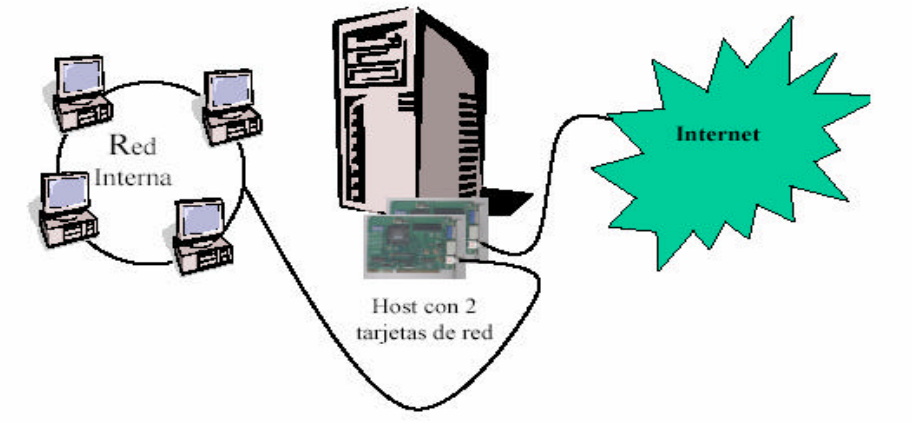


Figura. 3.4. Filtrado con Doble Conexión

Esta estructura de cortafuegos es empleada habitualmente debido a que es fácil de implementar. Al no reenviar el tráfico TCP/IP, bloquea completamente la comunicación entre ambas redes. Su facilidad de uso depende de la forma en la que el administrador proporciona el acceso a los usuarios:

- Proporcionando pasarelas para las aplicaciones.
- Proporcionando cuentas a los usuarios en el bastión host.

En el primer caso se está en una situación en la que lo que no está explícitamente permitido, está prohibido. El permiso para el uso de cada aplicación se suele habilitar instalando el software de proxy adecuado para cada una de ellas.

En el segundo caso, el acceso de los usuarios a Internet es más sencillo, pero la seguridad puede verse comprometida. Si un hacker gana acceso a una cuenta de usuario, tendrá acceso a toda la red protegida. La cuenta de un usuario puede verse comprometida por elegir una contraseña sencilla de adivinar, o por algún descuido.

El principal inconveniente es que un hacker mínimamente preparado puede borrar sus huellas fácilmente, lo que hace muy difícil descubrir el ataque. Si el único usuario es el administrador, la detección del intruso es mucho más fácil, ya que el simple hecho de que alguien entrado en el sistema es un indicativo de que sucede algo raro.

Esta estructura de cortafuegos ofrece la ventaja sobre un screening router, de que es más fácil actualizar el software del sistema para obtener registros del sistema en distintos tipos de soporte, lo que facilita el análisis de la situación en caso de que la seguridad se haya visto comprometida.

El aspecto más débil de esta estructura es su modo de fallo. Si el cortafuegos es destruido, es posible que un hacker preparado reactive el reenvío TCP/IP teniendo libre acceso a toda la red protegida.

Para detectar esta situación conviene tener al día las revisiones del software con el fin de eliminar los bugs de seguridad. Además no conviene hacer público el tipo y versión del sistema operativo instalado en la máquina para no facilitar el trabajo de los posibles atacantes.

3.5.4.4 Cortafuegos mediante filtrado de Host (Screened Host)

Es la configuración de cortafuegos más común. Está implementada usando un bastión host y un screening router. Habitualmente el bastión host está en la red privada, y el screening router está configurado de modo que el bastión host es el único nodo de dicha red que es accesible desde Internet para un pequeño número de servicios.

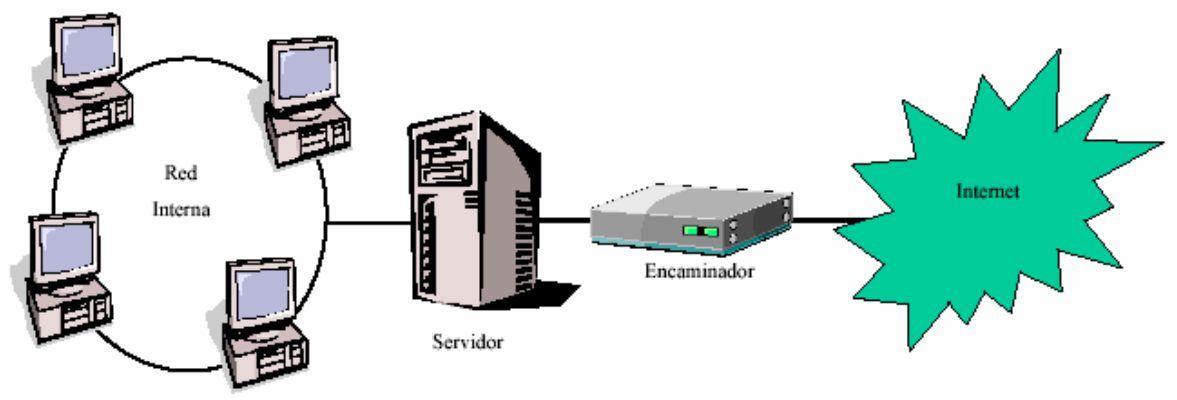


Figura. 3.5. Filtrado de Host

Como el bastión host está en la red privada, la conectividad para los usuarios es muy buena, eliminando los problemas que suelen aparecer al tener definidas rutas extrañas.

Si la red privada es una red local virtual extensa, el esquema funciona sin necesidad de cambios en las direcciones de la red local siempre que ésta esté usando direcciones IP válidas.

La zona de riesgo se circunscribe al bastión host y el screening router. La seguridad de este último depende del software que ejecute. Para el bastión host, las consideraciones sobre seguridad y protección son similares a las hechas para un sistema del tipo host de doble conexión.

3.5.4.5 Cortafuegos mediante filtrado de subred (Screened Subnet)

En algunas configuraciones de cortafuegos se crea una subred aislada, situada entre la red privada e Internet.

La forma habitual de usar esta red consisten emplear screening routers configurados de forma que los nodos dicha subred son alcanzables desde Internet y desde la red privada. Sin embargo, el tráfico desde Internet hacia la red privada es bloqueado.

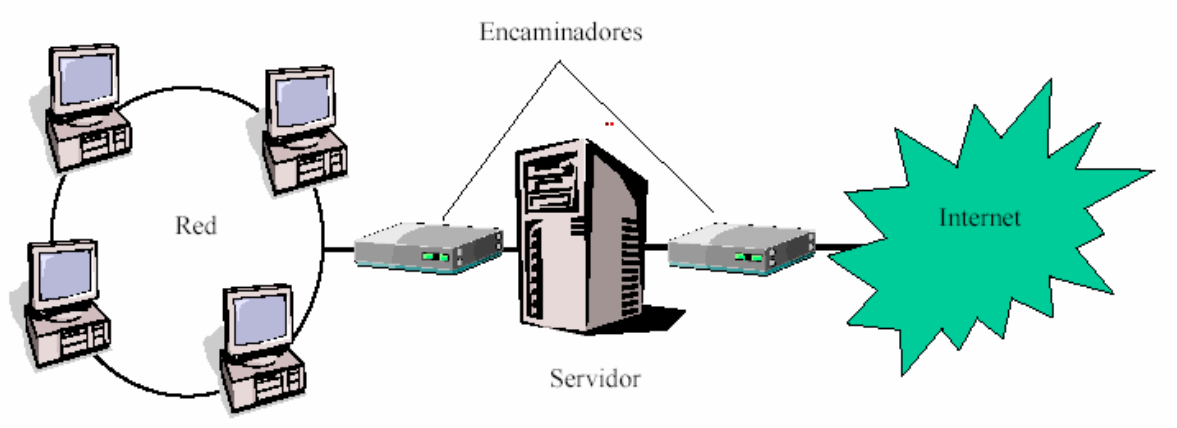


Figura. 3.6. Filtrado de Subred

En la subred suele haber un bastión host como único punto de acceso a la misma. En este caso, la zona de riesgo es pequeña y está formada por el propio bastión host, los screening routers que filtran el tráfico y proporcionan las conexiones entre Internet, la sudred y la red privada.

La facilidad de uso y las prestaciones de la subred varían, pero en general sus servicios se basan en un bastión host que ofrece los servicios a través de gateways para las aplicaciones, haciendo hincapié en que lo que no está explícitamente permitido, está prohibido.

Si este tipo de cortafuegos es atacado en un intento de destruirlo, la hacker debe reconfigurar el tráfico en tres redes, sin desconectarlas, sin dejarse encerrado a si mismo y sin que los cambios sean detectados por máquinas y usuarios. Aunque esto puede ser posible, todavía puede dificultarse más si los routers sólo son accesibles para su reconfiguración desde máquinas situadas en la red privada.

Otra ventaja de este tipo de cortafuegos es que pueden ser instalados de forma que oculten la estructura de la red privada. La subred expuesta es muy dependiente del conjunto de software que se ejecute en el bastión host. La funcionalidad es similar a la obtenida en los casos anteriores, sin embargo la complejidad de configuración y encaminamiento es mucho mayor.

La subred que incluye el cortafuego y los routers se denomina Zona Neutra o Zona Desmilitarizada (DMZ). En esta zona desmilitarizada pueden encontrarse más servidores, bien orientados a dar servicios a usuarios que acceden desde la red externa (red abierta), o

bien para facilitar los servicios de proxy y el acceso a internet a los usuarios de la red interna. Estos servicios pueden residir en una misma máquina, el propio bastión host, o en varias.

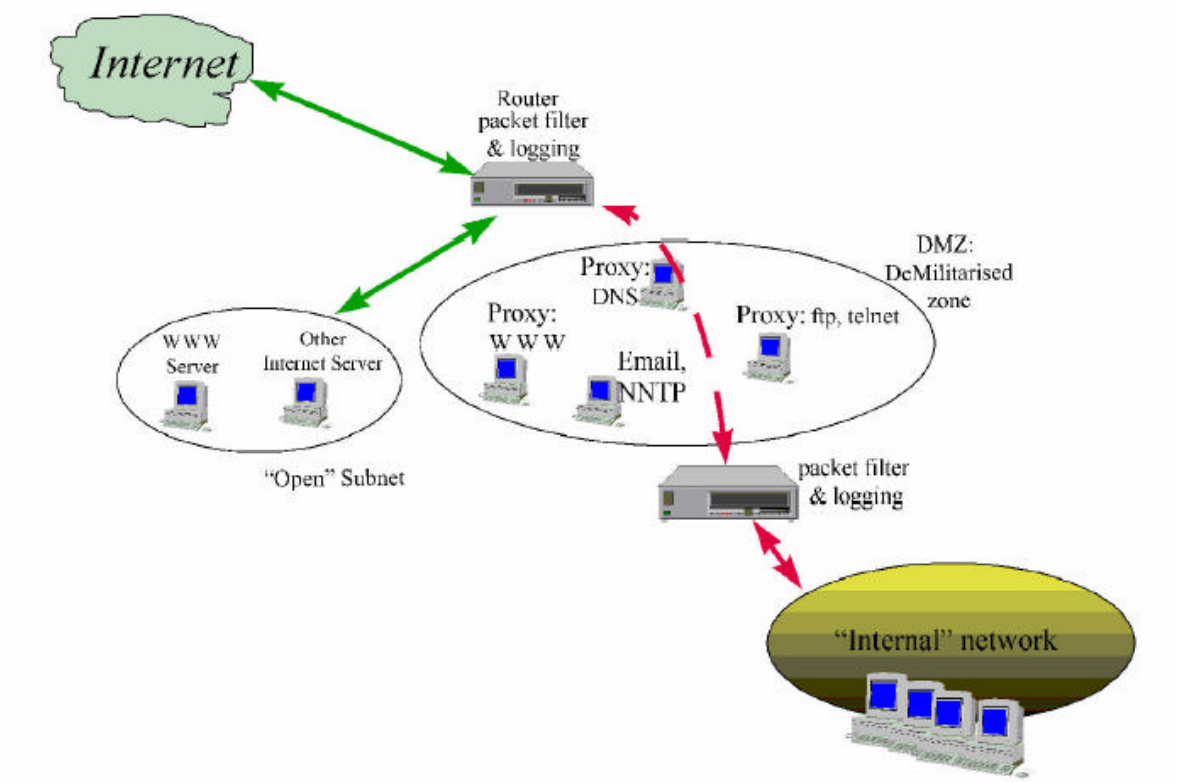


Figura. 3.7. Zona Desmilitarizada

3.5.5 Aplicabilidad

No se puede hablar de que tipo de cortafuegos es el mejor, ya que dicha afirmación depende de muchos factores que hacen que cada caso pueda tener una respuesta diferente. Entre dichos factores figuran el costo, la política de la empresa, la tecnología de red y el personal que se tiene disponible.

Conviene tener en cuenta que un cortafuegos es un dispositivo de red de importancia creciente, al menos desde el punto de vista de administración y seguridad. Debe considerarse como un punto desde el que poder controlar con más facilidad los riesgos a los que puede estar sometida una red de computadores. El concepto de zona de riesgo es fundamental. Lo ideal sería que cada nodo de la red protegida tuviese un alto nivel de seguridad de modo que el cortafuegos fuese redundante.

Otro aspecto fundamental es que un cortafuegos no puede ser considerado como una vacuna. No debe instalarse un determinado tipo de cortafuegos porque para alguien sea

suficientemente seguro. Dicho concepto debe ser resultado de un análisis del costo de implantación, administración, nivel de protección obtenido y valor de los datos que se protegen.

El uso del cortafuegos no se reduce a su diseño e implementación, ya que para garantizar su éxito en la defensa de la red privada es necesario una cuidada labor de administración y vigilancia del mismo.

3.5.6 Codificación en Cortafuegos. Las VPN.

Es posible utilizar los cortafuegos para conectar entre sí dos LAN de manera segura y transparente, es decir: los usuarios verán ambas redes como la misma LAN o como si estuvieran unidas entre si directamente, a través de puentes o conmutadores, y además los datos que se intercambien ambas redes viajarán cifrados por Internet, asegurando su privacidad.

Esta configuración se conoce como Red Privada Virtual o VPN.

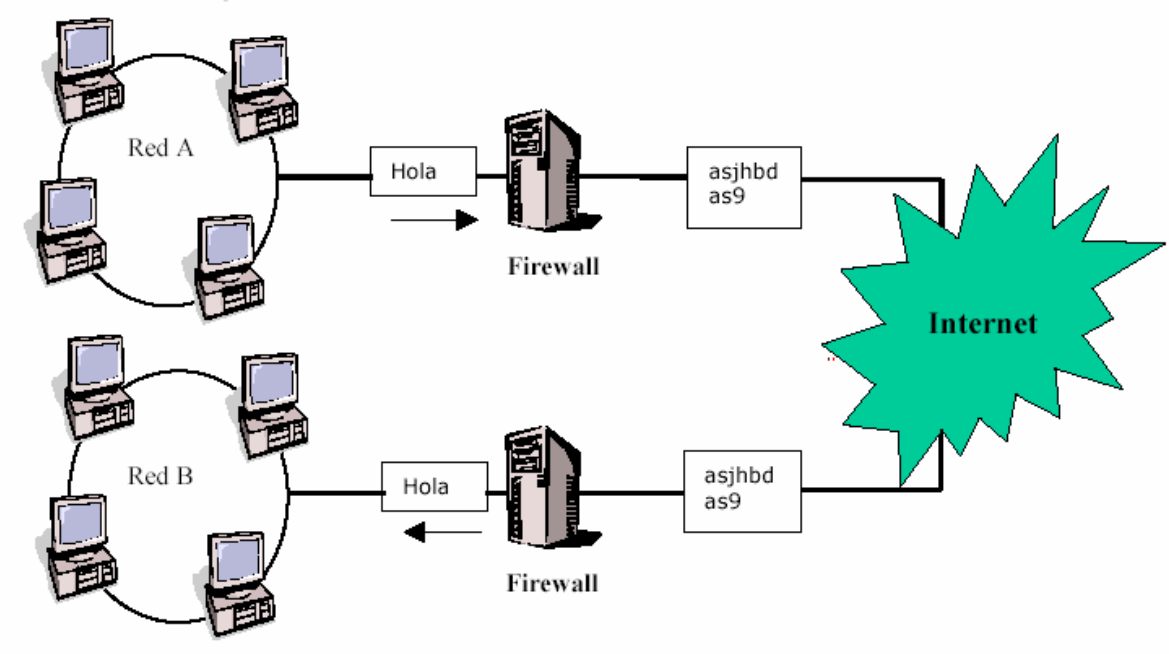


Figura. 3.8. Red Privada Virtual

3.5.7 Túneles en Cortafuegos

Con el rápido crecimiento del mercado de intranets, muchas empresas han descubierto la necesidad de crear túneles en sus cortafuegos que permitan a los usuarios autorizados acceder a los recursos que de otro modo serían inaccesibles. En otras palabras, pueden

bloquear el sitio FTP al exterior, a los usuarios de Internet y permitir que los usuarios de su Intranet se conecten a él desde sus casas.

Este proceso se conoce como tunneling y el cortafuego debe incluir un mecanismo que permita, de alguna manera segura, al cliente abrir un túnel a través de él.

Por ejemplo y debido al amplio uso de la capa de socket seguro SSL en los servidores seguros y a que en las intranets muchas conexiones se producen mediante servidores seguros, SSL debe ampliar el protocolo de proxy Web para que el cliente SSL pueda abrir el túnel. Sin embargo esta técnica tiene también sus inconvenientes.

3.6 SEGURIDAD EN EL CANAL

Aunque los usuarios de las computadoras que son extremo de una comunicación puedan estar tranquilos en cuanto a la seguridad de estas computadoras, la red de comunicaciones siempre es un punto de desconfianza.

La prevención ante los ataques a la red suele pasar siempre por el uso de alguna u otra manera de técnicas de criptografía tanto para proteger el secreto de los datos como para permitir la identificación de quienes los envían o reciben.

La criptografía es el estudio de técnicas de cifrado seguras, mientras que el criptoanalisis es el estudio de las técnicas orientadas a romper los cifrados. El conjunto de ambas ciencias se conoce como criptología.

El cifrado de los datos puede aplicarse a distintos niveles:

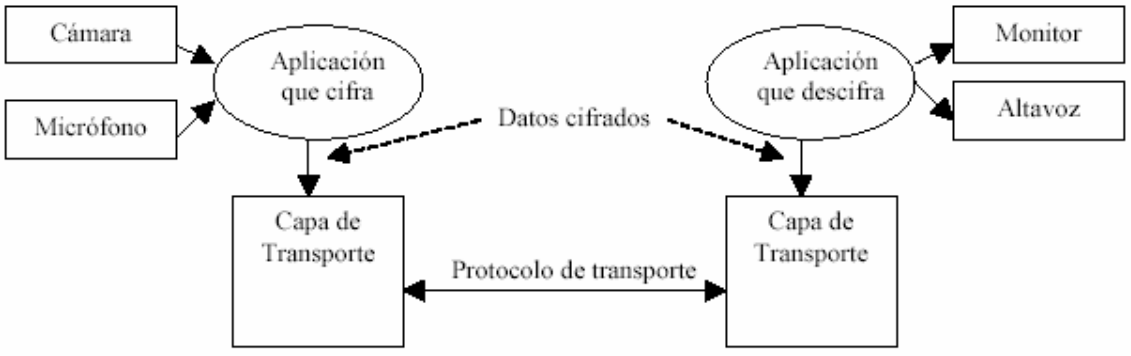


Figura. 3.9. Cifrado de datos

- **Aplicación**: La aplicación que envía los datos del usuario, por ejemplo una de videoconferencia, cifra los datos antes de entregárselos a la capa de transporte y son descifrados por la aplicación que recibe los datos antes de entregárselos al usuario receptor.

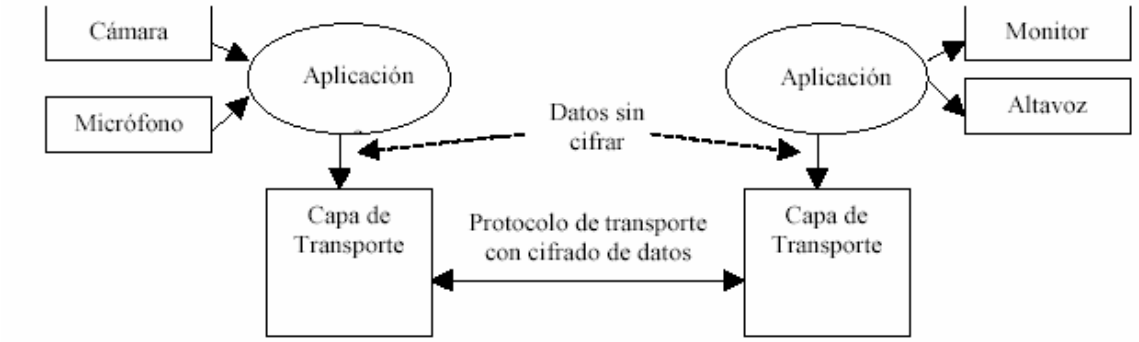


Figura. 3.10. Aplicación

- **Transporte**: La capa de transporte puede utilizar un protocolo que cifre el campo de datos de cada segmento que envía (TPDU) donde van los datos del usuario. Para ello ambas entidades de transporte, a uno y otro extremo han de ser capaces de negociar ese protocolo con cifrado de datos (por ejemplo SSL).

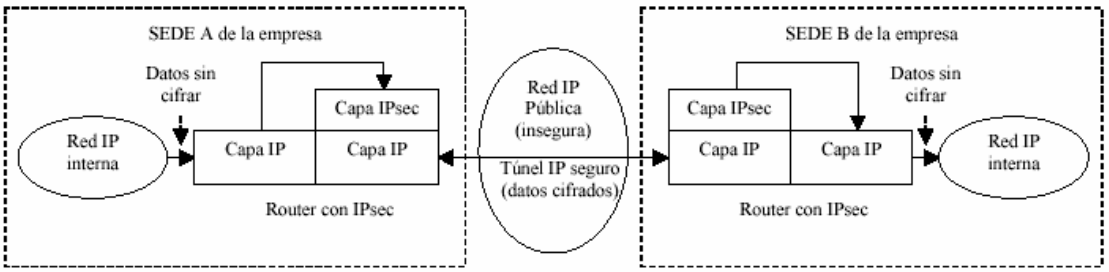


Figura. 3.11. Transporte

- **Red:** Se pueden utilizar protocolos de red que utilicen cifrado de datos, de manera que el campo de datos de las unidades que transmite el protocolo van cifrados. Pero esto exige que todos los nodos de la red, incluidos los que hacen el encaminamiento, soporten ese protocolo.

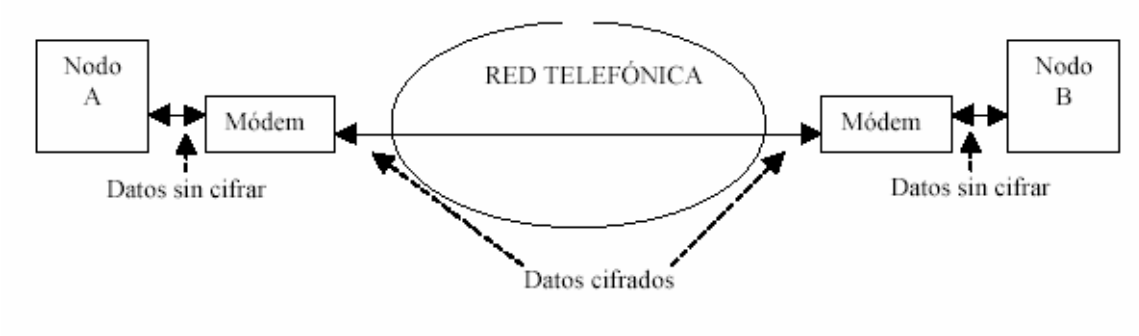


Figura. 3.12. Red con Cifrado de datos

- **Enlace**: En este caso el cifrado/descifrado lo realiza el ETCD (DTE) empleado por el usuario como interfaz con la línea física de comunicación que le une con el o los interlocutores. Un ejemplo son los módem capaces de cifrar la información que transmiten cuando dialogan con otro módem con las mismas capacidades.

3.6.1 Métodos básicos de criptografía

Los métodos básicos de cifrado son el cifrado por sustitución y el cifrado por transposición. Prácticamente todas las técnicas de cifrado se basan en uno de estos métodos o en combinaciones de ambos. Todos los métodos requieren el uso de algún tipo de clave.

3.6.1.1 Cifrado por sustitución

El cifrado por sustitución consiste en sustituir cada carácter, octeto o bloque de datos por otro de acuerdo con un algoritmo determinado, generalmente, basado en algún tipo de clave. Los ejemplos más sencillos son:

a) **Aplicación de máscaras XOR**: Se hace la operación XOR del dato a transmitir con la clave, y se recupera el dato original volviendo a hacer la operación XOR con la misma clave.

b) **Utilización de tablas de traducción**: Estas tablas asignan a cada dato un dato diferente que es el que se transmite. El receptor con la misma tabla podrá conocer el dato real que representa el dato recibido.

3.6.1.2 Cifrado por transposición

Consiste en tomar bloques de datos y cambiar el orden de estos dentro del bloque. Haciendo la transposición inversa se consigue recuperar el bloque original.

3.6.2 Criptografía simétrica

Si se utiliza la misma clave para el cifrado y el descifrado de los datos se habla de criptografía simétrica. Los métodos que usan claves simétricas se conocen también como métodos de clave secreta ya que sólo aquellos entes que intervienen en la comunicación deben conocer la clave.

Si se denomina M a la información a transmitir aún sin cifrar, K a la clave utilizada y ES() a la función de cifrado simétrico, en la criptografía simétrica el mensaje que se transmite es ES(K,M), resultado de cifrar M con la clave K. El mensaje original se recupera aplicando el mismo algoritmo de cifrado con la misma clave, es decir, M=ES(K,ES(K,M)).

El gran problema en la criptografía simétrica está en el uso de claves secretas. Estas deben ser generadas por elementos seguros (en muchos casos uno de los extremos de la comunicación) y transmitidas por canales también seguros, lo que implica generalmente una vía diferente de la red de comunicaciones.

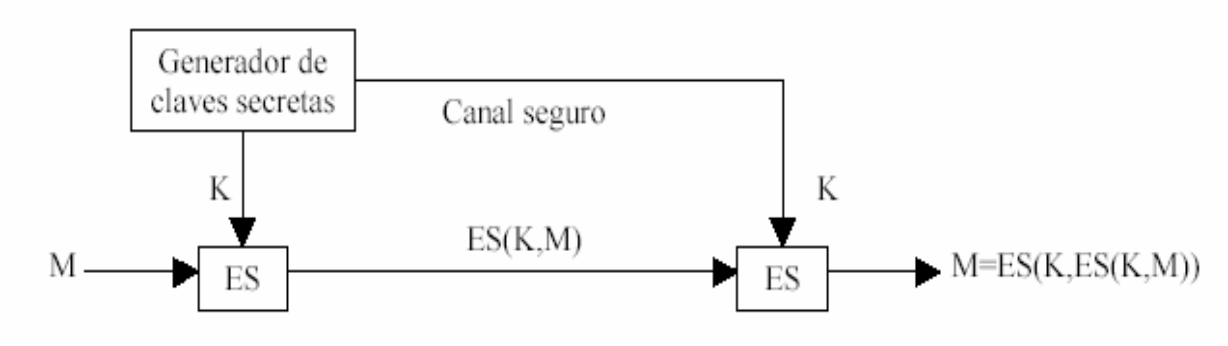


Figura. 3.13. Criptografía Simétrica

3.6.2.1 Data Encryption Standard (DES)

Un ejemplo de criptografía simétrica es el Data Encryiption Standard, DES, desarrollado por el US National Burean of Standards e IBM. Utiliza claves de 64 bits aunque en realidad solo 56 son útiles. El algoritmo combina métodos de transposición y sustitución para codificar normalmente bloques de 64 bits, aunque se puede aplicar de dos modos diferentes:

a) En modo bloque: De un bloque de información de 64 bits se genera otro bloque de 64 bits cifrado, siendo el resultado equivalente a una sustitución.

b) En modo stream: El algoritmo se puede aplicar a un flujo de octetos sin esperar a tener un bloque completo de 64 bits y resulta más difícil de romper por que la codificación de un octeto depende de la anterior.

La potencia del algoritmo DES está en el enorme espacio de claves 2^{56}, es decir, aproximadamente $7,6*10^{16}$ claves y en el diseño de las 8 tablas o cajas de sustitución que se emplean en el algoritmo y que nunca se han hecho públicas.

3.6.2.2 International Data Encryption Algorithm (IDEA)

IDEA es un algoritmo de cifrado por bloques patentado por la firma suiza Ascom. Sin embargo su uso no comercial está autorizado siempre que se solicite permiso.

Se trata de un algoritmo basado en el estándar DES, siendo tan rápido como éste y bastante más seguro. Ha superado todos los intentos de la comunidad científica de romper su cifrado hasta el momento.

IDEA utiliza 52 subclaves de 16 bits y cifra en 8 pasos. Cada bloque se divide en cuatro cuartetos de 16 bits y se utilizan 3 operaciones distintas para combinar dos valores de 16 bit produciendo un resultado de también 16 bit: XOR, suma (modulo 256) y una multiplicación con características especiales.

