FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

Creación de un Sistema de Monitoreo de Respaldo de Frecuencias de Radiodifusión y Televisión para la Jurisdicción de la Intendencia Regional Costa de la Superintendencia de Telecomunicaciones

Previa la obtención del Título

INGENIERO EN TELECOMUNICACIONES

CON MENCION EN GESTIÓN EMPRESARIAL EN TELECOMUNICACIONES

ELABORADO POR:

ANDREA CECILIA TORRES AVILÉS

ANGY KAROLINA USCA COROZO

GUAYAQUIL, ENERO DE 2013

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por la Srta. Andrea Cecilia Torres Avilés y la Srta. Angy Karolina Usca Corozo como requerimiento parcial para la obtención del título de INGENIERO EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL EN TELECOMUNICACIONES

Guayaquil, Enero de 2013

ING. LUZMILA RUILOVA

DIRECTORA

REVISADO POR

ING. JUAN GONZALEZ BAZAN

ING. CARLOS ZAMBRANO MONTES

ING. MIGUEL HERAS SANCHEZ

RESPONSABLE ACADÉMICO

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

DECLARACIÓN DE RESPONSABILIDAD

TORRES AVILÉS ANDREA CECILIA

USCA COROZO ANGY KAROLINA

DECLARAN QUE:

El proyecto de grado denominado "Creación de un Sistema de Monitoreo de Frecuencias de Radiodifusión y Televisión para la Jurisdicción de la Intendencia Regional Costa de la Superintendencia de Telecomunicaciones" ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de nuestra autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto de grado en mención.

Guayaquil, Enero de 2013

LAS AUTORAS

TORRES AVILÉS ANDREA CECILIA

USCA COROZO ANGY KAROLINA

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Nosotras, TORRES AVILÉS ANDREA CECILIA Y

USCA COROZO ANGY KAROLINA

Autorizamos a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del proyecto titulado: "Creación de un Sistema de Monitoreo de Frecuencias de Radiodifusión y Televisión para la Jurisdicción de la Intendencia Regional Costa de la Superintendencia de Telecomunicaciones", cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Guayaquil, Enero de 2013

LAS AUTORAS

TORRES AVILÉS ANDREA CECILIA

USCA COROZO ANGY KAROLINA

AGRADECIMIENTO

Agradezco a Dios, por darme la vida y la oportunidad de estar donde estoy. A mi familia: mis padres y hermanos, por apoyar cada paso que doy y por brindarme todo su inmenso amor. Y finalmente, a mi familia Ampuño Avilés, por acogerme en su hogar y hacerme sentir una de los suyos.

Andrea

Agradezco a Dios por dame la fuerza para superar cualquier adversidad que se cruzara en mi camino. A mi madre por ese apoyo incondicional durante todos estos años que me han llevado a donde estoy. A mi compañera de tesis, por su paciencia y esfuerzo para sacar este proyecto adelante.

Angy

DEDICATORIA

Este trabajo lo dedico a mis padres, Cecilia y Guilbert, a quienes amo con todo mí ser y han sido mi inspiración y ejemplo a seguir desde siempre. Ellos con su trabajo constante, dedicación y abnegación me han enseñado que se debe sentir amor por lo que se hace y me han demostrado que un profesional debe ser ante todo, honesto y responsable.

Andrea

Dedico este proyecto a mi madre, ya que si no fuera por ella, su trabajo duro y confianza en mi no hubiese podido alcanzar las metas que me propuse, por ser ese ejemplo de vida para mis hermanos y para mí, por ser mi todo.

Angy

RESUMEN

En el presente trabajo se proporciona una opción de solución a la problemática que representa para la Intendencia Regional Costa (IRC) de la Superintendencia de Telecomunicaciones, SUPERTEL, la inhibición periódica de su *Sistema Automático para el Control del Espectro Radioeléctrico (SACER),* con el cual se realiza el monitoreo de las frecuencias del espectro radioeléctrico de las provincias que se encuentran bajo su jurisdicción. Con este monitoreo la IRC de la SUPERTEL se asegura de que la programación transmitida por las estaciones radiales y televisivas cumplen con los parámetros establecidos por la ley; de manera contraria, si detecta irregularidades, procede a emitir las sanciones respectivas. Para cumplir con este cometido se deben mantener registros ininterrumpidos de dichas transmisiones para contar con un respaldo de la infracción cometida, pero durante el lapso en el que se inhibe el SACER, no hay manera de continuar con el monitoreo. Es por eso que se propone un sistema de monitoreo de respaldo que reemplace al SACER durante el tiempo en el que se mantenga fuera de funciones.

En este trabajo se desarrollan 4 capítulos, de los cuales, en el primero se detallan los antecedentes, problemática, hipótesis y los objetivos planteados para alcanzar la solución. En el segundo capítulo se presentan las opciones de conexión sobre las cuales se podría basar el sistema. Una vez escogida la conexión WAN sobre infraestructura pública, se definen, en el tercer capítulo las VPN (*Virtual Private Network*, Red Privada Virtual) que ofrecen un nivel de seguridad a los datos a transmitir ya que se lo hará por un medio inseguro. Finalmente en el cuarto capítulo se realiza una integración de todos los conceptos expuestos y se indica el funcionamiento del sistema de monitoreo de respaldo.

ÍNDICE GENERAL

CAPÍTULO 3 VIRTUAL PRIVATE NETWORK

ÍNDICE DE GRÁFICOS

CAPÍTULO 1 GENERALIDADES

CAPÍTULO 2 OPCIONES DE CONEXIÓN WAN

CAPÍTULO 3 VIRTUAL PRIVATE NETWORK

CAPÍTULO 4 FUNCIONAMIENTO DEL SISTEMA DE MONITOREO DE RESPALDO

ÍNDICE DE TABLAS

CAPÍTULO 1

GENERALIDADES

En este capítulo se expone la problemática que llevó a desarrollar el presente trabajo, la hipótesis planteada y los objetivos propuestos para resolver dicho problema; partiendo de los antecedentes de la SUPERTEL, institución para la cual se busca brindar una solución.

1. 1 INTRODUCCIÓN

La Constitución de la República del Ecuador en el artículo 213 establece que: "Las superintendencias son organismos técnicos de vigilancia, auditoría, intervención y control de las actividades económicas, sociales y ambientales, y de los servicios que prestan las entidades públicas y privadas, con el propósito de que estas actividades y servicios se sujeten al ordenamiento jurídico y atiendan el interés general".

La Ley Especial de Telecomunicaciones publicada en el Registro Oficial No. 996 de 10 de agosto de 1992, creó la Superintendencia de Telecomunicaciones. Luego, en la Ley Reformatoria a la Ley Especial de Telecomunicaciones publicada en el Registro Oficial No. 770 de 30 de agosto de 1995, establece que **la Superintendencia es el único ente autónomo encargado del control de las telecomunicaciones del país**, en defensa de los intereses del Estado y del pueblo, usuario de los servicios de telecomunicaciones. Tiene personería jurídica, régimen de contrataciones, administración financiera y contable y administración de recursos humanos autónomos, para tales efectos se rige por los reglamentos que expida el Presidente de la República.

La Superintendencia de Telecomunicaciones (SUPERTEL) es el organismo encargado de realizar el control técnico del espectro radioeléctrico y de los diferentes servicios de telecomunicaciones, realiza el control preventivo y correctivo de los parámetros técnicos establecidos en los contratos, registros y autorizaciones.

Los servicios controlados por esta entidad son:

- **Telecomunicaciones:**

Telefonía Fija; Servicio Móvil Avanzado (Telefonía Móvil); Servidores Portadores; Valor Agregado (Acceso a Internet); "Cyber Cafés"; Terminales de uso público.

- **Radiocomunicaciones:**

Fijo y Móvil terrestre; Sistemas comunales; Buscapersonas; Sistema Troncalizado; Enlaces Radioeléctricos; Transmisión de datos; Satelital privado; Banda ciudadana; Radioaficionados; Homologaciones; Emisiones no ionizantes.

- **Radiodifusión y Televisión:**

Radiodifusión sonora; Televisión abierta; Televisión codificada; Audio y video por suscripción.

1.2 ANTECEDENTES

Para el cumplimiento de sus funciones, la SUPERTEL se divide en Delegaciones e Intendencias Regionales cuya jurisdicción se observa en la figura 1.1 y comprenden las siguientes provincias:

Intendencia Regional Norte:
Su jurisdicción comprende las provincias de Esmeraldas, Carchi, Imbabura, Pichincha, Cotopaxi, Sucumbíos, Orellana, Napo. Su sede es la ciudad de Quito.

Intendencia Regional Costa:
Su jurisdicción comprende las provincias de Guayas, El Oro, Los Ríos, Santa Elena. Su sede es la ciudad de Guayaquil.

Intendencia Regional Sur:
Su jurisdicción comprende las provincias de Loja, Azuay, Zamora Chinchipe y Morona Santiago. Su sede es la ciudad de Cuenca.

Delegación Regional Centro:

Su jurisdicción comprende las provincias de Tungurahua, Chimborazo, Bolívar y Pastaza. Su sede es la ciudad de Riobamba.

Delegación Regional Manabí:

Su jurisdicción comprende la provincia de Manabí. Su sede es la ciudad de Portoviejo.

Delegación Regional Galápagos:

Su jurisdicción comprende la provincia de Galápagos. Su sede es la ciudad de Puerto Ayora, Isla Santa Cruz.

El desarrollo del presente trabajo, se centrará en la jurisdicción de la **Intendencia Regional Costa.**

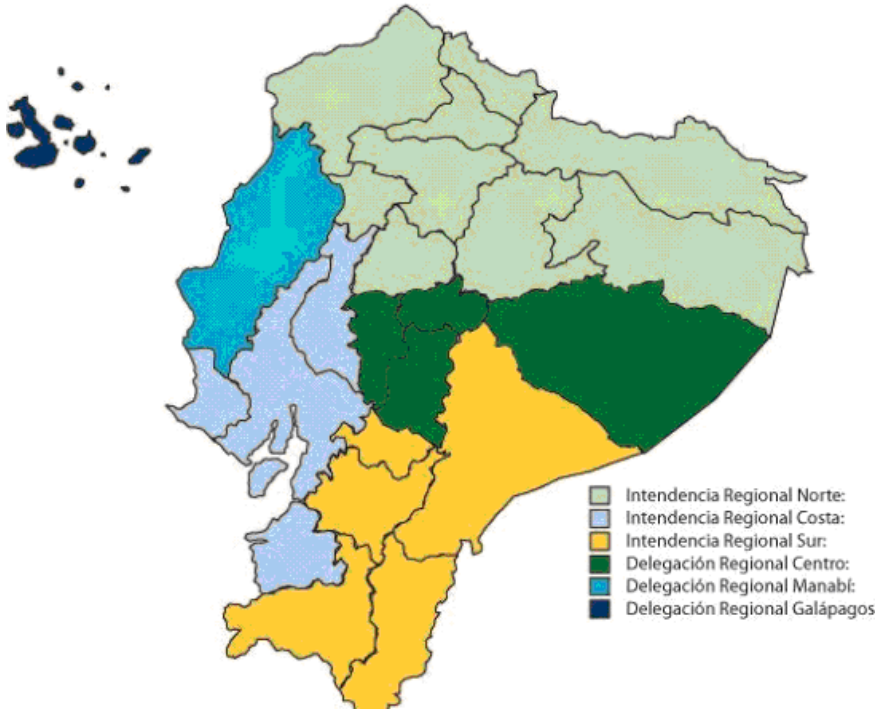


Figura 1.1 Mapa de las jurisdicciones de la SUPERTEL

Fuente: Trípticos de la SUPERTEL

Cada Intendencia Regional y la Delegación Regional Manabí cuenta con un ***Sistema Automático para el Control del Espectro Radioeléctrico (SACER)***, que básicamente consiste en un conjunto de equipos que se utilizan para el monitoreo remoto de la transmisión de las estaciones y canales de televisión en las frecuencias asignadas en el espectro radioeléctrico en las provincias de dicha región.

1.3 PLANTEAMIENTO DEL PROBLEMA

La Intendencia Regional Costa (IRC), con la cual se trabajará en este proyecto, tiene en su jurisdicción las provincias de Santa Elena, Guayas, los Ríos y El Oro. Actualmente el SACER realiza el monitoreo 24 horas al día de las frecuencias de radio y televisión de las provincias mencionadas, lo que provoca que en ocasiones el sistema se inhiba y en este lapso se dejan de grabar las transmisiones. Es justo aquí donde surge el inconveniente, la SUPERTEL es un organismo de control por lo que la IRC requiere tener registros de transmisión ininterrumpida.

Definición del problema: La Intendencia Regional Costa no puede quedarse sin registros de las transmisiones ya que sin los mismos, no puede proceder frente a los posibles reclamos o denuncias hechas sobre aquellas difusiones realizadas durante los periodos de tiempo en los que no se cuenta con el respaldo del SACER.

1.4 OBJETIVOS

Los objetivos planteados para la solución a la problemática presentada son:

1.4.1 OBJETIVO PRINCIPAL

Determinar una solución ante los periodos de inhibición del SACER para que la Intendencia Regional Costa de la SUPERTEL pueda monitorear ininterrumpidamente las provincias bajo su jurisdicción.

1.4.2 OBJETIVOS ESPECÍFICOS

- Diagnosticar el sistema actual de monitoreo.
- Diseñar un sistema de monitoreo con el iCOM para reemplazar al SACER en los periodos en los que no pueda almacenar las transmisiones debido a la inhibición del sistema.
- Verificar las funciones del iCOM para garantizar su óptima utilización en el nuevo sistema.
- Obtener información para plantear una solución eficaz para el acceso remoto al sistema.

1.5 HIPÓTESIS

La IRC cuenta con un equipo de recepción para computadoras denominado iCOM en su modelo IC-PCR2500, el cual es utilizado en la IRC para grabar el audio de la programación de las estaciones radiales y los canales de televisión. Luego, estas grabaciones son revisadas para verificar si las estaciones han transmitido las cadenas nacionales programadas con anterioridad por la Secretaria Nacional de Comunicación.

Utilizando el iCOM se formará un sistema de *backup* similar al SACER, utilizándolo para grabar las transmisiones que no almacene el SACER y mediante un enlace de banda dedicado o Internet se podrá acceder remotamente (desde las instalaciones de la IRC en Guayaquil) a las grabaciones de las demás ciudades para realizar el monitoreo adecuado.

En el siguiente capítulo se plantearán las opciones de enlaces que se podrían utilizar para realizar la conexión entre las instalaciones de la IRC en Guayaquil y los lugares remotos en los que se instalaría el nuevo sistema de monitoreo.

CAPÍTULO 2

OPCIONES DE CONEXIÓN WAN

Actualmente existen gran cantidad de opciones para implementar soluciones para redes WAN (*Wide Area Network*, Red de Área Amplia). Estas soluciones se pueden establecer sobre infraestructuras privadas o públicas, como el Internet.

2.1 OPCIONES DE CONEXIÓN WAN PRIVADAS

Una característica de los enlaces privados es la seguridad que brindan entre puntos finales de una transmisión de datos. Siempre hacen uso de una red de transmisión y en ocasiones de conmutación par realizar la conexión entre dichos puntos. Los enlaces privados van desde el orden de los Kbps hasta los Gbps; estos enlaces pueden ser Dedicados o Conmutados.

2.1.1 Enlaces Dedicados

Los enlaces dedicados, llamados también líneas arrendadas, utilizan líneas punto a punto a diferentes velocidades para conectar, a través de la red del proveedor, las distintas instalaciones de un cliente, de manera exclusiva, sin restricción de horarios o límites de utilización. Estos enlaces son usados para transmitir bidireccionalmente voz, datos y video entre dos ó más puntos que el cliente necesite conectar. Este tipo de enlaces presenta las siguientes ventajas:

- *Alto nivel de seguridad.* La información se transporta de manera confiable y segura.
- *Flexibilidad y adaptabilidad a las necesidades del cliente.* Se pueden combinar diversos elementos, como opciones de gestión y medio de transporte y así proporcionar soluciones específicas a medida que la empresa lo necesite.
- *Escalabilidad.* Las redes poseen gran flexibilidad, pudiendo expandir el dimensionamiento de las mismas cuando se lo necesite.

- *Eliminación de latencia.* La capacidad dedicada elimina los retardos y las fluctuaciones de fase extremo a extremo.
- *Disponibilidad.* No hay niveles de compartición, se trata de un enlace exclusivo para el cliente, pudiendo utilizarlo con las mismas características en cualquier momento.

Aunque cuentan con ventajas muy atractivas, las líneas arrendadas también presentan desventajas, tales como desaprovechamiento de capacidad, dado que ésta es fija, pero el tráfico frecuentemente es variable. La implementación de estas líneas supone un costo bastante elevado, dependiendo del ancho de banda y de la distancia entre los puntos. Además, cada punto terminal requiere de una interfaz física independiente en el *router*, lo cual aumenta el costo de mantenimiento.

Entre los enlaces dedicados podemos citar: enlaces inalámbricos, de fibra óptica y satelitales.

2.1.1.1 Enlaces Inalámbricos

Loe enlaces inalámbricos permiten grandes velocidades por lo cual son de los medios más utilizados, este tipo de transmisión a alta frecuencia requiere de línea de vista directa entre los puntos a enlazar. Como características principales se tiene:

- Cobertura de grandes distancias.
- Comparado con otros tipos de enlace, como el satelital, se presenta retardo de transmisión bastante bajo, hasta 30 milisegundos.
- Requiere línea de vista, lo que lleva a colocar repetidoras en zonas muy montañosas.
- Ancho de banda más barato que el satelital.

- Más mantenimiento que el satelital. Estaciones transmisoras y repetidoras que muchas veces estén en zonas de alto riesgo.
- Velocidades de transmisión altas. El, E3, ATM.

Los enlaces inalámbricos pueden ser punto a punto o punto-multipunto (Figura 2.1), proporcionando soluciones de conectividad para empresas con centros de trabajo con una o varias sucursales, que requieren compartir información con gran coordinación. De esta manera, todas las localidades conectadas por el enlace formarán parte de una única red local, exactamente como si estuvieran en el mismo edificio, pero con la flexibilidad que proporciona la distribución multicentro.

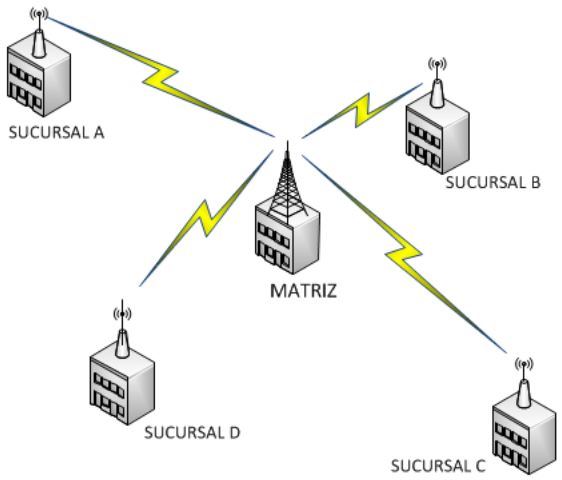


Figura 2.1: Enlaces Inalámbricos

Fuente: Las Autoras

2.1.1.2 Enlaces Satelitales

Los enlaces satelitales se presentaron como una de las soluciones más atrayentes debido a su gran cobertura y facilidad de instalación, siendo uno de los primeros sistemas utilizados para conectar puntos distantes. Para la utilización de esta tecnología se requiere de un satélite artificial para la conexión entre estaciones receptoras y transmisoras.

Con el propósito de mantener el satélite relativamente fijo con respecto a la Tierra se lo coloca a una altura de 36000km sobre la superficie de la misma, en una órbita geoestacionaria llamada "Cinturón de Clarke". Se utilizan señales microondas como portadoras para la transmisión desde el satélite hasta la Tierra (*Up Link*) y desde la Tierra hasta el satélite (*Down Link*).

Características

- Son necesarios solo tres satélites para cubrir toda la superficie terrestre, haciendo a esta tecnología ideal para áreas de difícil acceso.
- Se presentan retardos en la propagación de hasta 660ms en el envío de datos.
- Debido a que no hay mayor dificultad en apuntar hacia una estación satelital, la instalación de esta tecnología en un punto final es bastante fácil, haciendo a la misma ideal para trasmisiones móviles de emisión masiva como las de radio y televisión
- Costo elevado de ancho de banda.

2.1.1.3 Enlaces con Fibra Óptica

En los últimos años se ha ampliado el uso de la fibra óptica debido a su capacidad de manejo de grandes cantidades de datos, al evitar el ruido asociado y el aislamiento eléctrico, en conjunción con otra cantidad de características que hacen de la fibra una tecnología idónea para su uso en sistemas industriales y comerciales.
Estos enlaces se utilizan para extender la distancia y superar limitaciones de sistemas tales como RS-232, RS-422/485 y Ethernet y a su vez garantizar la transmisión de gran cantidad de datos disminuyendo el impacto de la interferencia eléctrica. Mediante esta tecnología se convierten las señales eléctricas en un rayo de luz modulada que será transportada por la fibra, que tiene un diámetro realmente pequeño, hasta el equipo receptor que realiza la conversión de luz a señal eléctrica nuevamente.

Beneficios[1]

- Gran ancho de banda
- Baja atenuación de la señal
- Seguridad de la señal inherente
- Baja tasa de errores
- Inmunidad contra el ruido
- Peso ligero
- Diámetro pequeño
- Aislamiento eléctrico
- Seguro en áreas peligrosas
- No hay interferencia entre conductores

2.1.2 Enlaces Conmutados

Los enlaces conmutados tienen un tiempo de ocupación variable y se relaciona a la cantidad de datos que se va a transmitir, ya que el enlace se establece cuando se desea iniciar una comunicación y se mantiene durante el tiempo que dure la misma.

De la disponibilidad de la red depende la del enlace, en ocasiones no se logra establecer la comunicación ya que otros terminales están utilizando los recursos de red.

Los enlaces de comunicación conmutados pueden ser por conmutación de circuitos o conmutación de paquetes.

[1] www.fibraoptica.com/informacion-tecnica/vistazo-tecnologia

Enlaces por conmutación de circuitos: se establece de forma dinámica una conexión virtual por medio de una conmutación de circuitos, para transmitir datos o voz entre emisor y receptor. Pero se debe establecer primero una conexión a través de la red del proveedor de servicios. Entre los enlaces de comunicación por conmutación de circuitos se encuentran el acceso telefónico analógico e ISDN (*Integrated Services Digital Network*, Red Digital de Servicios Integrados).

Enlaces de comunicación por conmutación de paquetes: en las redes que utilizan este tipo de comunicación, los datos que se transmiten son previamente ensamblados en paquetes. Cada paquete se transmite individualmente pudiendo tomar diferentes rutas hacia el destino; una vez que llegan al mismo, los paquetes son reensamblados. Los enlaces de comunicación por conmutación de paquetes incluyen *Frame Relay*, ATM, X.25 y Metro Ethernet.

2.1.2.1 ISDN

ISDN fue desarrollada por compañías telefónicas como una tecnología digital fuera de banda *end-to-end* apropiada para datos, voz y video. La conectividad sobre ISDN ofrece a los usuarios finales ancho de banda incrementado, tiempo de establecimiento de llamada y latencia reducidos y da una razón señal/ruido más baja. En Estados Unidos, las definiciones de ISDN son descritas en estándares NI (*National ISDN*, ISDN Nacional) para asegurar la interoperabilidad entre una variedad de servicios y proveedores. El estándar define arquitectura de capas, servicios, protocolos, canales, puntos de referencia y dispositivos.

Canales ISDN

El bucle local típico transporta voz, datos o video. El término canal, al contrario de otras técnicas, se refiere a un conducto unidireccional que transporta señalización e información de usuario. Se definen tres canales básicos:

- **Canal D (Canal Delta, Canal de señalización):** es un canal con conmutación de paquetes que transporta señalización e información de control para canales B entre el CPE (*Customer Premise Equipment*, Equipamiento de Premisa del Cliente) y la red. También es usado para datos de usuario. Típicamente, el canal D provee señalización para uno a más puntos de acceso ISDN. Cuando ISDN proporciona señalización para más de un punto de acceso, el canal D ahorra equipamiento y recursos. Opera a 16 o 64Kbps, dependiendo de la implementación.

- **Canal B (*Bearer Channel*, Canal Portador):** Transporta datos de usuario, incluyendo datos, voz y video. Opera a tasas de señal digital de nivel 0 (DS-0), es decir 64Kbps. Puede ser usado para conmutación de circuitos o de paquetes. También proporciona servicios adicionales dependiendo de la información de señalización del canal D.

- **Canal H (Canal Híbrido):** El estándar define H_0, H_{10}, H_{11}y H_{12}, que operan a tasas de 384Kbps, 1.472Mbps, 1.536Mbps y 1.920Mbps respectivamente. El canal H_0 es una agrupación lógica de 6 canales B y el H_{11} es equivalente a cuatro canales H_0. Los canales H son usados para información de usuario que requiere velocidades más altas así como videos de alta calidad.

Todos los tipos de canales comparten un solo medio físico. Los canales B y D definen la BRI (*Basic Rate Interface*, Interfaz de Acceso Básico), como se muestra en la figura 2.2. Para BRI, los canales D usan la tecnología de multiplexación por división de tiempo (TDM) para proporcionar señalización. Lo mismo aplica para el PRI (*Primary Rate Interface*, Interfaz de Acceso Principal), pero al contrario de BRI, en Estados Unidos y Canadá, PRI usa 23 canales B (del número 1 al 23 y un canal D, número 24).

