REDES INTELIGENTES

SERVICIO RED PRIVADA VIRTUAL

GIOVANNA DELGADO HURTADO

POPAYAN
UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERIA ELECTRONICA Y TELECOMUNICACIONES
GRUPO DE REDES INTELIGENTES
2002

REDES INTELIGENTES

SERVICIO RED PRIVADA VIRTUAL

GIOVANNA DELGADO HURTADO

Monografía del trabajo de grado presentada como requisito para optar al título de Ingeniero en Electrónica y Telecomunicaciones

Director:
Mg. RAFAEL RENGIFO

POPAYAN
UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERIA ELECTRONICA Y TELECOMUNICACIONES
GRUPO DE REDES INTELIGENTES
2002

A mis padres,
porque gracias a todos sus innumerables esfuerzos, sacrificios y dedicación, pude cumplir esta meta y llegar hasta donde he llegado.

AGRADECIMIENTOS

Quiero expresar mis más sinceros y profundos agradecimientos al Ing. Rafael Rengifo, mi presidente de tesis, por su asistencia, soporte y paciencia durante todos estos años, para que pudiera culminar con éxito este trabajo de grado.

A mis amigos Carlos Caicedo, Hugo Nelson Gómez, Jorge Alfredo Ramos, Ruby Pantoja, Clara Eugenia Pabón, Uriel Salomón Salas, Luis Fernando Sánchez, Carlos Enrique Sanz, Juan Pablo López, por todos los maravillosos años que compartimos juntos en la universidad, por haberme enseñado las cosas más valiosas de mi vida, y por haber creído en mí durante todo este tiempo.

A Diana Paola Miranda, por ser mi mejor amiga y estar conmigo en las buenas y en las malas, por darme aliento cuando me sentía desfallecer y también por regañarme cuando era necesario.

A todos mis grandes y excelentes amigos que he conseguido durante mi vida laboral, en especial a Jorge Quiroz, Hector Ponce, Heitor Faroni, Nelson Estrada, Yovanny Quintero, porque me han ayudado a alcanzar mis metas, incluyendo mi tesis, y me han regalado toda su amistad.

A mis jefes y grandes maestros en la vida, Manuel Rebellón, Leonidas Lara, Gustavo Castellanos, Manuel de la Torre, Mario Uribe, Manuel Verdeguer y en especial Antonio Vásquez, por haber confiado en mí a pesar de no haber terminado mi tesis y porque gracias a todos sus buenos consejos, lecciones y enseñanzas he podido recorrer nuevos caminos y escalar montañas muy altas.

A mi familia, por todo su amor, paciencia y confianza durante esta larga etapa de mi vida.

A Juan Carlos, por creer en mí, por ser mi soporte y mi alegría, por enseñarme a disfrutar y a no tomar la vida tan seriamente y por ayudarme a ser mejor cada día.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

PRESENTACION

Durante los últimos años las telecomunicaciones se han convertido en parte fundamental de nuestras vidas, permitiéndonos estar comunicados y ofreciendo a las empresas nuevas maneras de hacer negocios y obtener mayores beneficios.

La tendencia de desregularización y liberalización de las telecomunicaciones en el ámbito mundial, dio inicio a una fuerte competencia entre los diferentes operadores de telecomunicaciones por capturar la mayor porción del mercado, aprovechando los rápidos adelantos tecnológicos en esta área.

La necesidad de tecnologías estandarizadas, abiertas y con una excelente relación costo-efectividad, propicio la aparición de las Redes Inteligentes, las cuales permitieron a los operadores desarrollar y controlar servicios más eficientemente, introducir rápidamente nuevas capacidades y posteriormente personalizar fácilmente los servicios para satisfacer las necesidades individuales de los clientes.

Entre estos servicios, aparecen las REDES PRIVADAS VIRTUALES, ofreciendo a las compañías de todos los tamaños, la posibilidad de reducir los costos de comunicación entre sus oficinas, al mismo tiempo que ofrecen la flexibilidad y rapidez para adicionar y remover puntos, incrementando su eficiencia.