3.6.3 Criptografía asimétrica

Si la clave es distinta para el cifrado y el descifrado, se habla de criptografía asimétrica. Los métodos que usan claves asimétricas generalmente mantienen secreta la clave empleada para el descifrado y hacen pública entre el resto de usuarios la clave con la que deben cifrar los mensajes para que sólo él los pueda descifrar, por lo que se conocen también como métodos de clave pública.

Si se denomina M a la información a transmitir aún sin cifrar, K_s a la clave secreta para el descifrado, K_p a la clave pública para el cifrado y EA() a la función de cifrado asimétrico, el mensaje que se transmite es $EA(K_p,M)$, resultado de cifrar M con la clave K_p. El mensaje original se recupera aplicando el mismo algoritmo de cifrado pero con la clave secreta, es decir, $M = EA(K_s,EA(K_p,M))$.

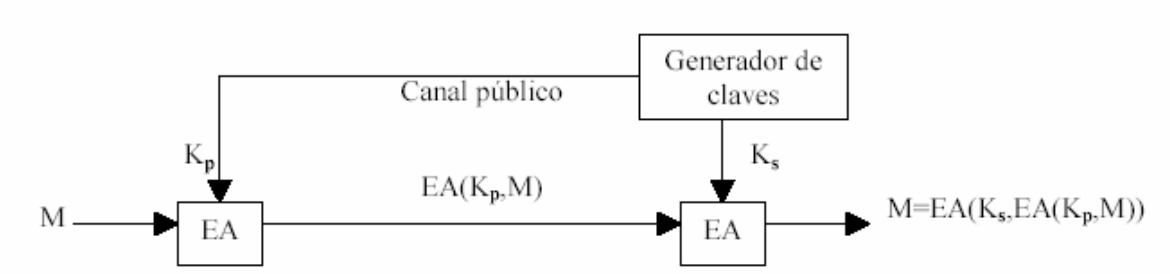


Figura. 3.14. Criptografía Asimétrica

Para que un método de clave pública sea funcional se han de cumplir dos requisitos:

a) Debe ser muy difícil averiguar Ks a partir de Kp.

b) Debe ser muy difícil obtener la información que contiene el mensaje cifrado si no se dispone de Ks.

3.7 SEGURIDAD DE ACCESO

La seguridad de acceso contempla básicamente la identificación del usuario o entidad que desea acceder, la autorización del acceso y la auditoria de las tareas realizadas en el sistema por la entidad que ha accedido.

La identificación de usuarios o entidades que acceden se realiza generalmente mediante palabras clave, sistemas de firma digital de los mensajes u otros medios. Esta identificación incluye a las máquinas involucradas en la comunicación en casos como el comercio electrónico.

Una problemática aún no resuelta por completo es el acceso de usuarios a través de redes extrañas a la empresa. Imagínese el caso de un empleado de una empresa A que visita a otra B y pide permiso para conectar su computadora portátil a la red de B para acceder a sus datos que residen en A:

a) Para la red B el empleado de A es un elemento completamente extraño y potencialmente peligroso por lo que su acceso a través de su red ha de ser vigilado y limitado.

b) Para el empleado de A la red B es extraña y potencialmente insegura, por lo que su acceso a través de ella es peligroso y se han de poner todos los medios necesarios para proteger la información que se intercambie durante la conexión.

c) Para la red A el empleado será conocido pero la red desde la que accede es potencialmente insegura. Por ello, se han de extremar las medidas para identificar correctamente y sin posibilidad de engaño al usuario y su equipo, y otorgarle un acceso temporal para evitar su posterior reutilización por parte de alguien extraño a la empresa.

Algunas de las técnicas que se describen a continuación son utilizadas para resolver algunos de los problemas que plantean estas situaciones.

3.7.1 Autentificación mediante firma digital

Una de las aplicaciones del cifrado asimétrico es comprobar la autenticidad de los mensajes, es decir, la confirmación para el receptor de que el mensaje recibido ha sido emitido realmente por quien dice ser su emisor. Para ello el algoritmo de cifrado asimétrico ha de cumplir además de $M=EA(K_s,EA(K_p,M))$, que $M=EA(K_p,EA(K_s,M))$.

El usuario A, emisor del mensaje X, lo firmará cifrándolo con su clave secreta KsA. Si se transmitiese así el mensaje $Y=EA(K_{sA},X)$, cualquier usuario que conozca la clave publica de A, K_{pA}, podría descifrarlo.

Por ello A hace un segundo cifrado utilizando la clave pública de B, K_{pB}, de tal manera que ahora sólo B podrá descifrar el mensaje $Z=EA(K_{pB},Y)$. Cuando B recibe el mensaje y le aplica su clave secreta el resultado que obtiene es un mensaje aún cifrado $Y=EA(K_{sB},Z)$. Si B consigue descifrar ese mensaje Y con la clave pública de A, $X=EA(K_{pA},Y)$ significará que A es realmente quien ha enviado el mensaje ya que sólo él tiene la clave secreta para cifrar el mensaje de esa manera.

Obsérvese además que la firma digital es sólo necesaria en el caso de la criptografía asimétrica. Si se empleara criptografía simétrica con claves secretas la autenticidad del mensaje está implícita puesto que sólo el otro interlocutor conoce la clave secreta si la distribución de la misma se ha hecho de manera segura.

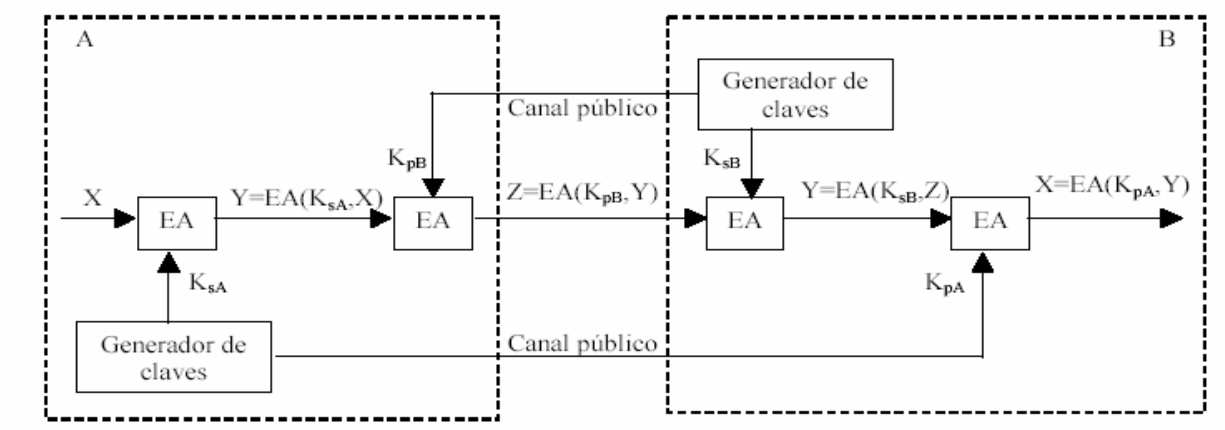


Figura. 3.14a. Firma Digital

El aplicar dos veces consecutivas un cifrado asimétrico a un mensaje completo puede ser muy costoso en tiempo de computación por lo que generalmente no se firma todo el mensaje sino un código reducido que lo represente.

Este código se suele obtener mediante la aplicación al mensaje completo de una función hash, H(), sencilla, irreversible y conocida públicamente, que aplicada a X nos da una cadena con unos pocos octetos J=H(X).

El mensaje completo sólo se cifra con la clave pública de B, $Y=EA(K_{pB},X)$, y junto con el se envía la firma consistente en aplicar la clave secreta de A al resultado de la función hash $F=EA(K_{sA},J)$. Una vez que recibe el mensaje cifrado y la firma, B obtiene $X=EA(K_{sB},Y)$ y $J=EA(K_{pA},F)$. Si B comprueba que al aplicar la función hash a X obtiene el mismo resultado J que le ha llegado en la firma, estará seguro de que el mensaje procede realmente de A.

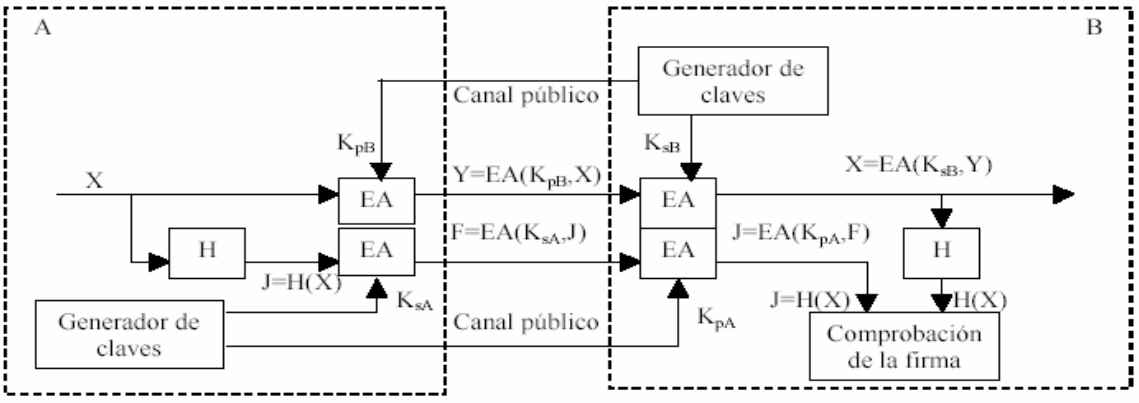


Figura. 3.14b. Firma Digital

Un algoritmo muy conocido para generar una firma digital para un conjunto de datos dado es el MD5.

MD5 genera una firma de 128 bits y se conjetura que es computacionalmenle imposible generar dos mensajes cuya firma MD5 coincida, así como reproducir el mensaje original a partir de ella.

El algoritmo está orientado a producir firmas para mensajes largos antes de su cifrado y es mucho más fiable que el checksum o cualquier otro método tradicional.

En las siguientes figuras se muestra un ejemplo de funcionamiento de la firma digital de un mensaje utilizando el algoritmo MD5.

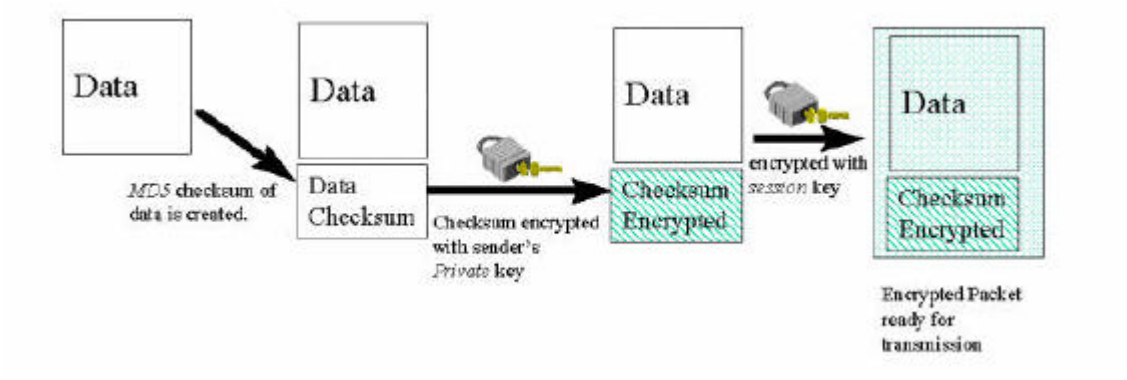


Figura. 3.15a. Firma Digital Utilizando Algoritmo MD5

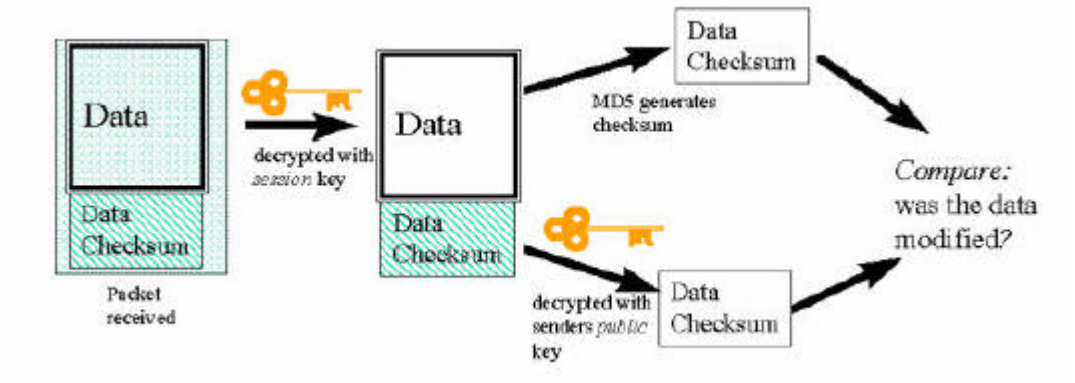


Figura. 3.15b. Firma Digital Utilizando Algoritmo MD5

3.7.2 Autoridades certificadoras

Para que los métodos de clave secreta funcionen es vital que las claves se distribuyan de forma segura. En el caso de los de clave pública, el problema es más sutil. ¿Cómo se sabe que la clave pública que distribuye una estación N que se incorpora a una comunidad es realmente distribuida por la estación N y no por alguien que la suplanta?

Un sistema de comunicaciones seguro debe disponer de una autoridad certificadora (denominada AC a partir de ahora) para la comunidad, encargada de gestionar las claves secretas y/o públicas y de asegurar su pertenencia exclusiva a un usuario de una forma automática y dinámica, agilizando así el intercambio de claves de una forma segura.

Dos situaciones pueden comprometer la seguridad del sistema:

a) La AC tiene que ser un sistema seguro ya que cualquier fallo en su seguridad comprometería la seguridad de todo el sistema que se fía de su integridad.

b) Cada entidad que se incorpora a la comunidad segura ha de establecer un enlace seguro con la AC mediante algún sistema de "entrevista personal" que asegure la identidad de ambas partes y en la que se realice el intercambio de las claves secretas o públicas que se utilizarán en el enlace seguro.

3.8 SEGURIDAD INTERNA

Los ataques a la seguridad pueden realizarse desde el interior de la red de la empresa, bien por parte de usuarios de esa red, por intrusos que acceden físicamente a alguno de los sistemas de la red o por intrusos que desde el exterior de la red han ganado el acceso a alguno de los sistemas internos de la red.

En estos dos últimos casos el intruso generalmente suplanta a uno de los usuarios legítimos de la red o acceden a través de algún agujero de seguridad en el sistema. Para prevenir el que estos ataques prosperen se pueden implantar técnicas como las siguientes.

3.8.1 Compartamentalización

Los repetidores y conmutadores que disponen de la posibilidad de filtrar el tráfico de red que circula por sus puertos permiten la compartamentalización de la red local. Estos equipos consiguen que el tráfico de tramas de unas zonas de la red o incluso de cada

puerto, no pueda ser visto por sistemas conectados en otras zonas u otros puertos. Las formas básicas de protección implementadas en estos equipos son:

- Seguridad anti-escuchas: A través de cada puerto sólo se podrán recibir las tramas en cuyo encabezamiento aparezca la dirección física de las computadoras conectadas a través de ese puerto o de las tramas enviadas a direcciones "broadcast".

- Seguridad anti-intrusos: A través de cada puerto sólo podrán enviar tramas aquellas computadoras cuya dirección física haya sido admitida como legítima para utilizar ese puerto.

Este tipo de dispositivos pueden llevar a cabo un aprendizaje inteligente que facilita la configuración de los mismos, de manera que a través del tráfico que escuchan determinan que dispositivos tienen conectados en cada puerto para realizar filtrado anti- escuchas o determinar que equipo es el legítimo usuario de un puerto frente a posibles intrusos.

También colaboran a la compartamentalización de la red los routers a nivel de protocolos de red {routers, encaminamiento en la capa de red). Al encaminar protocolos de red como IP, IPX, etc., permiten a la vez filtrarlos total o parcialmente, en función por ejemplo de las direcciones lógicas de los datagramas. Podrían introducirse incluso cortafuegos en el interior de la red para llevar el filtrado hasta niveles superiores.

3.8.2 Monitorización

La monitorización de una red suele ser uno de los procesos previos al ataque a la seguridad de los sistemas conectados a la misma. La red puede ser monitorizada por sniffers (programas que capturan tramas de la red para su posterior análisis) instalados en algún sistema de la red mediante el sistema de los programas troyanos o por el uso ilegítimo de alguna cuenta de usuario más o menos privilegiada.

La información obtenida sirve para explotar otros agujeros de seguridad u obtener contraseñas de usuarios de la red. La compartamentalización de la red descrita en el anteriormente, dificulta grandemente la labor de monitorización de los sniffers.

Sin embargo la misma técnica de monitorización puede servir para detectar y perseguir a los intrusos. La detección de determinados volúmenes o contenidos de tráfico sospechoso

mediante un programa analizador de protocolos permite la detección de ataques. El mismo programa puede ayudar a determinar la procedencia y responsabilidad del ataque.

3.8.3 Seguridad en servidores

Además de las actividades y actitudes de auditoria, formación, concienciación y responsabilidad descritas en las políticas de seguridad, se describen a continuación medidas a tener en cuenta cuando se instalan servicios de red en una máquina.

En primer lugar, conviene tener claro que existen muchos tipos servicios y que cada uno de ellos tiene sus propios requisitos de seguridad. Como norma común el administrador de la máquina que ofrezca algún servicio de red, debe preocuparse de conocer la problemática particular que cada servicio ofertado presenta y, además, mantener actualizado el software de soporte para dicho servicio con el fin de ir tapando los agujeros de seguridad que se descubran.

Puede considerarse la siguiente división de los servicios:

- En función de su visibilidad:
    - Servicios que sólo deben ser accedidos desde máquinas de nuestra propia red). En estos casos, puede ser suficiente con proteger el servidor interno de cualquier acceso desde máquinas fuera de nuestra red.
    - Servicios ofrecidos a otras redes, por ejemplo un servidor web. En estos casos la protección es más compleja, y es el conjunto servicio/protocolo /servidor, el que debe incluir aquellas medidas de seguridad necesarias para prevenir el acceso no autorizado o la modificación de información
- En función del tipo de usuario:
    - Servicios accesibles solo por usuarios de nuestra red. Por ejemplo. podemos desear que sólo usuarios de nuestra organización puedan utilizar nuestros servicios ftp o telnet.
    - Servicios accesibles por cualquier usuario. Por ejemplo, un ftp anónimo.

En general, es aconsejable dedicar máquinas diferentes para ofrecer servicios a cada grupo de usuarios, separando aquellos ofrecidos al exterior de los de uso interno. Esta práctica permite definir estrategias de administración diferentes sobre cada grupo de servicios, facilitando la tarea del administrador.

Debe evitarse al máximo la instalación en una misma máquina de servicios ofrecidos sólo a nuestros usuarios y los ofrecidos libremente. Cada uno de estos servidores será accesible a través de uno o varios cortafuegos que aseguran la partición de la red en función del nivel de seguridad que se requiera.

Hay que tener especial cuidado con aquellos servicios que permitan conexiones anónimas o a cuentas de invitado. Se debe poner especial hincapié en aislar dichos servidores del resto de la red protegida.

La tendencia actual es que cada sitio puede ser considerado responsable del contenido de la información que es públicamente accesible. Además, en estos casos hay que reforzar al máximo las medidas de auditoria, ya que presentan un fácil punto de penetración.

3.9 ANCHO DE BANDA

Es la medida de la capacidad que tiene un medio de transporte, elemento de red o sistema para llevar mensajes o información desde la fuente hasta el destino, aceptarla y procesarla. Se mide en Hertz (Hz)

Técnicamente, es la diferencia en frecuencia entre el extremo superior y el extremo inferior de un canal.

El Canal Telefónico Análogo tiene un ancho de banda de 0 a 4 KHz. Nominalmente de 0.3 a 3.4 KHz., es decir, 3,1 KHz.

El Canal Digital expresa su ancho de banda en unidades de Velocidad o Capacidad, por ejemplo, 64 Kbps.

3.9.1 Aspectos de Calidad de Servicio

Para determinar los aspectos de calidad se debe realizar un análisis del tráfico que va a pasar por nuestra red.

A los diferentes tipos de flujo que pasan por nuestra red se los debe tratar de una manera distinta, ya que tienen necesidades diferentes de acuerdo al: retardo o latencia, variación del retardo, tasa de transmisión y pérdida de paquetes.

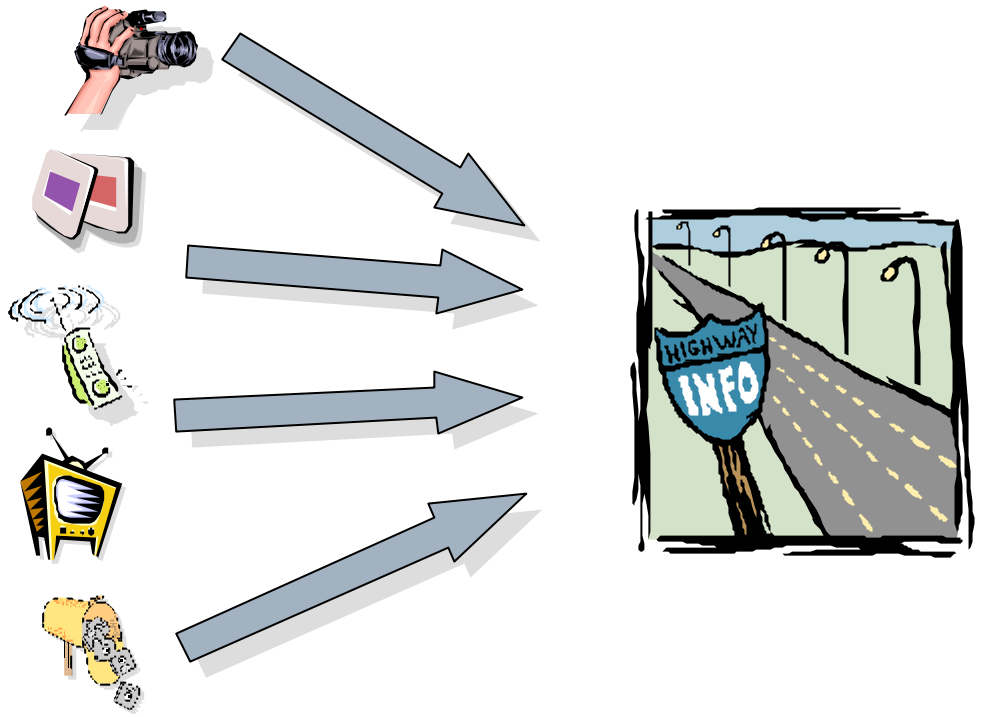


Figura. 3.16. Calidad de Servicio

3.9.2 Requerimientos

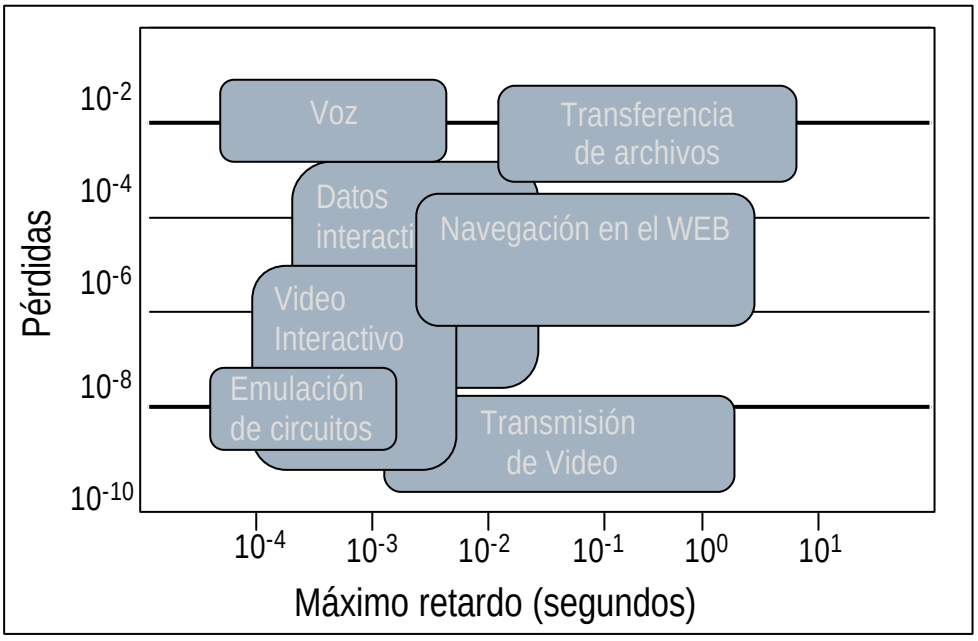


Figura. 3.17. Retardo de los Diferentes Servicios

- Parámetros que afectan a la calidad de una red, dando como resultado la congestión de la red.

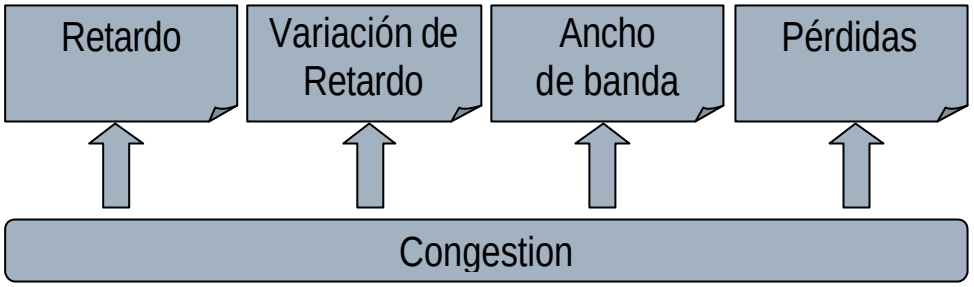


Figura. 3.18. Parámetros que Afectan la Calidad

CAPITULO IV

DISEÑO DE LA RED WAN

4.1 PLANTEAMIENTO DEL PROBLEMA

El centro de Capacitación Informática “CECAI”, cuya principal dependencia esta ubicada en la provincia de Pichincha (Sangolquí), ha decidido realizar una política de actualización tecnológica tendiente a optimizar sus procesos.

A fin de poder desarrollar esta propuesta, se esta haciendo un estudio sobre la necesidad de alcanzar una mejor interconexión entre las distintas áreas del CECAI y sus clientes actuales y potenciales.

El mencionado estudio debe concluir con la necesidad de desarrollar un sistema de comunicaciones que permita integrar distintos servicios a las diferentes sedes del CECAI y al CECAI con el mundo exterior.

4.1.1 Especificaciones del Proyecto

El Centro de Capacitación Informática CECAI, como proyecto de estudio de factibilidad y beneficios para la empresa requiere desarrollar un sistema comunicaciones antes mencionado.

Para tal efecto se necesita para concretar el estudio sobre el sistema de comunicaciones a implementar, complementar los siguientes requerimientos:

1. Desarrollar el gráfico de la red WAN general, además de un gráfico explicativo de la red WAN en cada provincia que se encuentran las instalaciones del CECAI, que mejor satisfaga las necesidades de la empresa, estipulando en el mismo sus conectividades con los distintos tipos de redes LAN, Internet y Extranet, anchos de banda previstos, topologías de red conectadas, tipo de protocolos y tecnologías a implementar, justificando las decisiones tomadas respecto de estos dos últimos puntos.

Asimismo se deberá estipular los tipos de dispositivos, e interfaces de estos, a interconectar y la cantidad de usuarios a satisfacer.

2. Estipular el mismo requerimiento para las distintas redes LAN interconectadas en cada dependencia de la empresa.

3. Determinar las políticas de seguridad básicas que permitan la adecuada constitución de la Extranet mencionada.

4. Determinar el listado de requerimientos estimado que abarcará la instalación y estar en condiciones de justificar el porque del empleo de cada uno de ellos especialmente en lo que a distintos tipos de tecnologías se refiere.

4.1.2 Requerimientos Comerciales:

- Implementar una Red WAN (Red de Área Amplia) que enlace los 20 Centros de Capacitación del CECAI, brindando acceso a los servicios y aplicaciones de la red desde un servidor central.

- Proveer Acceso a Internet controlado y restringido a los 20 Centros Asociados.

- Establecer seguridad en todos los niveles para que la red no quede expuesta a cualquier tipo de ataque o robo de información.

- Proveer del servicio FTP (File Trasfer Protocol) para la transferencia de archivos de gran tamaño, entre los puntos de mayor flujo de información.

- Implementar el hardware y soporte necesario para los servicios anteriores y otros servicios adicionales.

- Posibilitar un ahorro en comunicaciones telefónicas entre sucursales.

Actualmente no se cuenta con un Sistema de Comunicaciones de Datos que integre en una sola Red todos los centros.

4.2 INSTALACIONES DEL “CECAI”

- Provincia de Pichincha:
    - ESPE 1: Ubicada en la ciudad de Sangolquí, Av. El progreso s/n

- ESPE 2: Ubicada en la ciudad de Quito, Av. 6 de diciembre y Tomás de Berlanga.
- Escuela de Servicios: Ubicada en la ciudad de Quito, Av. Mariscal Sucre y Sbte. Michelena
- 13-BI Pichincha: Ubicada en Machachi, Panamericana Sur, vía a Ambato sector Machachi Fuerte Militar Atahualpa
- Santo Domingo: Ubicada en Santo Domingo, Av. Quito y Sachila No. 107, frente al parque central.
- DIREL: Ubicada en Sangolquí, vía Amaguaña, Sector Chaupitena
- Center Systems 2000: Ubicada en Cayambe, Centro Comercial de Vencedores Autónomos local 62
- 23-BE Cenepa: Ubicada en Sangolquí, La Balvina, Hcda. Chillo Jijón Vía Amaguaña.
- I-DE Shyris: Ubicada en Quito, Av. Maldonado s/n y Catarama, Sector San Bartola
- Centro de Computo "Shalom": Ubicada en Sangolquí, calle Ascazubi 128 entre Bolívar y Olmedo
- YNCA: Ubicada en Quito, Av. Maldonado 260 y Francisco Gómez, Sector Villaflora
- ESIN: Ubicada en Conocoto, Vía Amaguaña.