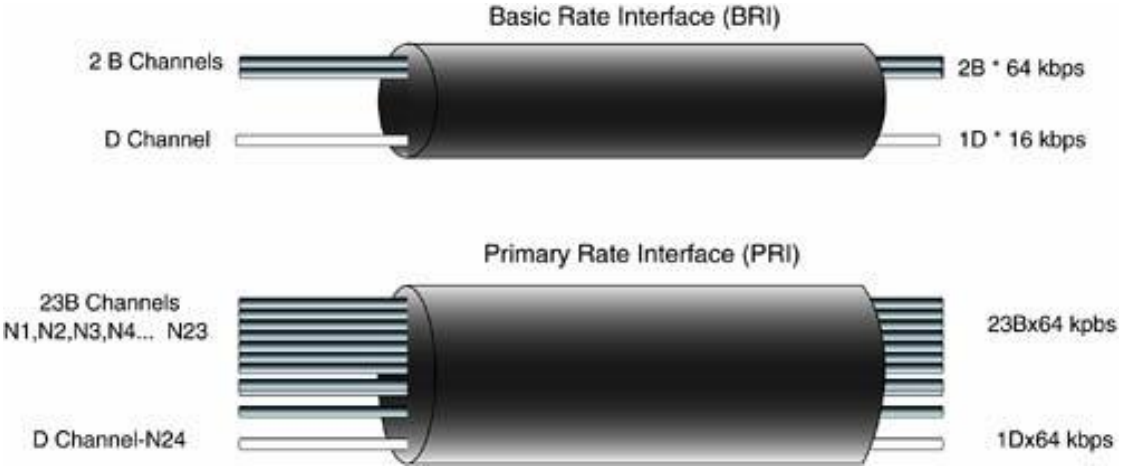


Figura 2.2: Canales BRI y PRI ISDN

Fuente:

www.informit.com/library/content.aspx?b=Troubleshooting_Remote_Access&seqNum=76

2.1.2.2 ATM

ATM (*Asynchronous Transfer Mode*, Modo de Transferencia Asíncrono) es una tecnología diseñada para la transferencia a alta velocidad de voz, video y datos a través de redes públicas y privadas usando tecnología de retransmisión de celdas. ATM es un estándar de la ITU-T (*International Telecomunication Union Telecomunication Standardization Sector*, Unión Internacional de Telecomunicaciones Sector de Estandarización de Telecomunicaciones).

ATM combina los beneficios de conmutación de circuitos (retraso de transmisión constante, capacidad garantizada) con aquellos de la conmutación de paquetes (flexibilidad, eficiencia para tráfico intermitente). Para lograr estos beneficios, ATM usa las siguientes características:

- *Celdas de tamaño fijo*, permitiendo conmutación en hardware más eficiente de lo que es posible con paquetes de longitud variable.

- *Servicio orientado a la conexión,* permitiendo enrutamiento de celdas a través de redes ATM sobre conexiones virtuales, también llamados Circuitos Virtuales, usando simples identificadores de conexión.
- *Multiplexación asíncrona,* permitiendo el uso eficiente del ancho de banda e intercalado de datos de prioridad y tamaño variables.

La combinación de estas características le permite a ATM proveer diferentes categorías de servicios para diferentes requerimientos de datos y establecer un contrato de servicio a la vez que se establece la conexión. Esto significa que una conexión virtual para un servicio de categoría dado puede ser garantizada a un cierto ancho de banda, así como también otros parámetros de tráfico, para la vida de la conexión.

Tipos de Interfaces de Redes ATM

Hay dos tipos de interfaces que interconectan dispositivos ATM sobre enlaces punto a punto: la UNI *(User-Network Interface,* Interfaz Usuario-Red) y la NNI (*Network-Network Interface,* Interfaz Red-Red). Un enlace UNI conecta un sistema final ATM (lado del usuario) con un *switch* ATM (lado de la red). Un enlace NNI conecta dos *switches* ATM, en este caso, ambos lados son redes.

Las interfaces UNI y NNI son también subdivididas en UNIs y NNIs públicas y privadas. Como se muestra en la figura 2.3, una UNI privada conecta un punto final ATM y un *switch* ATM privado; una UNI pública conecta un punto final ATM o un *switch* privado a un *switch* público. Una NNI privada conecta dos *switches* ATM dentro de la misma red privada; una NNI pública conecta dos *switches* ATM dentro de la misma red pública. Un tercer tipo de interfaz, la BICI (*Broadband Inter-Carrier Interface*, Interfaz de Banda Ancha Inter-portadora) conecta dos *switches* públicos desde diferentes redes públicas.

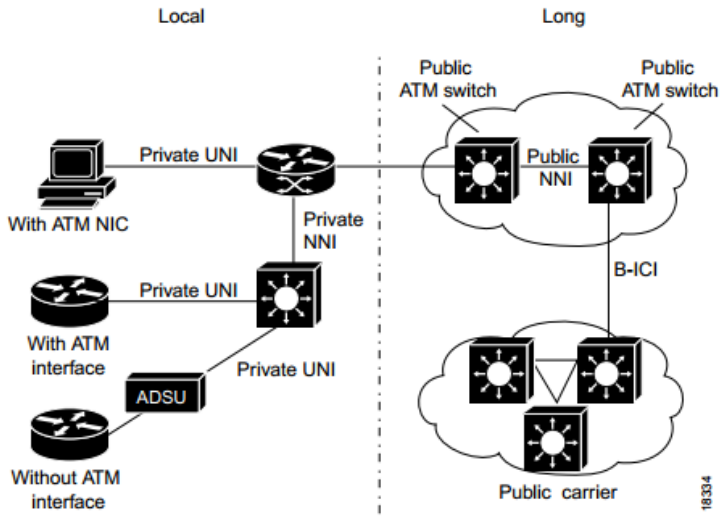


Figura 2.3: Interfaces de Redes ATM

Fuentes: Guide to ATM Technology for the Catalyst 8540 MSR, Catalyst 8510 MSR, and Light Stream 1010 ATM Switch Routers

Servicios ATM

- Servicio PVC (*Permanent Virtual Connection*, Conexión Virtual Permanente), la conexión entre puntos es directa y permanente. De esta manera, un PVC es similar a una línea arrendada.
- Servicio SVC (*Switched Virtual Connection*, Conexión Virtual Conmutada), la conexión es creada y liberada dinámicamente. Debido a que la conexión permanece establecida sólo cuando está en uso, un SVC es similar a una llamada telefónica.
- Servicio sin conexión.

2.1.2.3 *Frame Relay*

Frame Relay es un ejemplo de tecnología por conmutación de paquetes. Las redes de paquetes conmutados permiten a las estaciones finales compartir dinámicamente el medio de red y el ancho de banda disponible. Se usan las siguientes técnicas en la tecnología de conmutación de paquetes:

- Paquetes de longitud variable, son usados para trasferencia de datos más eficiente y flexible. Estos paquetes son conmutados entres varios segmentos en la red hasta que se la alcanza.
- Multiplexación estadística, esta técnica controla el acceso a la red en una red de paquetes conmutados. La ventaja de esta técnica es que tiene capacidad para más flexibilidad y uso de ancho de banda más eficiente.

Circuitos Virtuales *Frame Relay*

Frame Relay proporciona comunicación de capa de enlace de datos orientada a la conexión. Esto significa que una comunicación definida existe entre cada par de dispositivos y que estas conexiones se asocian con un identificador de conexión. Este servicio es implementado usando un circuito virtual *Frame Relay*, que es una conexión lógica creada entre dos DTE (*Data Terminal Equipment*, Equipos Terminales de Datos) a lo largo de la red de paquetes conmutados *Frame Relay*.

Los circuitos virtuales proporcionan un camino de comunicación bidireccional desde un dispositivo DTE a otro y son identificados únicamente por un DLCI (*Data-Link Connection Identifier*, Identificador de Conexión de Enlace de Datos). Gran número de circuitos virtuales pueden ser multiplexados dentro de un único circuito físico para la transmisión a lo largo de la red. Esta capacidad a menudo reduce el equipamiento y la complejidad de la red requerida para conectar múltiples dispositivos DTE.

Los valores DLCI tienen significancia local, lo que significa que sus valores son únicos en la LAN (*Local Area Network*, Red de Área Local) pero no necesariamente en la WAN *Frame Relay*, como se muestra en la figura 2.4.

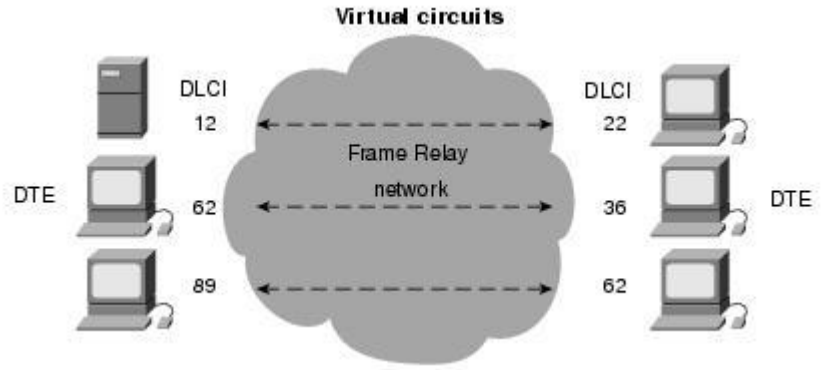


Figura 2.4: Significancia de los DLCI

Fuente: http://docwiki.cisco.com/wiki/Frame_Relay

Los circuitos virtuales *Frame Relay* tienen dos categorías:

- **SVC** (*Switched Virtual Circuits*, Circuitos Virtuales Conmutados), son conexiones temporales usadas en situaciones en las que se requiere transferencia esporádica de datos entre dispositivos DTE a lo largo de la red *Frame Relay*.
- **PVC** (*Permanent Virtual Circuits*, Circuitos Virtuales Permanentes), son conexiones establecidas permanentemente que son usadas para transmisiones de datos frecuentes y consistentes entre dispositivos DTE a lo largo de la red *Frame Relay*.

2.2 OPCIONES DE CONEXIÓN WAN PÚBLICAS

Este tipo de conexiones se establecen sobre una infraestructura de red pública como lo es el Internet, se presentan también varias opciones como las que se detallan a continuación.

2.2.1 DSL

DSL (*Digital Suscriber Line*, Línea de Abonado Digital), es una tecnología que entrega velocidades de banda ancha sobre distancias de kilómetros a través de cable de cobre.

Aunque hay varios tipos de medios que se pueden usar para proporcionar acceso de banda ancha para suscriptores residenciales y empresariales, ninguno de ellos tiene el nivel de desarrollo de la red telefónica. Los servicios telefónicos son proporcionados a casi todo suscriptor residencial y empresarial en todo el mundo, con varios cientos de millones de líneas telefónicas de pares cruzados e instaladas globalmente a la fecha.

Originalmente, DSL era entregada sobre los mismos cables que se usan para proporcionar servicios tradicionales de voz. Estos cables parten desde la CO (*Central Office*, Oficina Central) de una compañía, el lugar donde la conmutación de voz y otras funciones telefónicas tradicionales se llevan a cabo, hacia la casa o empresa del abonado. DSL es entregado desde un dispositivo situado más cerca de la casa o empresa que se conecta a la CO a través de un enlace de fibra óptica y luego a las instalaciones del abonado vía cables de cobre.

En la figura 2.5 se ilustra la arquitectura descrita, en la CO, o en una locación remota típicamente conectada a ella a través de fibra óptica, hay un DSLAM (DSL *Access Multiplexer*, Multiplexor de Acceso DSL) que envía y recibe datos de banda ancha a muchos abonados por medio de la tecnología DSL. En cada lugar de abonado hay un *modem* (modulador-demodulador) que se comunica con el DSLAM para enviar y recibir los datos de banda ancha hacia y desde el Internet y otras redes. Un DSLAM se comunica con muchos *módems* individuales de abonado. Cada modem de abonado es dedicado a esa conexión de banda ancha.

En términos simples, las tecnologías DSL pueden ser subdivididas en dos amplias clases:

- **SDSL (*Symmetric DSL*, DSL Simétrico).** Dentro de esta clase, la tasa de datos transmitida en ambas direcciones (subida y bajada) es la misma. Este es un típico requerimiento de clientes corporativos.
- **ADSL (*Asymmetric DSL*, DSL Asimétrico)**. En este caso, la velocidad de bajada es típicamente más alta que la de subida, se da una asimetría en la tasa de transmisión de datos.

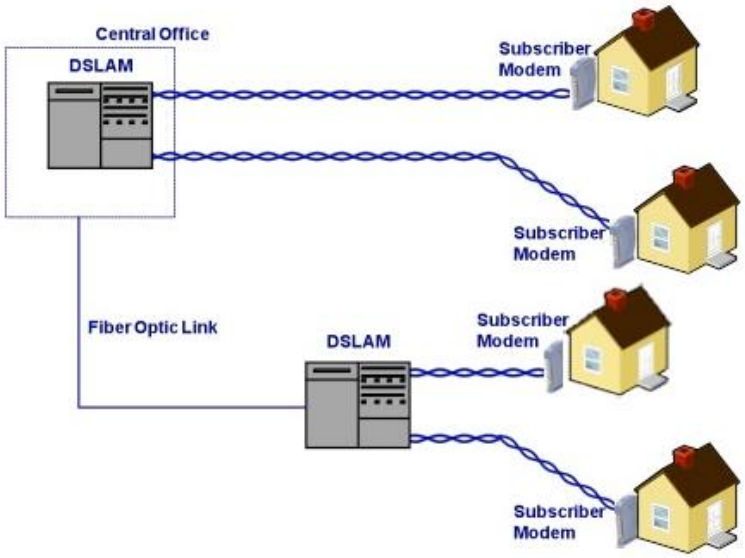


Figura 2.5: Arquitectura DSL

Fuente: http://www.assia-inc.com/DSL-technology/DSL-knowledge-center/tutorials/DSL-technology-tutorial.php

De estas dos clases se presentan muchas variantes, como por ejemplo: ADSL2, ADSL+, SHDSL (*Symmetric High-Speed DSL*, DSL simétrico de alta velocidad), VDSL (*Very High-Speed DSL*, DSL de muy Alta Velocidad), etc.

2.2.2 Modem por cable

Debido a que el tráfico de video y audio solo usa parte de la canalización de una compañía de cable, usualmente hay espacio para ofrecer más servicios, tal como acceso de Internet de alta velocidad, si se agrega la tecnología digital.

Modem por cable es la puerta de enlace que permite a un hogar o empresa aprovechar esa canalización al Internet. Una red HFC (*Hybrid Fiber-Coaxial*, Híbrida Fibra-Coaxial) puede entregar datos a tasas que van desde los 3Mbps a los 10Mbps, más de 100 veces más rápido que un modem *dial-up* de 56Kbps. Esa red también promueve, entre muchos servicios, el despliegue de servicio telefónico local de VOIP (*Voice Over Internet Protocol*,

Voz Sobre Protocolo de Internet); servicios digitales de TV que entregan cientos de canales de video y aplicaciones interactivas de TV.

2.2.3 Acceso inalámbrico de banda ancha

El espectro de radiofrecuencia es utilizado por tecnologías que proporcionan acceso inalámbrico a Internet para la recepción y envío de datos. Las redes inalámbricas pueden ofrecer tasas equivalentes a algunas redes alámbricas, como ADSL o cable modem.

2.2.3.1 WiMAX

WiMAX (*Worldwide Interoperability for Microwave Access,* Interoperabilidad Mundial para Acceso por Microondas) es una tecnología de telecomunicaciones dirigida a proveer conexión inalámbrica a largas distancias en una variedad de formas, desde enlaces punto a punto hasta acceso tipo celular. Es un sistema de comunicaciones digitales destinado para redes inalámbricas de área metropolitana. Esta tecnología puede proveer acceso inalámbrico de banda ancha de hasta 50km para estaciones fijas y de 5 a 15km para estaciones móviles.

Básicamente, el sistema WiMAX, mostrado en la figura 2.6, consiste en dos partes: estación base y receptor WiMAX. La estación base es una torre similar al concepto de torre telefónica que trabaja en conjunto con electrónica interna. Una sola torre WiMAX puede cubrir hasta un radio de 48km como máximo, dependiendo de la altura de la torre, ganancia de la antena y poder de transmisión.

La estación base se conecta con una cantidad de estaciones suscriptoras, que se denominan receptores CPE (*Customer Premises Equipment,* Equipo Local del Cliente). El receptor WiMAX puede ser instalado ya sea como una pequeña caja fuera de la casa o edificio, o integrado en una computadora personal como tarjeta de memoria.

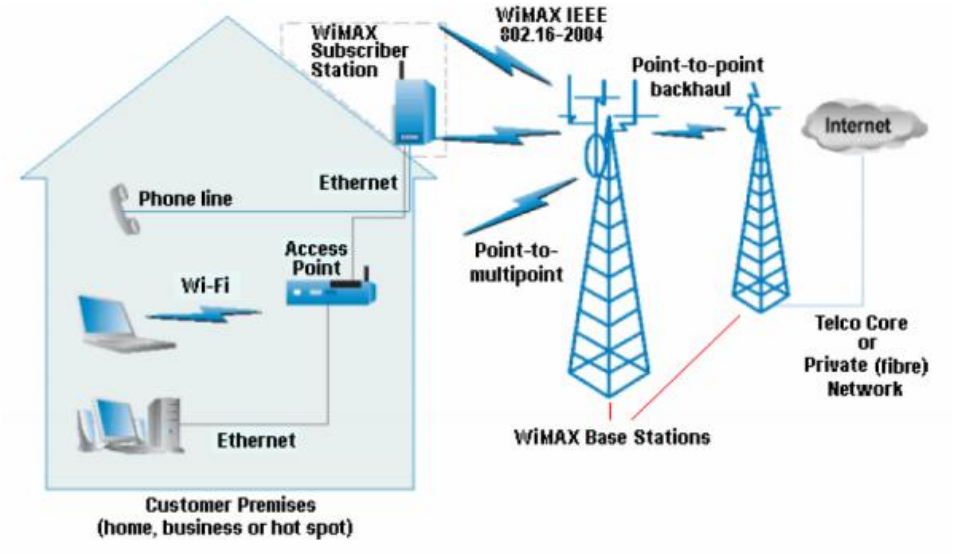


Figura 2.6: Red WiMAX

Fuente: Broadband Wireless Access based on WiMAX Technology with business analysis, Md. Mehedi Alam

2.2.3.2 Internet satelital

Generalmente es usado por usuarios rurales en emplazamientos de difícil acceso, a los que no llegan los servicios de cable y DSL. Una antena satelital provee la comunicación bidireccional, para dicha comunicación (figura 2.7), la capacidad de carga se aproxima a la décima parte de la capacidad de carga de 500kbps. El equipamiento del cliente consiste en un plato pequeño, de 60cm a 3.7m de diámetro, equipado al menos con un módulo receptor y un módulo transmisor.

La comunicación se da en bandas de frecuencia de microondas llamadas banda C (4/6Ghz), banda Ku (11/14Ghz) y banda Ka (20/30Ghz). La banda C es ideal para lugares en los que llueve fuertemente. La banda Ku es más popular con tamaños de plato en el rango de 60cm a 1.8m de diámetro. Amplios anchos de banda están disponibles en el servicio satelital en banda Ka y esto combinado con satélites que tienen muchos haces puntuales, se traduce en reducción de costos para el usuario final.

Figura 2.7: Acceso a Internet Satelital

Fuente: http://www.skygrabber.com/en/skygrabber.php

Debido a la cantidad de localidades, de acuerdo a la jurisdicción de la Intendencia Regional Costa, que se podrían monitorear con el sistema de respaldo y al costo elevado y complejidad de configuración que significaría establecer enlaces dedicados desde la IRC en Guayaquil hacia cada uno de esos puntos para dicho monitoreo, se ha decidido implementar una opción de conexión WAN pública, es decir, sobre Internet.

Dado que el Internet es una plataforma realmente insegura para la transmisión de datos, se debe complementar la opción escogida con una tecnología que ofrezca seguridad a los datos, para que no sean interceptados y fácilmente malversados. Para este fin se utilizará la tecnología VPN que se explicará en el siguiente capítulo.

CAPÍTULO 3

VIRTUAL PRIVATE NETWORK

En este capítulo se hará una descripción de la VPN (*Virtual Private Network*, Red Privada Virtual); qué es, cómo funciona, sus elementos, protocolos, etc., con el fin de llegar a la comprensión del mecanismo que se utilizará como "columna vertebral" del sistema de respaldo para la SUPERTEL.

3.1 GENERALIDADES

El termino *VPN* ha sido utilizado para describir una amplia gama de servicios de redes y configuraciones, que van desde los servicios tan simples como una línea dedicada, a arquitecturas complejas que proporcionan acceso seguro, autenticando un acceso WAN sobre una red publica, como se muestra en la figura 3.1.

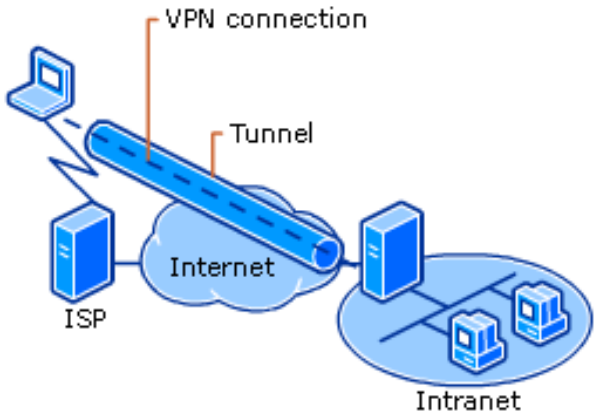


Figura 3.1 Conexión VPN

Fuente: http://technet.microsoft.com/en-us/library/cc779919(v=ws.10).aspx

Una VPN se define como una WAN con las siguientes características y funcionalidades:

- Proporciona una WAN privada sobre una red pública, normalmente Internet. Las conexiones a esta WAN pueden ser permanentes entre los sitios, o por medio de

conexiones bajo demanda a través de la PSTN (*Public Switched Telephone Network*, Red Telefónica Publica Conmutada).

- Interconecta nodos dispersos de la red. Estos nodos pueden representar sucursales o empleados que trabajan desde casa o desde la carretera. Si el VPN ofrece un servicio de extranet, los nodos pueden ser oficinas de otras compañías, tales como clientes, proveedores o socios comerciales.
- Proporciona privacidad e integridad de los datos a medida que atraviesa la red compartida.
- Requiere autenticación del usuario antes de permitir la comunicación o la concesión de acceso a los recursos de VPN. La autenticación debe aplicarse en conjunción con procedimientos adecuados de gestión de acceso con el fin de regular el acceso a los diversos servicios prestados dentro de la VPN.
- Una VPN debería proporcionar la calidad de servicio (QoS) y las instalaciones de multidifusión cuando sea apropiado.

Muchos de estos servicios pueden ser proporcionados ya sea por el proveedor de servicios o por el cliente, en función de los requisitos del usuario VPN, con problemas tales como el costo, la seguridad y la escalabilidad para ser considerado. Por ejemplo, tener que proporcionar ciertos servicios al cliente puede resultar de bajos costos por la prestación, pero puede requerir la compra de equipos y la contratación de técnicos expertos para instalar y dar mantenimiento a la infraestructura necesaria.

El término VPN se aplica a menudo en la literatura, como si se describiera una solución específica o única. Cada solución VPN distinta tiene sus fortalezas y debilidades asociadas, por lo que no se prevé que una solución única se convertirá en dominante, sino más bien que una serie de enfoques seguirán abordando diversas necesidades.

3.1.1 Motivos para usar VPN

La comunicación segura de los datos requiere una ruta de confianza entre redes de computadoras en diferentes lugares. El uso de redes compartidas para transportar datos privados introduce problemas de seguridad. Este riesgo se considera lo suficientemente grave para que en algunas industrias, como en el sector de la salud, esté prohibido por la ley en algunos países, la transmisión de datos confidenciales a través de redes públicas como internet.

A pesar de las preocupaciones de seguridad asociadas con las redes compartidas, un gran número de organizaciones necesitan interconectar lugares separados geográficamente, y para muchos la implementación de una WAN dedicada no es factible. Específicamente, las redes dedicadas son demasiado costosas para las organizaciones pequeñas. VPN ofrece una solución de compromiso, lo que minimiza la cantidad de infraestructura a ser comprada, instalada y gestionada, y aun así ofrecer una seguridad sólida asociada a una red dedicada; disminuyendo el capital de inversión y también el "riesgo tecnológico" asociado con la compra de hardware para una tecnología en rápida evolución.

Podemos resumir los motivos por los que se usa VPN:

- Tiene amplia conectividad geográfica.
- Mejora la seguridad donde las líneas de datos no han sido cifradas.
- Reduce costos de operación en comparación con la WAN tradicional.
- Reduce el tiempo de transito y los costos de transporte para los usuarios remotos.
- Simplifica la topología de la red en ciertos escenarios.
- Proporciona oportunidades sobre redes globales.

3.1.2 Tipos de VPN

Se diferencian dos tipos de VPN: Segura y Confiable.