Las Redes Privadas Virtuales permiten a los operadores de telecomunicaciones aprovechar al máximo sus infraestructuras de redes públicas, y dan a las empresas la idea de manejar una red totalmente Privada, sobre ellas.

El Capítulo 1 de esta monografía define la diferencia entre las redes privadas y las redes públicas y lo que las convierte en redes virtuales. También hace un análisis sobre la evolución del servicio VPN desde su origen a finales de la década de los 80s cuando tuvo aceptación mundial luego de ser introducido en Estados Unidos, hasta llegar al momento actual en el que los grandes operadores internacionales tradicionales, los nuevos operadores que utilizan tecnología de punta, los pequeños subdistribuidores y las grandes y pequeñas redes de valor agregado, buscan nuevas alternativas ya no sólo para el transporte de voz sino también para el transporte del tráfico de datos y vídeo.

El Capítulo 2 empieza exponiendo ampliamente la importancia, beneficios y características de este servicio, que lo han destacado para el nuevo milenio, como el principal servicio empleado por las empresas que requieren comunicaciones a lo ancho del mundo. El capítulo termina presentando las diferentes arquitecturas de redes sobre las cuales puede funcionar el servicio, ya que debido a su trascendencia, muchas de las más grandes compañías de comunicaciones en todo el mundo, se vieron forzadas a implementar sus propias arquitecturas de redes al no contar con Redes Inteligentes. Así mismo se presenta una comparación de las características de cada una de las arquitecturas.

El Capítulo 3 se enfoca en dar una profunda visión del funcionamiento del servicio sobre las Redes Inteligentes, incluyendo la especificación del servicio a través del Modelo Conceptual de Red Inteligente, la ejecución paso a paso del servicio dentro de la arquitectura de Red Inteligente, los diferentes métodos de acceso, los tipos de llamadas que se pueden realizar, los planes de numeración que se pueden definir y los procedimientos de marcación que se deben utilizar.

El Capítulo 4 explica el surgimiento de las nuevas Redes VPN de datos, que permiten transportar ya no sólo voz sino también tráfico de datos y vídeo y permitiendo a los diferentes competidores del mercado ofrecer a sus clientes factores diferenciadores con la competencia.

Así en el Capítulo 4 se introducen las Redes Privadas Virtuales de Banda Ancha, con su relación tanto con ATM como con TINA, y se presentan algunas consideraciones para la utilización de las Redes Privadas Virtuales sobre Internet como el nuevo estándar mundial para la transmisión de datos en el ámbito corporativo. Además en este capítulo se resalta la permanencia e importancia de las Redes Inteligentes a pesar de la evolución y aparición de nuevas tecnologías, y su interoperabilidad con las Redes de Próxima Generación (NGN) emergentes.

En el Capítulo 5, se mencionan algunos aspectos que permiten determinar si es recomendable implementar una Red Privada Virtual dentro de una empresa. Se explica como los grandes beneficios que se pueden obtener con este servicio, muchas veces se logran realizando profundos cambios estructurales dentro de la compañía que podrían generar traumatismos.

Adicionalmente en el Capítulo 5, se hace un análisis sobre los factores que influyeron en que el servicio VPN no fuera implementado en Colombia a pesar de que varios operadores cuentan con la infraestructura para hacerlo. Y finalmente se presentan varios ejemplos de operadores internacionales que ofrecen el servicio VPN y sus principales características.

Hasta aquí el objetivo de esta monografía, ha sido exponer una visión completa del servicio “Red Privada Virtual”, sus orígenes, sus características, su implementación, su presente y su futuro. Con el deseo de que su importancia sea reconocida y divulgada a un público mucho más amplio, se desarrolló un tutor gráfico en ambiente html, lo que permite su publicación en la página Web de la Universidad del Cauca. Su descripción y manual de usuario pueden ser encontrados en el Capítulo 6. Con esto se busca impulsar los espacios de difusión de los trabajos realizados en la Universidad y difundirlos no sólo dentro del Grupo RI sino también en un ámbito nacional e internacional.