- Provincia del Azuay:
  - III de Tarqui: Ubicada en la ciudad de Cuenca, Mariano Cueva y Muñoz Vernaza (Base de Movilización Sur del Azuay)

- Provincia del Chimborazo:
  - Tecniexito: Ubicada en la ciudad de Riobamba, Rocafuerte No. 27-78 y Venezuela esquina
  - EC-11 "Riobamba": Av. De los Héroes s/n, Brigada de Caballería Blindada No. 11 Galápagos.

- Provincia del Guayas:
  - 5-BI Guayas: Ubicada en la ciudad de Guayaquil, Km. 8 ½ Vía Daule
  - II- DE Libertad: Ubicada en la ciudad de Guayaquil, 9 de Octubre y Santa Elena entre Lorenzo de Garaicoa y Rumichaca

- Provincia de Tungurahua:
  - Hispanoamérica: Ubicada en la ciudad de Ambato, Av. Bolivariana y Moyurco, frente al estadio Bellavista

- Provincia de Imbabura:
  - JMSYSTEMS: Ubicada en la ciudad de Ibarra, Sánchez y Cifuentes 358 entre Troya y Mejía

- Provincia de Esmeraldas:
  - GFE-25 Esmeraldas: Ubicada en la ciudad de Esmeraldas, Fuerte Militar Esmeraldas

De acuerdo al análisis desarrollado, las máquinas a interconectar de acuerdo a sus requerimientos de manejo de información será:

- Provincia de Pichincha:
  - ESPE 1: 9 equipos
  - ESPE 2: 28 equipos
  - Escuela de Servicios: 40 equipos
  - 13-BI Pichincha: 20 equipos
  - Santo Domingo: 12 equipos
  - DIREL: 9 equipos
  - Center Systems 2000: 9 equipos
  - 23-BE Cenepa: 12 equipos
  - I-DE Shyris: 25 equipos
  - Centro de Computo “Shalom”: 19 equipos
  - YNCA: 10 equipos
  - ESIN: 12 equipos

- Provincia del Azuay:
  - III de Tarqui: 11 equipos

- Provincia del Chimborazo:
  - Tecniexito: 17 equipos
  - EC-11 “Riobamba”: 10 equipos

- Provincia del Guayas:
  - 5-BI Guayas: 10 equipos
  - II- DE Libertad: 10 equipos

- Provincia de Tungurahua:
  - Hispanoamérica: 30 equipos

- Provincia de Imbabura:
  - JMSYSTEMS: 12 equipos

- Provincia de Esmeraldas:
  - GFE-25 Esmeraldas: 10 equipos

4.2.1 Distribución Física del CECAI

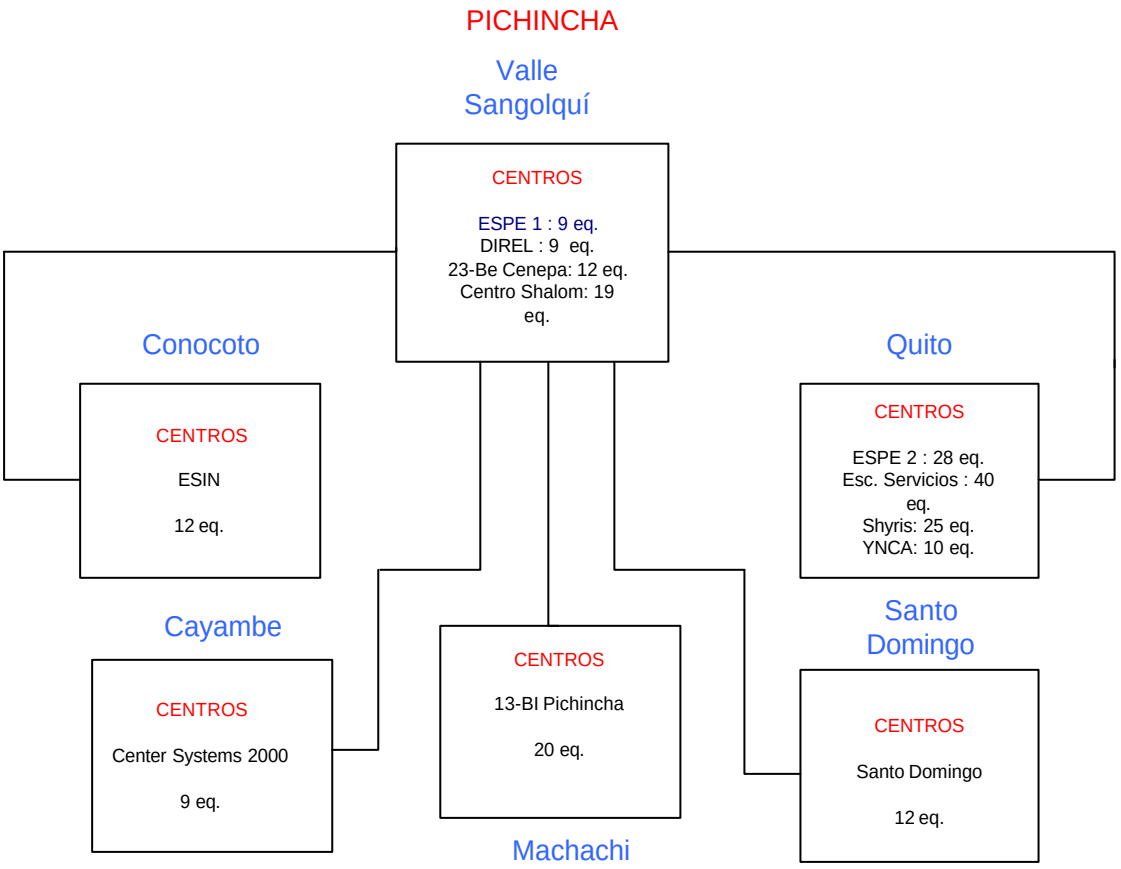


Figura. 4.1. Distribución Física de Pichincha (CECAI)

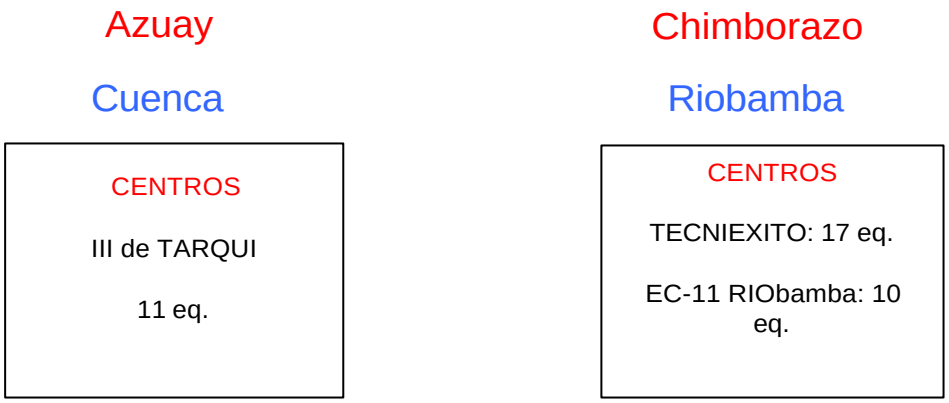


Figura. 4.2. Distribución Física de Azuay y Chimborazo (CECAI)

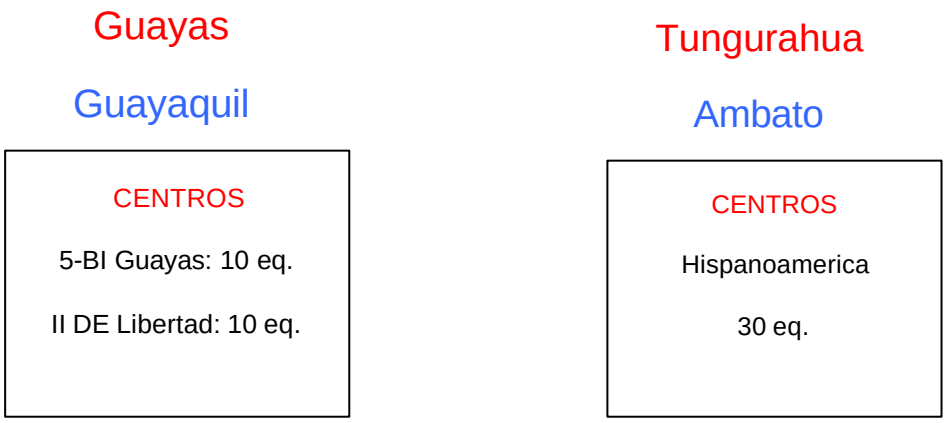


Figura. 4.3. Distribución Física de Guayas y Tungurahua (CECAI)

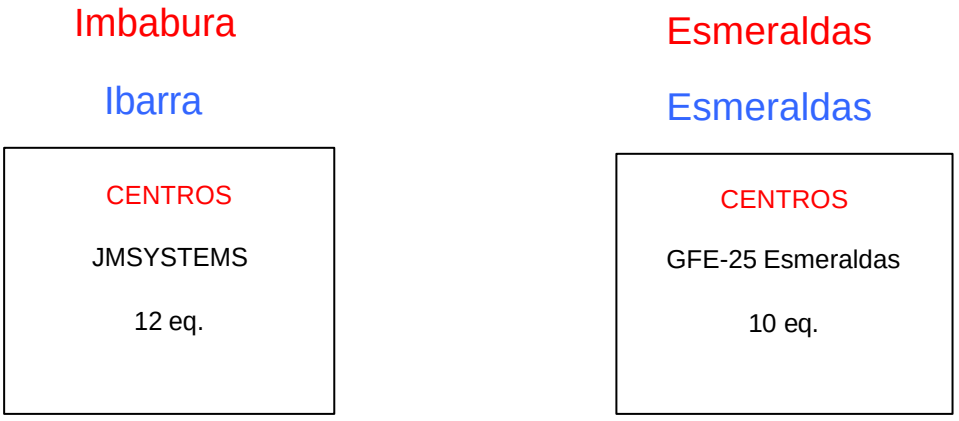


Figura. 4.4. Distribución Física de Imbabura y Esmeraldas (CECAI)

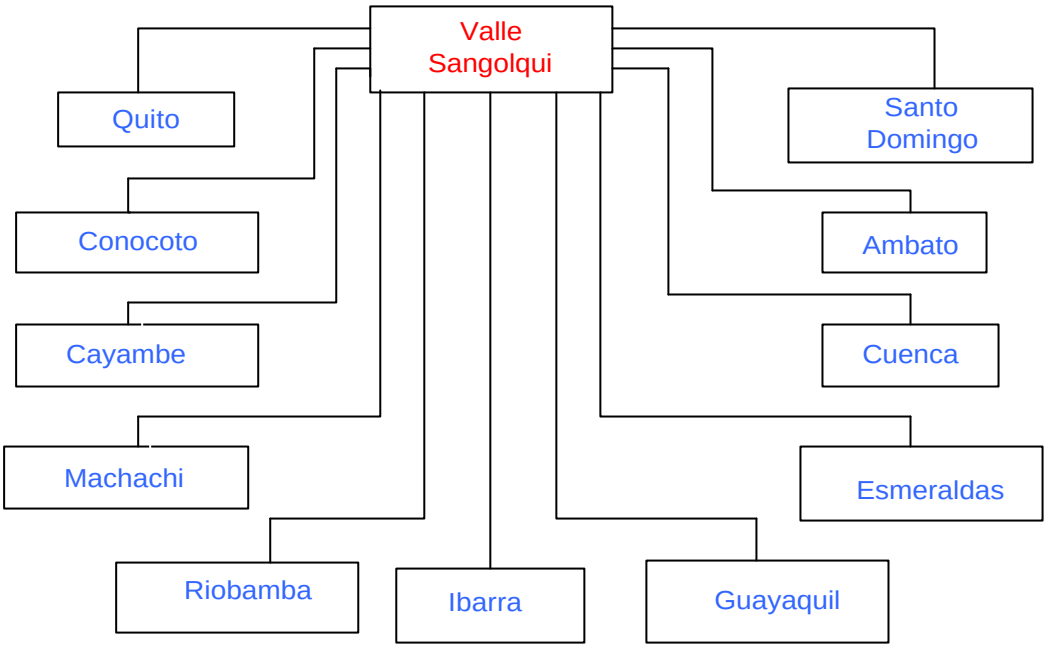


Figura. 4.5. Distribución Física del CECAI

4.3 SOLUCIÓN INTEGRAL

Necesidades del cliente:

- El CECAI necesita tener un servicio de comunicaciones con sus demás centros asociados, para un mejor control de sus procesos.
- Tener un medio de control centralizado de centros
- Reducir costos de su Sistema de Comunicaciones

Ejemplo:

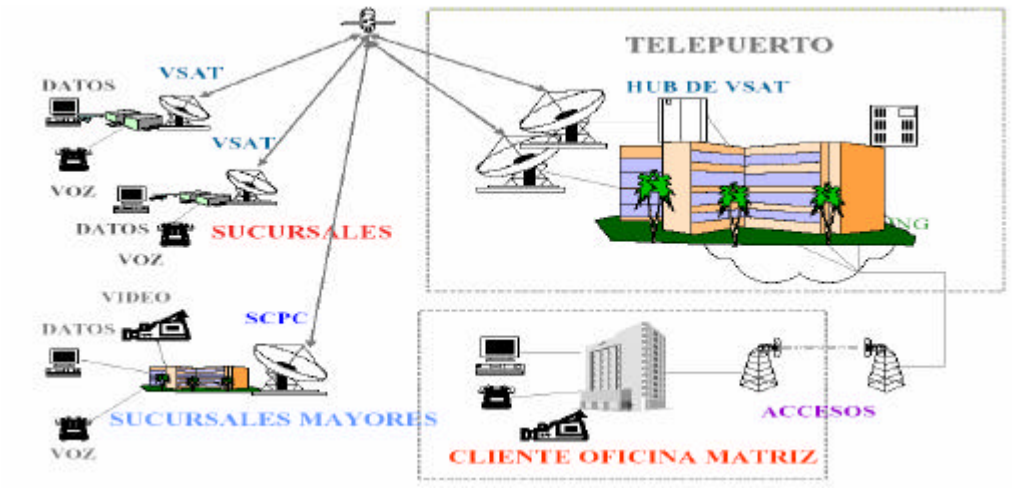


Figura. 4.6. Ejemplo de Solución

4.3.1 Requerimientos Técnicos

4.3.1.1 Evaluación de posibles soluciones

Solo haciendo el correspondiente estudio y análisis de acuerdo a las necesidades, se diseñará una solución integral de comunicación de datos, con 2 variantes, las cuales se pondrán a disposición del CECAI

Se realizarán básicamente 7 tareas para proyectar la solución más óptima en el diseño de la red WAN.

1. **Diseñar la solución más optima de una Red WAN que enlace los 20 Centros del CECAI, brindando acceso a los servicios de la red.**

Luego de un estudio del escenario, se ha determinado enlazar los distintos centros usando un servicio un servicio de Acceso a Internet como primera alternativa, como segunda opción se utilizará radio enlaces digitales para enlazar los centros asociados del CECAI

Esta Red WAN hará posible que todos los centros se conecten con la oficina principal ubicada en la Provincia de Pichincha, Sangolquí (ESPE 1) donde se encontraran ubicados los Servidores de Aplicaciones (notas, matriculas), WebMail, FTP, Proxy y otros que se podrán implementar posteriormente. Así también en la ESPE 1 se tendrá el Centro de Gestión y Administración de la Red.

2. Proveer Acceso a Internet controlado y restringido a los Centros del CECAI.

Se analizo algunas propuestas y se eligió a Andinadatos que nos brindará un acceso a Internet mediante módems ADSL que proporciona la velocidad bajada requerida y 256 kbps de velocidad de subida y además sus precios son bastante flexibles (proporcionan equipos si la empresa no los tiene).

El acceso a Internet será controlado y restringido con la implementación de un Proxy Server en cada centro. Además el Proxy Server permitirá una navegación más rápida en Internet.

3. Establecer seguridad en todos los niveles para que la red no quede expuesta a cualquier tipo de ataque o robo de información.

Para dar seguridad en todos los niveles de la red se implementará un Firewall (Cortafuegos) y una VPN (Red Privada Virtual) permitiendo que todos los datos que fluyan entre los centros lo hagan a través de una red privada sobre una red pública que es el Internet. Esta información será encriptada para lograr la seguridad requerida.

4. Brindar el servicio Web para la publicación en Internet de las notas y matriculas.

Se implementará un Web Server para la publicación de contenidos e información pública disponible en Internet y en la Intranet de los Centros.

Se deberá también contratar el servicio de refresco de DNS para evitar contratar una IP Privada cuyo costo es mucho mayor.

5. Brindar el servicio de correo electrónico para el uso interno y externo del personal del CECAI.

Se implementará un Mail Server en el cual se podrá configurar cuentas de usuario de correo electrónico para uso de todo el personal, este servicio puede ser usado en la Intranet o Internet.

6. Proveer del servicio FTP para la transferencia de archivos de gran tamaño, entre los puntos de transferencia de Información.

Se implementará un FTP Server para compartir y transferir archivos de información de gran tamaño entre los diferentes centros de la red.

4.3.1.2 Alternativa 1 – Topología de Red 1

Para el diseño de nuestra red WAN se ha tomado en cuenta los siguientes aspectos:

- La tecnología existente en el país brindada por las empresas portadoras.
- La facilidad de la obtención de esta tecnología con sus respectivos servicios y la competitividad de costos que dichas empresas ofrecen.
- El ancho de banda necesario para el intercambio tanto de datos para cada Centro del CECAI.
- La ubicación prevista en cada una de las ciudades de los distintos Centros como de la ESPE1 (Nodo Central), siendo conveniente la utilización de la tecnología instalada en todo el país.

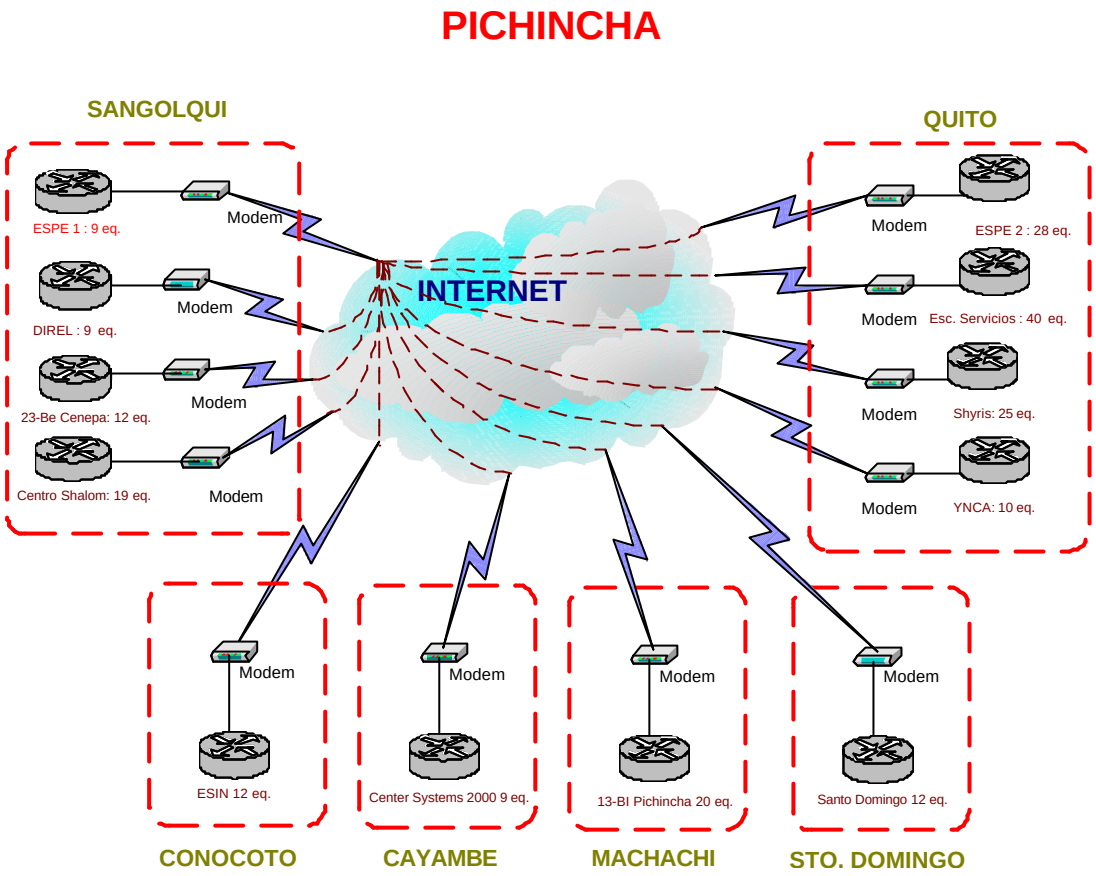


Figura. 4.7. Alternativa # 1, Pichincha

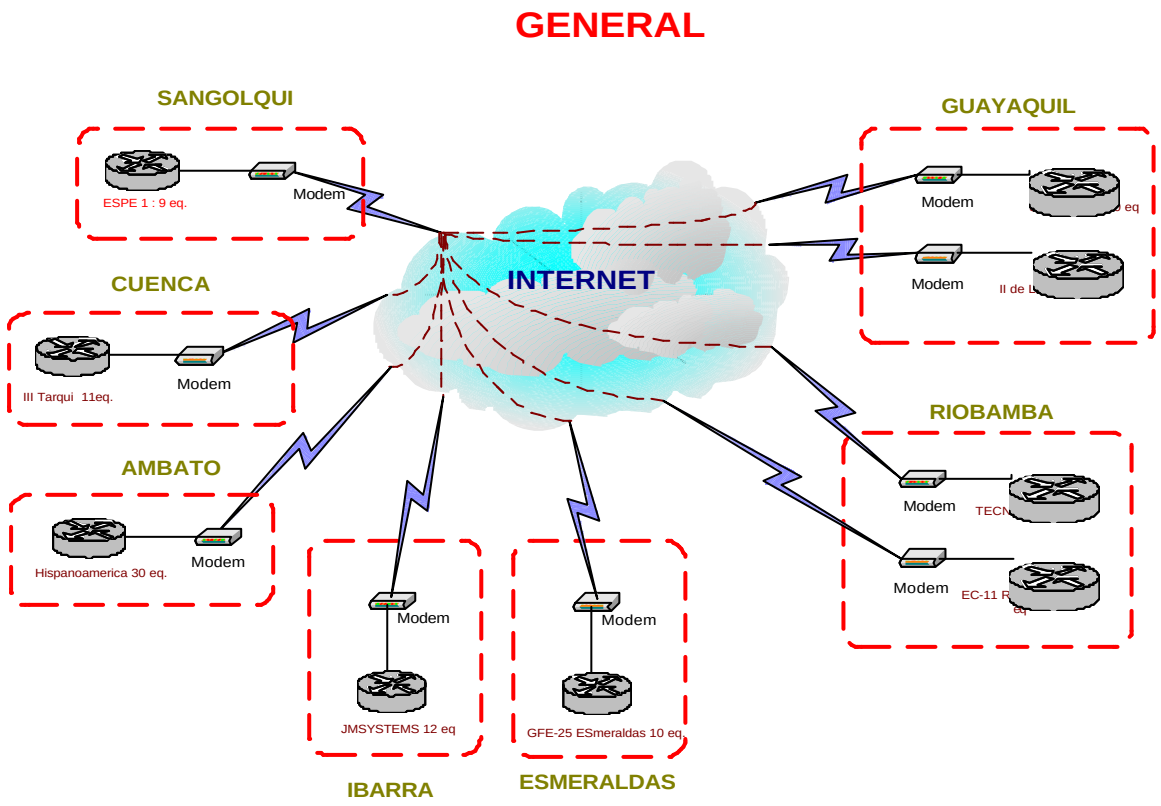


Figura. 4.8. Alternativa # 1, General

En esta solución se realizarán los enlaces usando el acceso a Internet en cada una de los Centros del CECAI, por lo tanto el costo inicial será menor por cuanto no se requerirá la compra de equipos de comunicación mas que los necesarios para el acceso a Internet. Sin embargo se deberá contratar este servicio en los 20 puntos a interconectar.

4.3.1.2.1 Ancho de Banda Necesario

Para calcular el tráfico de la red analizamos las distintas dependencias y sus requerimientos. Para que el tráfico que circula por la red sea eficiente, a cada equipo se le asignará 10Kbps:

- Provincia de Pichincha:
  - ESPE 1: 9 equipos = 9 * 10Kbps = 90Kbps, debido a que este es el nodo central de la red, donde se encuentran los servidores se estima un Ancho de Banda de 2048Kbps.
  - ESPE 2: 28 equipos = 28 * 10Kbps = 280Kbps, a contratar 512Kbps
  - Escuela de Servicios: 40 equipos = 40 * 10Kbps = 400Kbps, a contratar 512Kbps
  - 13-BI Pichincha: 20 equipos = 20 * 10Kbps = 200Kbps, a contratar 256Kbps
  - Santo Domingo: 12 equipos = 12 * 10Kbps = 120Kbps, a contratar 128Kbps
  - DIREL: 9 equipos = 9 * 10Kbps = 90Kbps, a contratar 128Kbps
  - Center Systems 2000: 9 equipos = 9 * 10Kbps = 90Kbps, a contratar 128Kbps
  - 23-BE Cenepa: 12 equipos = 12 * 10Kbps = 120Kbps, a contratar 128Kbps
  - I-DE Shyris: 25 equipos = 25 * 10Kbps = 250Kbps, a contratar 256Kbps
  - Centro de Computo “Shalom”: 19 equipos = 19 * 10Kbps = 190Kbps, a contratar 256Kbps
  - YNCA: 10 equipos = 10 * 10Kbps = 100Kbps, a contratar 128Kbps

- ESIN: 12 equipos = 12 * 10Kbps = 120Kbps, a contratar 128Kbps

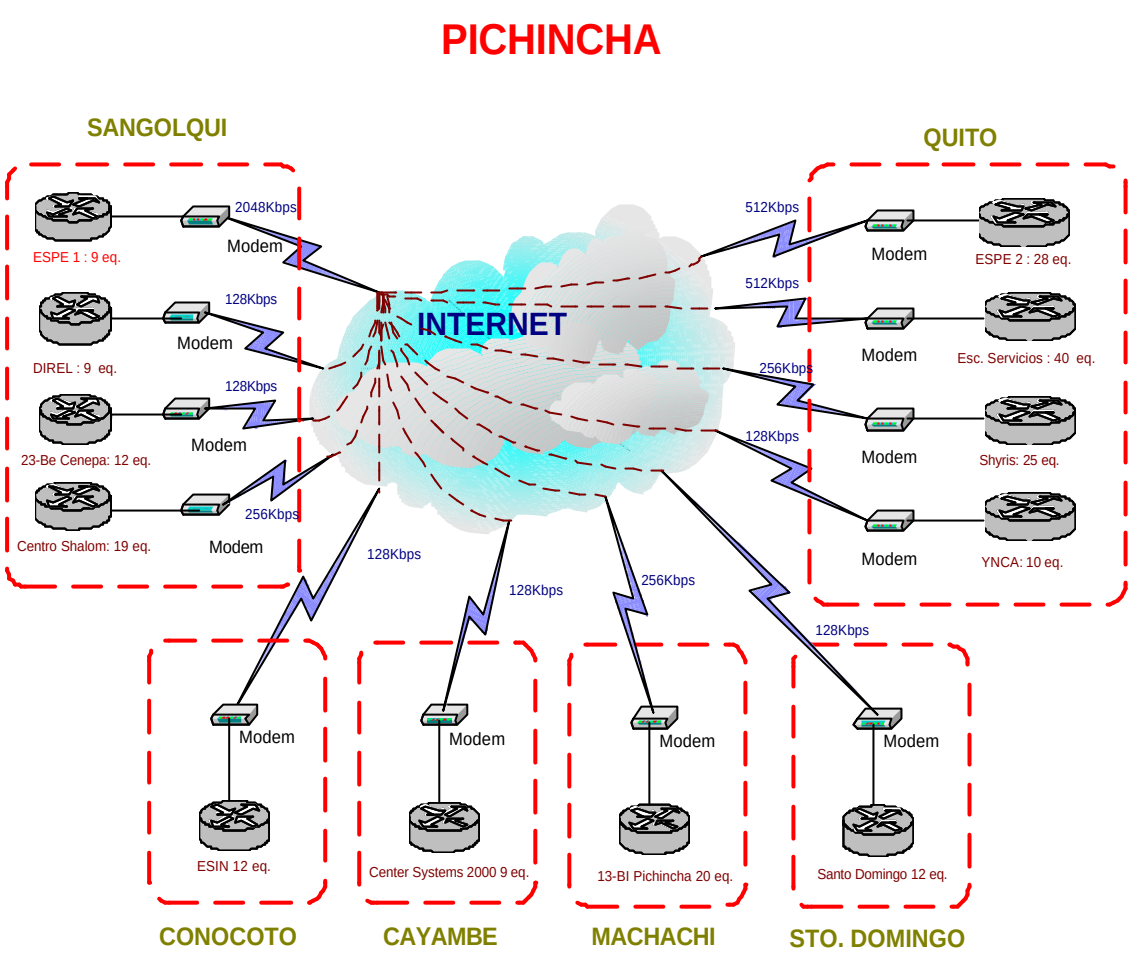


Figura. 4.9. Alternativa # 1, Pichincha Completo

- Provincia del Azuay:
  - III de Tarqui: 11 equipos = 11 * 10Kbps = 110Kbps, a contratar 128Kbps