3.1.2.1 VPN Segura

Usa protocolos de túnel cifrado para proporcionar la confidencialidad prevista, autenticación del remitente y la integridad del mensaje para lograr privacidad. Cuando se las aplica apropiadamente, implementar y utilizar estas técnicas puede proporcionar comunicaciones seguras a través de redes no seguras. La característica principal es su capacidad para utilizar las redes públicas como el Internet en lugar de depender de las líneas privadas alquiladas.

En un túnel los datos se transmiten a través de una red pública de tal manera que los nodos de enrutamiento en la red pública no son conscientes que la transmisión es parte de una red privada. Los túneles son generalmente aplicados mediante la encapsulación de los datos de la red privada y la información de protocolo dentro de los datos de protocolo de redes públicas, de tal manera que es difícil para cualquiera examinar las tramas de datos transmitidas por el túnel.

Los protocolos de VPN segura son los siguientes:

- IPSec (*Internet Protocol Security*, Seguridad de Protocolo de Internet)
- SSL (*Secure Socket Layer*, Capa de Conexión Segura)

3.1.2.2 VPN Confiable

No utiliza túneles cifrados, en lugar de esto, se confía la seguridad de la red a un proveedor único para proteger el tráfico.

Las VPN confiables son suministradas y manejadas por proveedores de Servicios de Internet mediante la definición de caminos a través de sus redes, para garantizar que el tráfico de los clientes se enruta de manera confiable. Un cliente puede elegir una VPN confiable porque no hay equipos que comprar ya que esto es totalmente gestionado por el proveedor de servicios y por lo tanto no requiere mantenimiento, y a menudo incluyen

acuerdos a nivel de servicio. Por lo general, las VPN confiables son menos costosas al inicio pero más caras con el paso del tiempo.

Ya que las VPN confiables trabajan sobre líneas privadas, se utilizan redes de circuitos conmutados en lugar de redes de conmutación de paquetes por razones de calidad del servicio (QoS).

Los protocolos de VPN confiable incluyen los siguientes:

- L2VPN (*Layer 2 VPN*, VPN de Capa 2)
- L3VPN (*Layer 3 VPN*, VPN de Capa 3)

3.1.3 Elementos

Una VPN segura consiste en dos dispositivos conectados a Internet que, después de haberse autenticado mutuamente, intercambian datos a través de internet de una manera segura. Los cuatro procesos que comprenden una VPN segura son: túneles, confidencialidad, integridad y autenticación.

- **Túneles:** Esta es la característica que define a una VPN, ya que permite a los paquetes viajar a destinos que normalmente no serían accesibles a través de Internet. Esto permite que la infraestructura existente de internet reemplace una línea dedicada arrendada entre sitios o servicios de acceso telefónico. Un túnel VPN consiste en dos dispositivos conectados a Internet, uno a cada extremo; estos dos extremos del túnel envían y reciben paquetes enviados por los pares, que emergen al formar el túnel.
- **Confidencialidad:** Es esencial para evitar la posibilidad remota de que los paquetes puedan ser interceptados y examinados por un tercero. La confidencialidad de la información se puede lograr mediante el cifrado de la carga útil de los paquetes que están destinados para el extremo remoto de un túnel VPN. El proceso de cifrado es

un compromiso entre el inevitable aumento de los retardos de transmisión y la fuerza del sistema de cifrado criptográfico empleado.

- **Integridad:** Es vital que se garantice que todos los datos que llegan a uno de los extremos de una VPN, se originaron a partir de la protección reconocida por pares y no se hayan modificado en la ruta.
- **Autenticación:** Al introducir la tecnología VPN a la red, los servidores que de otra manera serían protegidos de los peligros de la exposición al internet pueden ser vulnerables. Es imprescindible, entonces que se tomen medidas para garantizar que solo las estaciones remotas aprobadas sean capaces de inyectar paquetes a través de un túnel en la red local.

Estas características de las VPN se examinarán más a fondo en la siguiente sección.

3.2 SEGURIDAD EN LAS VPN

Los riesgos asociados con el Internet son anunciados cada día por los medios. Para las empresas, los riesgos son realmente grandes. Información corporativa robada o borrada puede afectar negativamente el sustento del personal y le cuesta dinero a la compañía. Si archivos de proyectos o bases de datos de clientes son robados de una compañía pequeña, ésta podría quedar fuera del negocio.

Si la red corporativa está conectada al Internet y su seguridad es débil, un intruso podría ser capaz de acceder a la misma desde cualquier ISP (*Internet Service Provider*, Proveedor de Servicios de Internet) en el mundo. Incluso usuarios no sofisticados pueden obtener y usar herramientas automatizadas de "verificación de seguridad" para buscar agujeros en la red de la compañía. Y lo peor es que hay posibilidades de que nunca se sepa lo que está sucediendo.

Antes de colocar información privada en Internet, hay que asegurarse de que la VPN es lo suficientemente robusta para protegerla.

Existen varias tecnologías que las VPN usan para proteger los datos que viajan a lo largo de Internet. Los conceptos más importantes son encriptación, autenticación y túneles.

3.2.1 Criptografía

La criptografía es una de las tecnologías esenciales usadas en la construcción de una VPN segura. Diferentes aplicaciones de los mismos algoritmos básicos pueden proporcionar tanto la encriptación que mantiene secretos los datos, como la autenticación que garantiza que los dos pares de seguridad en una VPN son quienes dicen ser.

3.2.1.1 Sistemas de cifrado simétrico y asimétrico

La confidencialidad de datos puede ser proporcionada por una de las dos categorías de algoritmo de encriptación, a saber, cifrado simétrico y cifrado asimétrico. La criptografía simétrica o convencional, requiere que el emisor y receptor compartan una clave, que es un artículo de información secreta usado para encriptar y desencriptar datos. El proceso por el cual dos dispositivos pares acuerdan una clave sobre un medio inseguro puede ser problemático ya que, hasta que se acuerde la clave, los pares no tienen manera de comunicarse en secreto.

La criptografía asimétrica o de clave pública, resuelve el problema de intercambio de claves usando dos de ellas, cualquiera de las cuales puede ser usada para encriptar un mensaje. Entonces, los datos encriptados solo puede ser desencriptados por medio de la otra clave.

- **Cifrado Simétrico**

El cifrado simétrico emplea la misma clave para encriptar el texto plano (datos originales, sin encriptar) y para desencriptar el texto cifrado. El emisor y receptor debe, por lo tanto, acordar por adelantado la clave que no debe ser conocida por nadie más. La fortaleza criptográfica de un algoritmo simétrico puede ser medida por el tamaño de la clave que emplea.

Como ejemplo de cifrado cimétrico tenemos, DES (*Data Encryption Standard*, Estándar de Encriptación de Datos), *Blowfish* y AES (*Advanced Encryption Standard*, Estándar de Encriptación Avanzada). El algoritmo DES usa una clave de 64 bits, de los cuales 8 son reservados, dejando 56 bits variables. Es posible proteger información con 3DES en lugar de DES. Esto significa que la información se somete a tres encriptaciones sucesivas. El uso de ciclos de encriptación múltiple no necesariamente va de la mano con el incremento en la seguridad y puede ser visto como desperdicio de potencia informática para muchas aplicaciones.

Blowfish permite a los implementadores seleccionar una longitud de clave entre 32 y 448 bits; las implementaciones disponibles comercialmente a menudo usan claves de 128 bits. En el año 2002 DES fue remplazado por AES como un estándar de encriptación por el gobierno de los Estados Unidos. Desde entonces AES se ha vuelto muy popular ya que combina la velocidad de DES con el nivel de seguridad de 3DES. AES puede usar claves de 128, 192 y 256 bits.

Los algoritmos simétricos son populares porque su velocidad les permite encriptar eficientemente grandes cantidades de texto plano. Hay dos subcategorías de cifrado simétrico: cifrado de flujo y cifrado en bloque.

- **Cifrado de Flujo:** Estos algoritmos operan un bit a la vez. Los mensajes encriptados con un cifrado de flujo siempre son del mismo tamaño del texto plano original. La encriptación toma lugar por medio de una operación en la cual cada bit del texto plano es manipulado por el operador Booleano XOR (OR exclusiva) con un bit aleatorio para producir el texto cifrado. La figura 3.2 muestra un generador de bit aleatorio.

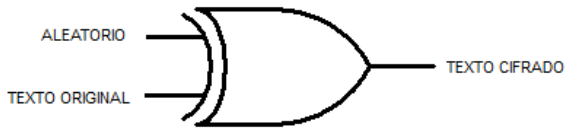


Figura 3.2 Generador de bit aleatorio

Fuente: Las autoras

- **Cifrado de Bloques:** Este cifrado encripta datos en bloques de bytes, en lugar de un solo bit a la vez. El tamaño de los bloques varía de acuerdo al algoritmo, el más común es el de 64 bits. Debido a que es poco probable que el texto plano sea múltiplo del tamaño del bloque del algoritmo, a menudo es necesario rellenar la entrada. Por ejemplo, si la longitud del bloque es 64 bits y el último bloque contiene solo 40 bits, entonces deben ser agregados 24 bits de relleno. La cadena de relleno puede consistir en ceros, ceros y unos alternados, bits aleatorios, o alguna otra secuencia. DES, *Blowfish* y AES son cifrados en bloque.

Existen dos métodos para encriptar una secuencia de bloques. Ya sea que los bloques sean tratados independientemente y el cifrado sea usado en cada bloque sin referencia a lo que ha pasado antes, o que los resultados de bloques encriptados anteriormente afecte la encriptación del cloque actual. Estos dos métodos son conocidos como modo ECB (*Electronic Code Book*, Libro de Código Electrónico) y CBC (*Cipher Block Chaining*, Cifrado con Encadenamiento).

Modo ECB. En este modo, bloques idénticos de texto plano generarán bloques idénticos de texto cifrado. Por lo tanto, un intruso puede aprovechar la repetición en el texto cifrado para dar a conocer la versión en texto plano.

Modo CBC. En este caso, se agrega un mecanismo de retroalimentación de manera que los resultados del cifrado de bloques previos influyan en el cifrado del bloque actual. Cada bloque de texto cifrado se hace dependiente no solo del bloque de texto plano que lo generó, sino también de todos los bloques de texto plano previos. Esto garantiza que incluso si el texto plano contiene muchos bloques idénticos, cada uno se encripta como un bloque de texto cifrado diferente.

- **Cifrado Asimétrico**

La gran ventaja del cifrado asimétrico es que una clave secreta compartida no tiene que ser intercambiada en un medio inseguro como el Internet público. Se genera un par de claves y una de ellas es denominada como la Clave Pública y es divulgada. Cualquiera de las partes que desee comunicarse de manera segura con el propietario de la clave, encripta el mensaje usando la Clave Pública del receptor. El descifrado solo se puede lograr conociendo la segunda clave, privada, que el propietario se asegura, nunca sea publicada.

El cifrado de bloques asimétrico más popular es RSA (nombrado por sus inventores, Ron Rivest, Adi Shamir y Leonard Adleman). Las claves del algoritmo RSA están compuestas de dos partes. La primera es llamada módulo. Usualmente es un número de 512 bits y es el producto de dos números primos de 256 bits.

$$N = p\ X\ q \qquad [3.1]$$

Las claves pública y privada comparten el mismo módulo. La segunda parte de una clave RSA es llamada exponente. Este es un número de longitud variable, diferente para las dos claves, siendo usualmente el exponente de la clave pública, el más pequeño de los dos.

RSA funciona de la siguiente manera. El texto plano (visto como un número binario) es elevado a la potencia del exponente Público y el texto cifrado es el residuo de dividir para el módulo. Para desencriptar, el texto cifrado es elevado a la potencia del exponente Privado y el texto plano es el residuo de dividir para el módulo.

$$C = T^k\ mod\ N \qquad [3.2]$$

$$T = C^l\ mod\ N \qquad [3.3]$$

Donde C es el texto cifrado, T es el texto plano, k y l son los exponentes públicos y privados y N es el módulo.

La seguridad del cifrado asimétrico deriva de la dificultad de factorizar estos módulos de vuelta a sus primos constituyentes. Sin conocer los dos primos usados para generar el módulo, no es posible calcular el exponente Privado a partir del Público.

3.2.1.2 Intercambio de claves

Aunque los algoritmos de cifrado asimétrico son más seguros que los simétricos, también son mucho más lentos y no es factible usarlos para asegurar grandes cantidades de datos, ya que el incremento en los tiempos de transmisión serían excesivos. De manera similar, aunque los algoritmos de modo simétrico pueden procesar grandes cantidades de texto plano a gran velocidad, no ofrecen el requisito de nivel de seguridad debido a que la clave es un secreto compartido que debe ser intercambiado sobre un medio inseguro antes de la transmisión del texto cifrado.

Un compromiso útil entre la velocidad de los algoritmos simétricos y la seguridad del tipo asimétrico se logra fácilmente. Un algoritmo simétrico veloz se utiliza para asegurar el flujo de datos con la clave secreta compartida (la clave de sesión) la cual es encriptada usando un cifrado asimétrico. Esto significa que los tiempos de transmisión para paquetes que atraviesan la VPN se mantienen a un mínimo sin comprometer la seguridad mediante el intercambio de la clave de sesión en texto claro. Es práctica normal para la clave de sesión que se le asigne una vida útil limitada de modo que debe ser periódicamente renovada. Esto aumenta la seguridad adicional, ya que el atacante no tendría suficiente tiempo para descubrir la clave de sesión por medio de algún ataque de fuerza bruta antes de que venza y se sustituya por una clave completamente nueva.

- **Intercambio de clave RSA**

El algoritmo RSA debe ser empleado para proporcionar una forma simple de intercambio seguro de clave. Por ejemplo, si A desea asegurar una cantidad algo grande de datos con un algoritmo rápido como el DES, antes de transmitirla a B, primero escoge un número aleatorio de 56 bits como la clave DES y encriptarlo usando la Clave Pública de B. Solo B

será capaz de desencriptar este intercambio usando su clave RSA privada. El inconveniente con esta propuesta es que cualquiera, incluyendo a un intruso, puede cifrar cualquier cosa usando la Clave Pública de B. Por lo tanto B no tiene prueba de que sea realmente A con quien se está comunicando. El canal de comunicaciones solo es seguro si A firma digitalmente la clave DES y cifra tanto la clave como su firma con la Clave Pública de B. El problema con este enfoque es que la firma puede ser demasiado grande para asegurar en una sola operación RSA.

- **Intercambio Diffie-Hellman**

El intercambio de clave Diffie-Hellman fue el primer criptosistema de Clave Pública y sustenta el marco de trabajo entero por el cual los paquetes IP pueden ser transmitidos de manera segura en el Internet. Los participantes en el intercambio primero deben acordar un *grupo*, que define el número primo p y el generador g que deben ser usados. En la primera parte del intercambio, A y B seleccionan, cada uno, un número privado aleatorio (señalado por la letra inicial en minúscula de cada parte) y elevar a la potencia para producir un valor público correspondiente (inicial en mayúscula de cada parte):

$$A = g^a \ mod \ p \qquad [3.4]$$

$$B = g^b \ mod \ p \qquad [3.5]$$

A y B intercambian estos dos valores públicos y vuelven a elevar a la potencia, usando el valor público de la otra parte como generador para producir la clave compartida:

$$\text{A: } g^{ab} = (g^b)^a \ mod \ p \qquad [3.6]$$

$$\text{B: } g^{ba} = (g^a)^b \ mod \ p \qquad [3.7]$$

A y B ahora tienen una clave secreta compartida:

$$g^{ab} = g^{ba} = k \qquad [3.8]$$

Lo importante de este intercambio es que los valores públicos *A* y *B* pueden ser intercambiados sobre una red pública insegura sin reducir la seguridad del intercambio. Un espía podría conocer *g* y *p* e interceptar en intercambio de valores públicos y aun así no sería capaz de descubrir la clave porque uno de los valores privados debe ser conocido para generar la clave compartida.

El intercambio Diffie-Hellman es vulnerable a un ataque de "hombre en la mitad" en el cual un intruso pretende ser B ante A y viceversa. Ambos, A y B creen que están desarrollando un intercambio de clave entre ellos, pero en realidad lo están haciendo con el intruso. Cuando A envía datos seguros a B, el intruso puede interceptar el tráfico y desencriptarlo antes de pasar los paquetes a B. Ni A ni B notarían algo fuera de lo común. Este tipo de ataques puede se frustrado si A y B firman digitalmente sus claves públicas.

3.2.2 Infraestructura de Clave Pública y Autenticación

El grado de seguridad de un sistema es en gran parte gobernado por la calidad de procedimientos de autenticación que son empleados. La autenticación puede definirse como el proceso por el cual se establece una prueba de identidad o integridad en respuesta a alguna forma de desafío.

Durante las fases de negociación inicial entre dos puntos finales de seguridad, cada par debe autenticar el otro por algún medio. Fallas al implementar tal autenticación de cada par podría permitir que un sistema desconocido se haga pasar por el punto remoto de una VPN con el objetivo de adquirir datos confidenciales. La autenticación mutua de los puntos finales de seguridad es siempre el primer escenario de establecimiento de una conexión VPN. Si ésta falla, todos los procesos subsecuentes deben detenerse de manera que no se establezca la VPN.

Una vez que las identidades hayan sido establecidas, los datos pueden ser transmitidos sobre la VPN. Todos los paquetes que lleguen a los puntos finales de seguridad deben ser sometidos a un proceso de autenticación de integridad para garantizar que su par (y no

algún otro dispositivo) los envió y que no han sido modificados durante el curso de la transmisión sobre la infraestructura pública. Esto se logra añadiendo una firma digital a cada paquete, que es verificada por el punto final receptor. El emisor encripta mensajes con su Cave Privada y el receptor los desencripta con la Clave Pública del emisor.

3.2.2.1 Firma digital

La criptografía de Clave Pública puede ser usada para autenticar, así como también para cifrar un mensaje, transmitiendo una firma digital conjuntamente con los datos del mensaje. Anteriormente se describió cómo los mensajes pueden ser cifrados con una Clave Pública del receptor. Solo el titular de la Clave Privada correspondiente es capaz de desencriptar el mensaje. Si estas acciones se realizan en el sentido opuesto, entonces se ha logrado una forma simple de firma digital, implicando que los mensajes son originarios del emisor y no de un impostor.

Este intento simplista de autenticación se basa en la transformación de garabatos encriptados en texto plano legible. El firmante pasa el mensaje a través de la función *hash* de una vía que produce un resumen de longitud fija y única llamada el *resumen* del mensaje a su salida. Éste es cifrado con la Clave Privada del emisor para producir una firma digital. Una función *hash* produce una impresión única del pulgar que es característica del mensaje del cual deriva. Es seguro asumir que un resumen firmado producido de esta manera es una firma digital confiable.

Más allá, es sensible a verificación por máquina. La firma, en la forma de un resumen cifrado, se adjunta al mensaje que se autentica. El receptor verifica la firma pasando el mensaje a través de la misma función *hash* y desencriptándola. Si los dos resúmenes son idénticos entonces la firma es válida.

Las firmas digitales construidas cifrando un resumen de mensaje con la Clave Privada del emisor son extremadamente difíciles de falsificar, luego no pueden ser repudiadas ni transferidas. Esto las hace vehículos ideales para garantizar la autenticidad del emisor.

3.2.2.2 Integridad de los mensajes

Una firma digital puede garantizar la integridad del mensaje que acompaña así como la identidad del emisor ya que cualquier alteración a un mensaje firmado producirá un valor *hash* completamente diferente, haciendo inválida la firma. Sin embargo, las firmas digitales son lentas de calcular porque son generadas por medio de cifrado asimétricos. Para un flujo continuo de datos (como una serie de paquetes IP), firmar cada paquete protegido puede ser tan oneroso como cifrar la carga útil con la Clave Pública en lugar de usar un cifrado de bloque simétrico.

Afortunadamente existen funciones *hash* simétricas y asimétricas de la misma manera que existen cifrados simétricos y asimétricos. Una firma digital usa una función asimétrica lenta y altamente segura. Una vez que los pares se han autenticado uno a otro por estos medios, el emisor de los datos es de confianza y ya no necesita ser autenticado. Una función *hash* simétrica más rápida es suficiente para garantizar la integridad de cualquier paquete recibido. Las funciones *hash* simétricas en las que se usa una única clave compartida para firmar la entrada son conocidas como MAC (*Messages Authentication Code*, Código de Autenticación de Mensajes).

3.2.2.3 Certificados digitales

Las firmas digitales prueban que un mensaje ha sido recibido en estado inmaculado desde el par manejando una clave pública. Sin embargo, hay un elemento robusto de confianza involucrado ya que el receptor del mensaje no tiene pruebas de la identidad del emisor. Un certificado es un mecanismo, expedido y digitalmente firmado por una tercera parte de confianza, que liga la identidad del propietario a una Clave Pública. Los certificados son archivos no transferibles, no falsificables que actúan como una insignia de identidad digital o pasaporte para ayudar a garantizar que usuarios o computadoras son quienes dicen ser.

- **Autoridades de Certificación**

Un certificado puede obtenerse aplicando a una parte emisora, denominada CA (*Certification Authorities,* Autoridades de Certificación). Ésta puede ser una compañía que se especialice en emitir certificados digitales o una organización privada que requiere que los usuarios presenten un certificado emitido anteriormente como prueba de la identidad digital. La CA debe tomar medidas razonables para confirmar la identidad de los aplicantes antes de emitir un certificado y debe emprender varias tareas de mantenimiento a lo largo de la vida de un certificado. Esto incluye la revocación de cualquier certificado cuya Clave Privada haya sido comprometida o cuyo propietario haya dejado la organización emisora. Más importante, la CA debe asegurarse de que sus propias Claves Privadas nunca sean reveladas ya que esto le permitiría a un atacante emitir certificados fraudulentos bajo el nombre del emisor, poniendo así en tela de juicio todos los certificados que emite la CA.

- **Autoridades de Registro**

El propósito de las RA (*Registration Authorities,* Autoridades de Registro) es verificar la información proporcionada por un aplicante para un certificado. La CA puede delegar esta tarea a la RA o realizar ella misma la verificación. Si el certificado confirma la identidad de una persona (a diferencia de una computadora), dicha verificación puede comprender el chequeo de una dirección de *email* proveída o, para aplicaciones más demandantes, requiere una visita personal a las oficinas del RA para probar la identidad mostrando un documento como la licencia de conducir o pasaporte. Una vez que las verificaciones se hayan realizado, la RA aprueba la solicitud para el certificado presentándolo a la CA que emite el certificado. El certificado usualmente contendrá una indicación de las verificaciones de identidad realizadas.

3.2.2.4 Modelos de autenticación

Las VPN han sido clasificadas de acuerdo a si son utilizadas para conectar un sitio remoto o un usuario remoto al lugar principal. Diferentes modelos de autenticación de identidad son más apropiados para estos dos tipos de VPN.

La autenticación entre pares dentro de la categoría de ***sitio remoto*** de VPN puede ser lograda generalmente configurando una clave compartida por ambos pares.

Un ***usuario remoto*** de VPN requiere un enfoque más riguroso debido a que usuarios individuales controlarán las computadoras remotas. Es importante que, en caso de necesidad, el servicio de acceso remoto pueda ser retirado inmediatamente sin requerir acceso al dispositivo en cuestión. La autenticación de usuario es insegura ya que la suspensión de una cuenta no puede garantizar que el usuario no será capaz de obtener acceso remoto a la red usando la clave de un colega. Si la computadora remota se autentica usando un certificado digital entonces el acceso puede ser retirado colocando el certificado en la lista de revocación de las Autoridades de Certificación.

3.2.2.5 Protocolos de Autenticación

PAP (*Password Authentication Protocol*, Protocolo de Autenticación de Clave), es un esquema de autenticación de texto plano. El NAS (*Network Access Server*, Servidor de Acceso a la Red) solicita el nombre de usuario y contraseña y PAP los regresa en texto plano (sin encriptar). Obviamente, este esquema de autenticación no es seguro ya que usuarios malintencionados podrían capturar el usuario y clave y usarlos para obtener acceso al NAS y todos los recursos proporcionados por el mismo. PAP no provee protección contra ataques de reproducción o personificación de cliente remoto una vez que se ha comprometido la clave de usuario.

CHAP (*Challenge Handshake Authentication Protocol*, Protocolo de Autenticación por desafío mutuo), es un mecanismo de autenticación cifrada que previene la transmisión de

la clave real en la conexión. El NAS envía un desafío, que consta de un ID de sesión y una cadena de desafío arbitraria, para el cliente remoto. El cliente remoto debe usar algoritmo *hash* MD5 de una vía para regresar el nombre de usuario y un código *hash* del desafío, ID de sesión y la clave del cliente. El nombre de usuario se envía como texto plano.

CHAP es una mejora de PAP debido a que no se envía la contraseña en testo plano sobre el enlace. En lugar de esto, la contraseña se usa para crear un código *hash* desde el desafío original. El servidor conoce la contraseña en texto plano del cliente y puede, por lo tanto, replicar la operación y comparar los resultados de la clave enviada en la repuesta del cliente. CHAP protege contra personificación de cliente remoto enviando impredeciblemente repetidos desafíos al cliente remoto a lo largo de la duración de la conexión.