Al presenciar durante varios años la evolución del servicio VPN, partiendo como un servicio sobre las Redes Telefónicas Públicas Conmutadas hasta convertirse en un servicio basado en Internet, y al mezclarlo con la experiencia adquirida en empresas proveedoras de infraestructura de telefonía pública de VoIP y redes NGN, se logra un conocimiento mucho más amplio del tema y una visión más completa de la aplicación de la tecnología en el servicio de Redes Privadas Virtuales.

1. INTRODUCCION

Este capítulo presenta un análisis comparativo entre las redes públicas y privadas y la historia de la introducción de las Redes Privadas Virtuales en el mundo.

1.1. REDES PUBLICAS vs. REDES PRIVADAS

Una Red Pública de Telecomunicaciones es el conjunto de medios de transmisión, distribución y conmutación utilizados para prestar los servicios de telecomunicaciones. Típicamente las redes públicas son redes ofrecidas por portadores u operadores de telecomunicaciones.

Una Red Privada de telecomunicaciones es aquella que se utiliza para la prestación de servicios de telecomunicaciones no disponibles para todo el público. Es una solución capaz de resolver las necesidades de servicios de las empresas, utilizando medios alternativos a las redes públicas o los medios proporcionados por las redes públicas o una mezcla de los dos.

Hay dos razones principales por las cuales una empresa prefiere utilizar una red privada: control y economía.

El control tiene que ver con la capacidad de ofrecer privacidad, prioridad y conectividad:

- Cuando una compañía operadora de una red pública no puede automáticamente favorecer intereses particulares, ni dar prioridad a cierto tipo de información, ni brindar niveles mínimos de seguridad; las empresas preferían implementar sus propias redes. En un principio se construyeron redes de microondas o redes de cables propias y posteriormente alquilaron líneas privadas a los operadores de telecomunicaciones.

- Otro factor importante es la cobertura de la red. Las redes satelitales impulsaron el desarrollo de redes privadas permitiendo la comunicación con áreas remotas.

La economía es el motivo por el cual las empresas realizan importantes innovaciones en los servicios que prestan, basados en este concepto, se puede concluir que:

- Si una empresa puede implementar un servicio específico a un costo más bajo que una tarifa pública, entonces la justificación es directa. Un ejemplo de esta situación, es que muchas empresas interconectan redes de conmutadores de voz (PBX) a través de líneas dedicadas.

- Si una empresa necesita un servicio no ofrecido por el proveedor de red pública en cierta región geográfica, entonces no hay otra opción que construir su propia red. Por

ejemplo, Internet nació como una red privada por la necesidad de conectar una red de computadores a través de líneas privadas y fue fundada por la Agencia de Proyectos de Investigación Avanzados (ARPA) del departamento de defensa de los Estados Unidos.

La solución ideal para las empresas es utilizar la estructura de bajo costo de una red pública manteniendo la calidad, el control y la seguridad de una red privada, y esta precisamente es la definición de una Red Privada Virtual.

Una Red Privada Virtual busca obtener lo mejor de los dos mundos. Es privada en el sentido que los datos que una empresa transfiere sobre la VPN son seguros, y es pública en el sentido en que utiliza los recursos de las redes publicas.

1.2. EVOLUCION DE VPN

El pasado y el presente del servicio VPN han estado marcados por una constante competencia entre las diferentes empresas, que han buscado capturar un mayor número de usuarios, primero en Estados Unidos y posteriormente en todo el mundo. Esto ha dejado como principales beneficiarios a los usuarios, con mejores servicios, mayor cobertura y precios cada vez más atractivos.

1.2.1. DESARROLLO DE VPN EN ESTADOS UNIDOS

Después de la desregularización de AT&T en 1984 la competencia entre los diferentes operadores, obligó a definir ciertos controles respecto a la sectorización de la prestación del servicio de telefonía.