- Provincia del Chimborazo:
  - Tecniexito: 17 equipos = 17 * 10Kbps = 170Kbps, a contratar 256Kbps
  - EC-11 “Riobamba”: 10 equipos = 10 * 10Kbps = 100Kbps, a contratar 128Kbps

- Provincia del Guayas:
  - 5-BI Guayas: 10 equipos = 10 * 10Kbps = 100Kbps, a contratar 128Kbps
  - II- DE Libertad: 10 equipos = 10 * 10Kbps = 100Kbps, a contratar 128Kbps

- Provincia de Tungurahua:
  - Hispanoamérica: 30 equipos = 30 * 10Kbps = 300Kbps, a contratar 512Kbps

- Provincia de Imbabura:
  - JMSYSTEMS: 12 equipos = 12 * 10Kbps = 120Kbps, a contratar 128Kbps

- Provincia de Esmeraldas:
  - GFE-25 Esmeraldas: 10 equipos = 10 * 10Kbps = 100Kbps, a contratar 128Kbps

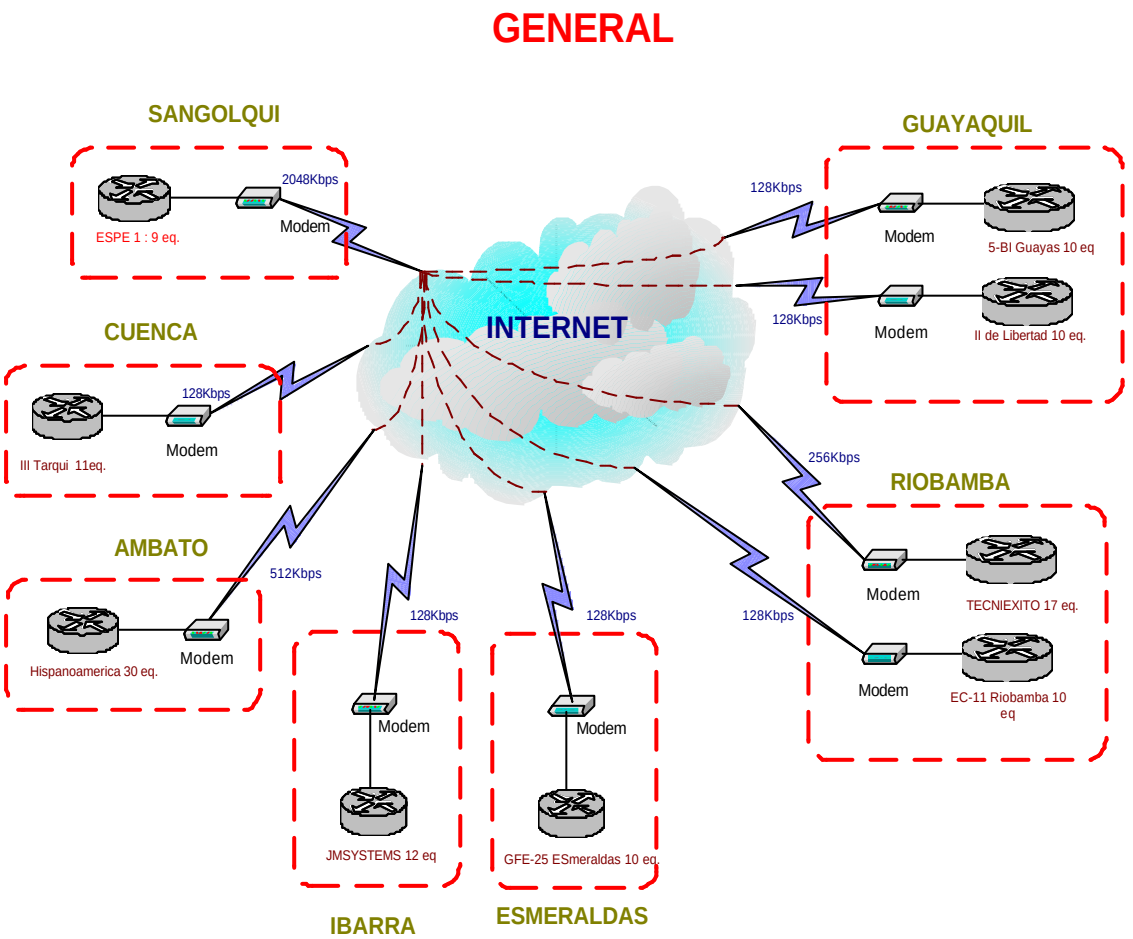


Figura. 4.10. Alternativa # 1, General Completo

4.3.1.2.2 Servidores

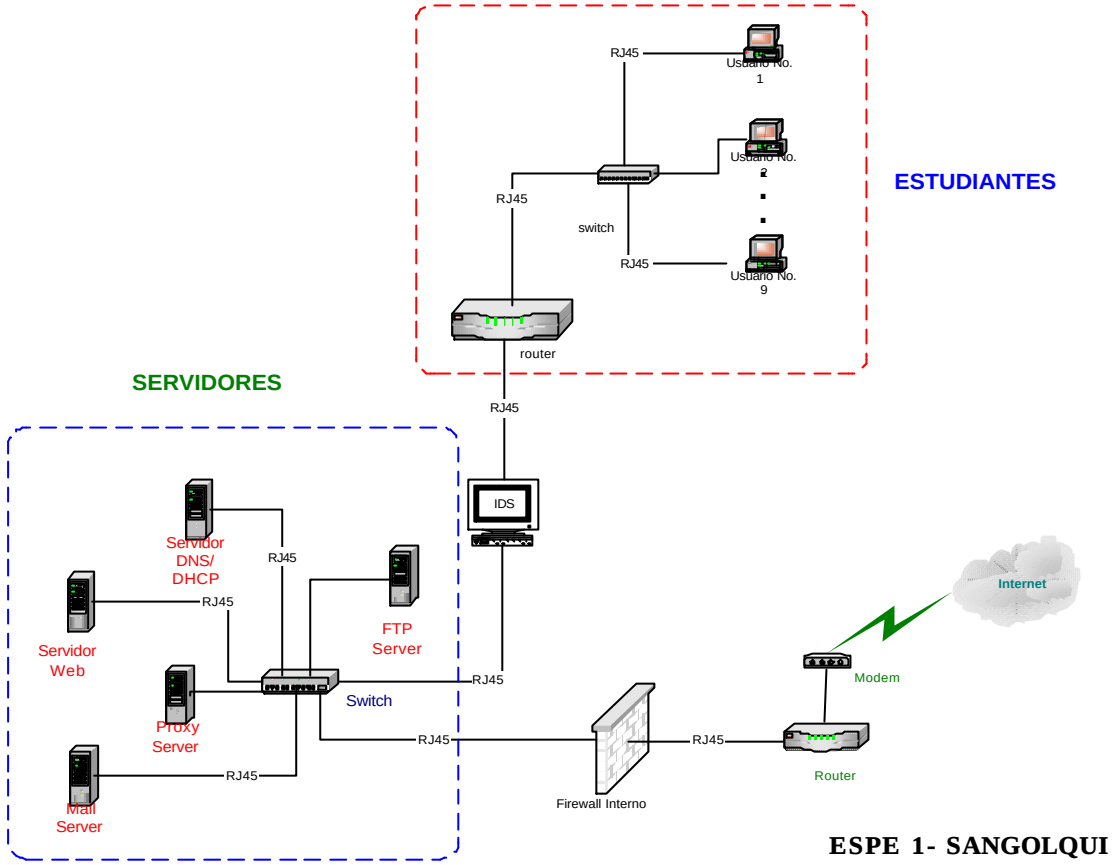


Figura. 4.10. a. Servidores

4.3.1.2.3 Protocolos Utilizados en el Nodo Central

Servidor Web: Tiene servidor de correo electrónico, servidor Proxy para dar servicio de Internet a los demás usuarios, servidor de DHCP para la asignación dinámica de direcciones IP del Modem para adentro y a través de un esquema de ruteo.

TCP

- FTP: Para transferencia y copiado de archivos con autenticación
- SMTP: para la transmisión de correo simple
- POP3: para la recepción de correo simple

UDP

- SNMP: para la administración de la red

- DNS: Traduce la dirección IP a un nombre significativo de alto nivel.

Servidores Internos: Tienen servidor de DHCP para asignar direcciones IP dinámicas a la red interna de la ESPE1, servidor de transferencia de correo electrónico, aplicaciones especificas de Notas de Alumnos, aplicaciones especificas de Servicio de Matriculas y de información en general.

Los cinco servidores estarán bajo el sistema operativo LINUX ya que este es más seguro y confiable que los sistemas operativos de Microsoft.

Además, para la organización del cableado estructurado se deberán contar de:

- 1 switch de 24 puertos para la conectividad de los 9 equipos que se encuentran en el Centro ESPE1, No usamos 1 de 16 porque no tendríamos puertos libres para un futuro.
- 1 switch de 24 puertos para la conectividad de los Firewall interno y externo, y para la conectividad de los cinco servidores internos
- 2 routers, uno con un puerto ADSL y un puerto LAN para salir a la nube del Internet.

4.3.1.3 Alternativa 2 – Topología de Red 2

La interconexión de las diferentes localidades (Centros Asociados), los cuales están ubicados en las ciudades de Ibarra, Cayambe, Quito, Sangolquí, Machachi, Latacunga, Ambato y Riobamba, dando un total de 8 centros, (los más importantes).

Este proyecto se logrará utilizando equipos de radio enlace digital que permiten transmitir datos a alta velocidad. Asimismo, se requiere líneas de vista para lo cual se ha realizado un estudio preliminar del terreno.

En el proyecto, el Sistema de Radio Enlace permitirá que 8 localidades estén interconectadas las 24 horas del día, los 365 días del año, utilizando infraestructura propia y, por lo tanto, teniendo mínimos costos de mantenimiento mensual.

El uso de esta tecnología permitirá conectar toda una red de computadoras en cada una de los Centros mencionadas, que se interconectarán a velocidades que estarán en el rango

de 128Kbps y 2Mbps. Así, cada una de los Centros podrá aumentar el número de computadoras sin necesidad de cambiar el tipo de conexión que existe entre ellas.

El acceso a Internet para los Centros interconectadas por radio enlace se logrará alquilando una conexión de gran ancho de banda en uno de los puntos de la red que será el la ESPE1. Esta única conexión dará acceso a los 8 Centros del CECAI que se están utilizando en este estudio para la alternativa # 2

Para la implementación del Sistema de Radio Enlace es indispensable que en cada una de los Centros se instale una torre de elevación en la cual se colocará la antena direccionada a algún punto de la red. En promedio, la altura de las torres que se instalarán es de 10m.

4.3.1.3.1 Cálculo del Enlace De Microonda Digital

Esta alternativa se basa en el diseño de un radio-enlace de telecomunicaciones digitales en la banda de microondas.

- Capacidad: Un SMT-1 (34Mbps) que tiene una capacidad de 1840 canales.
- Banda de microondas: 6.175GHz (5925MHz – 7110MHz)

4.3.1.3.2 Recopilación de Datos

Planos topográficos del Instituto Geográfico Militar de las distintas zonas en estudio con escala 1:50.000

4.3.1.3.2.1 Coordenadas Geográficas

- Ibarra:
  - Latitud: 0º 21’ 29" N
  - Longitud: 78º 06’ 41" W
  - Altura: 2228 m
- Cayambe:
  - Latitud: 0º 02’ 34" N
  - Longitud: 78º 08’ 26" W
  - Altura: 2960 m
- Quito:
  - Latitud: 0º 08’ 20" S

- Longitud: 78º 28’ 36" W
- Altura: 2850 m

- Sangolquí:
  - Latitud: 0º 19’ 31" S
  - Longitud: 78º 26’ 48" W
  - Altura: 2545 m
- Machachi:
  - Latitud: 0º 30’ 48" S
  - Longitud: 78º 32’ 59" W
  - Altura: 2880 m
- Latacunga:
  - Latitud: 0º 56’ 3" S
  - Longitud: 78º 37’ 45" W
  - Altura: 2800 m
- Ambato:
  - Latitud: 1º 14’ 09" S
  - Longitud: 78º 36’ 25" W
  - Altura: 2600 m
- Riobamba:
  - Latitud: 1º 39’ 47" S
  - Longitud: 78º 39’ 02" W
  - Altura: 2754 m

4.3.1.3.2.2 Cálculo de la Longitud de Cada Trayecto

$$D = \sqrt{(\Delta Long * 111.32)^2 + (\Delta Lat * 111.32)^2 + (\Delta h)^2}$$

Ibarra-Cayambe:

$$\Delta Long = Long(Cayambe) - Long(Ibarra)$$
$$= 78.14° - 78.11° = 0.03° \Rightarrow 0°1'48"$$

$$\Delta Lat = Lat(Cayambe) - Lat(Ibarra)$$
$$= 0.35° - 0.042° = 0.31° \Rightarrow 0°18'36"$$

$$\Delta h = h(Cayambe) - h(Ibarra)$$
$$= 2950m - 2228m$$
$$= 722m \Rightarrow 0.722Km.$$

$$D = \sqrt{(0.03*111.32)^2 + (0.31*111.32)^2 + (0.722)^2}$$
$$D = 34.67Km.$$

Cayambe-Quito:

$$\Delta Long = Long(Cayambe) - Long(Quito)$$
$$= 78.47° - 78.14° = 0.33° \Rightarrow 0°19'48"$$

$$\Delta Lat = Lat(Cayambe) - Lat(Quito)$$
$$= 0.35° - 0.13° = 0.22° \Rightarrow 0°13'12"$$

$$\Delta h = h(Cayambe) - h(Quito)$$
$$= 2950m - 2850m$$
$$= 100m \Rightarrow 0.100Km.$$

$$D = \sqrt{(0.33*111.32)^2 + (0.22*111.32)^2 + (0.100)^2}$$
$$D = 44.15Km.$$

Quito-Sangolquí:

$$\Delta Long = Long(Quito) - Long(Sangolquí)$$
$$= 78.47° - 78.44° = 0.03° \Rightarrow 0°1'48"$$

$$\Delta Lat = Lat(Quito) - Lat(Sangolquí)$$
$$= 0.13° - 0.32° = 0.19° \Rightarrow 0°11'24"$$

$$\Delta h = h(Quito) - h(Sangolquí)$$
$$= 2850m - 2545m$$
$$= 305m \Rightarrow 0.305Km.$$

$$D = \sqrt{(0.03*111.32)^2 + (0.19*111.32)^2 + (0.305)^2}$$
$$D = 21.41Km.$$

Sangolquí-Machachi:

$$\Delta Long = Long(Sangolquí) - Long(Machachi)$$
$$= 78.44° - 78.54° = 0.10° \Rightarrow 0°6'00"$$

$$\Delta Lat = Lat(Sangolquí) - Lat(Machachi)$$
$$= 0.32° - 0.51° = 0.19° \Rightarrow 0°11'24"$$

$$\Delta h = h(Sangolquí) - h(Machachi)$$
$$= 2545m - 2880m$$
$$= 335m \Rightarrow 0.335Km.$$

$$D = \sqrt{(0.10 * 111.32)^2 + (0.19 * 111.32)^2 + (0.335)^2}$$
$$D = 23.90Km.$$

Machachi-Latacunga:

$$\Delta Long = Long(Machachi) - Long(Latacunga)$$
$$= 78.54° - 78.62° = 0.08° \Rightarrow 0°4'48"$$

$$\Delta Lat = Lat(Machachi) - Lat(Latacunga)$$
$$= 0.51° - 0.93° = 0.42° \Rightarrow 0°25'12"$$

$$\Delta h = h(Machachi) - h(Latacunga)$$
$$= 2880m - 2800m$$
$$= 80m \Rightarrow 0.080Km.$$

$$D = \sqrt{(0.08 * 111.32)^2 + (0.42 * 111.32)^2 + (0.080)^2}$$
$$D = 47.59Km.$$

Latacunga-Ambato:

$$\Delta Long = Long(Latacunga) - Long(Ambato)$$
$$= 78.62° - 78.60° = 0.02° \Rightarrow 0°1'12"$$

$$\Delta Lat = Lat(Latacunga) - Lat(Ambato)$$
$$= 0.93° - 1.23° = 0.30° \Rightarrow 0°18'00"$$

$$\Delta h = h(Latacunga) - h(Ambato)$$
$$= 2800m - 2600m$$
$$= 200m \Rightarrow 0.200Km.$$

$$D = \sqrt{(0.02 * 111.32)^2 + (0.30 * 111.32)^2 + (0.200)^2}$$
$$D = 33.47Km.$$

Ambato-Riobamba:

$$\Delta Long = Long(Ambato) - Long(Riobamba)$$
$$= 78.60° - 78.65° = 0.05° \Rightarrow 0°3'00"$$

$$\Delta Lat = Lat(Ambato) - Lat(Riobamba)$$
$$= 1.23° - 1.66° = 0.43° \Rightarrow 0°25'48''$$

$$\Delta h = h(Ambato) - h(Riobamba)$$
$$= 2600m - 2754m$$
$$= 154m \Rightarrow 0.154Km.$$

$$D = \sqrt{(0.05*111.32)^2 + (0.43*111.32)^2 + (0.154)^2}$$
$$D = 48.19Km.$$

Enlace	Distancia
1. Ibarra-Cayambe	34.67 Km.
2. Cayambe-Quito	44.15 Km.
3. Quito-Sangolquí	21.41 Km.
4. Sangolquí-Machachi	23.90 Km.
5. Machachi-Latacunga	47.59 Km.
6.Latacunga-Ambato	33.47 Km.
7. Ambato-Riobamba	48.19 Km.