EAP (*Extensible Authentication Protocol,* Protocolo de Autenticación Extensible), es un protocolo de autenticación PPP (*Point to Point Protocol*, Protocolos de Enlace Punto a Punto). Difiere de los otros protocolos de autenticación en que, durante la fase de autenticación, en realidad no lleva a cabo la autenticación. En la fase 2 EAP solo negocia el uso de un método de autenticación EAP común (conocido como tipo EAP). La verdadera autenticación para el tipo de EAP negociado se realiza después de la fase 2. Durante la fase 2 de la configuración de enlace PPP, el NAS recolecta los datos de autenticación y luego los valida contra su propia base de usuario o un servidor de base de datos de autenticación central.

3.2.3 Túneles

Muchas redes corporativas son protegidas del mundo exterior por dispositivos *firewall* o por el simple recurso de ejecutar la red en direcciones IP privadas que no son enrutables sobre el Internet global. Cualquiera, o ambas de estas medidas pueden estar presentes en ambos lados de una VPN, previniendo que paquetes externos de sistemas conectados a la LAN. Sin embargo el propósito de una VPN es permitir que un *host* o sitio remoto se convierta en parte de la LAN y por eso, las medidas de seguridad usadas para protegerla de

la intrusión desde el Internet deben ser eludidas para permitir trabajar a la VPN. Otra razón más para aplicar túneles es un cifrado del paquete original: si todos sus campos incluyendo los de la cabecera IP son encriptados entonces los *routers* no pueden hacer su trabajo.

La solución es usar túneles, en los que un paquete destinado a un sitio remoto es ubicado dentro de otro paquete IP con direcciones de origen y destino globalmente enrutables. Una VPN consiste de dos estaciones, conocidas como puntos finales del túnel, que realizan las operaciones necesarias. Cuando un paquete tunelizado es recibido por el punto final de destino, las cabeceras concernientes al túnel son removidas para revelar el paquete original que es entregado al destinatario final.

Todos los túneles involucran la encapsulación del paquete original o trama antes de ser liberado en el Internet. Tres protocolos participan en el proceso:

- El **protocolo pasajero** es el paquete original y será un protocolo de capa de red (IP, IPX, *AppleTalk*, etc.) o una trama PPP.
- El **protocolo de encapsulación** es el protocolo de capa de transporte que envuelve a los datos originales.
- El **protocolo mensajero** es usado por la red para transportar el paquete tunelizado y debe ser IP si el túnel se ubica en el Internet.

Existen dos tipos de túneles, distinguidos por la naturaleza del protocolo pasajero: Túneles de capa 3 y túneles de capa 2.

3.2.3.1 Túneles de capa 3

Un datagrama IP es encapsulado y esto se lleva a cabo antes de que cualquier componente de capa 2 (cabeceras y *trailers*) sea aplicado. Este tipo de túnel es asociado a menudo con VPNs entre sitios en los cuales los dos puntos finales del túnel son *routers*.

Hay gran cantidad de tipos de túneles de capa 3 que se distinguen por el protocolo de encapsulación empleado. Los dos más comunes son túneles GRE y los IPSec.

3.2.3.2 Túneles de capa 2

En estos túneles el proceso de encapsulación toma lugar después de que el encabezado y *tráiler* de enlace de datos han sido aplicados. El corolario de esto es que el proceso de tunelización en capa 2 no puede ser aplicado selectivamente (decidir tunelizar un paquete basándose en, por ejemplo, su dirección IP de origen o destino). Una estación con un túnel de capa 2 activo envía a ciegas el tráfico saliente a su par en el túnel.

3.3 TOPOLOGÍA VPN

Una gama de soluciones VPN están disponibles para las empresas que contemplan la aplicación de una WAN. Cada tipo de VPN tiene una serie de características distintas, en términos de participación y funcionamiento, y como tal frente a necesidades especificas. Este punto trata sobre los diferentes tipos de topologías VPN e implementaciones, así como los distintos dispositivos de red que se utilizan para su construcción.

3.3.1 Tipos de VPN y sus pertenencias

Existe variedad de implementaciones y configuraciones VPN para satisfacer variedad de necesidades. Las organizaciones pueden requerir su VPN para ofrecer el acceso telefónico, o permitir que terceros, como clientes o proveedores accedan a los componentes específicos de su VPN. Las VPN se pueden clasificar en tres grandes categorías: Intranet, Extranet y VPN Móviles y de Acceso Telefónico.

3.3.1.1 Intranet VPN

Una Intranet conecta a una serie de LAN a través de una red compartida. El propósito de una Intranet es compartir información y recursos entre los empleados dispersos. Por

ejemplo, las sucursales pueden acceder a la red en la oficina central, que típicamente incluyen recursos clave como el producto o bases de datos de los clientes. El acceso a la Intranet se limita estrictamente a estas redes y las conexiones están autenticadas. Los diferentes niveles de acceso pueden ser asignados a diferentes sitios en la Intranet, dependiendo de su propósito.

Típicamente, una Intranet incluye conexiones a través de una o más puertas de acceso a la Internet. Estas conexiones generalmente pasaran a través de cortafuegos (*firewalls*), que tienen la capacidad para filtrar el tráfico para aplicar la política de uso de internet y mantener la seguridad.

3.3.1.2 Extranet VPN

Una Extranet VPN es esencialmente una Intranet VPN que, además, proporciona un acceso restringido a terceros tales como clientes, proveedores y vendedores externos. Estos usuarios están restringidos a áreas específicas de la Intranet, por lo general denotada como la DMZ (*Demilitarized Zone*, Zona Desmilitarizada). Es responsabilidad del servidor de seguridad, autenticación y acceso a servicios de gestión, identificar entre los empleados de la empresa y otros usuarios, y diferenciar sus privilegios de acceso en consecuencia, las conexiones de los empleados deben ser dirigidas a la Intranet de la empresa, mientras que las conexiones reconocidas de terceros deben ser dirigidas a la DMZ.

Esta configuración es compatible con una serie de importantes iniciativas de comercio electrónico, proporcionando oportunidades de ahorro de costos y mejoras de eficiencia. Sin embargo, aumenta la complejidad de la autenticación y gestión de acceso, así como el requisito de que una partición de red independiente proporcionada como apoyo a la zona de distensión podría contrarrestar esta ganancia.

3.3.1.3 VPN de Acceso Remoto

Una VPN de acceso remoto apoya a los empleados móviles y el teletrabajo en el acceso a la Intranet desde ubicaciones remotas. Los diales de los empleados remotos en el RAS (*Remote Access Server*, Servidor de Acceso Remoto) más cercano, en el que se conceden contingentes de acceso en la autenticación realizada. El proceso de establecer un túnel seguro variará, dependiendo de cuál de los enfoques siguientes son utilizados:

Conexión estática. En este modelo, el RAS establece una conexión segura automáticamente, utilizando L2TP a un lugar predeterminado dentro de la Intranet, proporcionando un acceso transparente para el usuario. Este modelo está dirigido a los teletrabajadores y usuarios necesarios para llamar a un RAS específico.

Conexión dinámica. Bajo este modelo, el usuario se conecta a un RAS de su ISP, y luego realiza la autenticación remota con un servidor designado en la Intranet, después de lo cual el usuario tiene permitido el acceso a través de un túnel seguro. El RAS no está directamente involucrado en la conexión VPN o el establecimiento de túnel, por lo que el usuario puede conectarse a la Intranet a través de cualquier RAS.

La implementación de una VPN de acceso telefónico puede resultar en un ahorro de costos considerables, lo que elimina la necesidad de la empresa para gestionar grandes *pools* modernos, y reemplazando la necesidad de peaje de llamadas a estos *módems* con llamadas locales a cuentas ISP. Al tomar ventaja de una infraestructura de acceso de alta velocidad como DSL o ISDN, algunas de las limitaciones de rendimiento típicamente asociados con el acceso remoto puede ser disminuido.

En la figura 3.3 se puede visualizar los diferentes tipos de VPN.

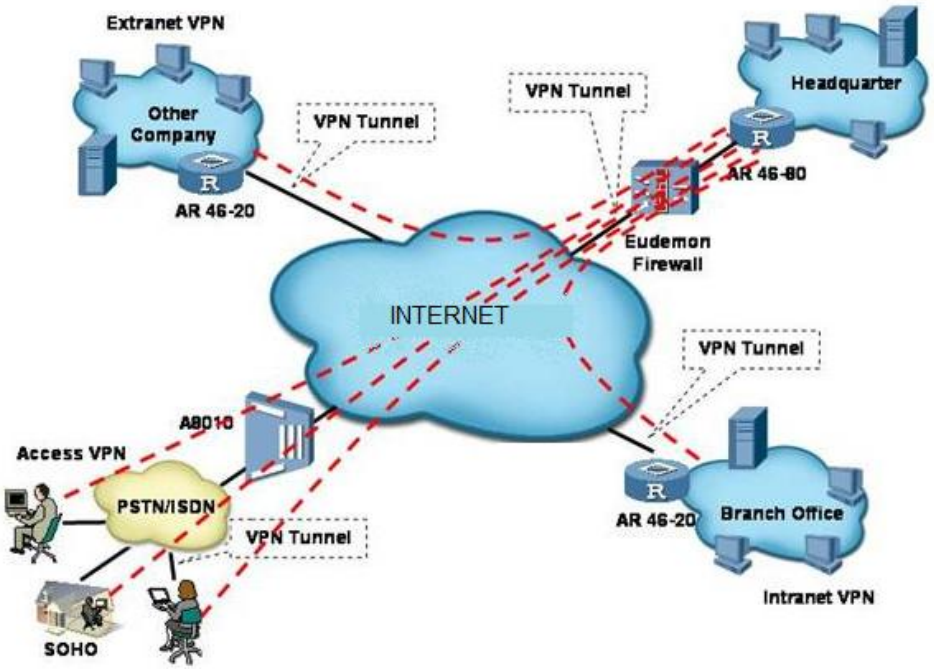


Figura 3.3 Tipos de VPN

Fuente:

http://www.h3c.com/portal/Products___Solutions/Products/Other_Products/Routers/Quidway_AR4600_Series_Routers/Detail_Material_List/200701/194282_57_0.htm

3.3.2 Implementaciones VPN

Una serie de enfoques diferentes para el problema de la creación de enlaces VPN y servicios pueden ser tomados. En particular, una VPN puede ser implementada y se sujeta en un número de las diferentes capas de la pila de protocolos. Por lo general, las VPN se implementan en la red o la capa de enlace, aunque las VPN de capa de aplicación también existen.

3.3.2.1 VPN de capa de enlace

Emplean una red troncal común, basada en una tecnología de capa de enlace conmutado tal como *Frame Relay* o ATM. Enlaces entre los nodos VPN se implementan como circuitos virtuales, que son económicos, flexibles, y pueden ofrecer un cierto nivel de rendimiento asegurado.

Las VPN de capa de enlace son las más apropiadas para la presentación de servicios de Intranet, el acceso *dial-up* no está bien respaldado. La mayor parte de los ahorros de costos asociados con las VPN, son el resultado del uso de los ISP, por lo que basados en IP, VPN de capa de red son más atractivas que las VPN de capa de enlace si el acceso telefónico se requiere.

3.3.2.2 VPN de capa de red

Las VPN de capa de red, principalmente basadas en IP, se implementan mediante el cifrado de capa de red, y posiblemente un túnel. Paquetes que entran en la red compartida se anexan con una cabecera IP adicional que contiene una dirección de destino que corresponde al otro extremo del túnel. Cuando este nodo recibe el paquete, la cabecera se retira y se recupera el paquete original, que se dirige a una localización dentro de la red de satélites dada. Debido a esta encapsulación, los paquetes originales podrían estar basados en cualquier protocolo de capa de red sin afectar a su transporte a través de la red compartida.

3.3.2.3 VPN de superposición

Pueden ser construidas a partir de redes de superposición, que conectan los subconjuntos de los recursos de una red subyacente y presentar el resultado como una capa de red virtual para protocolos de capa superior. Las redes superpuestas confían en que los túneles proporcionen enlaces virtuales, que están generalmente asegurados por el transporte IPSec para proporcionar seguridad de nodo a nodo.

3.3.2.4 VPN de capa de aplicación

Las VPN de capa de aplicación se implementan en *software*, por lo que las estaciones de trabajo y servidores están obligados a realizar tareas tales como la encriptación. Como resultado, las redes VPN de *software* son baratas de implementar, pero pueden tener un impacto significativo en el rendimiento, lo que limita la productividad de la red y

produciendo un uso algo excesivo de la memoria de los equipos utilizados, en particular a través de conexiones de banda ancha.

3.3.3 Componentes de *Hardware*

Un número de dispositivos de *hardware* son necesarios para implementar los diversos tipos de VPN. Muchos de estos dispositivos son comunes en redes estándares, pero algunos tienen una carga adicional y responsabilidades que se les impone cuando se aplica a una VPN y sus necesidades especificas. Los principales dispositivos de *hardware* utilizados por las VPN y las implicaciones de cualquier proceso adicional que deben realizar son las siguientes:

***Firewall*.** Las redes satelitales VPN deben ser protegidos de otros usuarios de la red troncal. Esto se logra utilizando un servidor de seguridad, que proporciona servicios críticos, tales como túneles, criptografía, filtrado de rutas y contenido.

***Router*.** Una conexión VPN *router* a *router* enlaza dos porciones de una red privada. El *router* que realiza la llamada (cliente VPN) se autentifica ante el *router* que responde (servidor VPN) y este a su vez se autentica ante el *router* que realiza la llamada y también sirve para la intranet.

***Switch*.** Algunos conmutadores ofrecen facilidades para mayor separación del tráfico, permitiendo que una red física sea dividida en un número de VLAN. En un conmutador normal, todos los puertos son parte de la misma red, mientras que un conmutador VLAN puede tratar diferentes puertos como partes de redes diferentes si se desea.

Servidor de túnel. Este servicio puede ser proporcionado por un *router* VPN o un *firewall*. La asignación de un componente de la red existente de esta responsabilidad adicional puede tener un serio impacto en el rendimiento.

***Cryptocard*.** IPSec ofrece la computacionalmente costosa Triple-DES, algoritmo de cifrado que proporciona un cifrado compacto. Sin embargo, puede limitar el ancho de banda efectivo al alrededor de 100Mbps y utiliza menos *hardware* criptográfico especializado. En una estación de trabajo, este *hardware* especializado se proporciona en forma de una tarjeta de expansión, que puede estar separado o integrado con el NIC. Algunos servidores de seguridad también ofrecen soporte de *hardware* para los algoritmos de cifrado diferentes.

3.4. PROTOCOLOS UTILIZADOS POR VPN

Viniendo de diferentes direcciones y soportando diferentes productos y servicios, varios protocolos de seguridad han sido desarrollados a lo largo de los años.

Se presentan los más renombrados.

3.4.1 GRE

GRE (*Generic Routing Encapsulation*, Encapsulación de Enrutamiento Genérico) es un protocolo desarrollado por Cisco® que puede encapsular una amplia variedad de tipos de paquetes dentro de túneles IP. Es un protocolo de transporte (capa 4) operando al mismo nivel que TCP, UDP e ICMP. Cuando se emplea en forma nativa, GRE es adecuado para túneles estáticos que permaneces configurados en los dos puntos finales del túnel, a menudo *routers* conectados a Internet, sin importar si los datos están fluyendo en cualquier momento dado. El proceso de encapsulación se ilustra en la figura 3.4 e involucra la anteposición de una cabecera GRE y una nueva cabecera IP al datagrama.

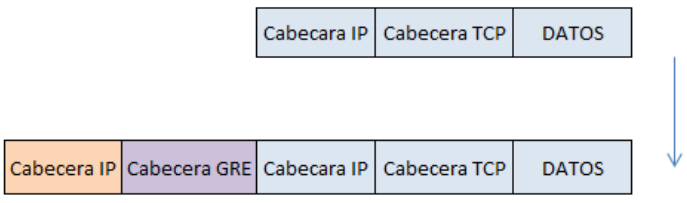


Figura 3.4 Encapsulación GRE

Fuente: Las autoras

Usualmente, el destino del paquete original no se puede alcanzar sobre el Internet debido a que es una dirección de un rango de IP privadas. El proceso de tunelización crea una nueva cabecera IP con una dirección de destino que es el punto final remoto del túnel y es alcanzable a través del internet. Cuando un par recibe este paquete, es desencapsulado (las cabeceras IP y GRE son removidas), exponiendo de esta manera la cabecera IP original. El datagrama reconstituido es entonces enrutado dentro de la red interna y entregado a la estación específica.

3.4.2 IPSec

IPSec es un conjunto de protocolos de capa de red, principalmente, que provee seguridad inter-operable y criptográfica para IPv6 y también ha sido adaptada para IPv4, ya que IPv6 no se expandió tan rápido como se esperaba. Gran cantidad de servicios de seguridad son proporcionados por IPSec, incluyendo control de acceso, integridad sin conexión, no repudio, protección contra ataques de repetición, y confidencialidad de flujo de tráfico limitado. Estos servicios son administrados en la capa de transporte, ofreciendo protección para el protocolo IP y protocolos de capas inferiores.

Las características de seguridad ofrecidas por IPSec son provistas a través de AH *(Autentication Header,* Cabecera de Autenticación), de la ESP *(Encapsulation Security Payload*, Seguridad de Encapsulación de Carga Útil) y de procedimientos de administración de claves criptográficas. Estos mecanismos son independientes de algoritmos, proporcionando una modularidad que permite la selección de diferentes conjuntos de algoritmos sin afectar otros aspectos de la implementación. Por ejemplo, comunidades de usuarios diferentes dentro de una VPN pueden seleccionar diferentes opciones de autenticación o cifrado si se requiere, permitiendo implementar facilidades de seguridad multiniveles.

El método de autenticación preferido es el uso de certificados digitales, que requiere un intercambio de clave pública para ejecutar la administración y distribución de clave segura. Desafortunadamente, SCEP, el principal protocolo para ejecutar solicitudes automatizadas

de certificados, no es soportado por la mayoría de productos VPN. Esto crea una debilidad para IPSec: es robusto autenticando los puntos finales del túnel usando IKE *(Internet Key Exchange,* Intercambio de Clave de Internet), pero débil autenticando al usuario detrás del punto final.

IPSec puede ser implementado bajo las siguientes topologías:

Implementación de Cliente. También llamada "*Bump In The Stack*" (BITS), porque es insertado entre la pila IP y los controladores de red local. Esta implementación es particularmente útil para sistemas de legado debido a que no se requiere acceso al código fuente de la pila IP.

Implementación de *Gateway*. También llamada "*Bump In The Wire*" (BITW), esta implementación emplea equipamiento con IPSec habilitado en el borde de la red. Este equipamiento puede operar IPSec en *software*, tales como vía *router* o *firewall*, o en *hardware* vía corredores de túnel específicamente diseñados, que ofrece desempeño superior, pero un gasto mayor.

Los paquetes IPSec tienen cabeceras IP estándar y por lo tanto pueden ser enrutados por *routers* estándar entre nodos VPN. El paquete IPSec es creado cifrando y encapsulando el paquete IP original en el segmento de datos de un nuevo paquete IPSec. El algoritmo de cifrado y claves son negociados e intercambiados usando IKE. Todas las implementaciones de IPSec deben soportar algoritmos de cifrado DES y 3DES y algunas otras implementaciones adicionalmente deben soportar algoritmos tales como *Blowfish*.

IPSec tiene un pequeño número de limitaciones que tienen implicaciones para su uso en VPNs, los más serios son los problemas de compatibilidad con NAT, ICMP, FTP, fragmentación IP y facilidades Qos

3.4.2.1 *Encapsulation Security Payload*

La cabecera ESP (*Encapsulation Security Payload*, Seguridad de Encapsulación de Carga Útil) proporciona una variedad de servicios de seguridad para IP. ESP puede ser aplicado solo, en combinación con AH o a través del modo túnel.

ESP suministra confidencialidad, no repudio, integridad sin conexión, protección de reproducción y confidencialidad de tráfico de flujo. La decisión de cuál de estas facilidades utilizar se hace en el establecimiento de asociación de seguridad (*Security Association*). Éstas deben ser escogidas cuidadosamente, ya que el uso de confidencialidad sin verificaciones de integridad o autenticación puede volver el tráfico vulnerable a ciertas formas de ataques activos. Los servicios de no repudio e integridad son soportados por firmas digitales y la detección de reproducción es suministrada por números de secuencia. La confidencialidad de tráfico de flujo se ofrece en conjunto con el modo túnel y es más efectiva si se implementa en una *gateway* de seguridad, donde la adición de tráfico puede ser capaz de enmascarar patrones de origen/destino del análisis de tráfico.

3.4.2.2 *Authentication Header*

La cabecera de autenticación (AH) proporciona integridad sin conexión y autenticación para datagramas IP y provee protección contra ataques de reproducción. AH provee autenticación a la cabecera IP tanto como es posible, así como también para datos de nivel superior.

AH puede ser aplicado solo, en combinación con ESP, o en una forma anidada a través del uso del modo túnel. ESP puede ser usado para dar los mismos servicios de seguridad, la diferencia principal es el grado de cobertura; ESP no protege ningún campo de la cabecera IP a menos que sean encapsulados por ESP en modo túnel.

3.4.2.3 *Internet Key Exchange*

El protocolo IKE (*Internet Key Exchange*, Intercambio de Clave de Internet) es un sofisticado intercambio de claves y sistema de administración, que se incluye en la pila de protocolo IPSec para proporcionar servicios de distribución segura de clave entre partes que deseen comunicarse sobre una red insegura.

IKE es un protocolo híbrido compuesto de características del ISAKMP *(Internet Security Association and Key Management Protocol*, Protocolo de Asociación de Seguridad de Internet y Administración de Clave), *Oakley* y SKEME *(Secure Key Exchange Mechanism*, Mecanismo de Intercambio de Clave Segura). IKE usa partes de estos tres protocolos para obtener material de clave autenticado para asociaciones de seguridad tales como AH y ESP para IPSec.

La negociación modo cliente, donde las partes negociantes no son puntos finales para las cuales la negociación de asociación de seguridad está tomando lugar, se soporta en IKE. Cuando se usan en modo cliente, las direcciones IP de los puntos finales no son reveladas, de manera que las identidades de las partes finales permanecen ocultas.

3.4.2.4 Asociaciones de Seguridad IPSec

Una SA (*Security Association*, Asociación de Seguridad) es un acuerdo entre dos partes sobre los métodos que emplearán para soportar comunicaciones seguras. Este acuerdo es alcanzado para la terminación de la fase de negociación que discierne las características comunes soportadas por las potencialmente diferentes implementaciones en cada punto final.

Los servicios de seguridad son costeados por una SA IPSec mediante el uso de AH o ESP, pero no ambas. Por lo tanto, si ambas van a ser aplicadas a un flujo de tráfico, entonces deben ser creadas dos o más SAs. Para asegurar comunicaciones típicas y bidireccionales

entre dos *host* o *gateways* de seguridad, se requieren dos SAs; una en cada dirección, como se muestra en la figura 3.5, ya que las SAs son unidireccionales.

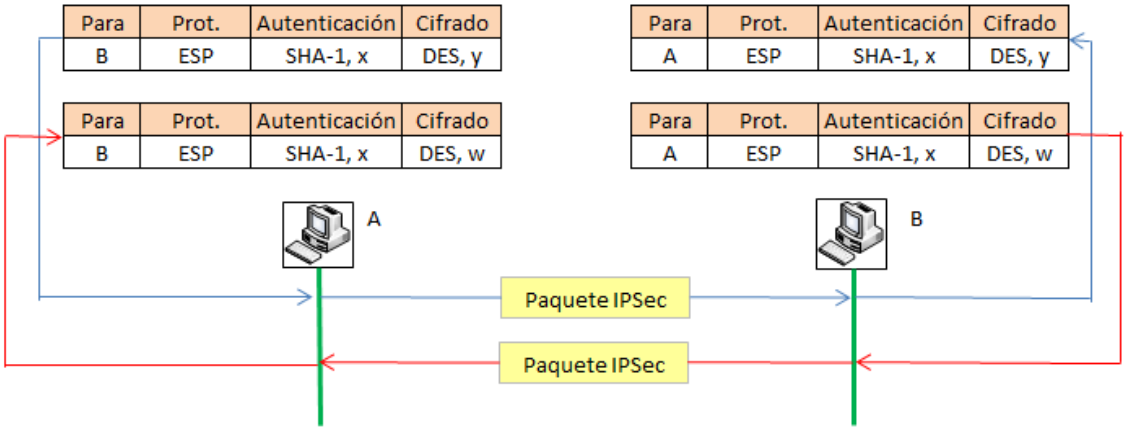


Figura 3.5 Comunicación bidireccional entre dos *host*

Fuente: Las autoras

Existen dos tipos de SAs definidas por IPSec:

Modo transporte. Una SA en modo transporte (figura 3.6) es un acuerdo entre dos *host*. En el caso de ESP, una SA en modo de transporte provee servicios de seguridad solo para protocolos de capa superior, no para la cabecera IP ni para ninguna extensión de cabeceras que precedan a la cabecera ESP. En el caso de AH, la protección también se extiende a porciones específicas de la cabecera IP y cualquier cabecera de extensiones.

Figura 3.6 Modo Transporte

Fuente: Configuración del Servicio VPN IPSec, Telefónica Telecom

Modo Túnel. Una SA en modo túnel (figura 3.7), es esencialmente una SA de modo de transporte que se aplica a un túnel IP. Este modo se requiere siempre que una SA termina en un *Gateway* de seguridad, para evadir la fragmentación y reensamblado de los paquetes IPSec y en situaciones donde los múltiples caminos al mismo destino detrás de los *gateways* de seguridad existentes. Dos *host* pueden establecer opcionalmente una SA en modo túnel si se requiere incrementar la seguridad.