Se establecieron “Áreas de Acceso y de Transporte Local” conocidas como LATAS (Local Access and Transport Areas) que solo podían ser operadas por “Operadores de Centrales Locales” (LEC – Local Exchange Carrier), y se restringió a AT&T y a otros operadores a proporcionar servicios de larga distancia entre las LATAS, llegando a conocerse como “Operadores entre Centrales” (IXCs - Inter-eXchange Carriers).

El acceso a la red de un operador IXC se realiza a través de un Punto de Presencia (POP) dentro de cada Lata. Esta separación de las redes locales, de la larga distancia, permitió que las grandes compañías de telecomunicaciones (IXCs) compitieran por los clientes VPN.

El éxito de VPN en Estados Unidos se puede atribuir a la competencia entre las tres empresas operadoras, AT&T, MCI y US Sprint, y a su afán de expandir sus servicios. El acercamiento inicial realizado por las telcos fue la introducción del servicio en las principales áreas metropolitanas y su expansión desde esa base. Este fue un método particularmente efectivo para crecer, ya que desde el IXC tenían a su disposición extensas redes de transmisión óptica las cuales habilitaron el transporte económico de grandes cantidades de tráfico.

En 1988 se inició una batalla entre las operadoras por su porción del mercado, a través de una intensa competencia de precios. En 1989 la guerra terminó, pero por ese entonces ya había actuado como un efectivo catalizador para la propagación de VPN.

Simultáneamente, los operadores hicieron un esfuerzo común por reducir sus costos y optimizar sus operaciones, con el fin de ofrecer precios más bajos.

Con esta presión por disminuir costos, mejorando el servicio, las telcos se dieron cuenta que la infraestructura ideal para la prestación del servicio VPN, eran las Redes inteligentes. La meta a largo plazo de cada telco fue implementar Redes Inteligentes, y explotar al máximo las ventajas y beneficios del servicio VPN siendo ofrecido sobre esta arquitectura de red.

Muchas telcos podían justificar el costo de implementación de las Redes Inteligentes, soportando VPN y un número de otros servicios desde la misma plataforma.

Sin embargo, la implementación extendida de Redes Inteligentes solo se esperaba hasta 1993. En ese periodo las telcos, presionadas por el mercado, se vieron forzadas a introducir servicios VPN tan rápido como fuera posible, adoptando diferentes arquitecturas de redes.

Otro factor que tuvo mucho que ver con el posicionamiento de VPN, fue el que los clientes tuvieran un claro entendimiento de los costos de sus redes y de los niveles de uso del tráfico, justificando el cambio a VPN al permitirles obtener una muy buena relación costo-beneficio.

De la batalla por la porción de mercado los grandes beneficiados fueron los clientes. El resultado neto fue la amplia aceptación del servicio y su posicionamiento como el núcleo de los servicios ofrecidos por los operadores, para satisfacer las necesidades de comunicaciones corporativas de sus clientes.

1.2.2. VPNs INTERNACIONALES

El éxito alcanzado por VPN entre multinacionales y muy grandes usuarios en Estados Unidos, fue el motor para el desarrollo de VPN en el ámbito internacional.

Muchos países europeos se concentraron primero en implementar sus servicios internacionales y dejar para el final su implementación nacional. Esto se debió a que al manejar monopolios, eran renuentes a aceptar el lanzamiento del servicio o hacerlo disponible y al temor de disminuir sus ganancias con la RTPC.

Sin embargo, la presión de las empresas ocasionó que aunque con retardo casi todos los países europeos empezaran a implantar sus Redes Privadas Virtuales y a hacer asociaciones para ofrecer la solución internacional. Algunos de estos países implantaron Redes Inteligentes ofreciendo el servicio VPN, otros países en cambio conscientes de las características y de los beneficios del servicio se vieron forzados a implantar otros tipos de arquitecturas de redes con el fin de poder ofrecer a sus clientes los beneficios de este servicio.

1.3. UNA NUEVA ERA VPN

El éxito de las Redes Privadas Virtuales de voz tanto en Estados Unidos como en los mercados europeos y en el resto del mundo dio inicio a mediados de los 90s a una nueva generación de VPNs internacionales que buscaba ofrecer una mayor cobertura y obtener una gran parte del mercado de clientes corporativos ofreciendo un servicio con administración y facturación centralizadas.