Tabla. 4.1. Enlaces y Distancias

4.3.1.3.2.3 Mapas de Perfiles

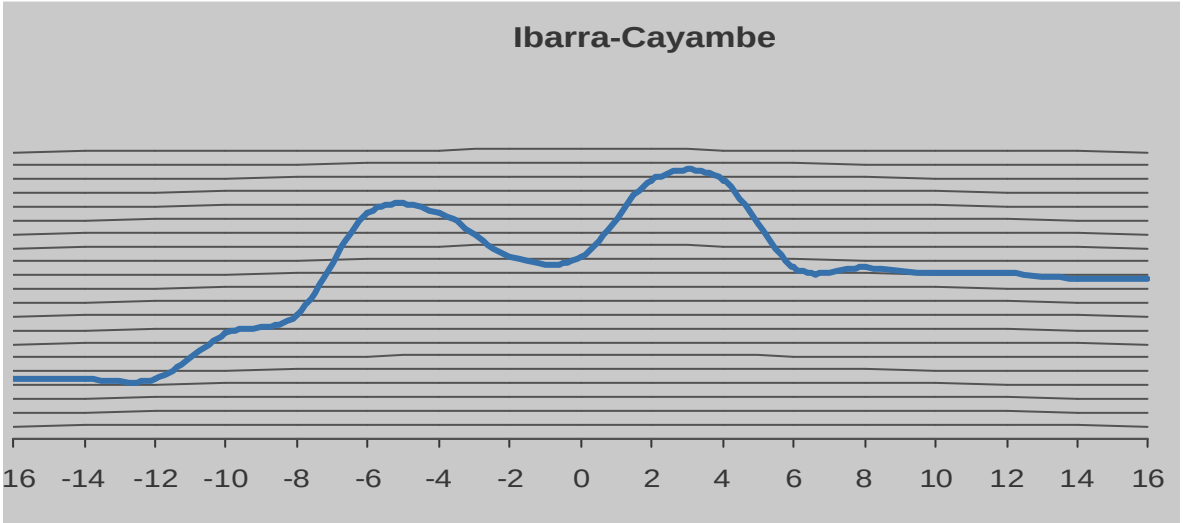


Figura. 4.11. Perfil Ibarra-Cayambe

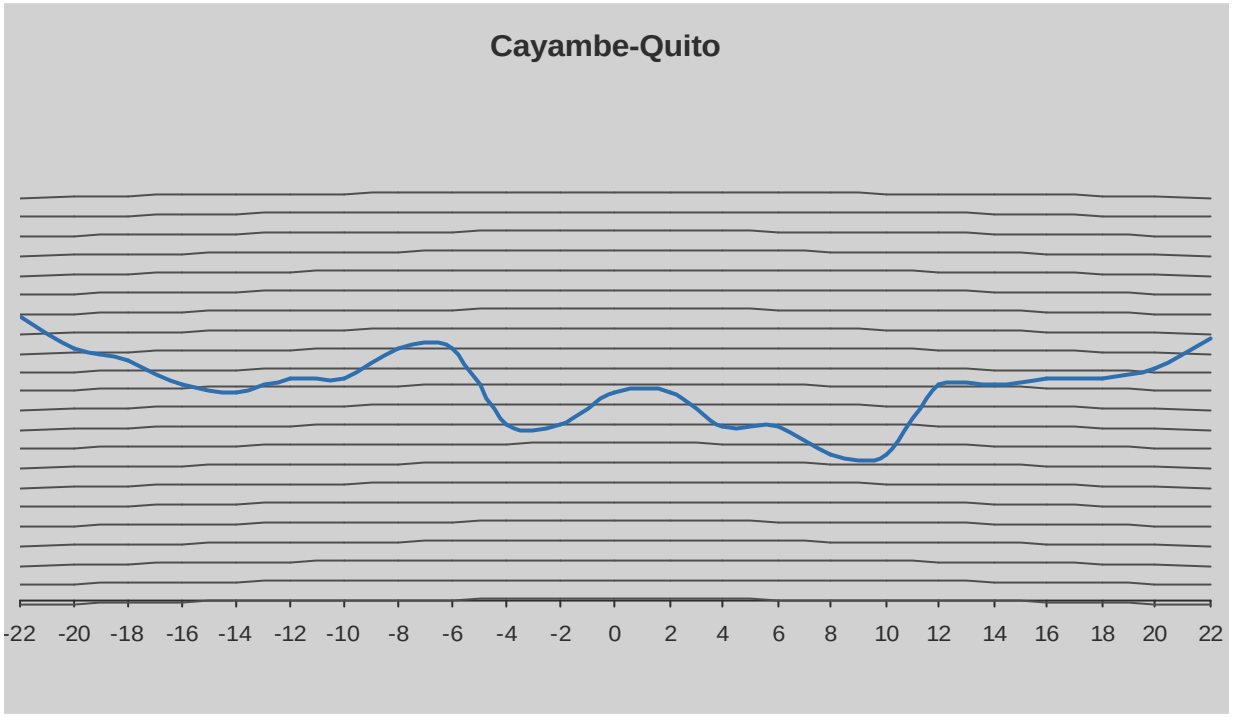


Figura. 4.12. Perfil Cayambe-Quito

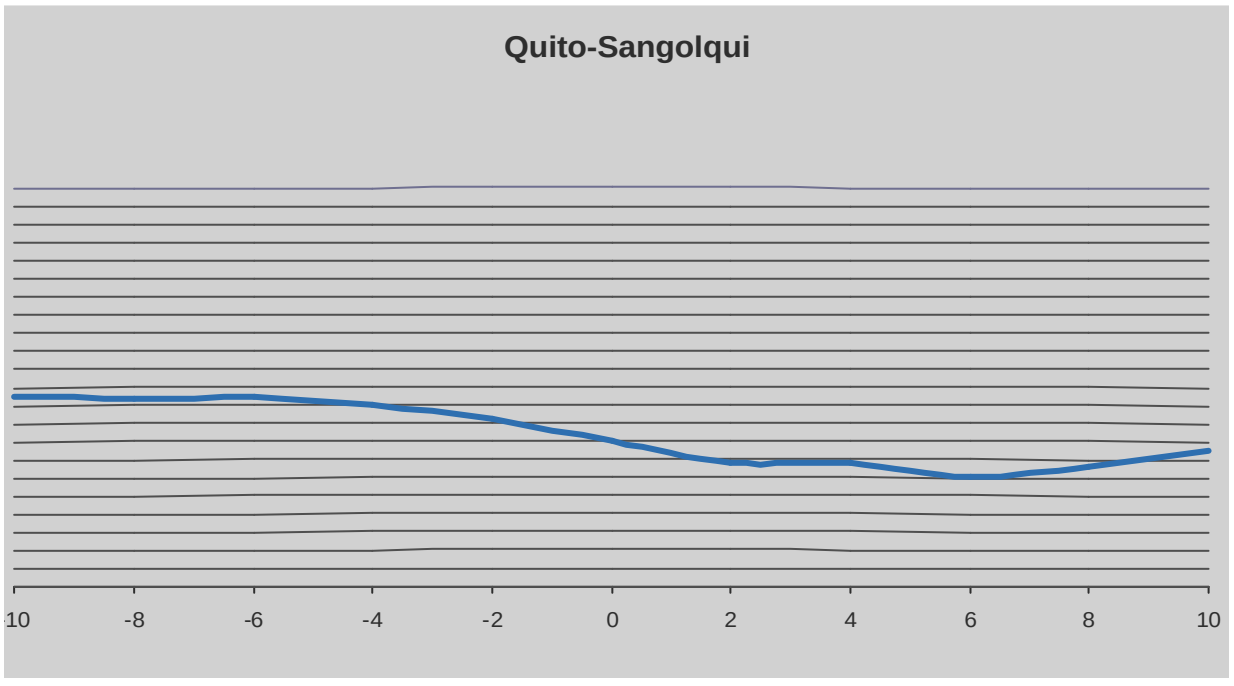


Figura. 4.13. Perfil Quito-Sangolquí

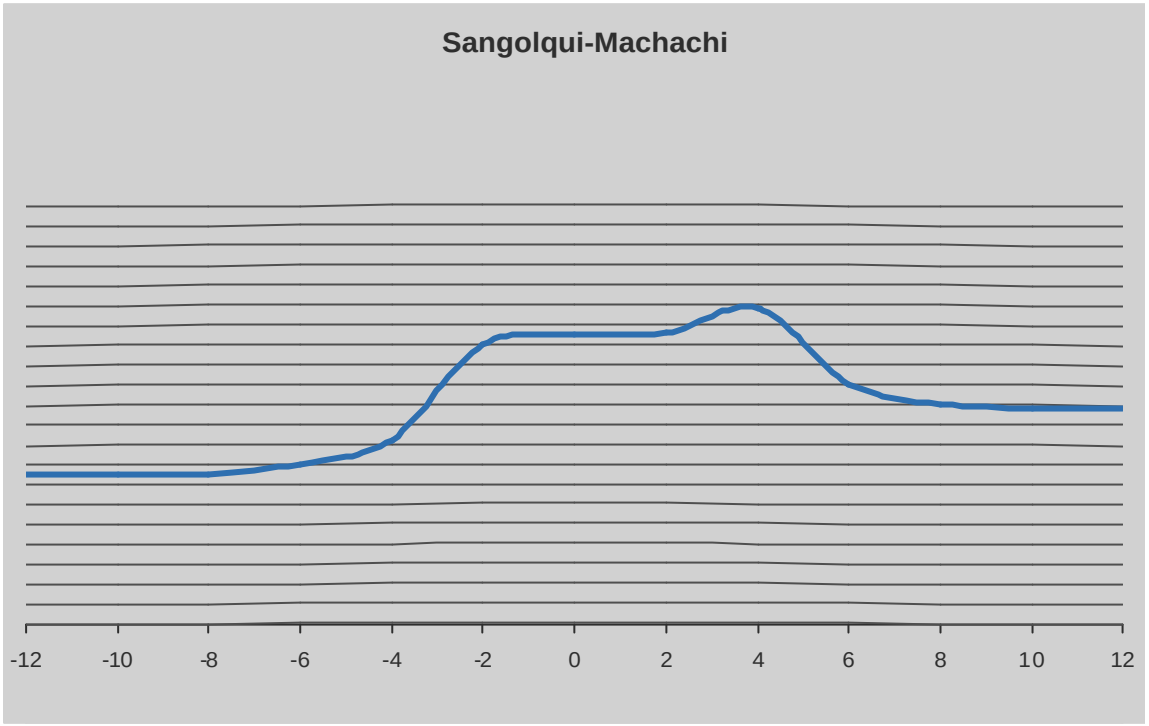


Figura. 4.14. Perfil Sangolquí-Machachi

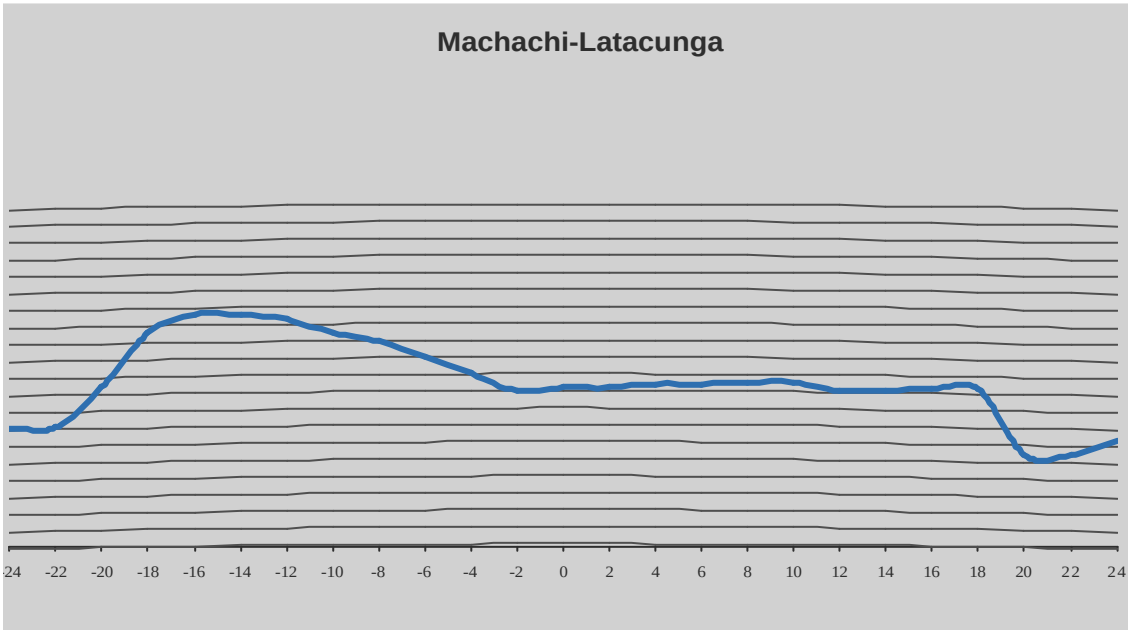


Figura. 4.15. Perfil Machachi-Latacunga

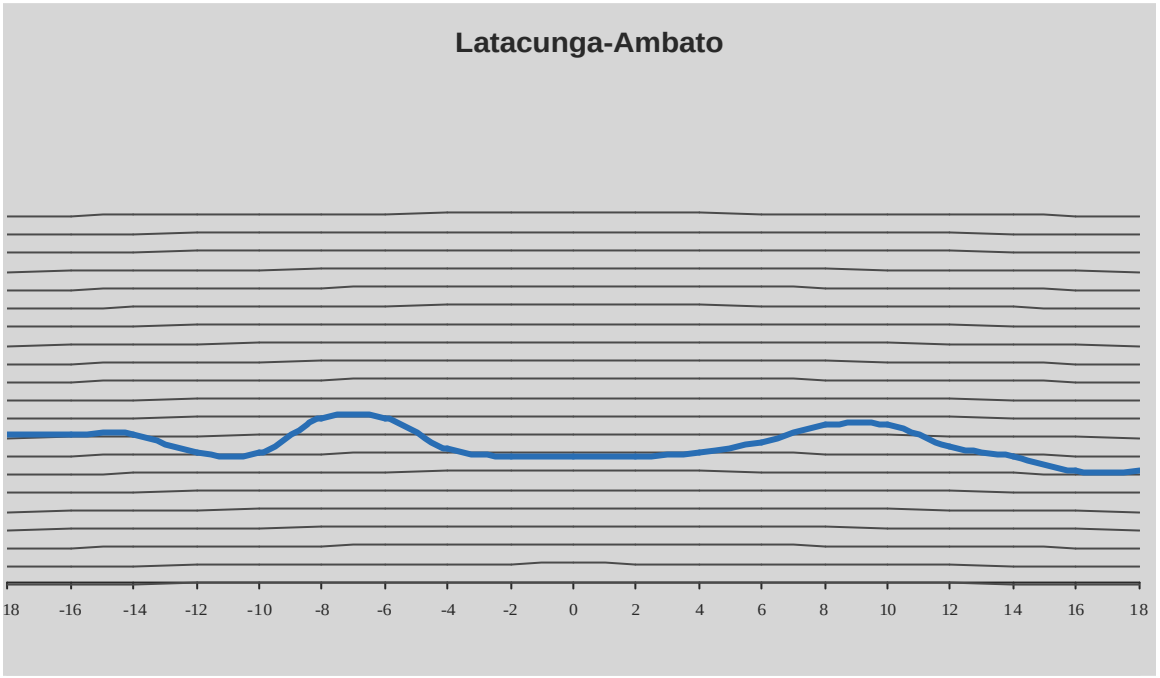


Figura. 4.16. Perfil Latacunga-Ambato

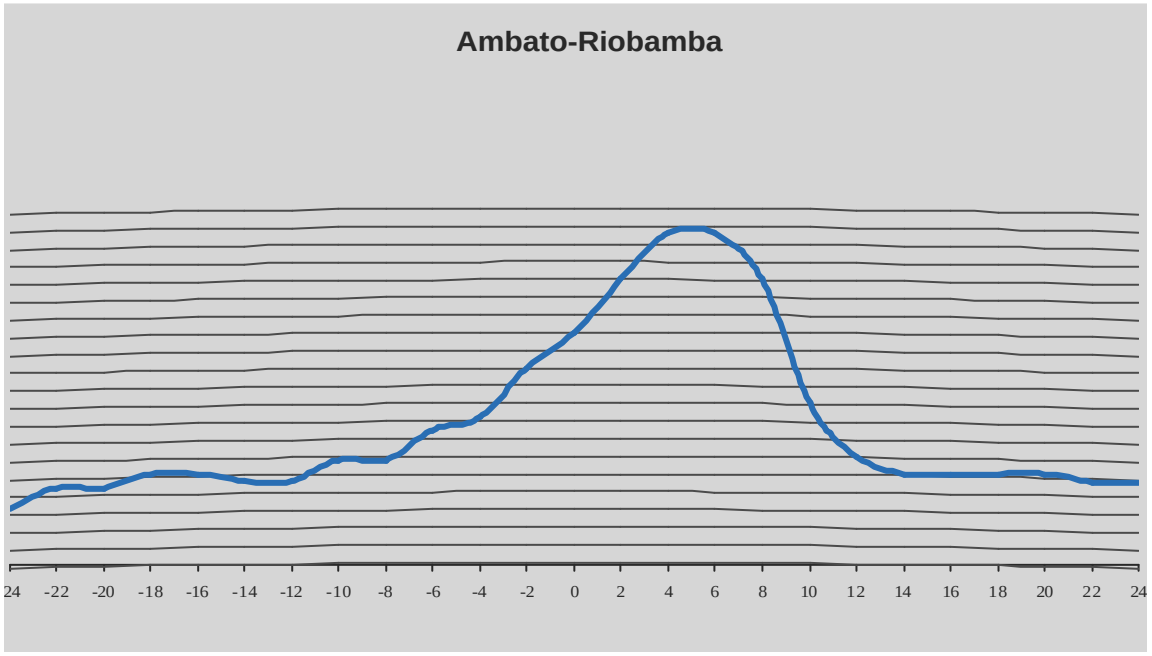


Figura. 4.17. Perfil Ambato-Riobamba

Parámetros	Potencia
1. Equipo	0.75 W
2. Ganancia de Antena	38.9 dB
3. Atenuación por Cables	2.7 dB
Potencia Total Radiada	**34.95 dB**

Tabla. 4.2. Potencia Radiada

Con estos parámetros procedemos a calcular las pérdidas por obstáculos ya que en algunos enlaces no existe línea de vista, teniendo como referencia los 38.5 dBµV/m de campo electromagnético como nivel mínimo para que exista enlace.

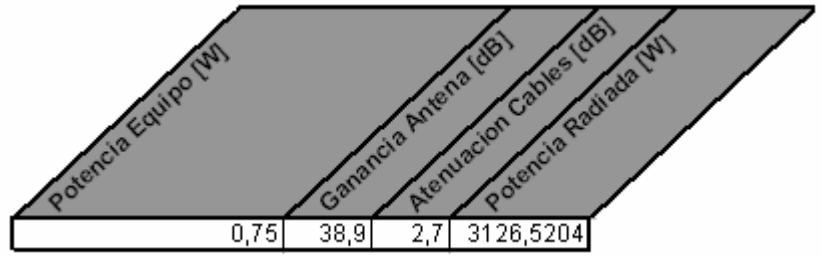
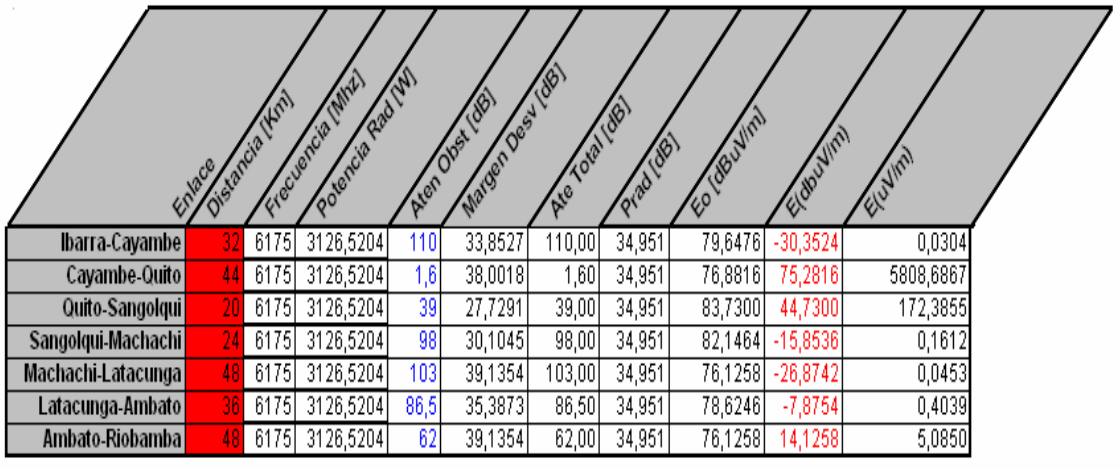


Figura. 4.18. Parámetros Considerados

Frecuencia = 6175 MHz.



Enlace	Distancia [Km]	Frecuencia [Mhz]	Potencia Rad [W]	Aten Obst [dB]	Margen Desv [dB]	Ate Total [dB]	Prad [dB]	Eo [dBuV/m]	E(dbuV/m)	E(uV/m)
Ibarra-Cayambe	32	6175	3126,5204	110	33,8527	110,00	34,951	79,6476	-30,3524	0,0304
Cayambe-Quito	44	6175	3126,5204	1,6	38,0018	1,60	34,951	76,8816	75,2816	5808,6867
Quito-Sangolqui	20	6175	3126,5204	39	27,7291	39,00	34,951	83,7300	44,7300	172,3855
Sangolqui-Machachi	24	6175	3126,5204	98	30,1045	98,00	34,951	82,1464	-15,8536	0,1612
Machachi-Latacunga	48	6175	3126,5204	103	39,1354	103,00	34,951	76,1258	-26,8742	0,0453
Latacunga-Ambato	36	6175	3126,5204	86,5	35,3873	86,50	34,951	78,6246	-7,8754	0,4039
Ambato-Riobamba	48	6175	3126,5204	62	39,1354	62,00	34,951	76,1258	14,1258	5,0850

Figura. 4.19. Cálculo del Campo Electromagnético

Como resultado de estos valores de E(dbµV/m), tenemos que no hay enlace en:

- Ibarra-Cayambe
- Sangolquí-Machachi
- Machachi-latacunga
- Latacunga-Ambato
- Ambato-Riobamba

Por lo cual se procede a instalar repetidores en los siguientes lugares para que no exista interferencia en la señal, por lo tanto que exista línea de vista:

- Repetidor Ibarra-Cayambe:
  - Latitud: 0º 13’ 56" N
  - Longitud: 78º 05’ 37" W
  - Altura: 3304 m

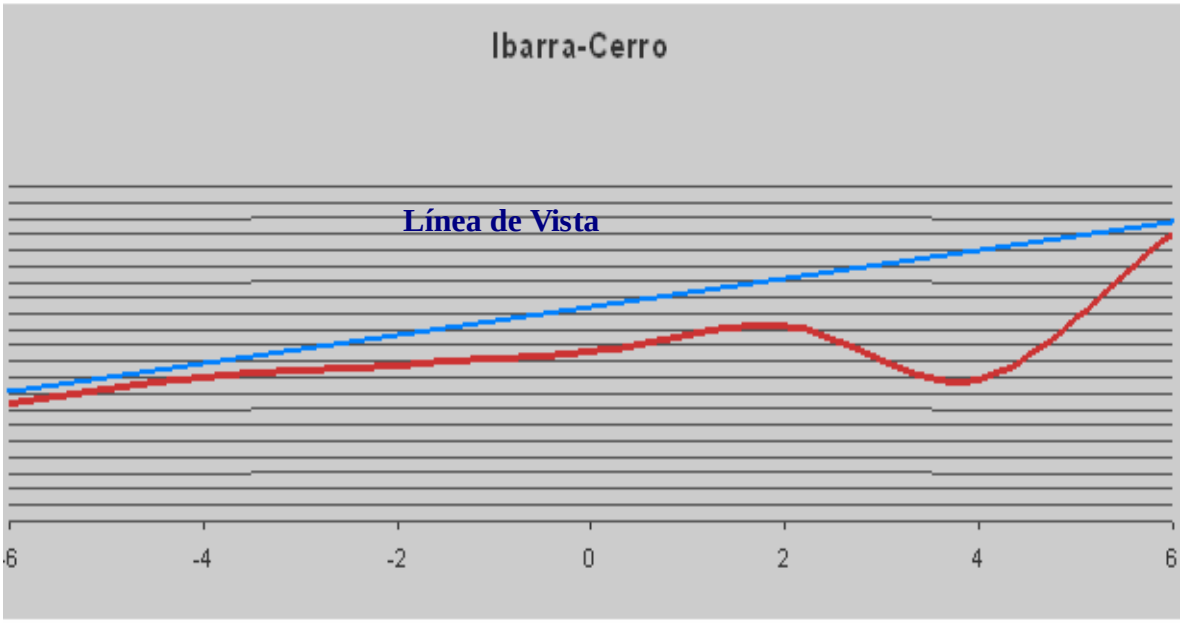


Figura. 4.20. Perfil Ibarra-Cerro

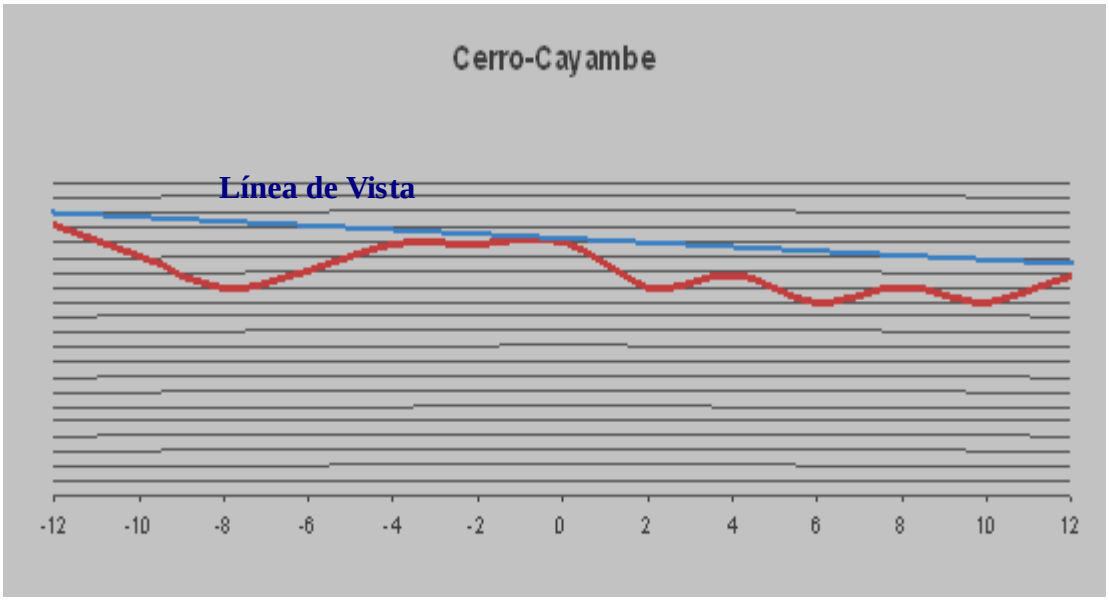


Figura. 4.21. Perfil Cerro-Cayambe

- Repetidor Sangolquí- Machachi:
  - Latitud: 0º 26’ 37" S
  - Longitud: 78º 30’ 42" W
  - Altura: 3382 m

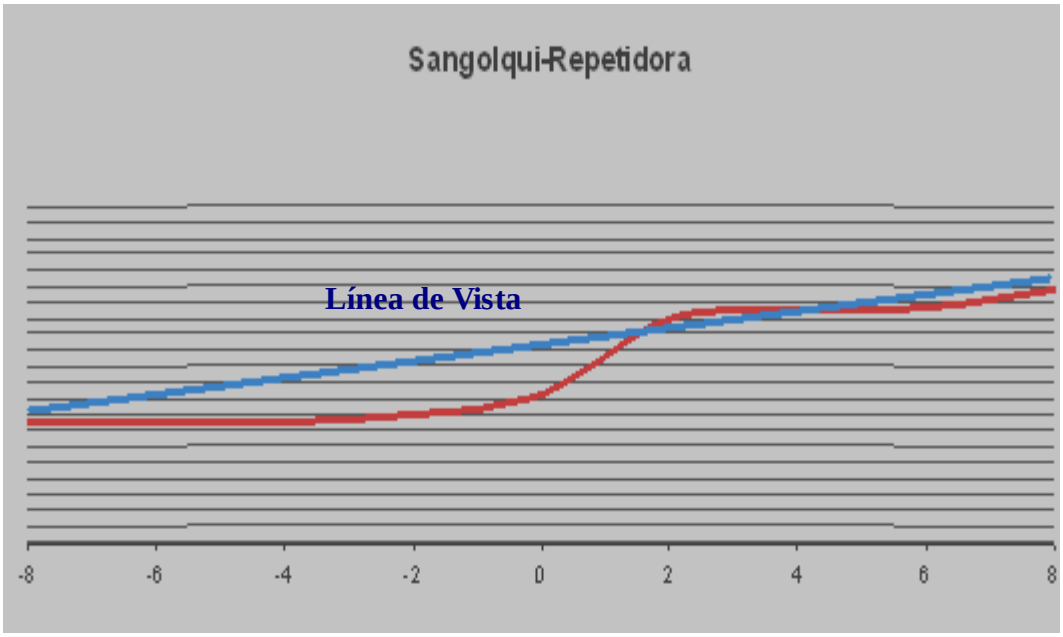


Figura. 4.22. Perfil Sangolquí-Repetidora

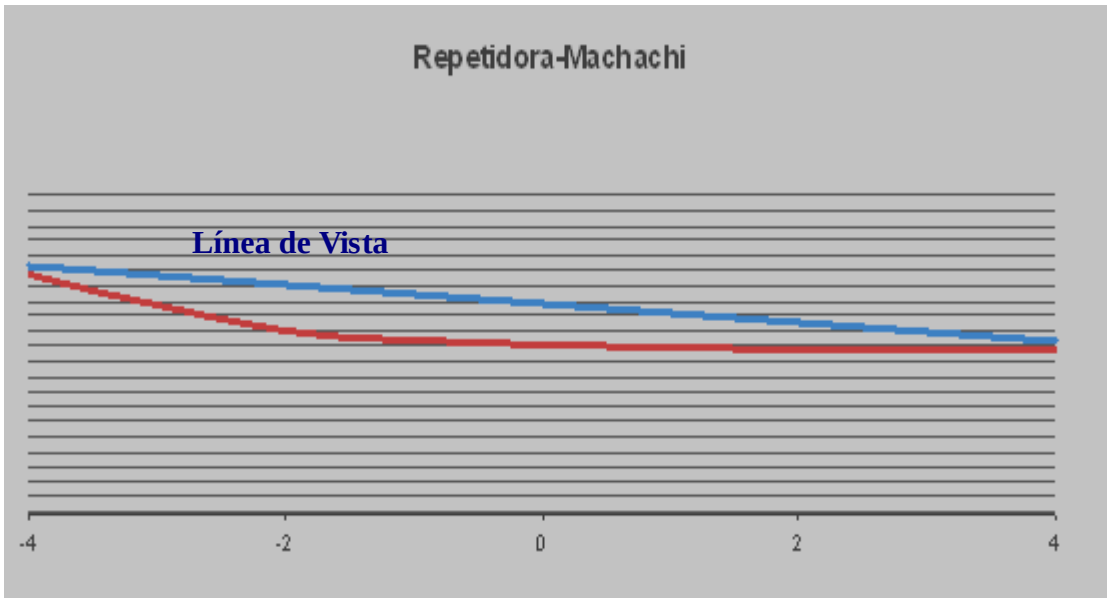


Figura. 4.23. Perfil Repetidora-Machachi

- Repetidor Machachi- Latacunga:
  - Latitud: 0º 35’ 57" S
  - Longitud: 78º 32’ 34" W
  - Altura: 3920 m

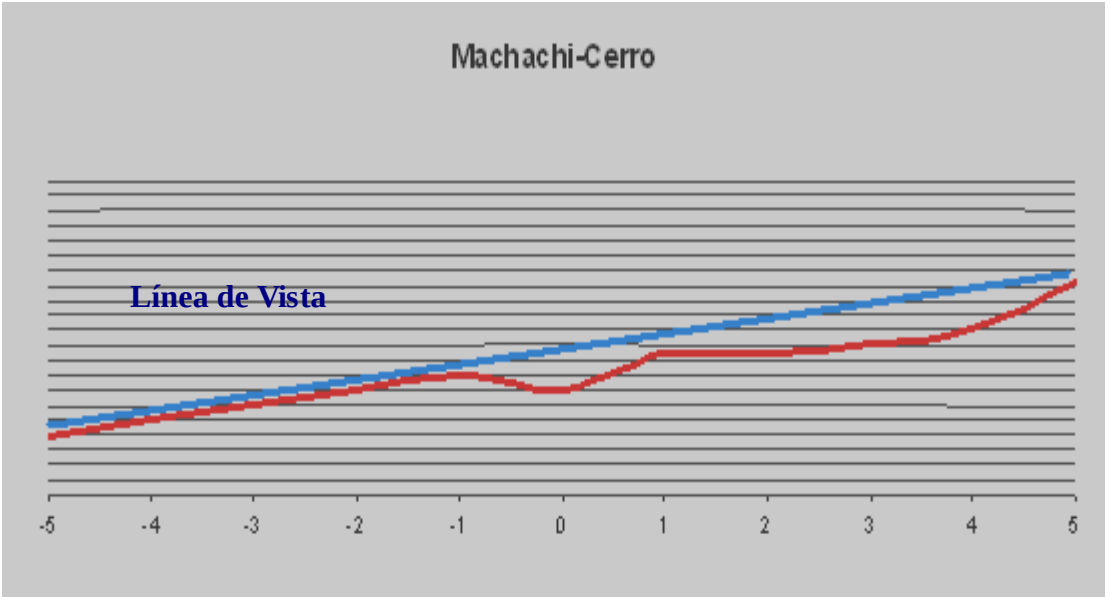


Figura. 4.24. Perfil Machachi-Cerro

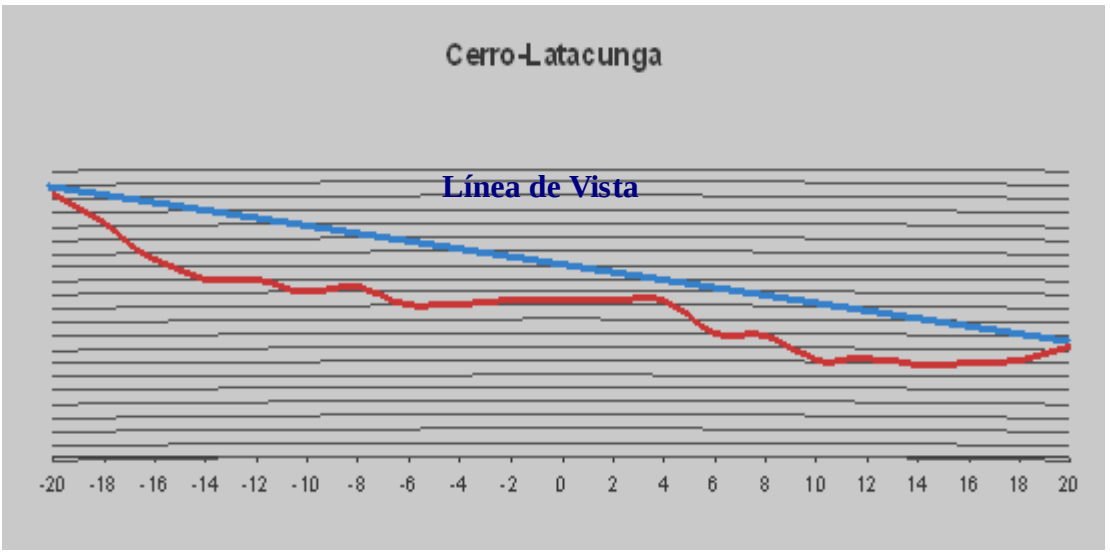


Figura. 4.25. Perfil Cerro-Latacunga

- Repetidor Latacunga-Ambato:
  - Latitud: 0º 21’ 29" S
  - Longitud: 78º 06’ 41" W
  - Altura: 2800 m

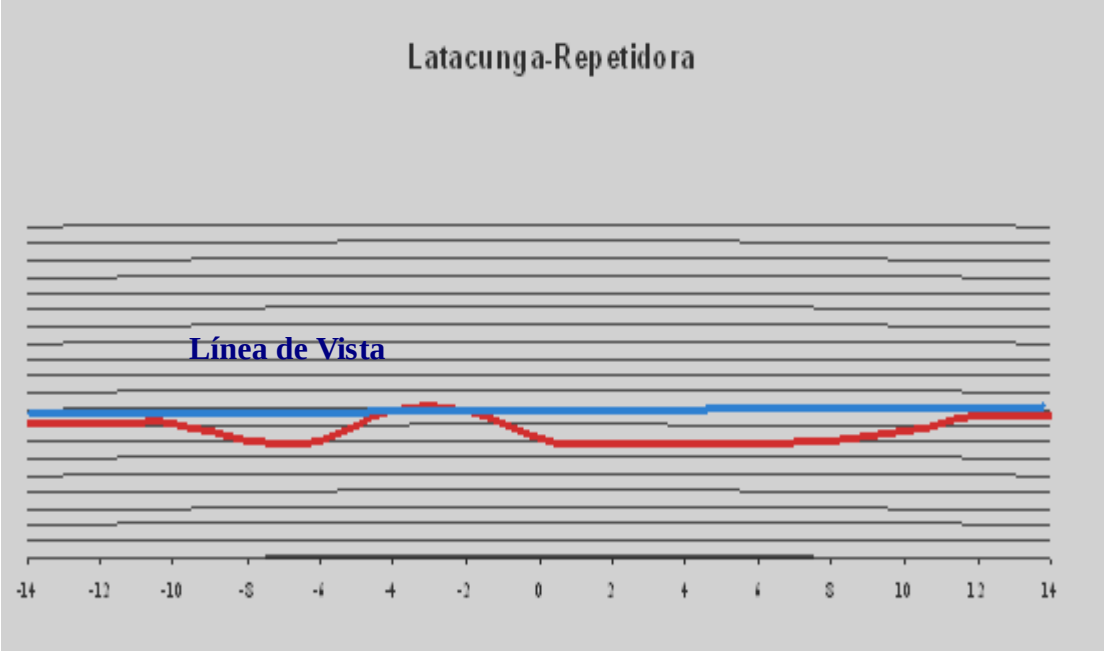


Figura. 4.26. Perfil Latacunga-Repetidora

Figura. 4.27. Perfil Repetidora-Ambato

- Repetidor Ambato-Riobamba:
  - Latitud: 1º 29’ 18" S
  - Longitud: 78º 37’ 48" W
  - Altura: 4160 m

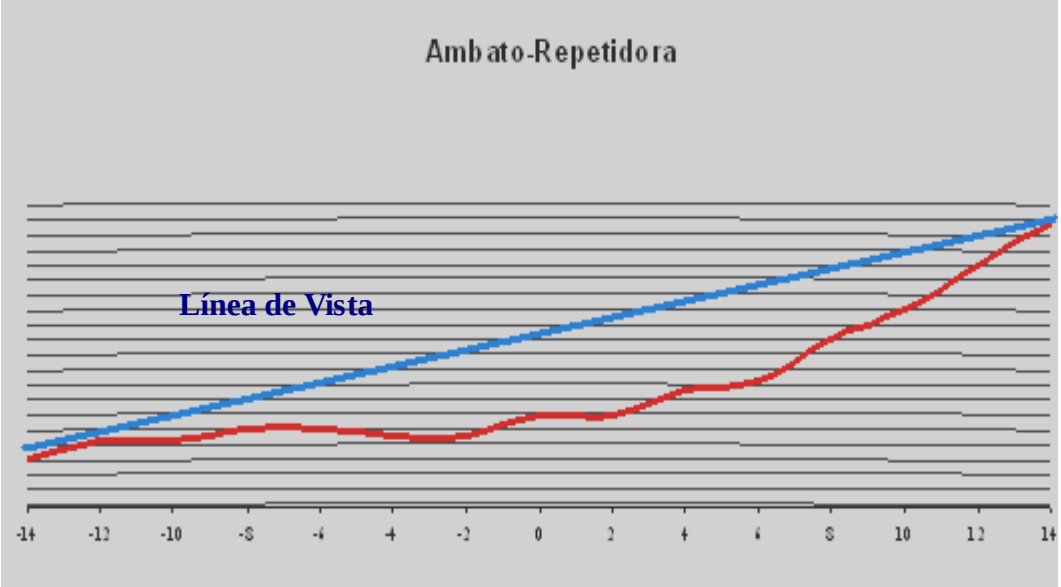


Figura. 4.28. Perfil Ambato- Repetidora

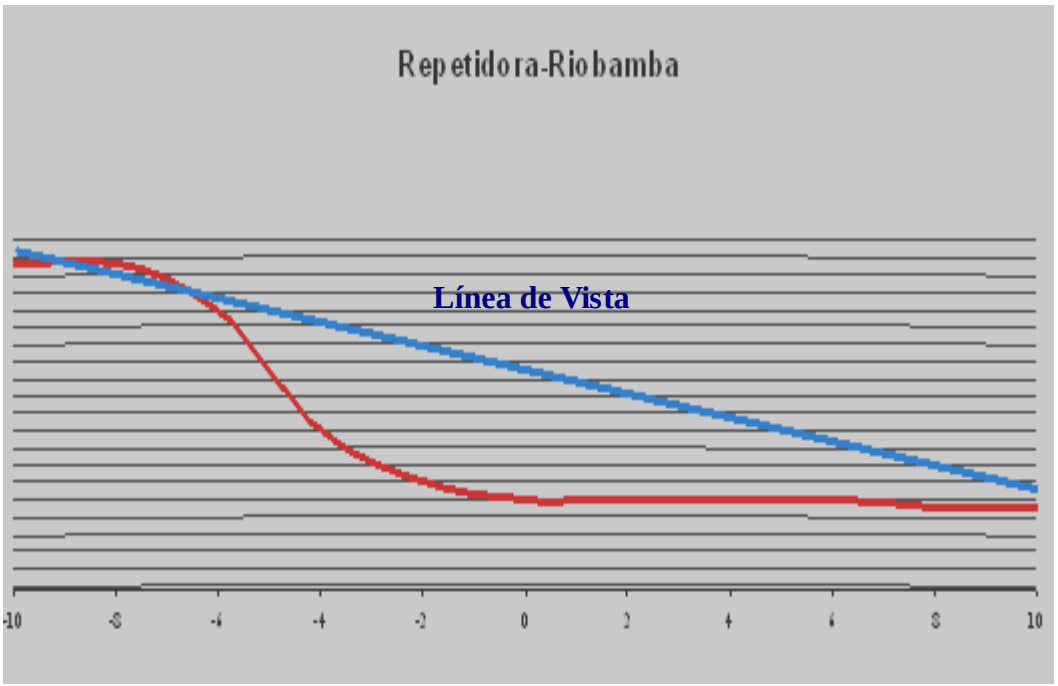


Figura. 4.29. Perfil Repetidora-Riobamba

Con estos nuevos enlaces procedemos a calcular nuevamente las pérdidas por obstáculos, teniendo como referencia los 38.5 dBµV/m de campo electromagnético como nivel mínimo para que exista enlace.