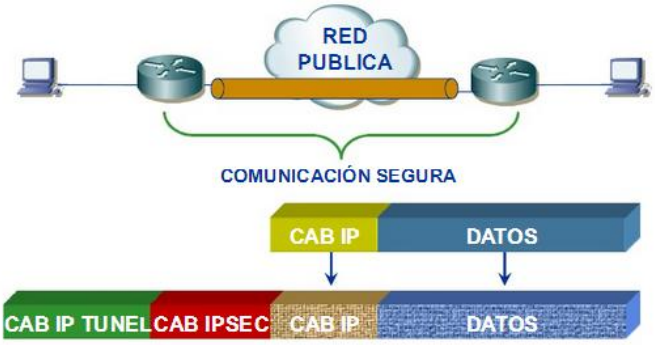


Figura 3.7 Modo Túnel

Fuente: Configuración del Servicio VPN IPSec, Telefónica Telecom

3.4.3 NAT

NAT (*Network Address Translation*, Traducción de Direcciones de Red) es el proceso de traducir una dirección IP dentro de una red origen a una dirección IP que corresponde a la máquina objetivo en la red receptora, de una manera transparente a los usuarios finales respectivos. Este proceso le permite a una empresa mapear sus direcciones locales a direcciones IP más globales y desempeñar un mapeo reverso en las direcciones IP globales ligadas a paquetes entrantes. Esta técnica oculta la estructura de direccionamiento de la red interna de la red no confiable y también proporciona un único punto de entrada a la red en el cual pueden ser forzadas la filtración y políticas de seguridad.

NAT opera a través de la creación y mantenimiento de una tabla de mapeos de direcciones IP. NAT puede operar estáticamente o puede traducir a y desde un *pool* de direcciones IP mantenido dinámicamente. El proceso de traducción de direcciones puede ser ejecutado conjuntamente con solicitud de autenticación o enrutamiento basado en políticas.

3.4.4 MPLS

MPLS (*Multi-Protocol Label Switching***,** Conmutación de Etiquetas Multiprotocolo) es un protocolo de administración de tráfico de red que establece un camino específico, conocido como Circuito Virtual (VC), para flujo de datos. Un VC es identificado por una etiqueta ligada a cada paquete, así que los *routers* no necesitan recuperar las direcciones del siguiente nodo en el camino. Como su nombre la sugiere, MPLS es compatible con gran cantidad de protocolos y arquitecturas, incluyendo IP, ATM y *Frame Relay*.

MPLS permite que la mayoría de los paquetes se reenvíen a la capa de enlace de datos en lugar de la capa de red y simplifica la administración de QoS mediante el soporte de acceso de conmutación orientado a la conexión. MPLS está diseñado para escalar eficientemente, proporcionando ingeniería de tráfico y mecanismos de re-enrutamiento.

Protocolos de capa de red sin conexión requieren que cada *router* tome una decisión de reenvío independiente para cada paquete que recibe, lo cual es ejecutado por un algoritmo de enrutamiento de capa de red que examina la cabecera del paquete para tomar la decisión.

Escoger el destino inmediato para reenviar (el "siguiente salto") se desarrolla en dos escenarios:

Establecer un conjunto de FECs (*Forwarding Equivalence Classes*, Reenvío de Clases Equivalentes). Esto involucra particionar el conjunto de posibles paquetes dentro de subconjuntos basados en su destino.

Mapear cada FEC semejante a un siguiente salto. Este proceso asegura que todos los paquetes recibidos desde un vecino dado, que pertenezcan a un FEC particular, seguirán el mismo camino.

El FEC al cual un paquete dado ha sido asignado es codificado con una etiqueta de longitud fija. Esta etiqueta se envía con el paquete a su próximo salto, así que no hay necesidad para

saltos subsecuentes de analizar la cabecera de capa de red debido a que la etiqueta es usada como índice dentro de una tabla que especifica el siguiente salto. La etiqueta anterior es luego remplazada con una nueva etiqueta y el paquete es reenviado a su siguiente salto con la nueva etiqueta.

Esta técnica de reenvío basada en etiquetas tiene gran cantidad de ventajas sobre reenvío convencional de capa de red. Estas facilidades pueden ser aprovechadas convenientemente para crear arquitectura de *backbone* de MPLS escalable que puede soportar concurrentemente múltiples VPN.

3.4.5 L2TP

VPN usa L2TP (*Layer 2 Tunnelling Protocol*, Protocolo de Entunelamiento de Capa 2) para crear túneles de capa de enlace de datos para transportar conexiones de datos punto a punto (PPP) entre punto finales. Si la conexión ha sido iniciada por un usuario conectándose desde casa a un ISP local, los NAS (*Network Access Server*, Servidores de Acceso a la Red) interceptan la conexión y tunelizan los paquetes al destino. L2TP también proporciona túneles autenticados, pero no integridad de mensajes ni confidencialidad.

Los dos componentes principales que se usan para suministrar servicio L2TP son el LAC (*L2TP Access Concentrator*, Concentrador de Acceso L2TP) y el LNS (*L2TP Network Server*, Servidor de Red L2TP).

El LAC es un dispositivo físico, como un *módem pool*, al cual un usuario *dial-up* establece una conexión. El uso de un LAC le permite al procesamiento de paquetes PPP estar separado de la terminación del circuito de capa 2. Un beneficio para la VPN de tal separación es que la conexión no necesita terminar en el NAS, lo cual podría requerir peaje de carga de larga distancia. En lugar de eso, la conexión puede terminar en el LAC, que luego tuneliza la sesión PPP a lo largo de la red compartida. El LNS es un mecanismo que termina y posiblemente autentica, estos flujos PPP tunelizados.

L2TP es orientado a la conexión; el LNS y LAC mantienen el estado para cada conexión que es iniciada o respondida por un LAC. Como se observa en la figura 3.8, una sesión L2TP se crea entre el LAC y LNS cuando se establece una conexión PPP fin a fin entre un sistema remoto y el LNS. Datagramas relacionados a la conexión PPP son enviados sobre el túnel entre el LAC y el LNS.

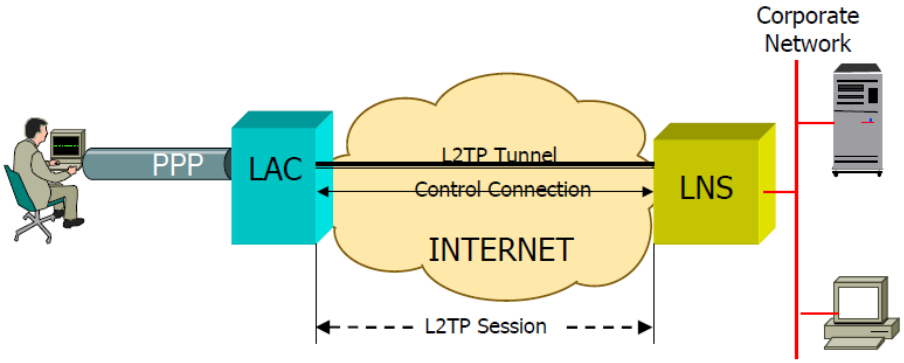


Figura 3.8 Sesión L2TP

Fuente: Presentación de diapositivas Mario Baldi y Luigi Ciminiera, Politécnico di Torino

3.4.6 *RADIUS*

RADIUS (*Remote Authentication Dial-In User Service,* Servicio de Autenticación Remota de Usuario Dial-In) es una herramienta de autenticación diseñada para su uso en sistemas distribuidos, que separa el proceso de autenticación y autorización de usuario del proceso de comunicaciones y establece una localización central para datos de autenticación de usuario. El proceso de separar la seguridad de las comunicaciones permite a la seguridad ser aplicada y mantenida más efectiva y eficientemente. Esto es deseable cuando se aplica a VPNs, así la política de seguridad puede ser rápidamente actualizada y modificada para adaptarse a requerimientos cambiantes y es particularmente valioso como una herramienta para autenticación de usuarios remotos VPN.

El siguiente capítulo tratará sobre el funcionamiento del sistema de monitoreo y respaldo y se expondrán los conceptos de los tres capítulos anteriores a utilizar.

CAPÍTULO 4

FUNCIONAMIENTO DEL SISTEMA DE MONITOREO DE RESPALDO

En este capítulo se detalla el funcionamiento, el equipo y la tecnología a utilizar para el desarrollo del sistema de monitoreo.

Como se indicó en el primer capítulo, el equipo a utilizar para la captación y barrido de frecuencias de radio y televisión es el iCOM IC-PCR2500, del que se presenta la información relevante a continuación.

4.1 iCOM

El iCOM IC-PCR2500 (figura 4.1), es un equipo de recepción para computadoras con el que se captan las señales RF y por medio de un software incluido se realiza la grabación y almacenamiento del audio en la PC a la cual se encuentra conectado.

Figura 4.1 iCOM IC-PCR2500
Fuente: www.icomamerica.com

4.1.1 Información General

A continuación se presenta la información general del equipo iCOM IC-PCR2500.

Capacidad de doble vigía

El IC-PCR2500 tiene la capacidad de doble vigía[2], lo que le permite recibir dos bandas simultáneamente. Cubre las frecuencias de 0.01-3299.999MHz en los modos AM, FM, WFM, SSB, CW, DV y P25 en el receptor principal, mientras que el subreceptor cubre las frecuencias de 50-1300MHz en los modos AM, FM y WFM.

Capacidad de diversidad de recepción

El modo de recepción de diversidad[3] es útil para operación móvil donde la señal de recepción cambia continuamente. Compara la intensidad de la señal y elige la antena con la mejor señal para mantener buen sonido y calidad de recepción.

Pantalla ancha de LCD para control independiente de banda

La pantalla ancha de LCD muestra las configuraciones del receptor principal y del subreceptor en una disposición simétrica de lado a lado fácil de leer. El controlador proporciona perillas independientes de sintonización, volumen, silenciamiento y botones de funciones para los receptores izquierdo (principal) y derecho (subreceptor).

Recepción en modo digital

La unidad digital opcional D-STAR UT-118 y la unidad digital P25 UT-122 proporcionan lo último en recepción en modo digital.

[1] Para recepción doble vigía se requieren dos antenas.

[2] Se requieren dos antenas. Disponible en el modo FM/DV/P25 entre 50–1300MHz únicamente. La diversidad de recepción no está disponible cuando se utiliza doble vigía.

1000 canales de memoria alfanuméricos

Con el escaneo dinámico de memoria (DMS) de iCOM, se cuenta con un versátil sistema de control de canales de memoria. Los 1000 canales de memoria se pueden organizar por preferencia de servicio o personal dentro de los 21 bancos de memoria.

Otras características

- Función de alerta meteorológica (Únicamente en la versión de los Estados Unidos).
- Capacidad DSP opcional con la UT-106.
- El VSC (control de silenciamiento de voz) ignora las señales no moduladas o heterodinas.
- Selección del filtro de IF para cambiar el ancho del filtro de IF.
- El supresor de ruido elimina el ruido tipo pulsos (sólo en el modo SSB, CW y AM).
- La función AFC sigue automáticamente a una señal de FM cuando esta se desplaza (ancho de banda: 6kHz ó 15kHz).
- Función de desplazamiento de IF (sólo en modo SSB y CW).
- Temporizador de apagado automático de 30 minutos — 2 horas.
- Configuración rápida/lenta de AGC.
- Retardo de silenciamiento corto/largo.
- Tonos CTCSS/DTCS y operación en modo dúplex para monitorear un repetidor.
- Atenuador de RF, atenúa 20dB (aproximadamente, inferior a 1300MHz).
- Todas las funciones del IC-PCR2500 están disponibles cuando se conecta a una PC.
- La función de clonación le permite leer/escribir el contenido de la memoria desde la PC.

En la tabla 4.1 se presentan las características generales y en la 4.2 las características del receptor del IC-PCR2500.

Tabla 4.1 Especificaciones Generales

Fuente: http://www.icomamerica.com/es/products/receivers/mobile/r2500/specifications.aspx

<table>
<tr><td>Cobertura de frecuencia</td><td>
<table>
<tr><th></th><th>Cobertura de frecuencia</th><th>Modo</th></tr>
<tr><td rowspan="3">Receptor principal</td><td>0.010–3299.999MHz</td><td>AM, FM, WFM,</td></tr>
<tr><td>(Garantizado en 0.495–3000MHz)</td><td>DV, P25</td></tr>
<tr><td>0.495–1300MHz</td><td>USB, LSB, CW</td></tr>
<tr><td>Subreceptor</td><td>50–1300MHz</td><td>AM, FM, WFM</td></tr>
</table>
</td></tr>
<tr><td>Rango de temperatura de operación
Cuando se utiliza con una PC</td><td>–10°C a +60°C; +14°F a +140°F
0°C a +60°C; +32°F a +140°F</td></tr>
<tr><td>Estabilidad de frecuencia</td><td>Inferior a ±3ppm sobre la base de 25°C (–10°C a +60°C)</td></tr>
<tr><td>Pasos de sintonización</td><td>10Hz (mínimo con controlador)
1Hz (mínimo con PC)</td></tr>
<tr><td>Fuente de alimentación</td><td>12.0V C.C. ±15%</td></tr>
<tr><td>Consumo de corriente (a 12.0V C.C.)
Audio máx.
En espera</td><td>
Inferior a 1.5A (modo dual)
0.85A típica (modo dual)</td></tr>
<tr><td>Impedancia de antena</td><td>50Ω (BNC)</td></tr>
<tr><td>Dimensiones
Unidad principal
Controlador</td><td>(ancho × alto × profundidad ; No se incluyen las proyecciones)
146 × 41 × 206 mm; 5 3/4 × 1 5/8 × 8 1/8 pulgadas
140 × 50 × 39 mm; 5 1/2 × 1 31/32 × 1 3/32 pulgadas</td></tr>
<tr><td>Peso (aprox:)
Unidad principal
Controlador</td><td>
1350 grs; 3 libras
250 grs; 8.8 onzas (incluyendo el cable)</td></tr>
</table>

Tabla 4.2 Especificaciones del Receptor

Fuente: http://www.icomamerica.com/es/products/receivers/mobile/r2500/specifications.aspx

<table>
<tr><td>Sistema de receptor</td><td>Sistema de triple conversión superheterodina + conversor-reductor de frecuencia</td></tr>
<tr><td>Frecuencias intermedias</td><td>1ra 266.70MHz
2ª 10.70MHz
3ª 450kHz (Excepto WFM)</td></tr>
<tr><td>Sensibilidad (inferior a)</td><td>
<table>
<tr><th></th><th>SSB, CW</th><th>AM</th><th>FM</th><th>WFM</th></tr>
<tr><td>0.495–1.799MHz</td><td>5.0µV</td><td>25µV</td><td>–</td><td>–</td></tr>
<tr><td>1.8–49.999MHz</td><td>0.5µV</td><td>2.5µV</td><td>0.63µV</td><td>–</td></tr>
<tr><td>50–699.999MHz</td><td>0.4µV</td><td>2µV</td><td>0.5µV</td><td>1.4µV</td></tr>
<tr><td>700–1300.000MHz</td><td>0.5µV</td><td>2.5µV</td><td>0.63µV</td><td>1.8µV</td></tr>
<tr><td>1300–2299.999MHz</td><td>–</td><td>–</td><td>5.6µV</td><td>18µV</td></tr>
<tr><td>2300–3000.000MHz</td><td>–</td><td>–</td><td>18µV</td><td>56µV</td></tr>
</table>
</td></tr>
<tr><td>Selectividad (típica)
SSB, CW, AM
SSB, CW, AM, FM
FM, AM
FM, AM, WFM
WFM</td><td>
Superior a 2.8kHz/–6dB
Superior a 6.0kHz/–6dB
Superior a 15kHz/–6dB
Superior a 50kHz/–6dB
Superior a 230kHz/–6dB</td></tr>
<tr><td>Potencia de salida de audio</td><td>Superior a 500mW a una distorsión del 10% con una carga de 8Ω load</td></tr>
<tr><td>Conector para altavoz externo</td><td>2 conductores de 3.5mm (profundidad)(⅛ pulgadas)/8Ω</td></tr>
</table>

4.1.2 Requerimientos de la PC

Para uso con el *software* de control de la PC:

- Microsoft® Windows® XP/2000/ME/98SE.
- USB 1.1 ó 2.0.
- Intel® Pentium® III 450MHz o más rápido (se recomienda Pentium® 4).
- Disco duro con al menos 50MB de espacio libre de disco.
- Al menos 128 MB de memoria (se recomienda 256 MB o más).
- Pantalla con resolución de 1024 × 768 píxeles y color de alta definición.
- Para instalar el software se requiere un lector de CD-ROM o DVD.

- Pueden ocurrir pausas o discontinuidad de audio de USB debido a la falta de potencia de la PC.
- Para grabación de sonido o almacenamiento de datos del indicador se requiere espacio adicional de disco duro.

4.2 VNC

VNC (*Virtual Network Computing*, Computación Virtual en Red) es una tecnología para uso compartido de escritorio remoto. VNC permite ver y controlar remotamente la pantalla del escritorio de una computadora sobre una conexión de red. Esta tecnología es bastante útil para administradores de red en ambientes empresariales.

La VNC fue creada como un proyecto de investigación de código abierto a finales de los 90. Desde entonces, varias soluciones de escritorio remoto han sido creadas, basadas en VNC. El equipo de desarrollo original produce el paquete RealVNC. Otras derivaciones populares incluyen UltraVNC y TightVNC.

VNC trabaja de manera similar a la aplicación de escritorio remoto construida dentro de la nueva versión de Microsoft Windows. Pero a diferencia de ésta, VNC corre en computadoras con Windows antiguos, Linux/Unix y otros sistemas operativos. Si embargo, las aplicaciones VNC, generalmente son consideradas más lentas y ofrecen menos características y opciones de seguridad que el escritorio remoto de Windows.

VNC trabaja sobre un modelo cliente/servidor, un espectador VNC (o cliente) es instalado en el computador local y se conecta al componente servidor, que debe ser instalado en el computador remoto. El servidor transmite un duplicado de la pantalla del computador remoto al cliente. También interpreta comandos provenientes del espectador y los lleva a cabo en el computador remoto.

4.3 INTEGRACIÓN DEL SISTEMA

Habiendo dejado claro la tecnología, herramientas y equipos a utilizar, el siguiente paso es hacer la integración de lo detallado por separado y desarrollar el sistema.

Para este sistema, cuyo diagrama de bloques se muestra en la figura 4.2, se utilizará una infraestructura de red pública, es decir se realizará una conexión entre red local y remota a través del Internet, esta conexión se la realizará a través de una VPN confiable para ofrecer un nivel de seguridad a los datos transferidos, simulando un enlace privado por el cual sólo circularán los datos de esta red.

El iCOM será configurado en el sitio remoto y conectado a una PC, en la que se instalará el *software* del iCOM y se almacenarán las grabaciones de las frecuencias captadas por el mismo. Los archivos que se guardan en la PC remota se obtendrán accediendo a dicha PC desde las instalaciones de la IRC en Guayaquil a través de una VNC.

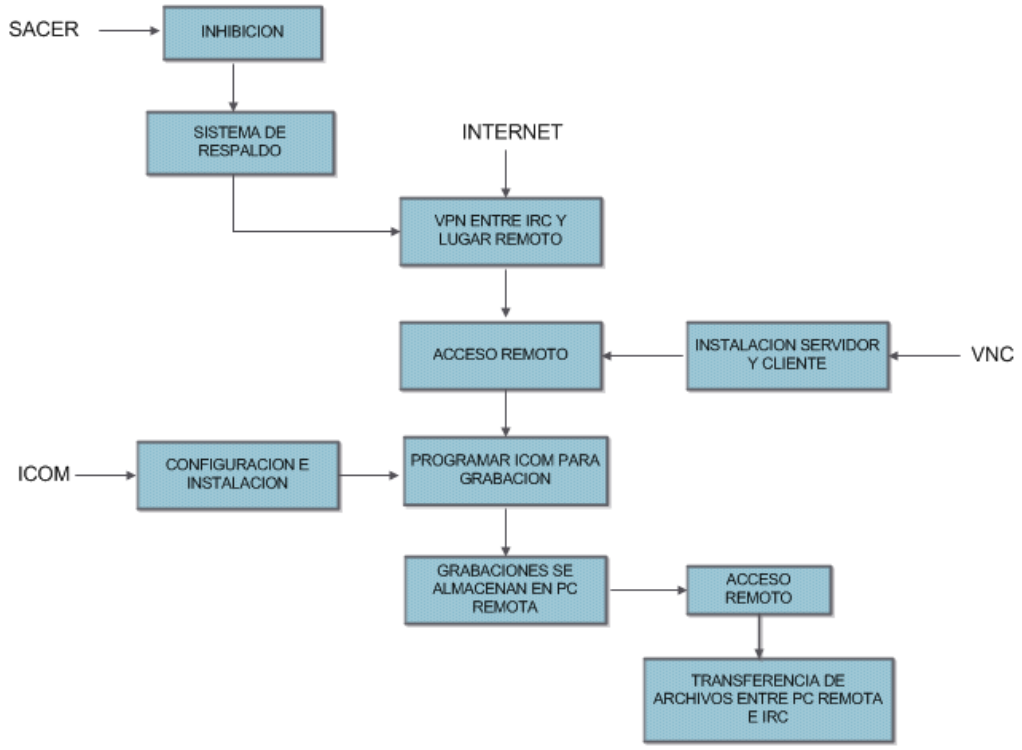


Figura 4.2 Diagrama de bloques del sistema de monitoreo de respaldo

Fuente: Las Autoras

4.3.1 Ambiente de trabajo del iCOM

En la figura 4.3 se presenta la mascarilla del IC-PCR2500, en la que se puede visualizar del lado izquierdo, en el receptor principal, el escaneo de la frecuencia de TV y del lado derecho, el escaneo de frecuencias de radio FM, en el subreceptor.

Se puede observar también, junto a la mascarilla, al lado derecho, los íconos de acceso directo a ciertas funciones del receptor.

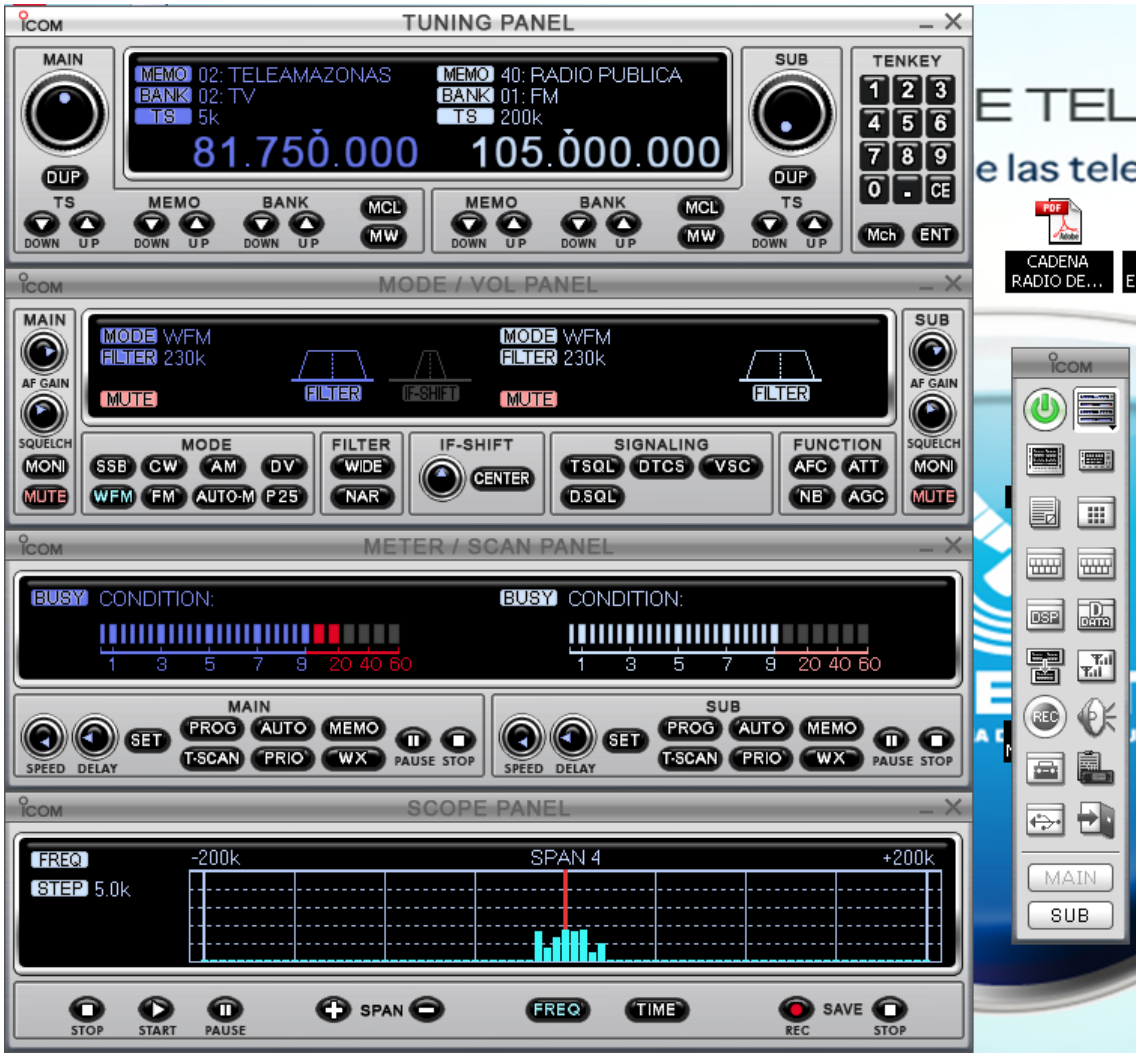


Figura 4.3 Mascarilla del IC-PCR2500

Fuente: Verificación del ambiente de trabajo del IC-PCR2500

Se puede observar en la figura 4.4 un banco de canales para frecuencias de TV. Por medio de este banco, guiándose con estas frecuencias, el IC-PCR2500 realizará el "Escaneo de banco de memoria" (Anexo 1).