Con este fin se crearon grandes alianzas globales tales como CONCERT (BT, AT&T), GLOBAL ONE (Sprint, France Telecom, Deutsche Telecom) y WORLDPARTNERS (AT&T, KDD, Telstra y 15 operadores más). Sin embargo, se enfrentaron con varios problemas, entre ellos la gran cantidad de tiempo y dinero que representaba construir un backbone global, el esfuerzo de involucrar toda la fuerza de ventas en el ámbito mundial y por último la lentitud del proceso de desregulación de las comunicaciones en un gran número de países.

Adicionalmente, empezaron a aparecer nuevos competidores en el mercado. *Pequeños Sub-Distribuidores,* empezaron a recoger clientes de tamaño considerable (sin entrar a competir por las multinacionales) y *nuevos operadores internacionales con tecnología de punta, s*e apropiaron de los grandes y lucrativos enlaces entre las principales ciudades.

Los rápidos desarrollos y progresos de las diferentes tecnologías de datos (FR, ATM, MPLS, IP) y especialmente su amplia difusión impulsó fuertemente la aparición de nuevos y mejores operadores.

Las *grandes alianzas*, en el lado de los datos, absorbieron algunas de las más grandes redes de valor agregado (VAN - Value added network), permitiéndoles ofrecer un extenso portafolio de servicios incluyendo conmutación de paquetes, Frame Relay y redes IP. En el lado de la voz, basados en su experiencia y especialización continuaron desplegando VPNs internacionales.

Los *nuevos operadores* entre ciudades empezaron a empujar tanto voz como datos y las *VANs* que se habían mantenido alejadas de las alianzas empezaron a adicionar voz a sus servicios de datos.

Así a principios del nuevo milenio, la mayoría de los competidores pueden ofrecer soluciones tanto de voz como de datos y una amplia variedad de servicios, entre los cuales se encuentran VPNs de voz y VPNs de datos.

2. DESCRIPCION Y GENERALIDADES DEL SERVICIO

En este capítulo se presenta un estudio general del servicio Red Privada Virtual (VPN), en el cual se incluyen aspectos como: Definición y descripción del servicio, importancia, participantes, grupos interesados, beneficios para todos los participantes y servicios.

También se hace una descripción detallada de las características del servicio y su descripción dentro del Modelo Conceptual de Red Inteligente dado por el desarrollo del Plano del Servicio.

2.1. DEFINICION DEL SERVICIO VPN

El servicio Red Privada Virtual (VPN – Virtual Private Network), es un servicio de Red Inteligente diseñado para suministrar las características de una red privada, nacional o internacional, utilizando los recursos de la Red Telefónica Pública Conmutada (RTPC). Una Red Privada Virtual puede ser definida como *"un grupo lógico cerrado de usuarios, implementado sobre las facilidades de las telecomunicaciones públicas conmutadas".*

2.2. DESCRIPCION DEL SERVICIO VPN

Una Red Privada Virtual es un ente dentro de la red pública que actúa de tal forma que por medio del subscriptor del servicio, los usuarios finales parecen obtener de la red las mismas características de una red privada.

El servicio utiliza las funciones y los recursos de la red pública para suministrarle a sus suscriptores una configuración privada personalizada. Además de utilizar la RTPC, una Red Privada Virtual puede ser configurada utilizando la Red Digital de Servicios Integrados (RDSI), la Red Mundial Pública Móvil (PLMN) y las redes privadas con las que ya cuenta el suscriptor del servicio, permitiéndole expandir su propia red.

La Red Privada Virtual es ofrecida a nivel mundial por diferentes compañías de telecomunicaciones (telcos) utilizando la plataforma de Red Inteligente (RI); sin embargo, en muchos sitios donde no se trabaja con RI, las implementaciones son propietarias. Comparada con una red privada una VPN ofrece la confianza,
flexibilidad, mantenimiento y expansibilidad de una red pública.