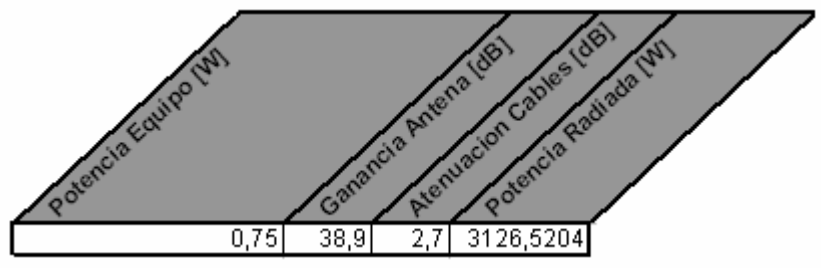


Figura. 4.30. Parámetro de Equipos

Frecuencia = 6175 MHz.

Enlace	Distancia [Km]	Frecuencia [Mhz]	Potencia Rad [W]	Aten Obst [dB]	Margen Desv [dB]	Ate Total [dB]	Prad [dB]	Eo [dBuV/m]	E(dbuV/m)	E(uV/m)
Ibarra-Cayambe	32	6175	3126,52038	110	33,8527	110,00	34,9506	79,6476	-30,3524	0,0304
Cayambe-Quito	44	6175	3126,52038	1,6	38,0018	1,60	34,9506	76,8816	75,2816	5808,6867
Quito-Sangolqui	20	6175	3126,52038	39	27,7291	39,00	34,9506	83,7300	44,7300	172,3855
Sangolqui-Machachi	24	6175	3126,52038	98	30,1045	98,00	34,9506	82,1464	-15,8536	0,1612
Machachi-Latacunga	48	6175	3126,52038	103	39,1354	103,00	34,9506	76,1258	-26,8742	0,0453
Latacunga-Ambato	36	6175	3126,52038	86,5	35,3873	86,50	34,9506	78,6246	-7,8754	0,4039
Ambato-Riobamba	48	6175	3126,52038	62	39,1354	62,00	34,9506	76,1258	14,1258	5,0850
Ibarra-Cerro	11,4	6175	3126,52038	0,8	20,4053	0,80	34,9506	88,6125	87,8125	24582,4849
Cerro-Cayambe	24	6175	3126,52038	39	30,1045	39,00	34,9506	87,8125	48,8125	275,8200
Machachi-Cerro	9,6	6175	3126,52038	1,6	18,1663	1,60	34,9506	90,1052	88,5052	26623,1475
Cerro-Latacunga	34,5	6175	3126,52038	0,8	34,8328	0,80	34,9506	88,5052	87,7052	24280,5991
Sangolqui-Repetidora	16	6175	3126,52038	46	24,8218	46,00	34,9506	85,6682	39,6682	96,2522
Repetidora-Machachi	8	6175	3126,52038	0,8	15,7909	0,80	34,9506	39,6682	38,8682	87,7830
Latacunga-Repetidora	28	6175	3126,52038	40,5	32,1129	40,50	34,9506	80,8075	40,3075	103,6031
Repetidora-Ambato	16	6175	3126,52038	0,8	24,8218	0,80	34,9506	40,3075	39,5075	94,4871
Ambato-Repetidora	28	6175	3126,52038	0,8	32,1129	0,80	34,9506	80,8075	80,0075	10008,5831
Repetidora-Riobamba	20	6175	3126,52038	1,6	27,7291	1,60	34,9506	80,0075	78,4075	8324,7768

Tabla. 4.3. Determinación de Enlaces

Con estos valores de campo electromagnético constatamos que existe enlace entre los centros en estudio.

4.3.1.3.2.4 Plan de Frecuencias

Utilizamos el plan de Dist5ribución de canales en la banda de 6 GHz, cuyo rango va 5925-7110 MHz, se utiliza en sistemas analógicos o digitales de gran capacidad (Rec. UIT-R F.386-6).

$$fo = 6175MHz$$

$$fn = fo - 259.45 + 29.65n$$
$$f'n = fo - 7.41 + 29.65n$$
$$n = 1,2,3,4,5,6,7u8$$

fn	Tx
f1	5945.20
f2	5974.85
F3	6004.50
F4	6034.15
F5	6063.80
F6	6093.45
F7	6123.10
F8	6152.75

f 'Q	Rx
f '1	6197.24
f '2	6226.89
f '3	6256.54
f '4	6286.19
f '5	6315.84
f '6	6345.49
f '7	6375.14
f '8	6404.79

Tabla. 4.4. Plan de Frecuencias

4.3.1.3.2.5 Diagrama de la Red

Ibarra-Cerro	**11,4 Km**
Cerro-Cayambe	**24 Km**
Machachi-Cerro	**9,6 Km**
Cerro-Latacunga	**34,5 Km**
Sangolqui-Repetidora	**16 Km**
Repetidora-Machachi	**8 Km**
Latacunga-Repetidora	**28 Km**
Repetidora-Ambato	**16 Km**
Ambato-Repetidora	**28 Km**
Repetidora-Riobamba	**20 Km**

Tabla. 4.5. Distancias entre Centros y Repetidoras

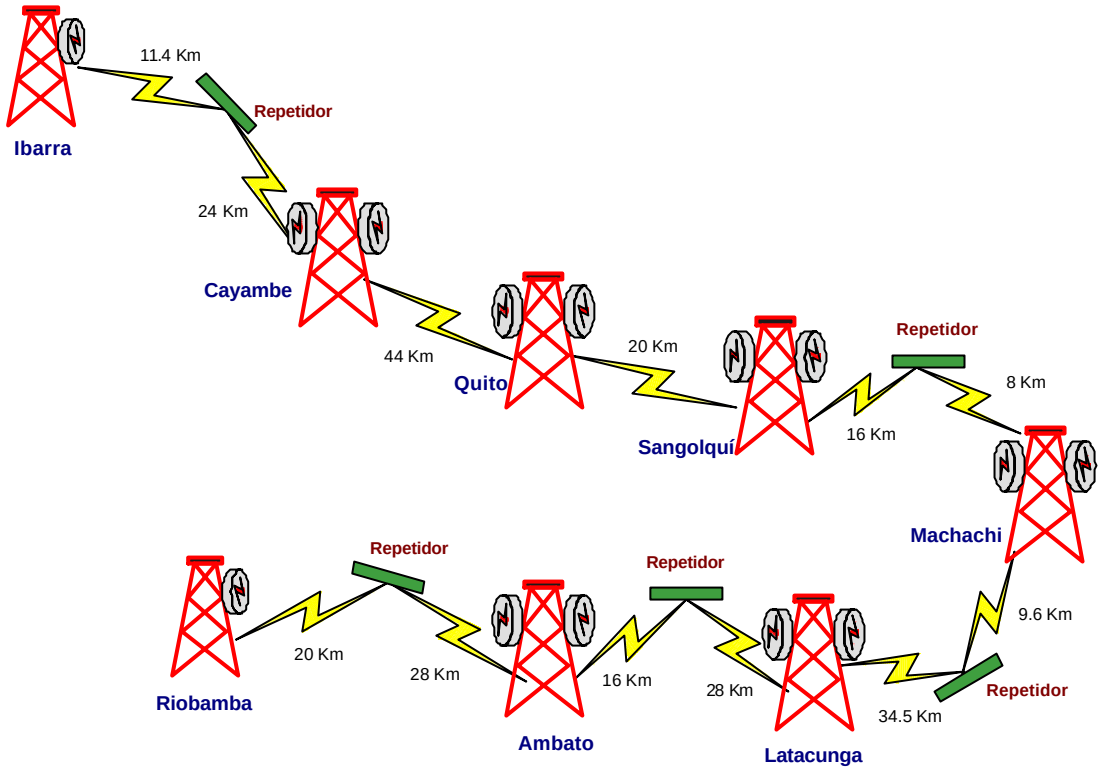


Figura. 4.31a. Diagrama de red

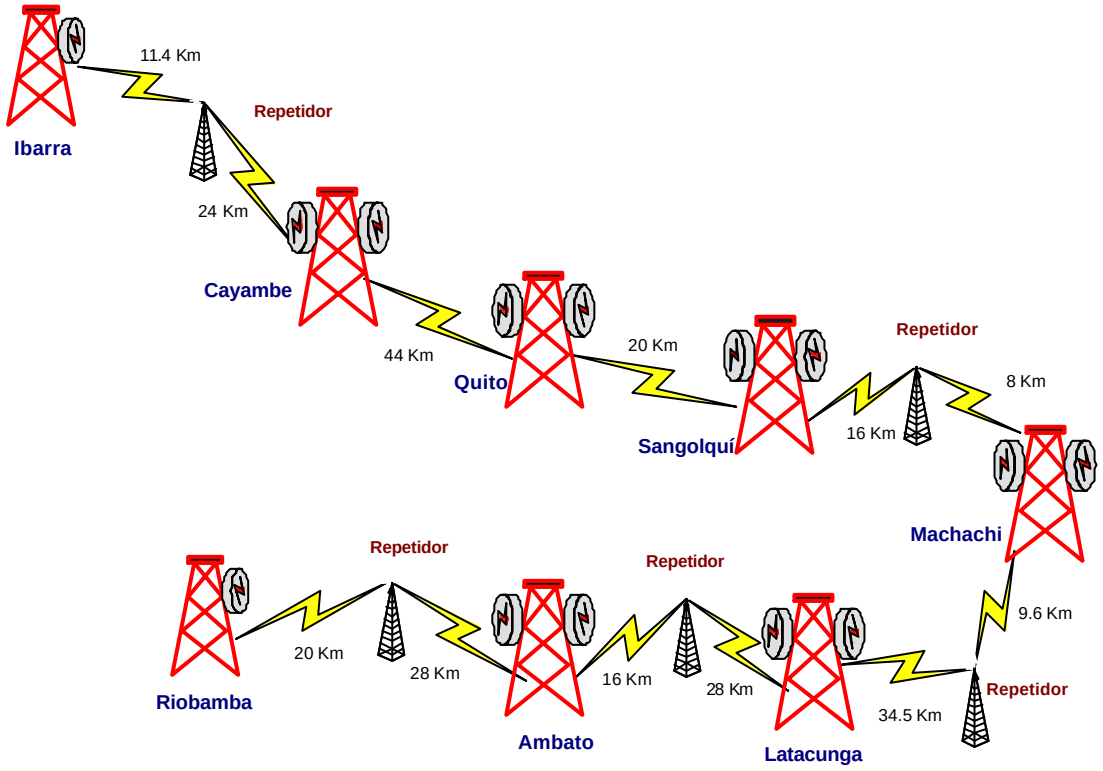


Figura. 4.31b. Diagrama de red

4.3.1.3.2.6 Diseño de las Torres

Las Torres en todos los centros será de 10 m y tendrán las respectivas luces de control aéreo, Toneles para guías de onda y sistema de tierras, todo esto esta diseñado un programa Power Tools de la siguiente manera:

- Altura:

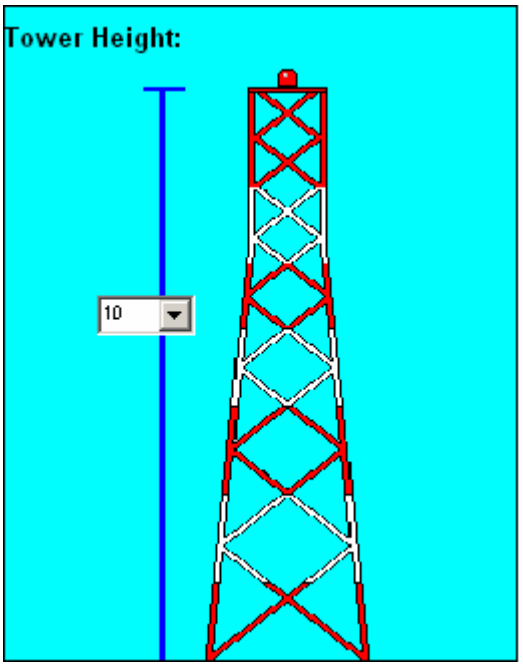


Figura. 4.32. Altura de Antena

- Accesorios:
  - Luces de Navegación

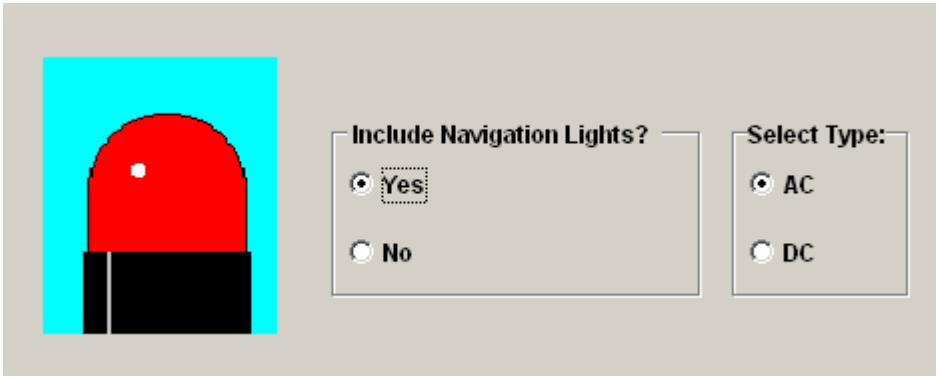


Figura. 4.33. Luces de Navegación

- Guías de Onda y Sistemas de tierra

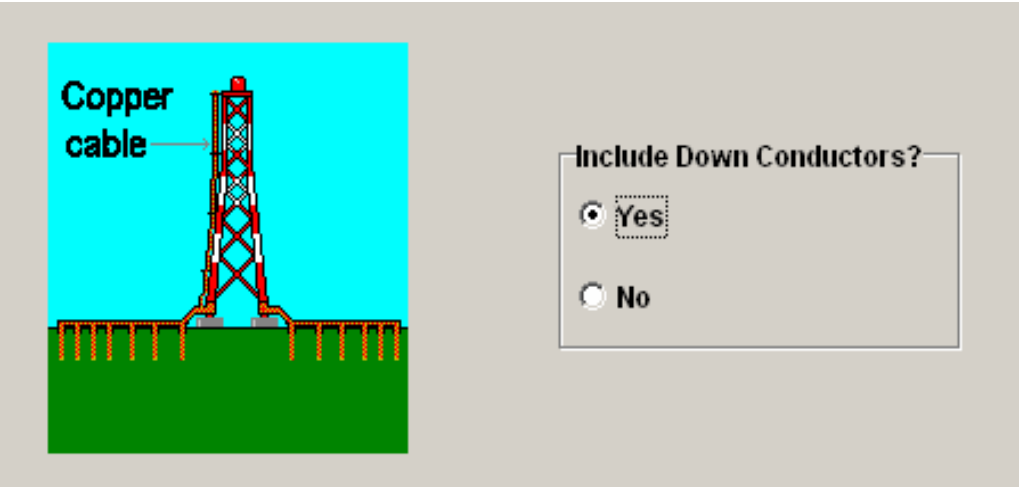


Figura. 4.34. Guías de Onda

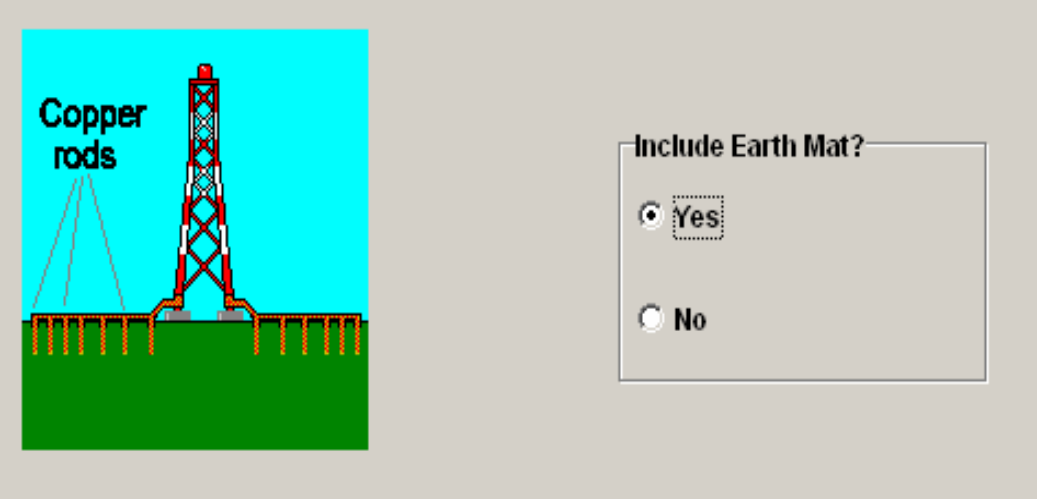


Figura. 4.35. Sistema de Tierra

4.3.1.3.2.7 Elección de la Guía de Onda

La elección de la guía de onda se la realizará de acuerdo a la frecuencia (fo) que es igual a 6175 MHz.

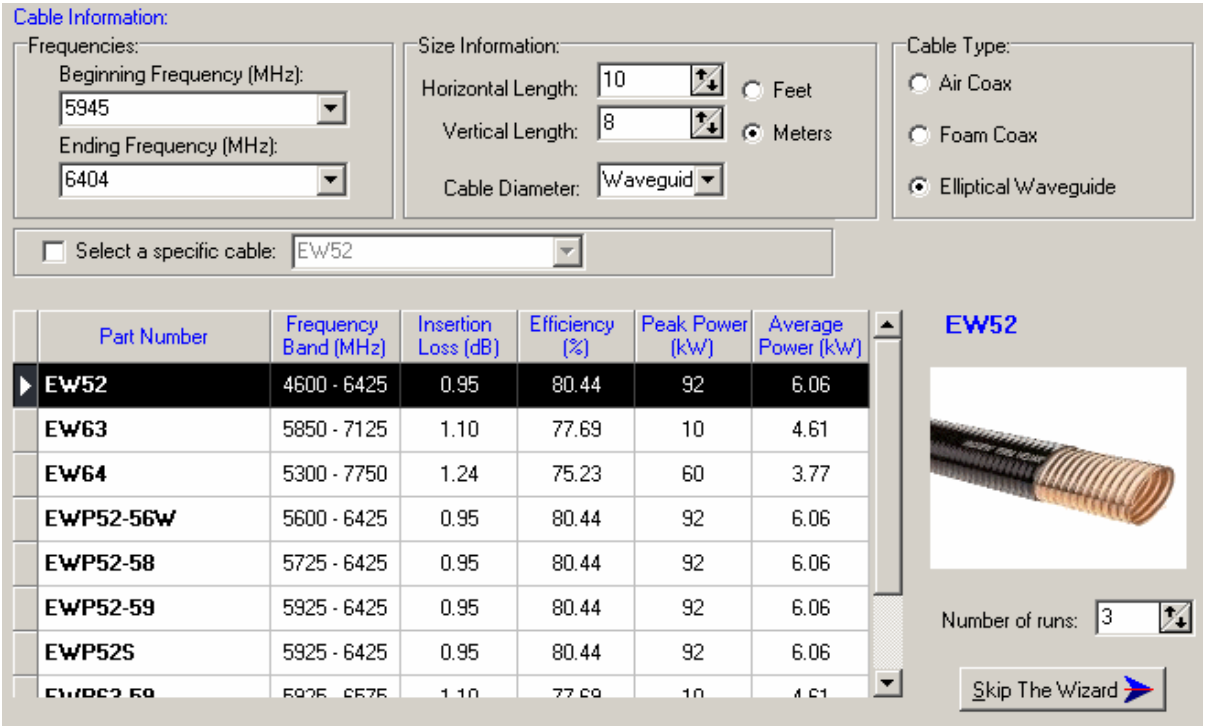


Figura. 4.36. Elección Guía de Onda

- Atenuación:

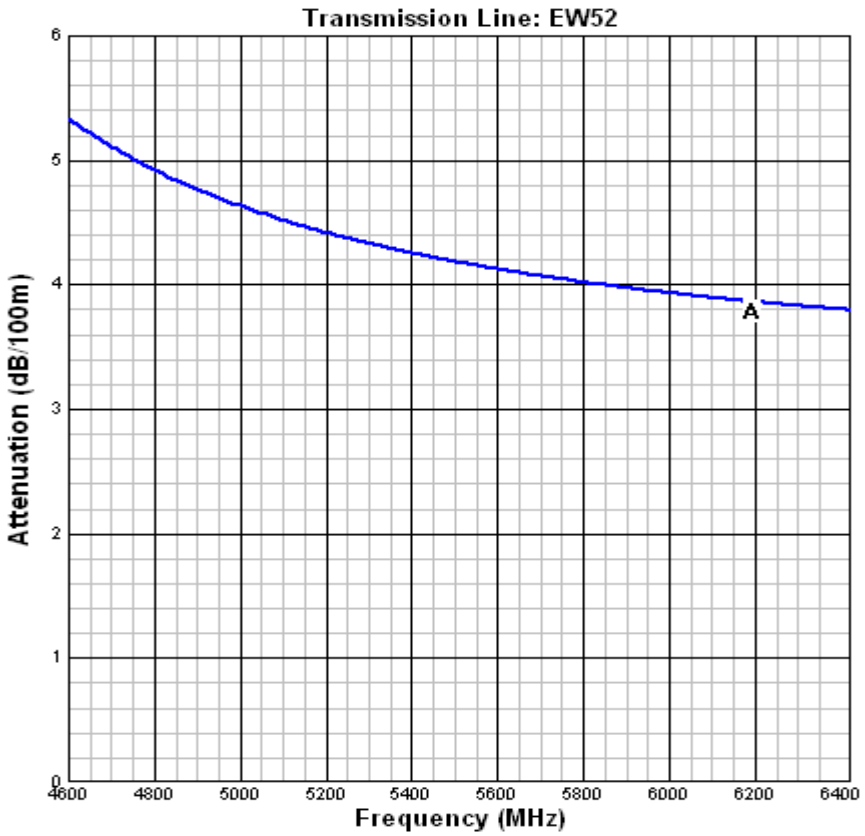


Figura. 4.37. Atenuación Guía de Onda

Performance

Frequency (MHz)	Attenuation (dB/100 ft)	Attenuation (dB/100 m)
4600	1.63	5.34
4800	1.5	4.92
5000	1.41	4.63
5200	1.35	4.42
5400	1.3	4.26
5600	1.26	4.13
5800	1.23	4.02
5850	1.22	4
5925	1.21	3.96
6000	1.2	3.93
6200	1.18	3.86
6400	1.16	3.8
6425	1.16	3.8

Figura. 4.38. Atenuación Guía de Onda por cada cien metros

- Accesorios:

Verticales

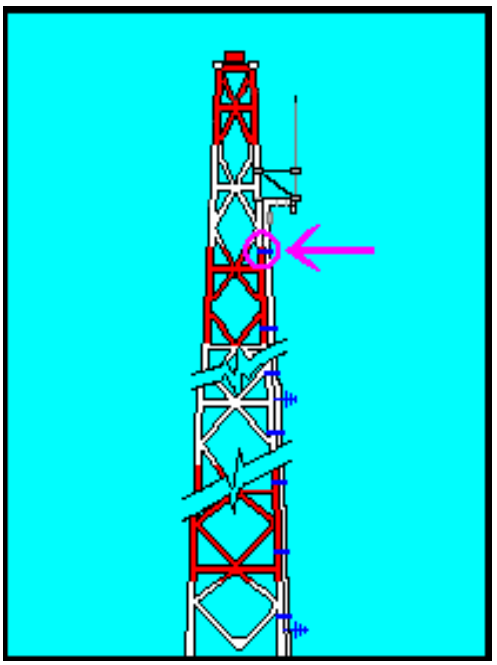


Figura. 4.39a. Accesorios Verticales

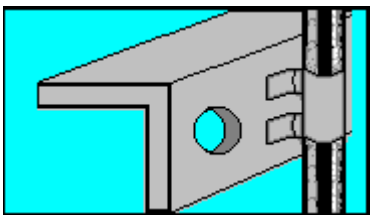


Figura. 4.39b. Accesorios Verticales

Horizontales

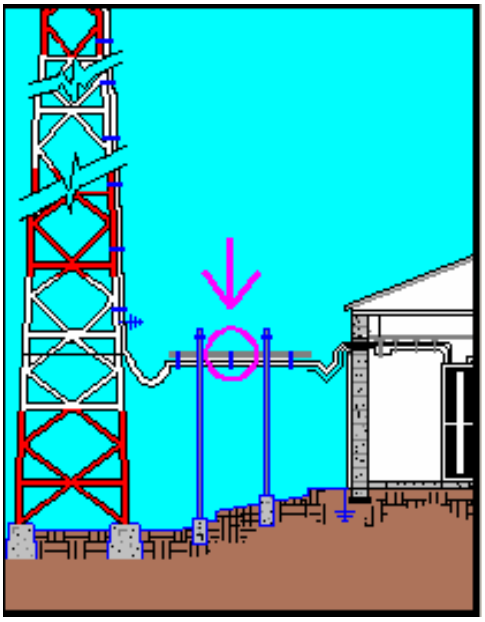


Figura. 4.40. Accesorios Horizontales

Verificando tanto en la tabla como en la grafica de la Guía elíptica EW52 tiene una atenuación L_{WG}= 3.88 dB/100 m a 6.175 Ghz, por lo tanto:

L = Longitud de la guía es 18 m en todas las estaciones.

$$L_{WG} = \frac{3.88dB}{100m} * 18m$$
$$L_{WG} = 0.70dB$$

4.3.1.3.2.8 Pérdidas en el Espacio Libre

$$FLS = 92.44 + 20\log d(km) + 20\log f(GHz)$$

- Ibarra-Cayambe:
  - Ibarra-Repetidora

    $FLS = 92.44 + 20\log 11.4 + 20\log 6.175$

    $FLS = 129.39dB$

  - Repetidora-Cayambe

    $FLS = 92.44 + 20\log 24 + 20\log 6.175$

    $FLS = 135.85dB$

    FLS_{total} = 265.24 dB

- Cayambe-Quito

  $FLS = 92.44 + 20\log 44 + 20\log 6.175$

  $FLS = 141.12dB$

  FLS_{total} = 141.12 dB

- Quito-Sangolquí

  $FLS = 92.44 + 20\log 20 + 20\log 6.175$

  $FLS = 134.27dB$

  FLS_{total} = 134.27 dB

- Sangolquí-Machachi:
  - Sangolquí-Repetidora

    $FLS = 92.44 + 20\log 16 + 20\log 6.175$

    $FLS = 132.33dB$

  - Repetidora-Machachi

    $FLS = 92.44 + 20\log 8 + 20\log 6.175$

    $FLS = 126.31dB$

    FLS_{total} = 268.64dB

- Machachi-Latacunga:
  - Machachi-Repetidora

$$FLS = 92.44 + 20\log 9.6 + 20\log 6.175$$
$$FLS = 127.89dB$$

- Repetidora-Latacunga

$$FLS = 92.44 + 20\log 34.5 + 20\log 6.175$$
$$FLS = 139dB$$

FLS_{total} = 266.89dB

- Latacunga-Ambato:

  - Latacunga-Repetidora

$$FLS = 92.44 + 20\log 28 + 20\log 6.175$$
$$FLS = 137.19dB$$

  - Repetidora-Ambato

$$FLS = 92.44 + 20\log 16 + 20\log 6.175$$
$$FLS = 132.33dB$$

FLS_{total} = 269.52dB

- Ambato-Riobamba:

  - Ambato-Repetidora

$$FLS = 92.44 + 20\log 28 + 20\log 6.175$$
$$FLS = 137.19dB$$

  - Repetidora-Riobamba

$$FLS = 92.44 + 20\log 20 + 20\log 6.175$$
$$FLS = 134.27dB$$

FLS_{total} = 271.46 dB

Enlace	FSL
1. Ibarra-Cayambe	265.24dB
2. Cayambe-Quito	141.12dB
3. Quito-Sangolquí	134.27dB
4. Sangolquí-Machachi	268.64dB.
5. Machachi-Latacunga	266.89dB
6.Latacunga-Ambato	269.52dB
7. Ambato-Riobamba	271.46dB

Tabla. 4.6. Pérdidas en Espacio Libre

4.3.1.3.2.9 Especificaciones de los Equipos a Utilizar

- **Datos:**

  - Nivel Rx = -70dBm
  - BER =10^{-6}
  - Ganancia Tx = 28.8dBm
  - Ganancia Antenas = 38.9dB
  - Pérdidas cables = 2.7dB
  - Ganancia del Repetidor Pasivo = 115 dB

- **Cálculo del Nivel Mínimo de Recepción y Margen de Desvanecimiento:**

  - Ibarra-Cayambe:

  $$Ganancias = G_{Tx} + G_{AntenaTx} + G_{AntenaRx} + G_{repetidor}$$

  $$Ganancias = 28.8dBm + 38.9dB + 38.9dB + 115dB$$
  $$Ganancias = 221.6dBm$$

  $$Pérdidas = L_{EspacioLibre} + L_{cablesTx} + L_{cablesRx}$$

  $$Pérdidas = 265.24dB + 2.7dB$$
  $$Pérdidas = 267.94dB$$

Nivel Mínimo de Recepción = Ganancias - Pérdidas

$$C\min = 221.6dBm - 267.94dB$$
$$C\min = -46.34dBm$$

$$M\arg en = C\min - NivelRx$$
$$M\arg en = -46.34dBm - (-70dBm)$$
$$M\arg en = 23.66dB$$

- Cayambe-Quito:

$$Ganancias = G_{Tx} + G_{AntenaTx} + G_{AntenaRx}$$

$$Ganancias = 28.8dBm + 38.9dB + 38.9dB$$
$$Ganancias = 106.6dBm$$

$$Pérdidas = L_{EspacioLibre} + L_{cablesTx} + L_{cablesRx}$$

$$Pérdidas = 141.12dB + 2.7dB$$
$$Pérdidas = 143.82dB$$

Nivel Mínimo de Recepción = Ganancias - Pérdidas

$$C\min = 106.6dBm - 143.82dB$$
$$C\min = -37.22dBm$$

$$M\arg en = C\min - NivelRx$$
$$M\arg en = -37.22dBm - (-70dBm)$$
$$M\arg en = 32.78dB$$

- Quito-Sangolquí:

$$Ganancias = G_{Tx} + G_{AntenaTx} + G_{AntenaRx}$$

$$Ganancias = 28.8dBm + 38.9dB + 38.9dB$$
$$Ganancias = 106.6dBm$$

$$Pérdidas = L_{EspacioLibre} + L_{cablesTx} + L_{cablesRx}$$

$$Pérdidas = 134.27dB + 2.7dB$$
$$Pérdidas = 136.97dB$$

Nivel Mínimo de Recepción = Ganancias - Pérdidas

$$C\min = 106.6dBm - 136.97dB$$
$$C\min = -30.37dBm$$

$$M\arg en = C\min - NivelRx$$
$$M\arg en = -30.37dBm - (-70dBm)$$
$$M\arg en = 39.63dB$$

- Sangolquí-Machachi:

$$Ganancias = G_{Tx} + G_{AntenaTx} + G_{AntenaRx} + G_{repetidor}$$

$$Ganancias = 28.8dBm + 38.9dB + 38.9dB + 115dB$$
$$Ganancias = 221.6dBm$$

$$Pérdidas = L_{EspacioLibre} + L_{cablesTx} + L_{cablesRx}$$

$$Pérdidas = 268.64dB + 2.7dB$$
$$Pérdidas = 271.34dB$$

Nivel Mínimo de Recepción = Ganancias - Pérdidas

$$C\min = 221.6dBm - 271.34dB$$
$$C\min = -49.74dBm$$

$$M\arg en = C\min - NivelRx$$
$$M\arg en = -49.74dBm - (-70dBm)$$
$$M\arg en = 20.26dB$$

- Machachi-Latacunga:

$$Ganancias = G_{Tx} + G_{AntenaTx} + G_{AntenaRx} + G_{repetidor}$$

$$Ganancias = 28.8dBm + 38.9dB + 38.9dB + 115dB$$
$$Ganancias = 221.6dBm$$

$$Pérdidas = L_{EspacioLibre} + L_{cablesTx} + L_{cablesRx}$$

$$Pérdidas = 266.89dB + 2.7dB$$
$$Pérdidas = 269.59dB$$

Nivel Mínimo de Recepción = Ganancias - Pérdidas

$$C\min = 221.6dBm - 269.59dB$$
$$C\min = -47.99dBm$$

$$M\arg en = C\min - NivelRx$$
$$M\arg en = -47.99dBm - (-70dBm)$$
$$M\arg en = 22.01dB$$

- Latacunga-Ambato:

$$Ganancias = G_{Tx} + G_{AntenaTx} + G_{AntenaRx} + G_{repetidor}$$

$$Ganancias = 28.8dBm + 38.9dB + 38.9dB + 115dB$$
$$Ganancias = 221.6dBm$$

$$Pérdidas = L_{EspacioLibre} + L_{cablesTx} + L_{cablesRx}$$

$$Pérdidas = 269.52dB + 2.7dB$$
$$Pérdidas = 272.22dB$$

Nivel Mínimo de Recepción = Ganancias - Pérdidas

$$C\min = 221.6dBm - 272.22dB$$
$$C\min = -50.62dBm$$

$$M\arg en = C\min - NivelRx$$
$$M\arg en = -50.62dBm - (-70dBm)$$
$$M\arg en = 19.38dB$$

- Ambato-Riobamba:

$$Ganancias = G_{Tx} + G_{AntenaTx} + G_{AntenaRx} + G_{repetidor}$$

$$Ganancias = 28.8dBm + 38.9dB + 38.9dB + 115dB$$
$$Ganancias = 221.6dBm$$

$$Pérdidas = L_{EspacioLibre} + L_{cablesTx} + L_{cablesRx}$$

$$Pérdidas = 271.46dB + 2.7dB$$
$$Pérdidas = 274.16dB$$

Nivel Mínimo de Recepción = Ganancias - Pérdidas

$$C\min = 221.6dBm - 274.16dB$$
$$C\min = -52.56dBm$$

$$M\arg en = C\min - NivelRx$$
$$M\arg en = -52.56dBm - (-70dBm)$$
$$M\arg en = 17.44dB$$

Con estos datos se sugiere utilizar el equipo MegaStar 155 PX (Ver Datasheet), que cumple con estos requisitos y opera en el rango de frecuencias de (5925-6425) MHz

4.3.1.3.2.10 Antenas

Figura. 4.41. Ejemplo de Antena

	Transmisión		Recepción	
Enlace	**Tamaño**	**Ganancia**	**Tamaño**	**Ganancia**
1. Ibarra-Cayambe	1.8m	38.9dB	1.8m	38.9dB
2. Cayambe-Quito	1.8m	38.9dB	1.8m	38.9dB
3. Quito-Sangolquí	1.8m	38.9dB	1.8m	38.9dB
4. Sangolquí-Machachi	1.8m	38.9dB	1.8m	38.9dB
5. Machachi-Latacunga	1.8m	38.9dB	1.8m	38.9dB
6.Latacunga-Ambato	1.8m	38.9dB	1.8m	38.9dB
7. Ambato-Riobamba	1.8m	38.9dB	1.8m	38.9dB

Tabla. 4.7. Antenas en Recepción y Transmisión

Se ha escogido la Antena UHX6-59W, la cual cumple con estos requisitos (Ver Datasheet).

4.3.1.3.2.11 Análisis Legal

Los requisitos, contratos, reglamentos y formularios, para la obtención del permiso de operación de redes privadas, se encuentran en el Anexo # 1, 2, 3.

4.3.1.3.2.12 Disponibilidad del Sistema

- **Método de Cálculo:**

1. Se necesita conocer la densidad de instantánea de lluvia (J), y además el margen de desvanecimiento de cada enlace (FM)
2. Luego se procede a obtener el valor de atenuación específica (dr) de acuerdo a la densidad instantánea de lluvia.
3. Se procede a encontrar las constantes de polarización (k, a), según la frecuencia de operación, según la norma ITU-R I.721-2.
4. Luego se encuentra la relación lluvia-distancia, es decir la distancia efectiva de lluvia (DEF), relacionada con la distancia del enlace
5. Finalmente se calcula la atenuación del enlace y la probabilidad de que exista desvanecimiento de la señal.

- Ibarra-Cayambe:

Datos:

J = 80mm/h

FSL = 265.24dB

FM = 23.66 dB

D = 34.67 Km.

K = 0.00175

a = 1.308

Calculo:

$$dr = K.J^{a} = 0.00175 * 80^{1.308}$$
$$dr = 0.539 dB / Km$$

$$DEF = \frac{d}{1 + 0.045d} = \frac{34.67}{1 + 0.045 * 34.67}$$
$$DEF = 13.54 Km.$$

$$A = dr * DEF = 0.539 * 13.54$$
$$A = 7.29 dB$$

US = Probabilidad de Desvanecimiento

$$\frac{FM}{A} = 0.12 * US^{-(0.546+0.043 Log(US))}$$
$$US = 9.9 * 10^{-10}$$

Probabilidad de que falle el enlace = $9.9*10^{-10}$, según la ITU-R lo mínimo es $6*10^{-5}$, es decir no hay corte de enlace.

- Cayambe-Quito:

Datos:

J = 80mm/h

FSL = 141.12dB

FM = 32.78 dB

D = 44.15 Km.

K = 0.00175

a = 1.308

Calculo:

$$dr = K.J^{a} = 0.00175 * 80^{1.308}$$
$$dr = 0.539 dB / Km$$

$$DEF = \frac{d}{1 + 0.045d} = \frac{44.15}{1 + 0.045 * 44.15}$$
$$DEF = 14.78 Km.$$

$$A = dr * DEF = 0.539 * 14.78$$
$$A = 7.96 dB$$

US = Probabilidad de Desvanecimiento

$$\frac{FM}{A} = 0.12 * US^{-(0.546+0.043 Log(US))}$$
$$US = 3.01 * 10^{-9}$$

Probabilidad de que falle el enlace = $3.01*10^{-9}$, según la ITU-R lo mínimo es $6*10^{-5}$, es decir no hay corte de enlace.

- Quito-Sangolquí:

Datos:

J = 80mm/h

FSL = 134.67dB

FM = 39.63 dB

D = 21.41 Km.

K = 0.00175

a = 1.308

Calculo:

$$dr = K.J^{a} = 0.00175 * 80^{1.308}$$
$$dr = 0.539 dB / Km$$

$$DEF = \frac{d}{1 + 0.045d} = \frac{21.41}{1 + 0.045 * 21.41}$$
$$DEF = 10.90 Km.$$

$$A = dr * DEF = 0.539 * 10.90$$
$$A = 5.87dB$$

US = Probabilidad de Desvanecimiento

$$\frac{FM}{A} = 0.12 * US^{-(0.546+0.043Log(US))}$$
$$US = imaginario$$

Probabilidad de que falle el enlace = imaginario, según la ITU-R lo mínimo es $6*10^{-5}$, es decir no hay corte de enlace.

- Sangolquí-Machachi:

Datos:

J = 80mm/h

FSL = 268.64dB

FM = 20.26 dB

D = 23.90 Km.

K = 0.00175

a = 1.308

Calculo:

$$dr = K.J^{a} = 0.00175 * 80^{1.308}$$
$$dr = 0.539dB / Km$$

$$DEF = \frac{d}{1 + 0.045d} = \frac{23.90}{1 + 0.045 * 23.90}$$
$$DEF = 11.51Km.$$

$$A = dr * DEF = 0.539 * 11.51$$
$$A = 6.20dB$$

US = Probabilidad de Desvanecimiento

$$\frac{FM}{A} = 0.12 * US^{-(0.546+0.043Log(US))}$$
$$US = 9.9 * 10^{-10}$$

Probabilidad de que falle el enlace = $9.9*10^{-10}$, según la ITU-R lo mínimo es $6*10^{-5}$, es decir no hay corte de enlace.

- Machachi-Latacunga:

Datos:

J = 80mm/h

FSL = 266.89dB

FM = 22.01 dB

D = 47.59 Km.

K = 0.00175

a = 1.308

Calculo:

$$dr = K.J^{a} = 0.00175 * 80^{1.308}$$
$$dr = 0.539 dB / Km$$

$$DEF = \frac{d}{1 + 0.045d} = \frac{47.59}{1 + 0.045 * 47.59}$$
$$DEF = 15.14 Km.$$

$$A = dr * DEF = 0.539 * 15.14$$
$$A = 8.16 dB$$

US = Probabilidad de Desvanecimiento

$$\frac{FM}{A} = 0.12 * US^{-(0.546+0.043 Log(US))}$$
$$US = 4.67 * 10^{-10}$$

Probabilidad de que falle el enlace = $4.67*10^{-10}$, según la ITU-R lo mínimo es $6*10^{-5}$, es decir no hay corte de enlace.

- Latacunga-Ambato:

Datos:

J = 80mm/h

FSL = 269.52dB

FM = 19.38 dB

D = 33.47 Km.

K = 0.00175

a = 1.308

Calculo:

$$dr = K.J^{a} = 0.00175 * 80^{1.308}$$
$$dr = 0.539 dB / Km$$

$$DEF = \frac{d}{1 + 0.045d} = \frac{33.47}{1 + 0.045 * 33.47}$$
$$DEF = 13.35 Km.$$

$$A = dr * DEF = 0.539 * 13.35$$
$$A = 7.19 dB$$

US = Probabilidad de Desvanecimiento

$$\frac{FM}{A} = 0.12 * US^{-(0.546+0.043Log(US))}$$
$$US = 4.67 * 10^{-10}$$

Probabilidad de que falle el enlace = $4.67*10^{-10}$, según la ITU-R lo mínimo es $6*10^{-5}$, es decir no hay corte de enlace.

- Ambato-Riobamba:

Datos:

J = 80mm/h

FSL = 271.46dB

FM = 17.44 dB

D = 48.19 Km.

K = 0.00175

a = 1.308

Calculo:

$$dr = K.J^{a} = 0.00175 * 80^{1.308}$$
$$dr = 0.539 dB / Km$$

$$DEF = \frac{d}{1+0.045d} = \frac{48.19}{1+0.045*48.19}$$
$$DEF = 15.20Km.$$

$$A = dr * DEF = 0.539 * 15.20$$
$$A = 8.19dB$$

US = Probabilidad de Desvanecimiento

$$\frac{FM}{A} = 0.12 * US^{-(0.546+0.043Log(US))}$$
$$US = 1.86 * 10^{-10}$$

Probabilidad de que falle el enlace = $1.86*10^{-10}$, según la ITU-R lo mínimo es $6*10^{-5}$, es decir no hay corte de enlace.

CAPITULO V

ANÁLISIS ECONÓMICO DEL PROYECTO

5.1 RENTABILIDAD

5.1 .1 Definición

Rentabilidad es una noción que se aplica a toda acción económica en la que se movilizan unos medios, materiales, humanos y financieros con el fin de obtener unos resultados.

En economía, aunque el término rentabilidad se utiliza de forma muy variada y son muchas las aproximaciones doctrinales que inciden en una u otra faceta de la misma, en sentido general se denomina rentabilidad a la medida del rendimiento que en un determinado periodo de tiempo producen los capitales utilizados en el mismo.

Esto supone la comparación entre la renta generada y los medios utilizados para obtenerla con el fin de permitir la elección entre alternativas o juzgar la eficiencia de las acciones realizadas, según que el análisis realizado sea a priori o a posteriori.

5.2 LA RENTABILIDAD COMO ANÁLISIS

La importancia del análisis de la rentabilidad viene determinada porque, aun partiendo de la multiplicidad de objetivos a que se enfrenta una empresa, basados unos en la rentabilidad o beneficio, otros en el crecimiento, la estabilidad e incluso en el servicio a la colectividad, en todo análisis empresarial el centro de la discusión tiende a situarse en la polaridad entre rentabilidad y seguridad o solvencia como variables fundamentales de toda actividad económica.

La base del análisis económico-financiero se encuentra inscrita en la relación rentabilidad-riesgo, que se presenta desde tres puntos de vista.

- Análisis de la rentabilidad.

- Análisis de la solvencia, entendida como la capacidad de la empresa para satisfacer sus obligaciones financieras (devolución de principal y gastos financieros), consecuencia del endeudamiento.

- Análisis de la estructura financiera de la empresa con la finalidad de comprobar su adecuación para mantener un desarrollo estable de la misma. Es decir, los límites económicos de toda actividad empresarial son la rentabilidad y la seguridad, normalmente objetivos contrapuestos, ya que la rentabilidad, en cierto modo, es la retribución al riesgo y, consecuentemente, la inversión más segura no suele coincidir con la más rentable.

  Sin embargo, es necesario tener en cuenta que, por otra parte, el fin de solvencia o estabilidad de la empresa está íntimamente ligado al de rentabilidad, en el sentido de que la rentabilidad es un condicionante decisivo de la solvencia, pues la obtención de rentabilidad es un requisito necesario para la continuidad de la cualquier empresa.

5.2.1 Consideraciones para Construir Índices de Rentabilidad

En su expresión analítica, la rentabilidad contable va a venir expresada como cociente entre un concepto de resultado y un concepto de capital invertido para obtener ese resultado. A este respecto es necesario tener en cuenta una serie de cuestiones en la formulación y medición de la rentabilidad para poder así elaborar un indicador de rentabilidad con significado.

1. Las magnitudes cuyo cociente es el indicador de rentabilidad han de ser susceptibles de expresarse en forma monetaria.

2. Debe existir, en la medida de lo posible, una relación causal entre los recursos o inversión considerados como denominador y el excedente o resultado al que han de ser enfrentados.

3. En la determinación de la cuantía de los recursos invertidos habrá de considerarse el promedio del periodo, pues mientras el resultado es una variable flujo, que se calcula respecto a un periodo, la base de comparación, constituida por la inversión, es una variable que sólo informa de la inversión existente en un momento concreto

del tiempo. Por ello, para aumentar la representatividad de los recursos invertidos, es necesario considerar el promedio del periodo.

4. Por otra parte, también es necesario definir el periodo de tiempo al que se refiere la medición de la rentabilidad, pues en el caso de breves espacios de tiempo se suele incurrir en errores debido a una periodificación incorrecta.

5.3 MÉTODOS DE ESTIMACIÓN DE LA RENTABILIDAD

Los métodos más comunes de evaluación de rentabilidad son los siguientes:

- Tasa de retorno sobre la inversión original
- Valor presente
- Valor Actual Neto
- Tasa interna de retorno

5.3.1 Valor presente (VP)

Este método compara los valores presentes (VP) de todos los flujos de caja con la inversión original. Supone igualdad de oportunidades para la re-inversión de los flujos de caja a una tasa de interés pre-asignada.

Esta tasa puede tomarse como el valor promedio de la tasa de retorno que obtiene la compañía con su capital o se lo puede designar como el retorno mínimo aceptable para el proyecto. El valor presente del proyecto es igual a la diferencia entre el valor presente de los flujos anuales de fondos y la inversión inicial.

El valor presente neto es una única cantidad referida al tiempo cero y representa un premio si es positiva, o un fracaso si es negativa, para una tasa de interés elegida.

Otra forma de definir el valor presente, es la cantidad adicional que será requerida al comienzo del proyecto, usando una tasa de interés pre-asignada, para producir ingresos iguales a, y al mismo tiempo que, la inversión total.

Los resultados no indican la magnitud del proyecto. Por esa razón, se define una variante del valor presente como la relación entre el valor presente de los flujos anuales de fondos y la inversión total.

5.3.2Valor Actual Neto (VAN)

Cuantifica el superávit o déficit neto para el período de años considerado expresado en valor actual para una tasa de actualización determinada. La tasa de actualización actúa como un factor de reajuste aplicado a los valores futuros, cuyo empleo es necesario para poder comparar los beneficios y costos netos.

Para el cálculo del VAN se utiliza la siguiente fórmula:

$$VNA = \sum_{i-1}^{n} \frac{Valores_i}{(1+tasa)^i}$$

5.3.3 Tasa Interna de Retorno (TIR)

La tasa interna de retorno (TIR), es un método que se emplea para evaluar la viabilidad económica de un proyecto. Este método calcula la tasa de interés que iguala el valor actual de las entradas de capital al proyecto con el valor actual de las salidas de capital a lo largo de la vida económica del proyecto.

5.4 COSTOS DE IMPLEMENTACIÓN

Para cualquiera de las alternativas propuestas anteriormente se tienen los siguientes costos para la implementación del Servidor y Servicios de Comunicaciones:

Descripción	Cantidad	Unidad	Valor	TOTAL
Hardware: Servidor de Comunicaciones	1	Unidad	1500	1500
Software: Sistema Operativo	1	Unidad	0	0
Implementación de VPN, Firewall, Proxy Server, FTP Server, Web Server	1	Unidad	500	500
			TOTAL	2000

Tabla. 5.1. Costos de Servicios de Comunicaciones

5.4.1 Alternativa # 1.

A continuación se muestran los costos de esta alternativa:

- Pagos Por única vez:

Descripción	Cantidad	Unidad	Valor	TOTAL
Instalación y Equipo Router 3600	1	Unidad	392	392
Instalación y Equipo Router	19	Unidad	70	1330
Instalación y configuración de equipos de comunicaciones: Modems, Router	20	Unidad	50	1000
			TOTAL	2722

Tabla. 5.2. Costos de Instalación

- Pagos Mensuales.:

Descripción	Cantidad	Unidad	Valor	TOTAL
Equipo Router 3600	1	Unidad	320	320
Equipo Router	19	Unidad	60	1140
			TOTAL	1460

Tabla. 5.3. Pagos Mensuales-Alternativa 1

5.4.2 Alternativa # 2.

Descripción	Cantidad	Unidad	Valor	TOTAL
Torre Tipo B - 10 m	1	unidad	3904,28	3904,28
Luces de Navegación AC	1	unidad	755,29	755,29
Down Conductors	1	unidad	116,08	116,08
Malla de Tierra	1	unidad	604,57	604,57
			TOTAL	5380,22

Tabla.5.4. Costo-Torres

Descripción	Cantidad	Unidad	Valor	TOTAL
Guía de Onda EW52	6	unidad	135	810
cable coaxial EW44,EW52, guía de onda elíptica EW63	3	unidad	49,44	148,32
grounding, cable with 1-hole factory attached	9	unidad	31,95	282,15
Conectores	3	unidad	33,48	100,44
			TOTAL	1340,91

Tabla. 5.5. Costo- Accesorios

	Descripción	Cantidad	Unidad	Valor	TOTAL
Equipos	Antenas	14	Unidad	11290	158060
	Transmisores	7	Unidad	27544	192808
	Receptores	7	Unidad	27544	192808
	Torres	13	Unidad	5380,22	69942,86
	Guías de Onda	14	Unidad	1340,91	18772,74
Instalación	Antenas	14		2743,03	38402,45
	Transmisores	7		2594,9	18164,36
	Receptores	7		2594,9	18164,36
	Torres	13		2194,42	28527,54
Trámites Legales	Derechos de Registro				500

Total Estimado Inicial	736150,31

Tabla. 5.6. Presupuesto-Alternativa 2

5.5 ANÁLISIS DEL PROYECTO

Para el análisis de rentabilidad del proyecto, se han utilizado dos índices de rentabilidad como son el TIR y el VAN, además de un parámetro denominado recuperación de la inversión, que básicamente se calcula el número de años en el que se va a recuperar el capital invertido.

Alternativa # 1:

CALCULO DE LA TASA DE RETORNO (TIR) Y VALOR ACTUAL NETO (VAN)

RED WAN - ALTERNATIVA # 1

RED WAN-RENTABILIDAD	ESTIMACION DEL FLUJO DE CAJA LIBRE RED WAN-RENTABILIDAD				
	0	1	2	3	4
	2005	2006	2007	2008	2009
Ingresos		400.000	400.000	400.000	400.000
Ingresos Matriculas		200.000	200.000	200.000	200.000
Ingresos ESPE		200.000	200.000	200.000	200.000
Costos		-294.902	-168.400	-168.400	-168.400
Costos de Explotación					
Gastos de Personal		3.600	3.600	3.600	3.600
Servicios		-294.502	-168.000	-168.000	-168.000
2,50% Depreciación de Activos		-5.000	-5.000	-5.000	-5.000
Materiales		-	-	-	-
Otros		1.000	1.000	1.000	1.000
MARGEN OPERACIONAL BRUTO		**105.098**	**231.600**	**231.600**	**231.600**
Otros Gastos		-	-	-	-
ADMINISTRACIÓN		-	-	-	-
CONTRALORIA		-	-	-	-
Gastos no desembolsables		**433**	**433**	**433**	**433**
Depreciación Tx,Cx y PE		433,47	433	433	433

Figura. 5.1. Análisis-Rentabilidad-1

En este cuadro se muestran valores de ingresos que se podrían tener en un plazo de cinco años, así como también los valores que se tienen que pagar por concepto de servicios y de personal, que la red necesita para su mantenimiento.

RED WAN-RENTABILIDAD	ESTIMACION DEL FLUJO DE CAJA LIBRE RED WAN-RENTABILIDAD				
	0 2005	1 2006	2 2007	3 2008	4 2009
MARGEN OPER. ANTES DE IMPUESTOS		105.531	232.033	232.033	232.033
4 Cálculo de Tasas e Impuestos		-24.913	-56.540	-56.542	-56.545
0% Participación de Trabajadores		-	-	-	-
25% Impuesto a la Renta		-26.383	-58.008	-58.008	-58.008
0,5% SuperIntendencia de Compañías		1.470	1.468	1.466	1.464
MARGEN OPER. DESPUES DE IMPUESTOS		80.619	175.493	175.491	175.489
5 Ajuste por Gastos no desembolsables		-433	-433	-433	-433
Depreciación por equipamiento		-433	-433	-433	-433
6 Costos y Beneficios no afectos a Impuestos	-294.502	-	-	-	-
Inversiones	294.502	-	-	-	-
Equipos	6.502				
Hardware e Implementación de Servicios	2.000				
Instalación y configuración de Equipos	2.722				
Equipo Router 3600	320				
Equipo Router 1751	1.460		-		
Servicio	168.000				
Arrendamiento ADSL	168.000				

Figura. 5.2. Análisis-Rentabilidad-2

En esta figura se presentan los valores iniciales de la red WAN, también se presentan valores por año que cada centro deberá pagar.

Tasa Interna de Retorno (TIR)	25,9%
Valor Actual Neto (VAN) (US$)	54.406
Periodo de Recuperación (Años)	2,22
Periodo Recuperación Descontado (Años)	2,92

Figura. 5.3. Resultados-Rentabilidad-1

Analizando los valores de TIR y VAN, vemos que son favorables para la alternativa # 1, teniendo un tiempo de recuperación de casi 3 años, por lo que se garantiza que puede ser una buena inversión.

Alternativa # 2:

Tasa Interna de Retorno (TIR)	----------
Valor Actual Neto (VAN) (US$)	----------
Periodo de Recuperación (Años)	----------
Periodo Recuperación Descontado (Años)	----------

Figura. 5.4. Resultados-Rentabilidad-2

De igual manera para la alternativa # 2, se ingresan los valores de inversión de la Tabla. 5.5, para calcular el TIR y el VAN, dando como resultado, valores indeterminados y negativos respectivamente, por lo que a pesar de que sería una red propia del CECAI, demandaría una inversión inicial de casi el doble de capital, por lo que no sería una alternativa rentable por el momento.

También se puede mencionar que con el capital inicial, para que exista rentabilidad en la alternativa # 2, se tendría que pensar en una inversión a largo plazo, ya que se obtendrían resultados positivos en casi el doble de tiempo que la alternativa # 1.

Por lo que la alternativa # 1 resulta más rentable que la alternativa # 2, dado los resultados de rentabilidad antes mencionados, es por eso que se recomienda a la alternativa # 1 como posible solución al problema de comunicación antes descrito.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

- Una Red Wan, es una red por la cual se puede transmitir información a larga distancia, independientemente de la tecnología que se utilice, pudiendo interconectar diferentes ciudades de un país.

- Unos de los grandes beneficios que presta una red Wan, es la de enlazar a las diferentes redes Lan que pueda tener una empresa, ya sea que estén ubicadas en distintas ciudades como es en nuestro caso, además existe una variedad de tecnologías, las cuales debemos ir adaptando según sean las necesidades de la empresa.

- Las redes por lo general se forman por un conjunto de enlaces, unidos de dos en dos, con esta posibilidad se pueden crear diferentes tipos de topologías, según la conveniencia y estudios del diseñador.