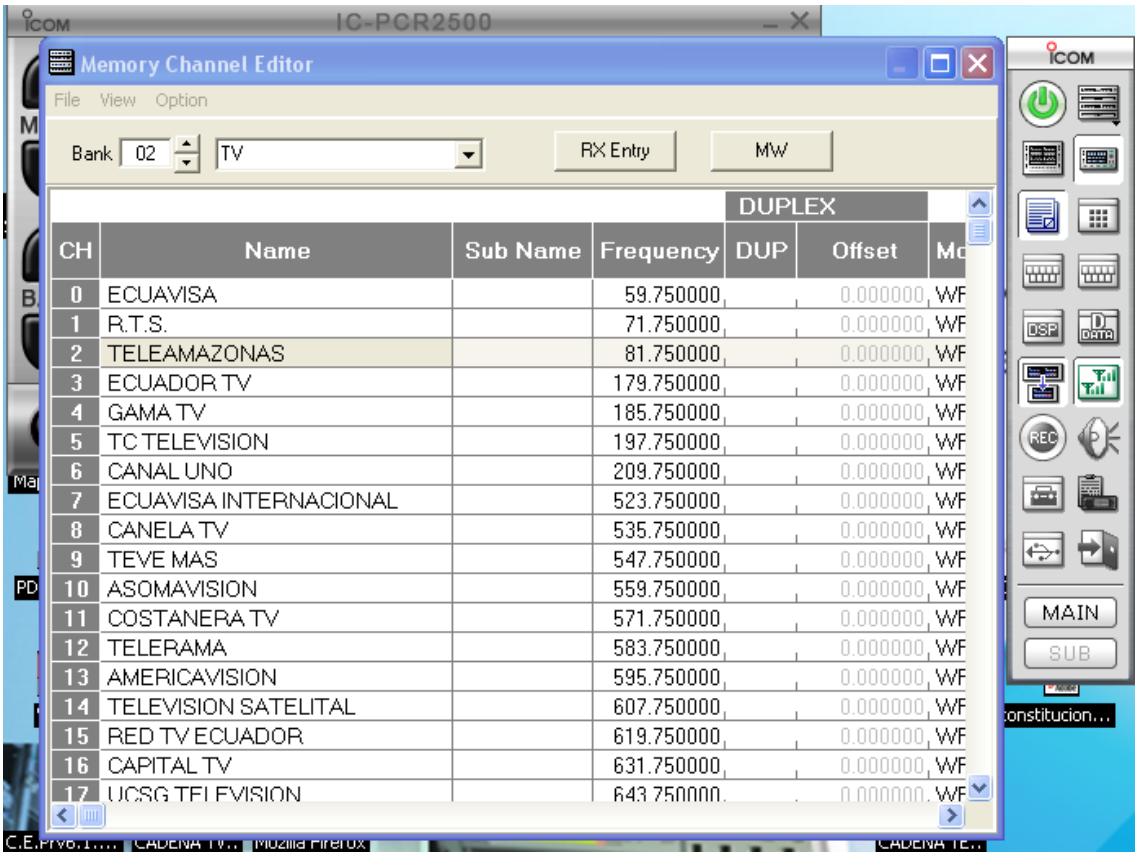


Figura 4.4 Banco de canales para frecuencias de TV.

Fuente: Verificación del ambiente de trabajo del IC-PCR2500

El receptor tiene 250 multicanales. Un total de 10 bancos de memoria están disponibles para usar por grupo y 25 canales son asignados en un banco.

La función de monitoreo multicanal escanea los multicanales programados y permite verificar el nivel de robustez de la señal recibida en los canales visualmente, figura 4.5.

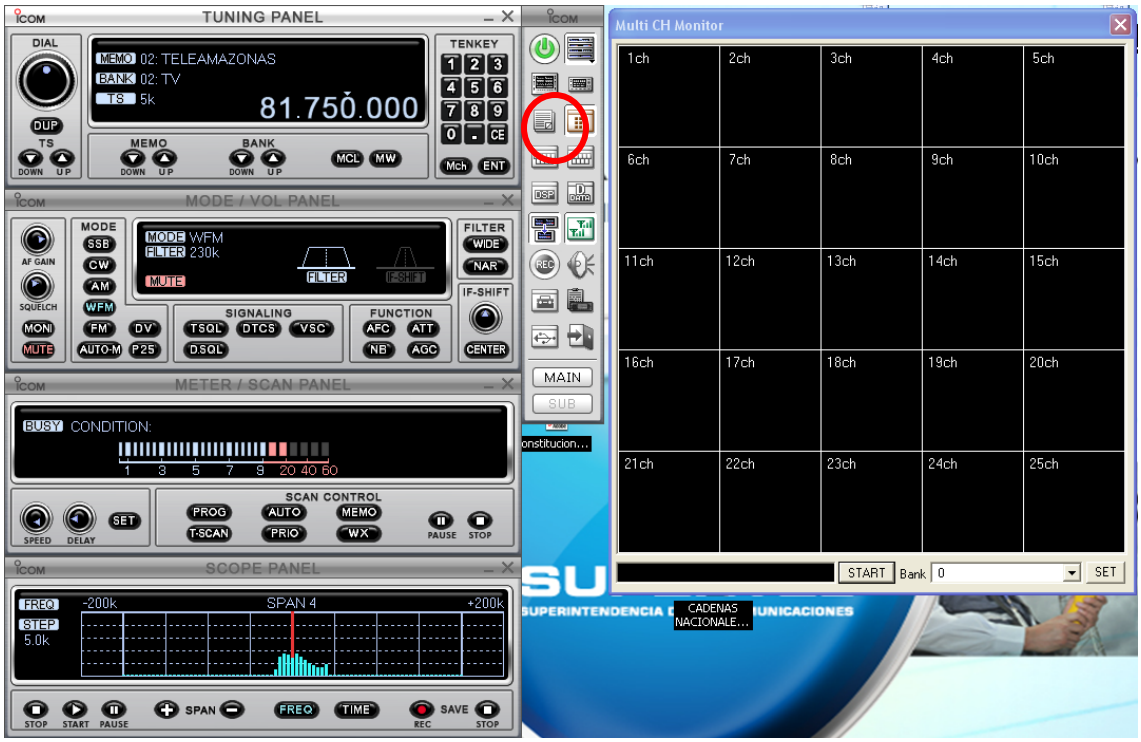


Figura 4.5 Monitoreo Multicanal

Fuente: Verificación del ambiente de trabajo del IC-PCR2500

En la figura 4.6 Se muestra la pantalla de funciones, de la cual se detallan los parámetros en el Anexo 2.

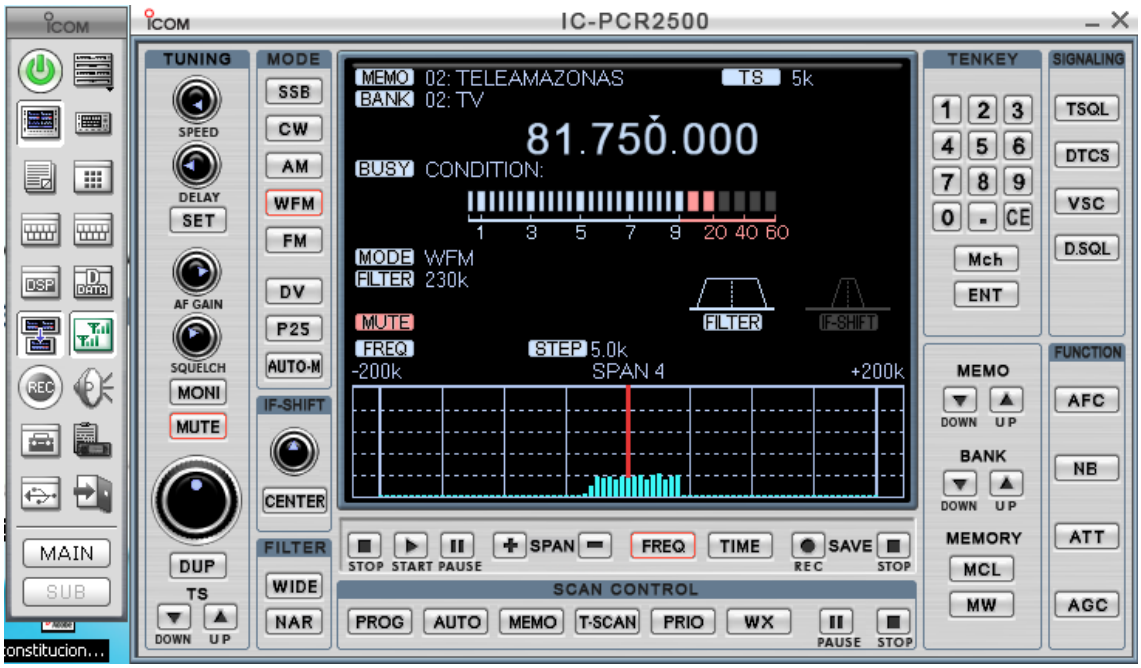


Figura 4.6 Pantalla del Receptor Multifuncional

Fuente: Verificación del ambiente de trabajo del IC-PCR2500

En la figura 4.7 Se muestra la consola de grabado, en la parte superior constan, de izquierda a derecha, los botones de Grabar, Detener y Pausa para el receptor principal y debajo de éstos, los mismos botones para el subreceptor. En la parte inferior está la dirección en la que se guardarán los archivos en la computadora.

El procedimiento para la grabación se detalla en el Anexo 3.

4.7 Consola de grabación de frecuencias.

Fuente: Verificación del ambiente de trabajo del IC-PCR2500

4.3.2 Instalación VNC

Principios de control remoto usando VNC

Para conectarse y controlar una computadora desde otra se necesita:

- Una aplicación llamada VNC *Server*, la cual debe estar corriendo en el *host*, es decir en la computadora que se desea controlar.
- Una aplicación llamada VNC *Viewer*, la cual debe estar corriendo en la computadora a la cual llamaremos cliente, desde la cual se quiere acceder al *host*.

- Las computadoras, *host* y cliente deben estar conectadas a la misma red TCP/IP. Esta puede ser una red privada ya sea LAN, VPN o internet.

Un ejemplo de la topografía del entorno bajo el cual se trabajará, se muestra en la figura 4.8.

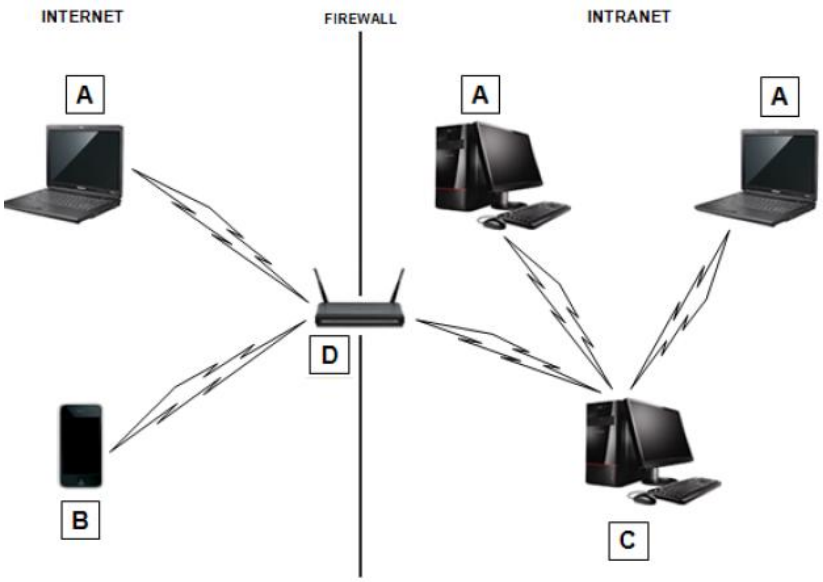


Figura 4.8 Topología de trabajo entre equipo cliente y servidor

Fuente: http://www.realvnc.com/products/vnc/documentation/latest/

A representa a la computadora cliente (normalmente una laptop o computadora de escritorio) en la cual estará corriendo VNC *Viewer*.

B puede ser otro tipo de equipo cliente en el cual también se puede correr la aplicación para el acceso remoto.

C es nuestra computadora *Host* (normalmente una estación de trabajo o un servidor) donde debe estar corriendo VNC *Server*.

D representa el *router* que debe estar brindando direcciones a la red pública para conexiones a internet para la computadora *Host*.

Para empezar una sesión de acceso remoto se debe correr VNC *Viewer* en la computadora cliente e identificar el equipo servidor donde se está corriendo el VNC *Server*. Después de realizar la autenticación correspondiente, VNC *Viewer* muestra el escritorio del equipo *host* en una nueva ventana donde se puede empezar a controlar el mismo con el teclado y *mouse* de la computadora cliente.

A continuación se detallan los pasos que se debe seguir para empezar a utilizar el escritorio remoto.

Paso 1. Descargar la aplicación en ambas computadoras: Se puede descargar la aplicación VNC *Server* de la página www.realvnc.com/download/vnc/, también es necesario obtener la licencia ya que se deberá ingresar en uno de los pasos siguientes.

Seguido de esto se debe descomprimir la carpeta con el archivo ejecutable del programa. Después de ejecutar el programa se abrirá una ventana con los pasos a seguir para instalarlo. Figura 4.9

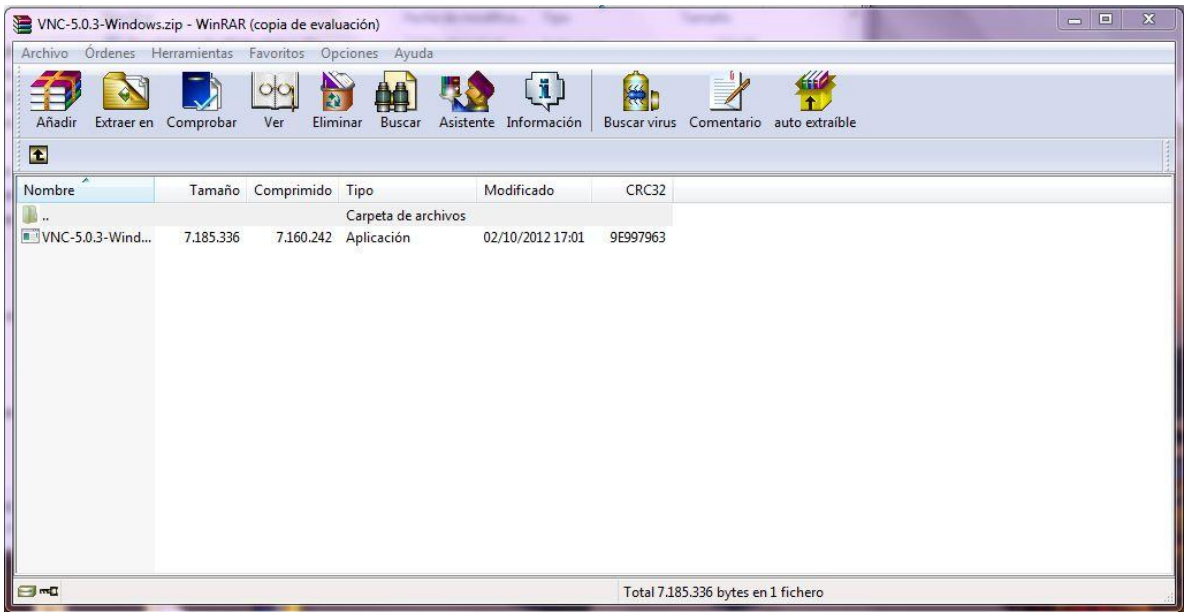


Figura 4.9 Ventana del archivo comprimido del instalador VNC Server

Fuente: Instalación de RealVNC

Seleccionar siguiente para continuar con la instalación como se muestra en la figura 4.10.

Figura 4.10 Inicio del asistente de tareas para la instalación de la aplicación.

Fuente: Instalación de RealVNC

Aceptar el acuerdo de licencia y dar clic en siguiente. Figura 4.11.

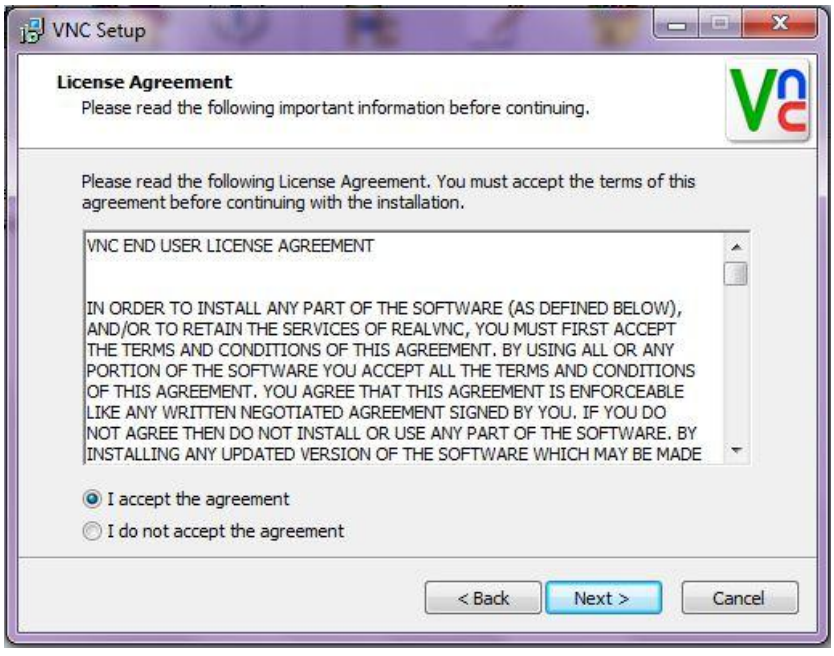


Figura 4.11 Ventana de acuerdo de licencia.

Fuente: Instalación de RealVNC

Instalar todos los componentes y dar clic en siguiente. Figura 4.12.

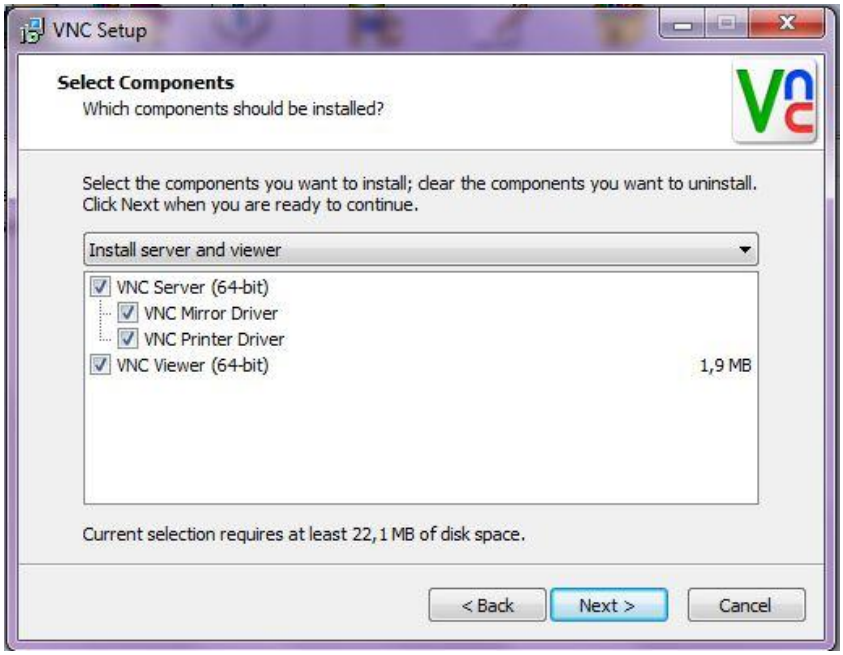


Figura 4.12 Selección de componentes a instalar.

Fuente: Instalación de RealVNC

Seguido de esto se selecciona la dirección de la carpeta donde se desea instalar el programa y dar clic en siguiente. Figura 4.13.

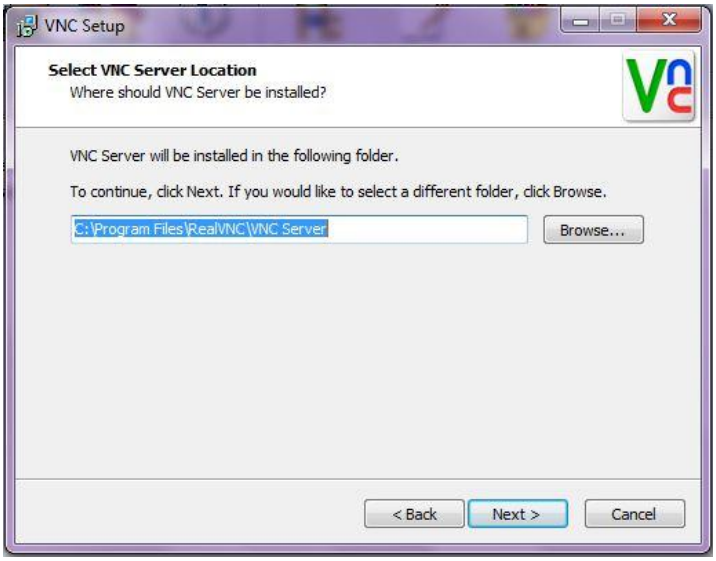


Figura 4.13 Ubicación de la instalación.

Fuente: Instalación de RealVNC

Si se desea, se puede crear un *shortcut* en Inicio, sino es así, dar clic en no crear *shortcut* y dar clic en siguiente. Figura 4.14.

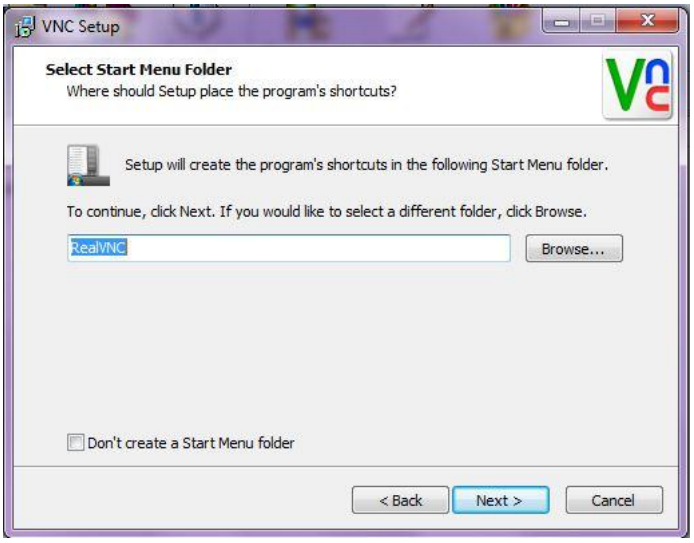


Figura 4.14 Ubicación de la carpeta de la aplicación.

Fuente: Instalación de RealVNC

Luego se mostrará todos los componentes a instalarse en el equipo, dar clic en instalar para comenzar la instalación del programa. Figura 4.15.

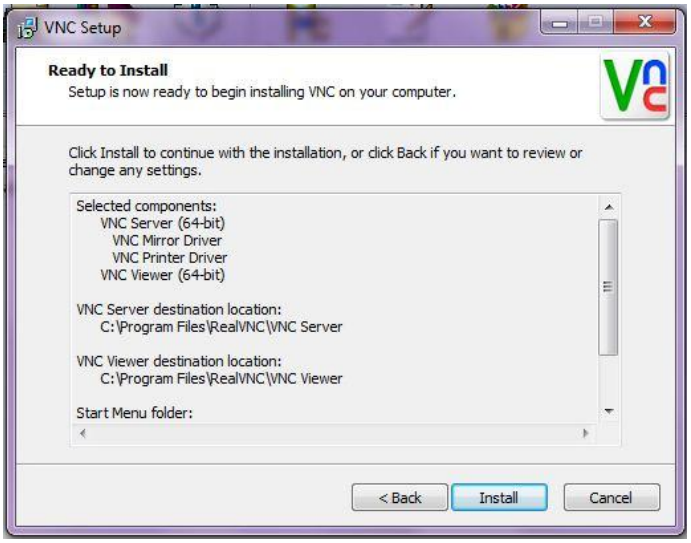


Figura 4.15 Ventana de inicio de la instalación.

Fuente: Instalación de RealVNC

Se debe agregar una excepción en el *firewall* para que se le permita el correcto funcionamiento al programa VNC, caso contrario no se podrá realizar la conexión entre el *host* y el cliente. Dar clic en siguiente. Figura 4.16.

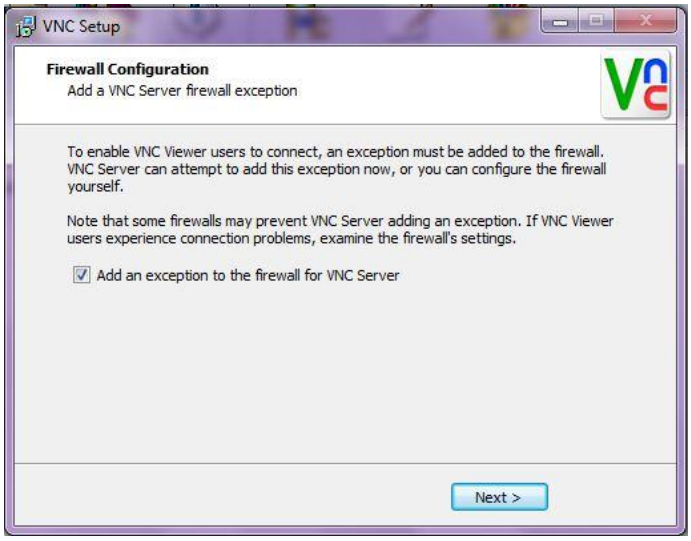


Figura 4.16 Ventana de configuración de firewall

Fuente: Instalación de RealVNC

Por último se mostrarán los errores que ocurrieron durante la instalación, estos pueden ser por falta de complementos actualizados y que no perjudicaran el funcionamiento del programa. Otro tipo de errores pueden resolverse instalando nuevamente el programa. Figura 4.17.

Figura 4.17 Ventana de finalización de configuración de instalación de la aplicación VNC Servidor

Fuente: Instalación de RealVNC

4.3.3 Transferencia de archivos con VNC

Para continuar con los pasos de uso del escritorio remoto, luego de instalado Servidor y Cliente de VNC, se puede realizar la transferencia de archivos:

Paso 2. Asegurar que VNC *Server* está corriendo en la computadora *Host*.

Para esto se debe ir al botón de Inicio, RealVNC y seleccionar VNC *Server* o simplemente dar doble clic en el icono de VNC *Server* en el escritorio y aparecerá una ventana como se muestra en la siguiente figura 4.17. En esta ventana se muestra la IP asignada al *host* con la cual el equipo cliente debe realizar la conexión.

Si en la computadora cliente no se ha instalado aun el VNC *viewer*, también se puede acceder vía *browser* instalando un complemento Java e ingresar utilizando la dirección privada del *host* por medio del puerto 5800 como se muestra en la figura 4.18.

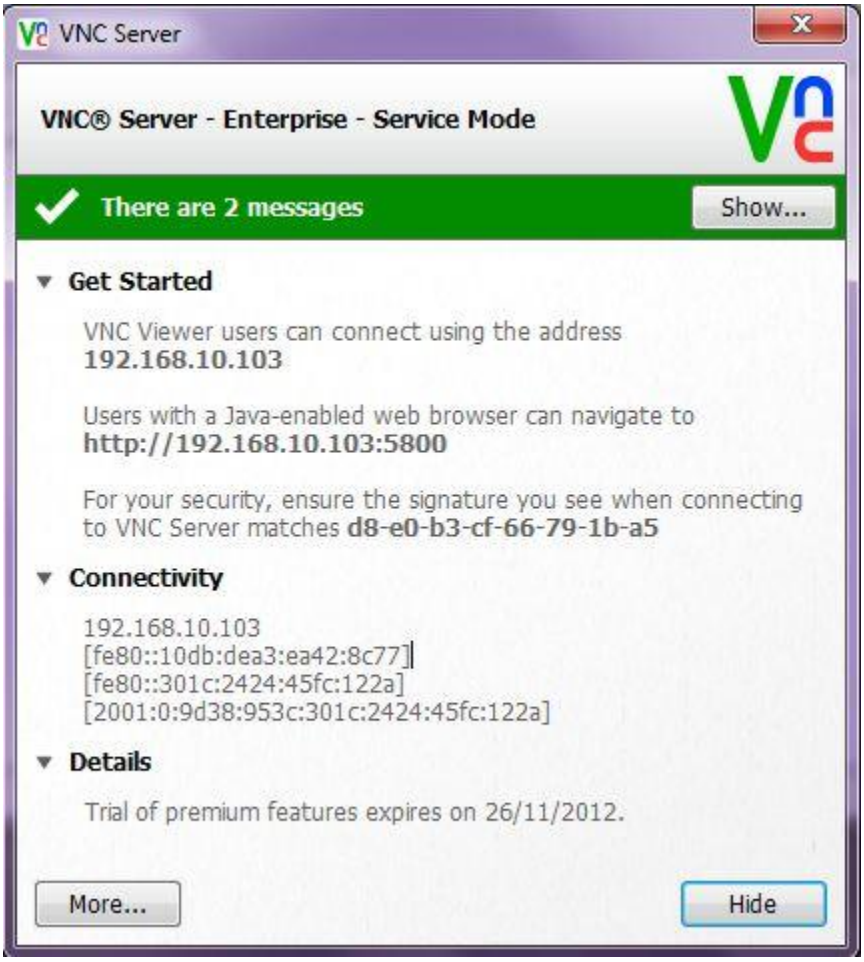


Figura 4.18 Interfaz de funcionamiento del VNC Servidor

Fuente: Transferencia de archivos en RealVNC

Paso 3. Correr VNC *Viewer* en la computadora cliente.

En este caso, se puede dar doble clic en el acceso directo del escritorio. Al correr la aplicación del cliente se mostrara la siguiente ventana. Figura 4.19.

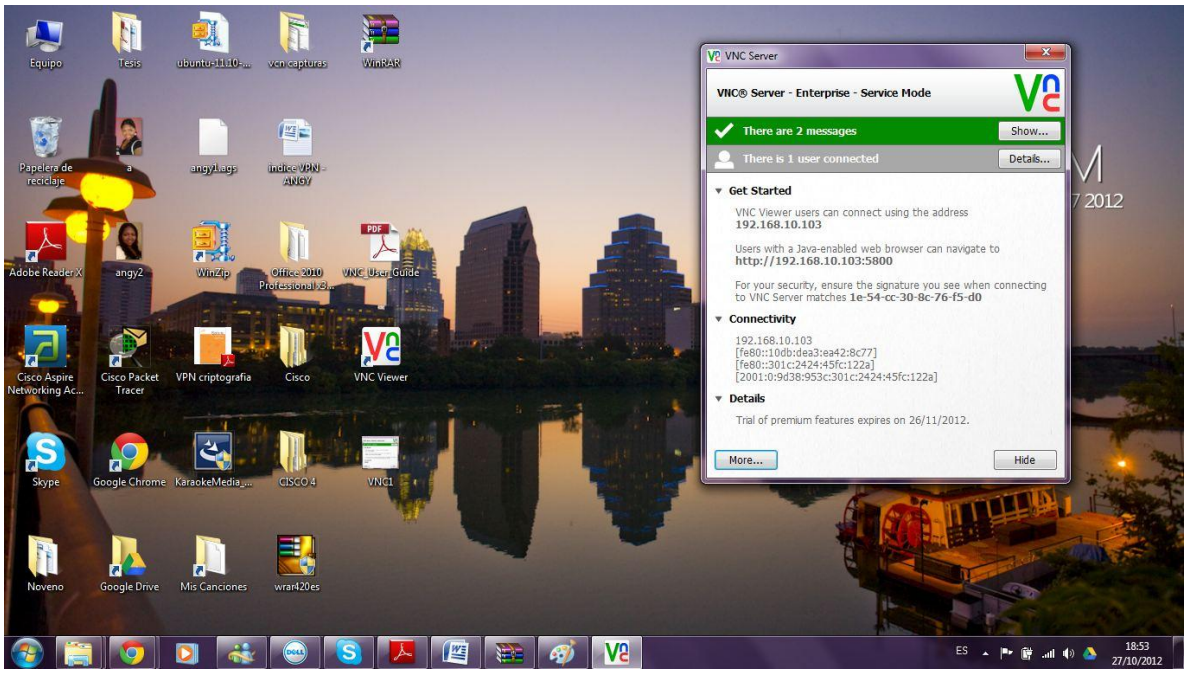


Figura 4.19 Inicio del control remoto

Fuente: Transferencia de archivos en RealVNC

Paso 4. Petición de conexión encriptada: En este paso se debe agregar la dirección IP del equipo host o servidor indicada en la ventana del programa servidor y seguido de esto dar clic en conectar para establecer el control remoto del equipo servidor. Figura 4.20.

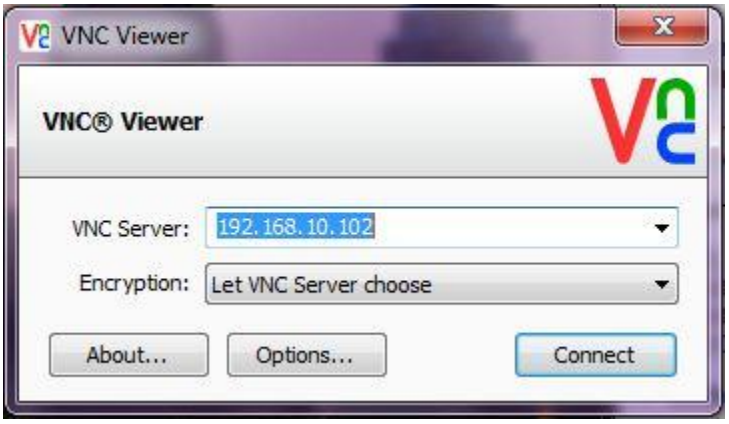


Figura 4.20 Petición de conexión por parte de cliente a dirección IP de servidor

Fuente: Transferencia de archivos en RealVNC

Para poder lograr una conexión segura el servidor configurará un usuario y contraseña que el equipo cliente utilizar para poder acceder al equipo *host*. Figura 4.21.

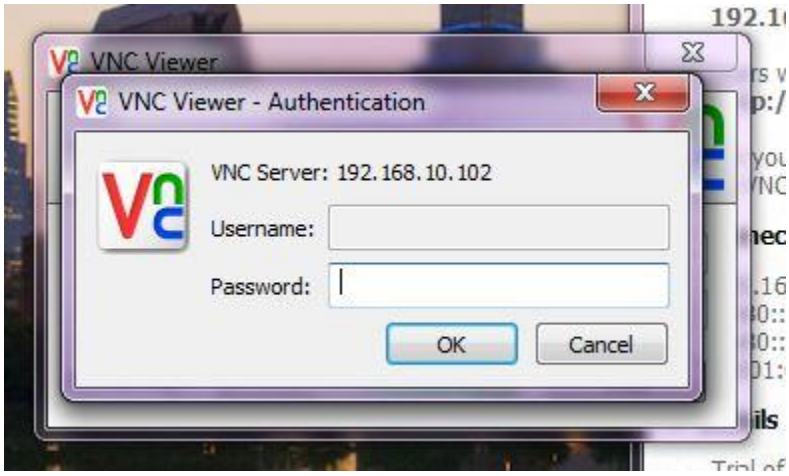


Figura 4.21 Ventana de autenticación de conexión.

Fuente: Transferencia de archivos en RealVNC

Paso 6. Conectarse a servidor VNC

Luego de realizar todo el proceso anterior se establece la conexión con el servidor con lo que se puede empezar a realizar varios tipos de tareas como, transferencias de documentos y *chat* interactivo entre *host* y cliente. Figura 4.22.

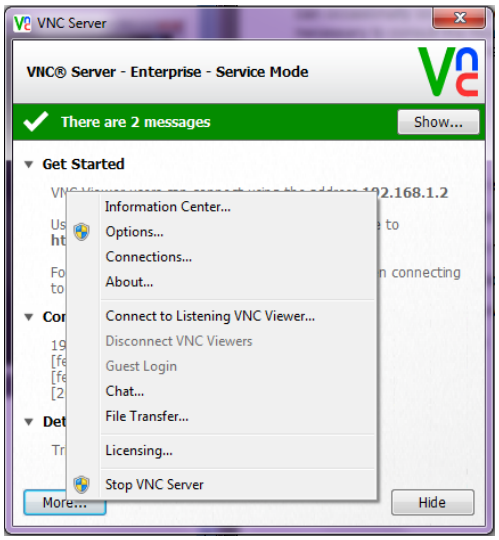


Figura 4.22 ventana de funciones que se pueden realizar durante el control remoto

Fuente: Transferencia de archivos en RealVNC

A continuación, figura 4.23, un ejemplo de transferencia de información entre equipo cliente y *host*.

1. Se accede a equipo *host*
2. Clic en el botón "*More*," seguido de esto seleccionar "*file transfer*."

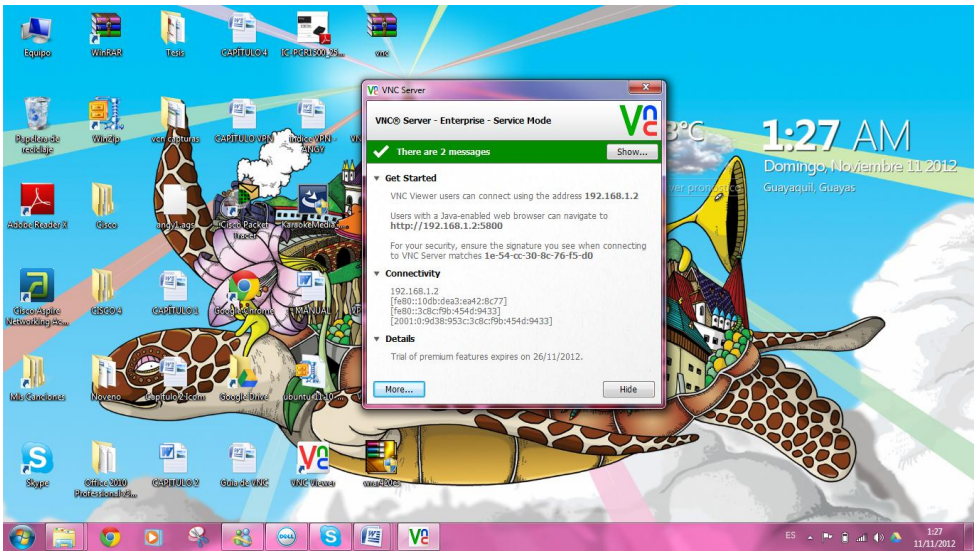


Figura 4.23 Ejemplo de control remoto.

Fuente: Transferencia de archivos en RealVNC

3. Al abrirse la ventana de transferencia de datos se debe hacer clic en "*send files*…", figura 4.2.
4. Seleccionar la ubicación del archivo que desea transferir.
5. Al completarse la transferencia, figura 4.25, se podrá observar el documento en la ubicación seleccionada en la computadora cliente.

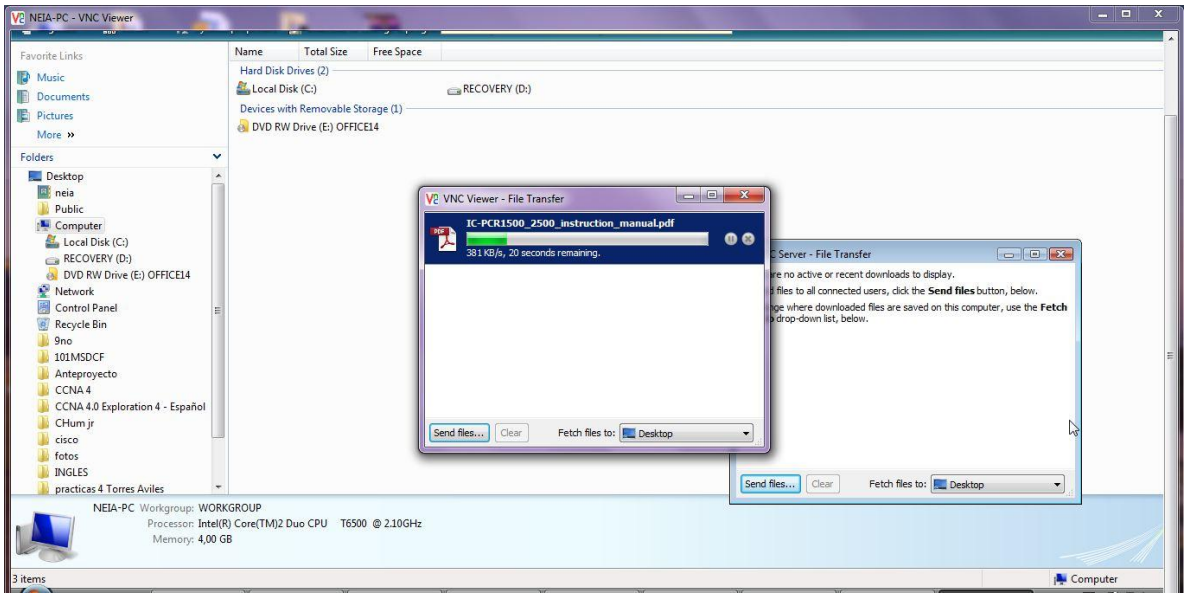


Figura 4.24 Proceso de transferencia de información.

Fuente: Transferencia de archivos en RealVNC

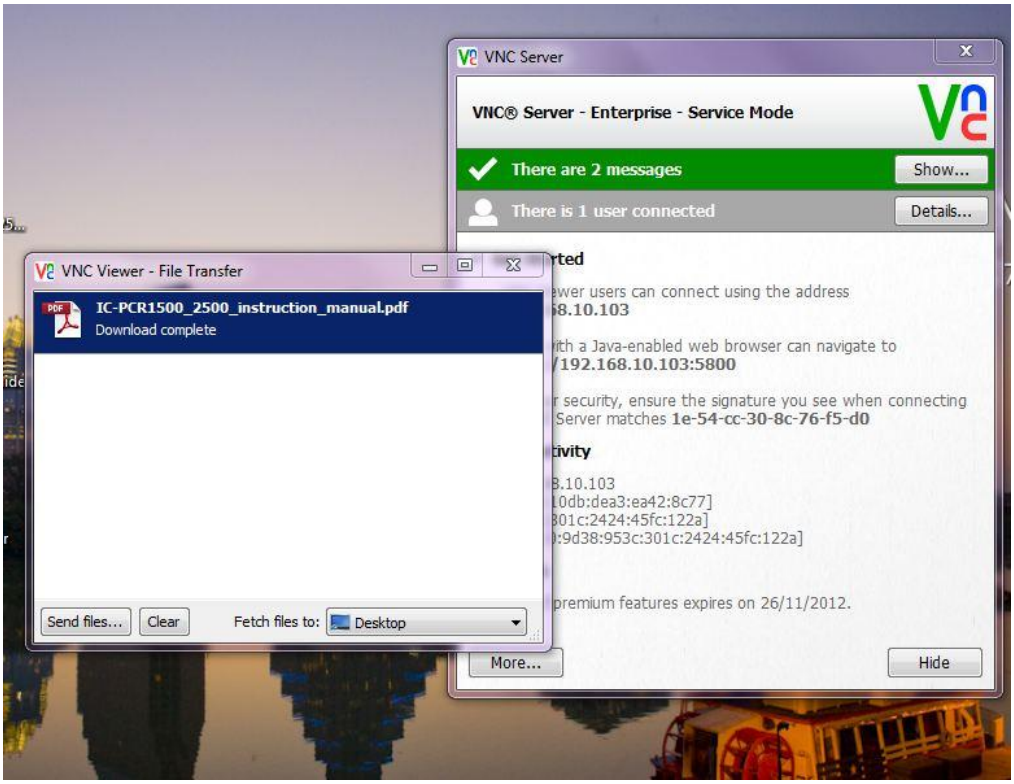


Figura 4.25 Proceso de transferencia de información 2.

Fuente: Transferencia de archivos en RealVNC

CONCLUSIONES Y RECOMENDACIONES

En este último capítulo se presentan las conclusiones que se obtuvieron en base a los objetivos planteados, así como las recomendaciones del caso, un glosario de términos y la bibliografía consultada.

CONCLUSIONES

- El SACER representa una herramienta muy eficaz y que brinda gran cantidad de opciones para el monitoreo, como el registro no solo de audio, sino también video; pero una vez que se pierde la conexión la IRC no cuenta con un sistema de contingencia, por lo cual se planteó un sistema de monitoreo de respaldo para el almacenamiento de las transmisiones de radio y televisión.

- El sistema de respaldo que se presenta en este trabajo es de diseño y funcionamiento simples, respaldados por conceptos muy utilizados en telecomunicaciones y más específicamente en el enlace de datos entre dos o más localidades. Su instalación, configuración y utilización pueden ser realizadas sin problema previo a una revisión del proyecto presentado.

- Se verificó gran cantidad de funciones que el receptor de comunicaciones iCOM IC-PCR2500 es capaz de realizar, pero con la ayuda del manual de instrucciones del mismo es posible identificar las que serán de más ayuda para el propósito planteado y así asegurar que lleve a cabo un mejor desempeño.

- Para el acceso remoto a los archivos creados por el iCOM y guardados en las computadoras de las localidades a monitorear se barajaron opciones como la instalación de un servidor FTP o de la creación de una aplicación en JAVA, pero se escogió la utilización de una VNC, más específicamente RealVNC por la simpleza que representa su instalación y uso y por ser un software de código abierto que no requiere de inversión significativa.

- La solución planteada en este trabajo se direccionó hacia el ahorro de recursos, debido a que el área de cobertura de la IRC comprende, como se detalló en el primer capítulo, cuatro provincias del Ecuador y si se desea extender este sistema a cada punto de esas provincias, la inversión a realizar sería realmente grande si se decidiera por ejemplo, utilizar enlaces dedicados para cada uno.

- Finalmente, aunque se haya apuntado hacia la economía, no se plantea una solución insegura, ya que aunque se trabaje sobre una infraestructura pública como lo es Internet, se realiza un canal de datos privado con la utilización de VPN, lo que proporciona seguridad a la información a transmitir.

RECOMENDACIONES

- Al momento de instalar VNC, es recomendable instalar tanto en la computadora local como remota la aplicación de servidor y de cliente, ya que se podría necesitar en algún momento el cambio de la arquitectura y convertirse el dispositivo remoto en cliente y el dispositivo en las instalaciones de la IRC en servidor.

- Para este trabajo se ha sugerido la implementación de una VPN confiable, dejando en manos del ISP la seguridad del enlace debido a la facilidad que brindan los proveedores de realizar la configuración en sus equipos al momento de la instalación del servicio. Pero si se desea tener la administración directa de la VPN se puede recurrir a una VPN segura, que correrá bajo los parámetros que desee el usuario.

- El iCOM, al hacer un barrido automático de frecuencias, cuenta con una opción de configuración del tiempo en que se detendrá el escaneo en una frecuencia específica. Para efectos de almacenamiento, es recomendable configurar este parámetro en al menos 10 o 15 segundos para poder hacer una distinción de lo que se transmitió.

- Se presentan varias opciones para realizar la conexión a la red pública, pero para brindar una estabilidad al enlace sería preferible contratar un acceso vía fibra óptica dadas sus características y beneficios, aunque actualmente los enlaces inalámbricos se presentan también como una buena opción.

GLOSARIO DE TÉRMINOS

ADSL.- *Asymmetric DSL*, DSL Asimétrico.

AES.- *Avance Encription Standard*, Estándar de Encriptación Avanzada

AH.- *Autentication Header*, Cabecera de Autenticación.

ATM.- *Asynchronous Transfer Mode*, Modo de Transferencia Asíncrona.

BRI.- *Basic Rate Interface*, Interfaz de Acceso Básico.

CA.- *Certification Authorities*, Autoridades de Certificación.

CBC.- *Cipher Block Chaining*, Cifrado con encadenamiento.

CHAP.- *Challenge Handshake Authentication Protocol*, Protocolo de Autenticación por desafío mutuo.

CO.- *Central Office*, Oficina Central.

CPE.- Customer Premises Equipment, Equipo de Premisas del Cliente.

DES.- *Data Encryption Standard*, Estándar de Encriptación de Datos.

DLCI.- *Data-Link Connection Identifier*, Identificador de conexión de enlace de datos.

DMZ.- *Demilitarized Zone*, Zona Desmilitarizada.

DSL.- *Digital Suscriber Line*, Línea de Abonado Digital.

DSLAM.- DSL Access Multiplexer, Multiplexor de Acceso DSL.

DTE.- *Data Terminal Equipment*, Equipo Terminal de Datos.

DWDM.- *Dense Wavelength Division Multiplexing*, Multiplexación por división en longitudes de onda densas.

EAP.- *Extensible Authentication Protocol*, Protocolo de Autenticación Extensible.

ECB.- *Electronic Code Book*, Libro de Código Electrónico.

ESP.- *Encapsulation Security Payload*, Seguridad de Encapsulación de carga Útil.

FEC.- *Forwarding Equivalence Classes*, Reenvío de clases equivalentes.

FTP.- *File Transfer Protocol*, Protocolo de Transferencia de Archivos.

GRE.- *Generic Routing Encapsulation*, Encapsulación de Enrutamiento Genérico.

HFC.- *Hybrid Fiber-Coax*, Híbrida Fibra-Coaxial.

ICMP.- *Internet Control Message Protocol*, Protocolo de mensajes de control de Internet.

IKE.- *Internet Key Exchange*, Intercambio de clave de Internet.