- Previo a la elección de las tecnologías se debe realizar estudios como por ejemplo: donde se encuentra ubicado cada centro, número de equipos, situación geográfica, costo de cada tecnología a implementar.

- Para la elección del medio de transmisión se debe tener en cuenta ciertos factores como los siguientes: la naturaleza de la información que debe soportar la red, la infraestructura que poseen nuestras instalaciones considerando distancias e interferencias.

- Las pérdidas de datos en la actualidad es insustituible y se convierte en un peligro real cuando la empresa conecta su red con el mundo exterior, y por lo general se debe recurrir a mecanismos de control y prevención para minimizar los riesgos que nuestra red pueda tener.

- Como la empresa tendrá acceso a Internet, que permitirá mejorar su forma de comunicación, tanto a profesores, alumnos y público en general, no obstante las

redes internas serán propensas a recibir ataques, también puede resultar afectada la red por el inadecuado uso por parte de alumnos o empleados.

- Para garantizar un buen nivel de seguridad, que una red requiere se deben tomar en cuenta preguntas muy sencillas, como por ejemplo: cuál es el valor de los datos que queremos proteger, cuál será el impacto en nuestra empresa si llegáramos a perder aquellos datos, y cuáles son los riesgos que nuestra empresa esta expuesta sino implementamos un sistema de seguridad

- Un firewall es un elemento muy importante dentro de las características de seguridad que una red debe tener ya que permite ejercer políticas de control de acceso entre las redes, además el firewall define los servicios a los que los usuarios pueden acceder, es decir que un firewall puede considerarse como un mecanismo para bloquear tráfico no permitido, y otro para dejar que tráfico seguro circule por nuestra red.

- Los firewall también son importantes ya que nos permiten ejercer restricciones y donde se pueden aplicar políticas se seguridad y auditorias, proporcionado al administrador de la red, información del tipo y cantidad de tráfico que fluye por nuestra red, además de informar del número de veces que se ha intentado violar la seguridad de la red.

- Es necesario nombrar ciertas normas o consejos de seguridad para una empresa como por ejemplo: exigir al personal que elijan contraseñas que no sean evidentes, cambiar contraseñas cada cierto tiempo, instruir al personal sobre riesgo de seguridad de archivos, implementar soluciones de seguridad que satisfagan los requerimientos de la empresa.

- Con cualquiera de las dos alternativas expuestas se logrará optimizar los procesos que se desarrollan en el CECAI, haciendo que la empresa sea más productiva y competitiva para beneficio de su personal y estudiantes, en general los procesos internos que se realizan en el CECAI, deberán tener un control de todas las operaciones que se realicen especialmente en el acceso a la base de datos y transferencia de archivos.

- Los enlaces a larga distancia son un punto fundamental para las comunicaciones punto a punto o para crear una red de área extensa, pudiendo abarcar el diseño distintas topologías que garanticen un correcto y eficaz traslado de la información de un extremo a otro.

- Mediante la alternativa número 1, se logró enlazar a veinte (20) centros asociados al CECAI, con un nodo central ubicado en la Escuela Politécnica del Ejercito (Sangolquí), con todos los niveles se seguridad, además controlando el acceso a internet mediante un Proxy Server.

- Mediante la alternativa número 2, se logró enlazar a ocho (8) centros asociados al CECAI, que se especifica en el capítulo IV, además se garantiza que los enlaces estén disponibles las 24 horas del día, así como los 365 días del año.

- Al realizar el estudio de un enlace se debe tomar en cuenta algunos factores como la visibilidad o línea de vista entre los sitios a enlazar, así como la distancia a la que se encuentran, para de esta manera escoger los equipos necesarios para garantizar un enlace confiable.

- Es indispensable a la hora de diseñar un radio enlace que acudamos al Instituto Geográfico Militar para la obtención de mapas que nos proporcionarán el perfil o situación real de los sitios en estudio, a fin de mejorar la ruta de enlace y proyectar la solución más adecuada.

- Dado el análisis de los datos y la destreza que se adquirió en la realización de los enlaces, se logró interpretar condiciones de potencia, atenuaciones y antenas, etc., que son parámetros que determinan que un enlace funcione correctamente.

- Algunos parámetros son indispensables al momento de decidir implementar un radio enlace, ya que no se puede correr el riesgo de perder capital y tiempo en el montaje de la infraestructura, parámetros como zonas de Fresnel y simplemente niveles de seguridad nos pueden evitar caer en un sin número de problemas.

- Los trámites legales para la obtención del título habilitante para la implantación de un red privada, son estrictamente necesarios, teniendo en cuenta que una red privada tiene prohibido la prestación de servicios a otros usuarios, además

cualquier incumplimiento del contrato producirá de manera automáticamente la anulación de dicho titulo.

- Existen ciertas ventajas en los enlaces microonda como por ejemplo: El volumen de inversión generalmente es más reducido comparada con otra tecnología, la instalación en ciertos casos es más rápida y sencilla, además se puede superar las irregularidades del terreno, la regulación solo debe aplicarse al equipo puesto que las características del medio de transmisión son prácticamente constantes en el ancho de banda, puede aumentarse la separación entre las repetidoras incrementado la altura de las torres.

- También se ha determinado ciertas desventajas como son la necesidad de acceso adecuado para la instalación de las estaciones repetidoras, las condiciones atmosféricas pueden ocasionar desvanecimientos intensos y desviaciones del haz, lo que implicaría utilizar sistemas de diversidad y equipos auxiliares

- Es importante el análisis de la rentabilidad ya que determinada el porque de una inversión, partiendo de beneficios y pérdidas, es decir en el crecimiento y estabilidad de la empresa. Un proyecto requiere de una inversión y se la puede considerar como una actividad económica por lo tanto se debe entender variables fundamentales como rentabilidad y seguridad.

- Analizando los valores de TIR y VAN, vemos que son favorables para la alternativa # 1, teniendo un tiempo de recuperación de casi 3 años, por lo que se garantiza que puede ser una buena inversión.

- En la alternativa # 2, se procedió a calcular el TIR y el VAN, dando como resultado, valores indeterminados y negativos respectivamente, por lo que a pesar de que sería una red propia del CECAI, demandaría una inversión inicial de casi el doble de capital, por lo que no sería una alternativa rentable por el momento.

- También se puede mencionar que con el capital inicial, para que exista rentabilidad en la alternativa # 2, se tendría que pensar en una inversión a largo plazo, ya que se obtendrían resultados positivos en casi el doble de tiempo que la alternativa # 1.

- Este proyecto se realizó con la intención de afianzar los conocimientos adquiridos a lo largo de la carrera, además de aprender a manejar ciertas situaciones que se presentan en la elaboración de un diseño de red.

BIBLIOGRAFÍA

SENDIN ESCALONS, Alberto, *Fundamentos de los Sistemas de Comunicaciones*, McGraw, 2004.

RABANOS, Hernando, *Transmisión por Radio*, 3ra Edición, Areces, 1998.

SACCHI, Enrico, *Manual de Electrónica y Telecomunicaciones*, Editorial Omega, 2002, 2238.

MARTÏNEZ, David, *Tecnología de Telecomunicaciones*, Editorial Copyright, 2001, 576.

FREEMAN, Roger, *Ingeniería de Sistemas de Telecomunicaciones*, Segunda Edición, Editorial Limusa S.A., 1993.

ORELLANA, Sergio, *Análisis de Rentabilidad Económica y Financiera*, Tercera Edición, ESAN Ediciones, 2003.

- www.qualita.com.mx, Optimización de Anchos de Banda
- www.conatel.gov, Derechos de Registro
- www.andrew.com, Fabricante de Equipos para Comunicaciones.
- www.microflect.com, Fabricante de Repetidores Pasivos
- www.harris.com, Fabricante de equipos de telecomunicaciones
- http://www.fao.org, Análisis y Selección de Alternativas

ANEXO 1

REGLAMENTO PARA EL OTORGAMIENTO DE TÍTULOS HABILITANTES PARA LA OPERACIÓN DE REDES PRIVADAS

ANEXO 1

REGLAMENTO PARA EL OTORGAMIENTO DE TÍTULOS HABILITANTES PARA LA OPERACIÓN DE REDES PRIVADAS

Capítulo I

Art. 1.- Objeto.- El presente reglamento tiene por objeto regular los procedimientos para la instalación y el otorgamiento de títulos habilitantes, para la operación de redes privadas de acuerdo a lo establecido en el Reglamento General a la Ley Especial de Telecomunicaciones.

Art. 2.- Definición.- Redes privadas son aquellas utilizadas por personas naturales o jurídicas exclusivamente, con el propósito de conectar distintas instalaciones de su propiedad que se hallen bajo su control. Su operación requiere de un permiso.

Una red privada puede estar compuesta de uno o más circuitos arrendados, líneas privadas virtuales, infraestructura propia o una combinación de éstos. Dichas redes pueden abarcar puntos en el territorio nacional y en el extranjero. Una red privada puede ser utilizada para la transmisión de voz, datos, sonidos, imágenes o cualquier combinación de éstos.

Art. 3.- Las definiciones de los términos técnicos usados en el presente reglamento serán las establecidas en la Ley Especial de Telecomunicaciones y su reglamento general.

Art. 4.- Las redes privadas serán utilizadas únicamente para beneficio de un solo usuario y no podrán sustentar bajo ninguna circunstancia la prestación de servicios a terceros. Las redes privadas no podrán interconectarse entre sí, ni tampoco con una red pública. Se considerará como un solo usuario a:

a) Cualquier grupo de personas naturales dentro del cuarto grado de consanguinidad o segundo de afinidad; o,

b) Dos o más personas jurídicas, si:

1) El cincuenta y uno por ciento (51%) o más del capital social de una de ellas pertenece directamente o a través de terceros a la titular del permiso; o,

2) El cincuenta y uno por ciento (51%) del capital social de cada una de ellas se encuentra bajo propiedad o control de una matriz común.

Art. 5.- Una red privada no podrá ser utilizada, directa o indirectamente, para prestar servicios de telecomunicaciones en el territorio nacional o en el extranjero. Por lo tanto, no podrá realizar transmisiones a terceros hacia o desde una red pública dentro del país.

Un representante debidamente autorizado por cada título habilitante para operar una red privada entregará anualmente a la Superintendencia un certificado confirmando que dicha red está siendo operada de conformidad con este reglamento.

Art. 6.- Título habilitante.- La operación de redes privadas, requiere de un título habilitante, que será un permiso otorgado por la Secretaría Nacional de Telecomunicaciones, previa autorización, del Consejo Nacional de Telecomunicaciones.

Capítulo II

Art. 7.- Cualquier persona natural o jurídica, domiciliada en el país, podrá solicitar a la Secretaria Nacional de Telecomunicaciones un permiso para la operación de redes privadas.

El plazo de duración de los permisos será de cinco (5) años, prorrogables por igual período, a solicitud escrita del interesado, presentada con tres meses de anticipación al vencimiento del plazo original, siempre y cuando haya cumplido con los términos y condiciones del título habilitante. Cumplido el plazo el permiso caducará ex lege.

Art. 8.- Requisitos.- Las solicitudes para el otorgamiento de títulos habilitantes para la operación de redes privadas deberán acompañarse con los documentos y previo el cumplimiento de los requisitos determinados en el Reglamento General a la Ley Especial de Telecomunicaciones:

a) Identificación y generales de ley del solicitante;

b) Proyecto técnico de la red a operar; y,

c) Requerimientos de conexión.

Art. 9.- Proyecto técnico.- El proyecto técnico, elaborado por un ingeniero en electrónica y telecomunicaciones, contendrá:

a) Descripción de los equipos, sistemas, recursos principales, y los requisitos de conexión interna y externa;

b) Descripción técnica detallada de la red propuesta, incluyendo los puntos geográficos de conexión; con redes existentes en caso de existir circuitos alquilados como parte de la red privada; y,

c) Identificación de los recursos del espectro radioeléctrico necesarios para operar la red y la respectiva solicitud de concesión.

En caso de utilizar los servicios de cualquier servicio portador, el solicitante deberá adjuntar copia simple del contrato respectivo.

Para efectos de la conexión se sujetará a lo dispuesto en el respectivo reglamento.

Toda la información anterior será considerada confidencial con excepción de la identificación del solicitante.

Art. 10.- El título habilitante especificará por lo menos:

a) El objeto;

b) La descripción de la red privada autorizada y ubicación geográfica; y,

c) Las causales de revocatoria y caducidad del permiso.

No se otorgarán títulos habilitantes de índole genérica, abierta o ilimitada.

Capítulo III

Art. 11.- En el caso de títulos habilitantes que no requieran de concesión para el uso de frecuencias, la Secretaría entregará su informe al Consejo Nacional de Telecomunicaciones en el término de veinte (20) días contados a partir de la fecha de presentación de la solicitud.

Si el informe de la Secretaría es favorable y no hay oposición, la solicitud se considerará aprobada a menos que el Consejo Nacional de Telecomunicaciones emita una

decisión negativa, en el término determinado en el Reglamento General a la Ley Especial de Telecomunicaciones. Para efectos de oposición de terceros, la Secretaria publicará, en su página electrónica las solicitudes presentadas mientras transcurre el término para presentación de su informe.

Cuando estén involucradas concesiones para el uso de espectro radioeléctrico los efectos del silencio administrativo se sujetarán a las normas del reglamento respectivo.

Art. 12.- Oposición. En caso de oposición de un legítimo interesado, las partes podrán ejercer su derecho de legítima defensa presentando pruebas y exposiciones de conformidad con lo establecido en el reglamento pertinente.

Art. 13.- Los títulos habilitantes para operación de una red privada otorgados por el Consejo Nacional de Telecomunicaciones, que requieren uso del espectro radioeléctrico deben obtener, además, el correspondiente título habilitante para la asignación del espectro radioeléctrico, debiendo realizarse los dos trámites simultáneamente.

Una vez aprobados los documentos y calificado el estudio técnico por la Secretaría Nacional de Telecomunicaciones se procederá a la entrega y registro del título habilitante para la operación de la red, previa autorización del Consejo Nacional de Telecomunicaciones.

Art. 14.- Modificaciones de la Configuración de la Red.- Toda modificación o adición a la infraestructura sobre la que se soporta la red debe ser reportado a la Secretaría Nacional de Telecomunicaciones así como a la Superintendencia de Telecomunicaciones.

La Secretaría Nacional de Telecomunicaciones registrará los cambios de configuración en el Registro Nacional de Telecomunicaciones.

Art.15.-Derechos.- Por concepto de derechos por los títulos habilitantes, los permisionarios pagarán el valor de 500 dólares de los Estados Unidos de América. Todo anexo o modificación al permiso original será gratuito siempre y cuando no implique el uso de espectro radioeléctrico o servicios que se encuentren sujetos a tasas, gravámenes, pago de derechos u otros, en cuyo caso deberá pagarse los correspondientes valores.

Art. 16.- Los costos de administración de contratos, registro, control y gestión serán retribuidos mediante derechos fijados por los, organismos competentes, en función de los gastos que demanden dichas tareas para los organismos de administración y control.

Art. 17.- Renovaciones.- Si la configuración de la red hubiese cambiado, el titular deberá presentar las actualizaciones de la misma. Si no hubiese cambiado la configuración de la red se procederá a la renovación con la actualización del certificado de existencia legal, la presentación del Registro Único de Contribuyentes y la cancelación del valor correspondiente por concepto de renovación.

La renovación procederá solamente, si el permisionario ha cumplido con las obligaciones que le imponen la ley, los reglamentos y el título habilitante respectivo.

Art. 18.- Revocatorias.- El incumplimiento de las condiciones y términos del título habilitante conllevará la caducidad del mismo, previa declaratoria de la Secretaria Nacional de Telecomunicaciones sin perjuicio de la aplicación de las causales aplicables que consten en el Estatuto Jurídico de la Función Ejecutiva.

El permiso podrá ser revocado en cualquier momento por razones de oportunidad o legitimidad por la Secretaría Nacional de Telecomunicaciones.

Capítulo III

Art. 19.- La operación de las redes privadas, esta sujeta a las normas de regulación, control y supervisión, emitidas por el Consejo Nacional de Telecomunicaciones, la Secretaría Nacional de Telecomunicaciones y la Superintendencia de Telecomunicaciones, de conformidad con las potestades que corresponden a dichos organismos.

Art. 20.- Control. La Superintendencia de Telecomunicaciones podrá realizar los controles que sean necesarios a la operación de las redes privadas con el objeto de garantizar el cumplimiento de la normativa vigente y de los términos y condiciones bajo los cuales se hayan otorgado los títulos habilitantes, y podrá supervisar e inspeccionar, en cualquier momento, las instalaciones de dichas redes, a fin de garantizar que no estén violando lo previsto en el presente reglamento.

Los titulares deberán facilitar las labores de inspección de la Superintendencia y proporcionar la información indispensable para fines de control.

Art. 21.- El titular deberá permitir y facilitar los controles que la Superintendencia de Telecomunicaciones requiera así como proporcionar la información técnica necesaria para la administración del contrato y supervisión de la red.

Art. 22.- Delegación Administrativa.- El Secretario Nacional de Telecomunicaciones podrá delegar a las direcciones regionales la capacidad de tramitar, para su posterior aprobación, por el Consejo Nacional de Telecomunicaciones, dentro del ámbito de su competencia, los correspondientes títulos habilitantes de operación de redes privadas, así como el cobro de los correspondientes derechos. Sin embargo toda la, documentación deberá reposar, en originales, en el Registro Nacional de Telecomunicaciones.

ANEXO 2

CONTRATO PARA EL OTORGAMIENTO DEL PERMISO PARA LA OPERACIÓN DE REDES PRIVADAS

ANEXO 2

CONTRATO PARA EL OTORGAMIENTO DEL PERMISO PARA LA OPERACIÓN DE REDES PRIVADAS

LA SECRETARÍA NACIONAL DE TELECOMUNICACIONES otorga el presente título habilitante, que constituye un permiso de operación de red privada a favor de.....

El presente título habilitante estará sujeto a las siguientes condiciones técnicas, legales y económicas:

1. CONDICIONES TÉCNICAS (Descripción de la red privada).

1.1. INFRAESTRUCTURA

1.2. UBICACIONES DE LAS INSTALACIONES A CONECTAR

1.3. CIRCUITOS ARRENDADOS: (En caso de haberlos)

2. CONDICIONES LEGALES

2.1. La red privada, solo podrá ser utilizada por el titular del presente instrumento.

2.2. Dicha red no podrá sustentar, bajo ninguna circunstancia, la prestación de servicios a terceros.

2.3. La red privada cuyo funcionamiento se autoriza en virtud del presente instrumento, no podrá interconectarse con otras redes, ni con una red pública. No obstante, de conformidad con el artículo 35 del Reglamento General a la Ley Especial de Telecomunicaciones Reformada, el permisionario podrá solicitar a cualquier concesionario de servicios de telecomunicaciones, la conexión de su red a la red pública que éste opere.

Las conexiones entre la red privada con determinada red pública, requerirán la suscripción de los respectivos convenios de conexión los que tendrán que ser registrados en la Secretaría Nacional de Telecomunicaciones.

2.4. ..... se compromete a entregar anualmente a la Superintendencia de Telecomunicaciones, un certificado confirmando que la red autorizada está siendo operada de conformidad con el presente título habilitante, la Ley y el Reglamento. Deberá anexar el diagrama y la descripción actualizada de la red, así como los convenios de conexión con redes públicas.

2.5. ..... , no podrá ceder o transferir a terceros sus derechos y obligaciones establecidas en el presente título habilitante. En caso de que así lo hiciera la Secretaría Nacional de Telecomunicaciones está facultada para declarar su terminación, previo informe de la Superintendencia de Telecomunicaciones.

2.6. El presente título habilitante podrá ser revocado por razones de oportunidad o legitimidad de oficio o a petición de parte, de conformidad con la Ley.

La Secretaría Nacional de Telecomunicaciones podrá declarar la terminación del presente permiso en caso de incumplimiento, por parte de su titular, de las obligaciones derivadas de este instrumento, la ley y los reglamentos. En caso de incumplimiento de orden técnico, se requerirá de un informe previo de la Superintendencia de Telecomunicaciones.

2.7. Este título habilitante tendrá una duración de cinco (5) años, prorrogables por igual período.

2.8. Dentro del plazo de cinco (5) días contados a partir de la expedición del presente instrumento, su titular deberá registrarlo en el Registro Público de Telecomunicaciones, previo el pago de los derechos que correspondan.

2.9. Toda modificación o adición a la infraestructura sobre la que se soporta la red privada objeto de este título habilitante, deberá ser reportada a la Secretaría Nacional de Telecomunicaciones y a la Superintendencia de Telecomunicaciones. La Secretaría Nacional de Telecomunicaciones registrará los cambios en el Registro Público de Telecomunicaciones.

3. CONDICIONES ECONÓMICAS

El permisionario cancela previo al otorgamiento del presente instrumento, la suma de US$ ..... por concepto de Derechos de Permiso.

En todo lo no contemplado expresamente en este Instrumento, su titular se sujeta a la Ley Especial de Telecomunicaciones Reformada, su Reglamento General, el Reglamento de Redes Privadas y más normativa aplicable expedida por el CONATEL.

ANEXO 3

REQUISITOS PARA OBTENER EL PERMISO DE OPERACIÓN DE UNA RED PRIVADA

ANEXO 3

REQUISITOS PARA OBTENER EL PERMISO DE OPERACIÓN DE UNA RED PRIVADA

PERSONA NATURAL:

1. Solicitud dirigida al Señor Secretario Nacional de Telecomunicaciones.
2. Copia del RUC.
3. Copia de la cédula de identidad.
4. Copia del último certificado de votación.
5. Anteproyecto técnico elaborado y suscrito por un ingeniero en electrónica y/o telecomunicaciones (debidamente colegiado, adjuntar copia de la licencia profesional).
6. Recibo de pago del uno por mil (Art. 12 de la Ley de Ejercicio Profesional de la Ingeniería).

COMPAÑIAS:

1. Solicitud dirigida al Señor Secretario Nacional de Telecomunicaciones.
2. Escritura de constitución de la compañía domiciliada en el país.
3. Nombramiento del Representante Legal, debidamente inscrito en el Registro Mercantil.
4. Certificado de obligaciones emitido por la Superintendencia de Compañías.
5. Copia del RUC.
6. Copia de la cédula de identidad del Representante Legal.
7. Copia del último certificado de votación, del Representante Legal.
8. Anteproyecto técnico elaborado y suscrito por un ingeniero en electrónica y/o telecomunicaciones (debidamente colegiado, adjuntar copia de la licencia profesional).
9. Recibo de pago del uno por mil (Art. 12 de la Ley de Ejercicio Profesional de la Ingeniería).

ANTEPROYECTO TÉCNICO

A fin de demostrar la viabilidad de la solicitud el Anteproyecto Técnico deberá contener lo siguiente:

1. Descripción técnica detallada del o los servicios que soportará la red, especificando el tipo de información que cursará sobre ella.
2. Diagrama funcional de la red, que indique claramente los elementos activos y pasivos de la misma. Describir su funcionamiento basado en el diagrama.
3. Gráfico esquemático detallado de la red a instalarse, el cual debe estar asociado a un plano geográfico, en el que se indiquen la trayectoria del medio físico de transmisión o los enlaces radioeléctricos que se van a utilizar. Dicho gráfico deberá contener las direcciones exactas de las instalaciones.
4. Especificaciones técnicas del equipamiento a utilizarse y de los medios físicos que se emplearían. Incluir una copia de los catálogos técnicos.
5. Indicar los recursos del espectro radioeléctrico requeridos, especificando la banda cual se va a operar, así como los requerimientos de ancho de banda. (Adjuntar una copia de los formularios de solicitud debidamente llenados). En caso de usar equipos que utilizan tecnología de Espectro Ensanchado, adjuntar una copia del certificado de homologación e indicar los números de serie y de las etiquetas de homologación de los mismos.
6. Si se requiere el arrendamiento de circuitos, deberá adjuntarse la carta compromiso otorgada por la empresa que va a proveer los mismos, que indique las características técnicas de operación.
7. Requerimiento de conexión. (Interna o Externa)

Redes privadas *son aquellas utilizadas por personas naturales o jurídicas en su exclusivo beneficio, con el propósito de conectar distintas instalaciones de su propiedad o bajo su control, por lo cual se servirá demostrar que las instalaciones a implementarse son de su propiedad o están bajo su control remitiendo una copia del titulo de propiedad o contrato (convenio) de arrendamiento del lugar donde se ubicarán los equipos y especificando el tipo de instalación a implementarse (estación repetidora o terminal) y la finalidad de la estación terminal (matriz, sucursal, bodega, oficina,.).*

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO DE TÉRMINOS

CECAI: Centro de Capacitación Informática

LAN: Red de Área Local

WAN: Red de Área Extensa

Multiplexores: Es un dispositivo que acepta varias líneas de datos a la entrada y la convierte en una sola línea de datos.

Host: Computadora destinada a ejercer tareas de red.

Enrutador: Elementos de conmutación 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.

ECD: Equipo de Comunicación de Datos, que presupone un cierto procesamiento o inteligencia.

ETD: Equipo Terminal de Datos, que consta de terminales o equipo periférico sin inteligencia.

PVC: Circuito Virtual Permanente.

CCR: Centro de Control de Red.

BPS: Bit por segundo.

CSU: Unidad de Servicio de Canal.

DSU: Unidad de Servicio de Datos.

NRZ: No Retorno a Cero

AMI: Alternate Marks Inverted, modo de Transmisión bipolar.

Simétrico: Velocidad de subida es igual a la velocidad de conexión de bajada.

Asimétrico: Las velocidades de conexión tanto de envío como recepción de datos es distinta.

SVC: Circuitos Virtuales Conmutados.

PSTN: Red Pública de Conmutación Telefónica.

Router: Un router es un conmutador de paquetes que opera en el nivel de red del modelo OSI.

X.25: Un estándar WAN de protocolos y formatos de mensajes, se utiliza para tener acceso a una red de datos.

Líneas de Transmisión: También llamados circuito o canales, por aquí circula la información de una máquina a otra.

RTB: Red Telefónica Básica.

MAC: Media Access Control, Especificación de la IEEE sobre la transmisión de datos del modelo OSI.

RDSI: Red Digital de Servicios Integrados.

ISP: Proveedor de Servicio de Internet.

ADSL: Bucle de Abonado Digital Asimétrico

ATM: Modo de transferencia Asincrónico, Tecnología de red que transfiere paquetes de datos para el posterior reenvío de diferentes tipos de información.

VPN: Red Privada Virtual.

Splitter: Es un filtro que separa las frecuencias correspondientes a la voz (o telefonía convencional) de las frecuencias sobre las que se modulan los datos digitales.

CMTS: Cable MODEM Termination System.

MODEM: Un dispositivo que convierte señales de datos digitales y binarias, a una señal compatible con el medio que se está utilizando.

QAM: Modulación en Amplitud y Cuadratura.

PLC: Power Line Communication

WLL: Wireless Local Loop, Bucle de Abonado Vía Radio.

DECT: Digital European Cordiess Telecommunication.

CDMA: Acceso Múltiple por División de Código.

PCM: Modulación por Codificación de Pulsos.

TDM: Modulación por División de Tiempo.

FDM: Modulación por división de Frecuencia.

UIT-T: Unión Internacional de telecomunicaciones.

ADM: Add-Drop Multiplexer.

SDH: Jerarquía Digital Sincrónica.

CCITT: Comité Consultivo Internacional para la Telefonía y Telegrafía.

SONET: Red Óptica Sincrónica.

STM: Synchronous Transfer Modem, velocidad fundamental del SDH.

PDH: Jerarquía Digital Plexórica.

LTE: Equipos Terminales de Línea.

ISO: Organización de Estándares Internacionales.

IETF: Internet Engineering Task Force.

ETA: Asociación de Industrias Electrónicas.

G.703: Recomendación de la ITU-T, relativas a los aspectos generales de una interfaz.

HSSI: Interfase Serial de Alta Velocidad.

SDLC: Control de Enlace Sincrónico de Datos.

HDLC: High level Data Link Control, protocolo de bit de la capa de conexión.

LAPB: Link Access Procedure Balanced.

PPP: Protocolo Punto a Punto.

VCC: Conexión de Canales Virtuales.

VPC: Conexión de Caminos Virtuales.

QoS: Calidad de Servicio.

BER: Tasa de Error de Bit.

UDP: Protocolo de Transporte de Internet.

ICMP: Internet Control Message Protocol, este es el proceso TCP/IP que prevé el set de funciones utilizado para ele control y manejo de la capa de red.

FTP: Protocolo de Transferencia de Archivos.

SMTP: Programa de Transferencia de correo simple, protocolo de aplicación para correo electrónico.

DES: Data Encryption Standard.

IDEA: Internacional Data Encryption Algorith.

HTTP: Protocolo de Transferencia de Hipertexto .

Proxy: Equipos usados para establecer el control del tráfico saliente de una red.

ÍNDICE DE DATA-SHEET

DATA SHEET-1

ROUTER CISCO 1751 (VER CD)

DATA SHEET-2

ROUTER CISCO 3600 (VER CD)

DATA SHEET-3

SWITCH CISCO 2950 (VER CD)

DATA SHEET-4

RADIO MEGASTAR 155 PX (VER CD)

DATA SHEET-5

ANTENA UHX6-59W (VER CD)

Sangolquí, _____

Elaborado por:

_____

Mauricio Fernando Navas Gallardo

Decano

_____

Ing. Xavier F. Martínez C.
Tcrn. de E.M.

Secretario Académico

_____

Ab. Jorge Carvajal R.