IPSec.- *Internet Protocol Security*, Seguridad de Protocolo de Internet.

IRC.- Intendencia Regional Costa.

ISAKMP.- *Internet Security Association and Key Management Protocol,* Protocolo de Asociación de Seguridad de Internet y Administración de Clave.

ISDN.- *Integrated Services Digital Network*, Red Digital de Servicios Integrados.

ISP.- *Internet Service Provider,* Proveedor de Servicio de Internet.

ITU-T.- *International Telecommunication Union Telecommunication Standardization Sector,* Unión Internacional de Telecomunicaciones Sector de Estandarización de Telecomunicaciones

L2TP.- *Layer 2 Tunnelling Protocol*, Protocolo de Entunelamiento de Capa 2.

L2VPN.- *Layer 2 VPN,* VPN de Capa 2.

L3VPN.- *Layer 3 VPN,* VPN de capa 3.

LAC.- *L2TP Access Concentrator,* Concentrador de Acceso L2TP.

LAN.- *Local Area Network*, Red de Área Local.

LNS.- *L2TP Network Server,* Servidor de Red L2TP.

MAC.- *Messages Authentication Code*, Código de Autenticación de Mensajes.

MPLS.- *Multi-Protocol Label Switching*, Conmutación de Etiquetas Multiprotocolo.

NAS.- *Network Access Server,* Servidores de Acceso a la Red.

NAT.- *Network Address Translation*, Traducción de Direcciones de Red.

NI.- *National ISDN,* ISDN Nacional.

NNI.- *Network-Network Interface,* Interfaz Red-Red.

PAP.- *Password Authentication Protocol,* Protocolo de Autenticación de Clave.

PPP.- *Point-to-Point Protocol,* Protocolo Punto a Punto.

PRI.- *Primary Rate Interface*, Interfaz de Acceso Principal.

PSTN.- *Public Switched Telephone Network,* Red Telefónica Pública Conmutada.

PVC.- *Permanent Virtual Connection*, Conexión Virtual Permanente.

QoS.- *Quality of Service*, Calidad de Servicio.

RA.- Registration Authorities, Autoridades de Registro.

RADIUS.- *Remote Authentication Dial-In User Service,* Servicio de Autenticación Remota de Usuario Dial-In.

RAS.- *Remote Access Server,* Servidor de Acceso Remoto.

SA.- *Security Association,* Asociación de Seguridad.

SACER.- Sistema Automático para el Control Radioeléctrico.

SDSL.- *Symmetric DSL*, DSL Simétrico

SHDSL.- *Symmetric High-speed DSL*, DSL simétrico de alta velocidad.

SKEME.- *Secure Key Exchange Mechanism*, Mecanismo de Intercambio de Clave Segura.

SSL.- *Secure Socket Layer*, Capa de Conexión Segura.

SUPERTEL.- Superintendencia de Telecomunicaciones.

SVC.- *Switched Virtual Connection*, Conexión Virtual Conmutada.

TCP.- Transmission Control Protocol, Protocolo de Control de Transmisión.

UDP.- *User Datagram Protocol*, Protocolo de Datagrama de Usuario.

UNI.- *User-Network Interface*, Interfaz Usuario-Red.

VDSL.- *Very high-speed DSL*, DSL de muy alta velocidad.

VLAN.- *Virtual Local Area Networks*, Redes Virtuales de Área Local.

VNC.- *Virtual Network Computing*, Computación Virtual en Red.

VOIP.- *Voice Over Internet Protocol*, Protocolo de Voz sobre Internet.

VPN.- *Virtual Private Network*, Red Privada Virtual.

WAN.- *Wide Area Network*, Red de Área Amplia.

WiMAX.- *Worldwide Interoperability for Microwave Access,* Interoperabilidad Mundial para acceso por microondas.

XOR.- *Exclusive OR*, OR exclusiva.

BIBLIOGRAFÍA

- Ajit Burad, Sanchit Garg, Prekshu Ajmera (2006). *Virtual Private Networks*. Department of Computer Science and Engineering, Indian Institute of Technology, Bombay Mumbai.
- Auerbach Publications (2006). *Fundamentals of DSL technology.* Boca Raton, FL, USA: Taylor & Francis Group. ISBN 10: 0-8493-1913-7.
- Charlie Scott, Paul Wolfe & Mike Erwin (1999). *Turning the Internet into your Private Network.* (Segunda Edición), Estados Unidos de América: O'Reilly & Associates, Inc. ISBN 1-56592-529-7.
- Chris Rodgers (2001). *Virtual Private Networks, Strong Security at What Cost?.*
- Cisco Systems, Inc (2000). *Guide to ATM Technology for the Catalyst 8540 MSR, Catalyst 8510 MSR, and LightStream 1010 ATM Switch Routers*. San Jose, CA 9.5134-1706 USA: Cisco Systems, Inc.
- Cisco Systems, Inc (2012). *Internetworking Technologies Handbook.* San Jose, CA 9.5134-1706 USA: Cisco Systems, Inc.
- Dr John S. Graham, Matthew Cook (2009). *Secure Virtual Private Networks*. Oxfordshire, England: JNT Association.
- Folletos para la capacitación del personal de la Intendencia Regional Costa de la Superintendencia de Telecomunicaciones para el manejo del Sistema Automático para el Control del Espectro Radioeléctrico (SACER).
- Germaine Bacon, Lizzi Beduya, Jun Mitsuoka, Betty Huang, Juliet Polintan (2002). *Virtual Private Network.*
- Icom, Inc. (2006), *Instructions Manual for Communication Receivers IC-PCR1500 and IC-PCR2500* . 1-1-32 Kamiminami, Hirano-ku, Osaka 547-0003, Japan
- Marc McGuinness (2007). *Virtual Private Networks*. De Montfort University, Leicester, England.
- Mario Baldi& Luigi Ciminiera (2004). Diapositivas *VPN Virtual Private Network.*
- Md. Mehedi Alam Siddiqui, Mehedi Hasan Mithu (2009). *Broadband Wireless Access based on WiMAX Technology with business analysis*. BRAC University, Dhaka, Bangladesh.

- Trípticos informativos de la Superintendencia de Telecomunicaciones (2011).

Páginas consultadas de Internet

- ASSIA, Inc. *DSL Technology Tutorial*. Recuperado el 27 de Octubre de 2012, de DSL Technology Tutorial: http://www.assia-inc.com/DSL-technology/DSL-knowledge-center/tutorials/DSL-technology-tutorial.php
- Bradley Mitchell. *VNC*. Recuperado el 5 de Noviembre de 2012, de VNC: http://compnetworking.about.com/od/softwareapplicationstools/g/bldef_vnc.htm 5 nov 2012
- Benjamin Odiyo, Mukunda Dwarkanath. *Virtual Private Nertwork*. Recuperado el 22 de Septiembre de 2012, de Virtual Private Network: http://www.it.uu.se/edu/course/homepage/sakdat/ht06/assignments/pm/programme/odiyo-dwarkanath.pdf
- Cable-Modem.net. *The Basics of Broadband*. Recuperado el 4 de Noviembre de 2012, de The Basics of Broadband: http://www.cable-modem.net/features/wpaper.html
- Cisco Systems, Inc (Octubre 2012). *Frame Relay*. Recuperado el 4 de Noviembre de 2012, de Frame Relay: http://docwiki.cisco.com/wiki/Frame_Relay
- *Edison Rafael Trujillo Machado (Marzo 2006). Diseño e Implementación de VPN en una empresa comercializadora utilizando IPSec. Recuperado el 30 de Agosto de 2012, de Diseño e Implementación de VPN en una empresa comercializadora utilizando IPSec: bibdigital.epn.edu.ec/bitstream/15000/214/1/CD-0210.pdf*
- GYCOM. *Beneficios de los enlaces de Fibra Óptica*. Recuperado el 29 de Septiembre de 2012, de Un vistazo rápido a la tecnología de Fibra Óptica: http://www.fibraoptica.com/informacion-tecnica/vistazo-tecnologia
- H3C Technologies Co, Limited. *Diagram for Quidway AR 46 Series Router s Applied to Secure VPN*. Recuperado el 6 de Noviembre de 2012 de Diagram for Quidway AR 46 Series Router s Applied to Secure VPN: http://www.h3c.com/portal/Products___Solutions/Products/Other_Products/Routers

/Quidway_AR4600_Series_Routers/Detail_Material_List/200701/194282_57_0.htm

- http://www.realvnc.com. Recuperado el 28 de Octubre de 2012
- http://www.satsig.net/. Recuperado el 31 de Octubre de 2012.
- http://www.supertel.gob.ec. Recuperado el 7 de Agosto de 2012.
- Icom America Inc. *Receptor de comunicaciones IC-R2500*. Recuperado 16 de Agosto de 2012, de Receptor de comunicaciones IC-R2500: http://www.icomamerica.com
- Microsoft (Enero 2005). *Router-to-Router VPN*. Recuperado el 6 de Noviembre de 2012, de Router-to-Router VPN: http://technet.microsoft.com/en-us/library/cc728081(v=ws.10).aspx
- Microsoft. *How VPN Works*. Recuperado el 7 de Noviembre de 2012 de How VPN Works: http://technet.microsoft.com/en-us/library/cc779919(v=ws.10).aspx
- Pearson Education, Informit. *ISDN Technology Background*. Recuperado el 27 de Octubre de 2012, de ISDN Technology Background: http://www.informit.com/library/content.aspx?b=Troubleshooting_Remote_Access&seqNum=76
- SkySoftware (2008). *2 way Satellite Internet*. Recuperado el 5 de Noviembre de 2012, de SkyGabber: http://www.skygrabber.com/en/skygrabber.php
- TechTarget (Agosto 2006). *Virtual Network Computing (VNC)*. Recuperado el 5 de Noviembre de 2012, de Virtual Network Computing (VNC): http://searchnetworking.techtarget.com/definition/virtual-network-computing
- Vicepresidencia Servicios de Red - Gerencia Ingeniería de Clientes y Servicios, Telefónica Telecom (Mayo de 2007). *IPSec*. Recuperado el 23 de Septiembre de 2012, de Configuración del servicio VPN IPSec: http://es.scribd.com/doc/81014150/VPN-Ipsec-2

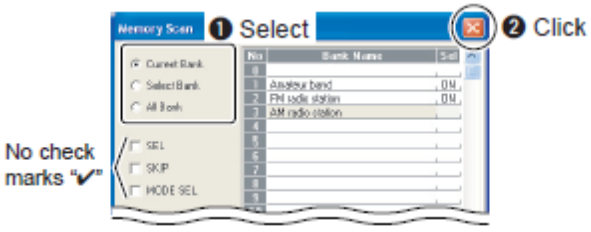
ANEXO 1

ESCANEO DE BANCO DE MEMORIA

Esta función busca todos los canales de memoria en un banco de memoria seleccionado.

Comenzar un escaneo de banco de memoria.

1. Asegurarse que el silenciador está configurado en el punto de umbral.
2. Hacer clic en [▲] (BANK) ó [▼] (BANK) para seleccionar el banco de memoria deseado.
3. Hacer clic derecho en el botón [MEMO] para llamar la pantalla de configuración [AutoMW Scan].
4. Seleccionar la condición de escaneo de banco de 'Current Bank', 'Select Bank' ó 'All Bank'.
    (a) Current Bank, escanea canales de memoria dentro del banco actual.
    (b) Select Bank, escanea canales de memoria dentro del banco seleccionado.
    (c) All Bank, escanea canales de memoria dentro de todos los bancos.
5. Asegurarse de que los recuadros de verificación no están con visto (✔), luego hacer clic en el botón de cerrar [X] para cerrar la pantalla de configuración.
6. Hacer clic en [MEMO] para iniciar el escaneo de escritura de memoria auto.
7. Para detener el escaneo, hacer clic en [STOP] ó [MEMO].

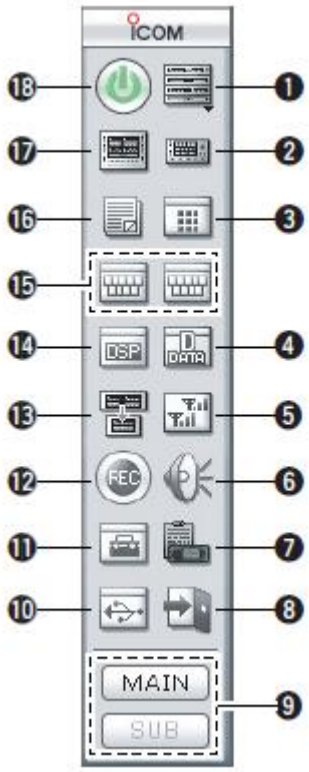


Configuración de escaneo de Banco de Memoria

ANEXO 2

DESCRIPCIÓN DE LA BARRA DE HERRAMIENTAS Y LA PANTALLA DE RECEPTOR MULTIFUNCIONAL.

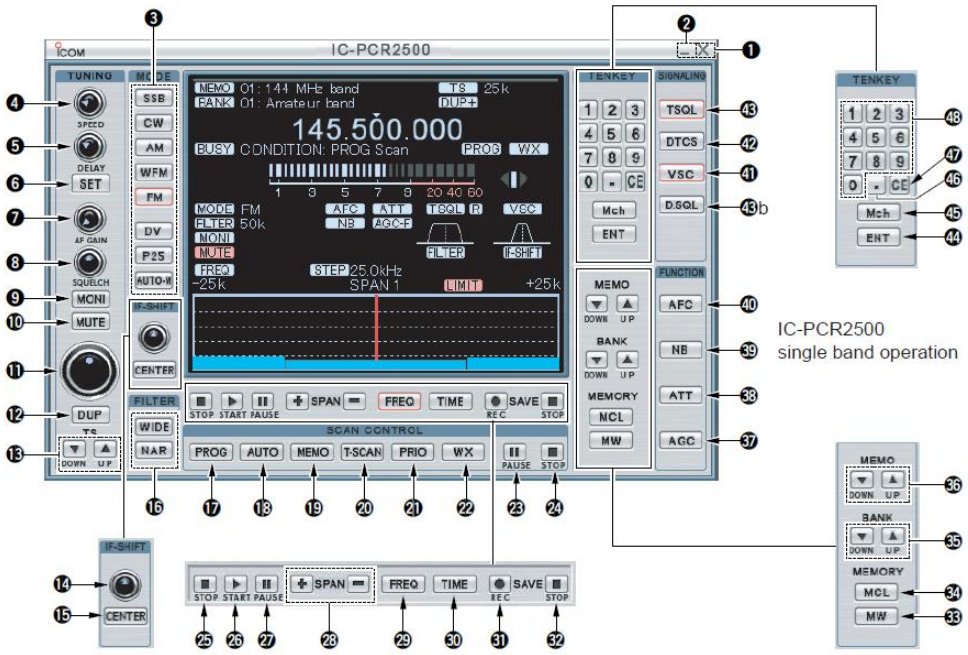
Barra de herramientas



1. Clic para mostrar la ventana de componentes.
2. Clic para mostrar un solo monitor.
3. Clic para que el monitor multicanal aparezca o desaparezca.
4. Clic para seleccionar el menú digital DV o el menú digital P25.
5. Clic para encender o apagar la recepción diversa.
6. Clic para que la pantalla de configuración de audio aparezca o desaparezca.
7. Clic para que la pantalla de clonación aparezca/desaparezca.
8. Clic para salir del programa
9. Clic para seleccionar la banda/sub principal durante la operación de doble vigilancia.

10. Clic para que la ventana de configuración USB aparezca.
11. Clic para que la configuración de lista automática, el acceso directo a la lista, la configuración del modo DV, la configuración del modo P25, etc. Aparezca/desaparezca.
12. Clic para que la pantalla de grabado aparezca/desaparezca.
13. Clic para alternar entre la operación de banda simple y doble vigilancia.
14. Clic para que el filtro digital DSP aparezca/desaparezca.
15. Clic para que la pantalla de comando remoto DTMF aparezca/desaparezca, para la banda principal utilizar el botón a la derecha y para la banda secundaria el izquierdo.
16. Clic para que la pantalla del canal de memoria aparezca o desaparezca.
17. Clic para que la pantalla del receptor multifuncional se muestre.
18. Clic para que el control de la conexión del programa a la unidad principal aparezca/desaparezca.

Pantalla del receptor multifuncional



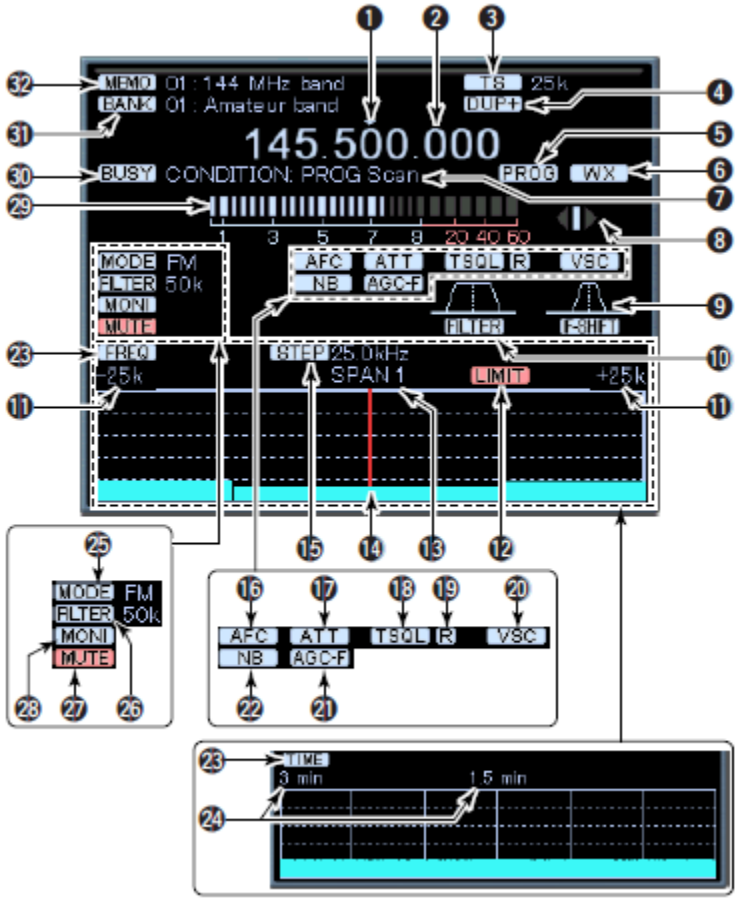
1. Clic para salir de la ventana de la aplicación.

2. Clic para minimizar la ventana.
3. Clic para seleccionar un modo de recepción.
4. Clic para establecer la velocidad del barrido de canales o frecuencias durante el funcionamiento del programa.
5. Clic para fijar el periodo de pausas después de recibir una señal. Clic derecho aumenta el periodo y el clic izquierdo disminuye el periodo.
6. Clic para mostrar la pantalla de retardo del barrido. Esta pantalla es utilizada para el rastreo de detalles demora.
7. Clic para ajustar el nivel de salida de audio. Clic derecho para aumentar el nivel y clic izquierdo para disminuirlo.
8. Clic para ajustar el nivel de Squelch o presencia de ruido en los parlantes de salida de audio cuando una señal no sea receptada. Clic derecho para aumentar, clic izquierdo para disminuir.
9. Clic para encender o apagar la función de monitoreo, es normalmente utilizado por ciertos lapsos de tiempo cuando el Squelch está rastreando señales bajas.
10. Clic para apagar o encender la función de silenciador.
11. Clic para establecer la frecuencia de recepción. Clic derecho para aumentar la frecuencia y el izquierdo para disminuirla.
12. Clic derecho para mostrar el ajuste de la frecuencia offset. Clic izquierdo para ajustar la dirección dúplex de apagado a DUP -, y DUP +.
13. Clic derecho para mostrar la ventana de pasos de sintonización.
14. Clic para ajustar la posición de una señal pasa banda.
15. Después de realizar los ajuste de posición de pasa banda haciendo clic en if-shift control, dar clic en esta opción para regresar a la posición central.
16. Clic para cambiar el filtro IF en uso.
17. Clic para iniciar o parar el barrido programado.
18. Clic para iniciar o detener la grabación del barrido automático.
19. Clic para iniciar o detener un barrido automático.
20. Clic para iniciar o detener un barrido simple.
21. Clic para iniciar o detener un barrido prioritario. En este modo el indicador PRIO Scan se enciende y apaga.

22. Pulsar para correr la función de alerta climática.
23. Pulsar para pausar o continuar un barrido.
24. Pulsar para cancelar un barrido.
25. Clic para cancelar una operación de banda scope.
26. Clic para empezar la operación de banda scope, la cual es utilizada para observar la condición de la señal alrededor de la frecuencia receptada.
27. Clic para pausar o continuar un borrado de banda scope.
28. Cuando el modo "Frecuency" se muestra, dar clic para seleccionar el ancho del borde de frecuencia, también para los intervalos de tiempo en los cuales se muestra la señal receptada.
29. Clic para mostrar la señal receptada con respecto a la intensidad de la señal durante el barrido.
30. Clic para mostrar la intensidad de la señal en un lapso de tiempo especifico durante el barrido.
31. Clic para guardar la información obtenida.
32. Clic para la grabación.
33. Clic para escribir la frecuencia obtenida recientemente en un canal de memoria.
34. Clic para borrar el contenido del canal de memoria mostrado.
35. Clic para cambiar el banco de memoria.
36. Clic para cambiar un canal de memoria.
37. Clic para interactuar con la velocidad del AGC.
38. Clic para encender o apagar la función ATT.
39. Clic para encender o apagar la función NB.
40. Clic para encender o apagar la función AFC.
41. Clic para encender o apagar la función VSC.
42. Clic para encender o apagar el squelch DTCS.
43. Clic para encender o apagar el tono squelch.
44. Clic para ingresar una frecuencia por medio del 10-keypad o mediante teclado.
45. Clic para abrir el canal de memoria cuando el número de canal es ingresado utilizando el teclado numérico.
46. Clic para fijar el digito en MHz cuando es ingresado por el teclado numérico.

47. Clic para borrar los errores cuando se ingresa la frecuencia deseada por medio del teclado numérico.
48. El teclado numérico en pantalla puede ser utilizado para varias funciones, como ingresar frecuencias, cambiar de canal, etc.

Indicadores de funcionamiento en la pantalla del receptor multifuncional.



1. Indica el paso del sintonizador digital.
2. Indica la frecuencia receptada y la información mostrada como el tipo de memoria de canal.
3. Este es el incremento de frecuencia usada cuando se selecciona la frecuencia utilizando el sintonizador dial y cuando se buscar señales utilizando la función de barrido.

4. DUP + aparece cuando se selecciona la función plus dúplex y DUP – cuando se selecciona la operación minus-dúplex.
5. PROG, AUTO, MEMO, T-SCAN o PRIO aparecen durante el barrido.
6. Aparecer cuando la función climática está encendida.
7. Indica la condición del receptor.
8. Aparecen cuando la señal receptada no está sintonizada en su frecuencia central, o el squelch está cerrado.
9. Indica que la señal receptada está en posición pasa banda.
10. Indica el ancho actual de la señal pasa banda.
11. Indica la frecuencia máxima o mínima que se puede observar alrededor de la frecuencia receptada. En el diagrama los limites max y min son +-500 kHZ.
12. LIMIT aparece cuando la opción del paso 3 es mayor que el barrido automático. PAUSE aparece cuando la búsqueda esta pausada.
13. Indica el Span de la frecuencia seleccionada con el botón SPAN + o SPAN -.
14. Indica la frecuencia central de la frecuencia SPAN; esto es para la frecuencia actual receptada.
15. Indica el ancho de banda del barrido.
16. Aparece cuando la función AFC está encendido.
17. Aparece cuando la función ATT está encendida.
18. TSQL aparece cuando se ajusta el tono squelch de la frecuencia. DTCS aparece cuando se ajusta el código y la polaridad del DTCS.
19. Los símbolos aparecen cuando se ajusta la acción de reversa y cuando la función beep está en funcionamiento.
20. Aparece cuando la función VSC está encendida.
21. AGC-F aparece cuando AGC fast se selecciona.
22. Aparece cuando la función NB está encendida.
23. FREQ aparece cuando el modo frecuencia se selecciona de la operación band scope.
24. Indica el intervalo de tiempo de barriendo cuando se recepta una señal.
25. Indica el modo de recepción actual.
26. Indica filtro IF seleccionado.
27. Aparece cuando el circuito squelch silencia la señal de audio receptada.

28. Aparece durante el monitoreo de la frecuencia en operación.
29. Indica la intensidad de señal receptada.
30. Aparece cuando una señal es receptada o cuando la señal de ruido abre el squelch.
31. Indica el número de banco de memoria que se recibe.
32. Indica el número del canal de memoria que se está receptando.

ANEXO 3

GRABAR UNA SEÑAL RECIBIDA

1. Recibir una señal.

2. Hacer clic en el ícono [Recording] en la barra de herramientas para llamar la pantalla [Recording] si no se ha mostrado.

3. Hacer clic en [Setting] para mostrar el menú de configuración.

4. Hacer clic en [...], luego seleccionar la carpeta en la que se desea guardar la información de grabado. Luego de seleccionar la carpeta, hacer clic en OK.

5. Hacer clic en el botón de inicio de grabación para empezar a grabar la señal.

La grabación se graba en formato WAVE.

6. Hacer clic en el botón de detenido para detener la grabación.