2.2.1. IMPORTANCIA DEL SERVICIO VPN

La Red Privada Virtual (VPN) ha revolucionado desde principio de los 90's las comunicaciones empresariales en todo el mundo, ocupando el lugar central del portafolio de servicios ofrecido por las compañías de telecomunicaciones a sus clientes corporativos.

En este rol central, VPN:

- Reemplaza muchos de los negocios RTPC. Esto ocurre para negocios grandes y pequeños, nacional e internacionalmente.
- Reemplaza servicios de líneas arrendadas usados para comunicaciones de voz. Esto ocurre por todas partes excepto en el centro de grandes redes corporativas, nacional e internacionalmente.
- Complementa servicios de líneas arrendadas usados para comunicaciones de datos y video. VPN es usado para incrementar el número de aplicaciones, particularmente sobre una base internacional.
- Promueve la fundación de empresas, ya que las telcos pueden ofrecer a sus clientes servicios de banda ancha.

Para este nuevo siglo, VPN se ha constituido a lo ancho del mundo como el principal servicio empleado por las empresas que requieren comunicaciones. Servicios de líneas arrendadas han sobrevivido, pero cada vez serán más usados para optimizar las redes y para aplicaciones que son inherentemente más adecuadas para este servicio.

Durante esta década, VPN hará una significativa contribución al incremento y perfeccionamiento de las comunicaciones a escala global. El único ingrediente en la fórmula para el éxito del servicio VPN es que los usuarios comprendan todas las ventajas competitivas que pueden obtener y sigan presionando su entrada al mercado.

2.3. PARTICIPANTES DEL SERVICIO VPN

- **USUARIO DEL SERVICIO**: Es la persona que hace uso del servicio de Red Privada Virtual. Corresponde a un abonado que accede a la VPN con el fin de establecer una comunicación dentro o fuera de ella.

- **SUSCRIPTOR DEL SERVICIO**: Es el encargado de proveer y gestionar el servicio VPN dentro de los límites definidos por el operador del servicio. Se encarga de mantener los datos adecuados para cada usuario. Bajo esta denominación se encuentran grandes empresas que se suscriben al servicio para utilizarlo en sus comunicaciones internas, al igual que empresas que ofrecen servicios y necesitan una eficiente comunicación externa.

- **PROVEEDOR / OPERADOR DEL SERVICIO.** Se encarga de la planeación, la instalación, la administración y el mantenimiento de los datos, y de la lógica específica del servicio de Red Inteligente. Es responsable de la operación de las redes del suscriptor.

2.4. GRUPO INTERESADO

El servicio VPN fue inicialmente enfocado a grandes compañías que cumplen con algunas de las siguientes características:

- Se encuentran geográficamente dispersas, es decir, poseen múltiples puntos de presencia en el ámbito local, nacional e incluso internacional.
- Necesitan servicios de comunicaciones privados y ajustados a la medida.
- Poseen redes privadas y desean expandirlas y mejorarlas con ayuda de los avances tecnológicos.
- Cuentan con una estructura básica de redes privadas que conectan sus principales oficinas y sucursales, donde el volumen de tráfico es alto.
- Necesitan un cubrimiento total sobre las actividades de la empresa (incluyendo usuarios remotos y usuarios móviles) que no es posible alcanzar con las redes privadas.

Algunas empresas que cumplen con estas características son:

* Corporaciones multinacionales.
* Instituciones financieras.
* Empresas del sector industrial (manufactureras, químicas).
* Compañías de alta tecnología (Áreas electrónica y computación).
* Compañías del área de las impresiones (fotografía, fotocopiadoras, fax).

Con el desarrollo del mercado VPN a nivel mundial, compañías de pequeño tamaño y organizaciones de servicios y de ventas al por menor, las cuales no cuentan con sus propias redes privadas, tienen la posibilidad de interconectarse corporativamente, obteniendo las ventajas de VPN en cuanto a costos, flexibilidad, eficiencia y efectividad.

Algunas de estas empresas son:

* Servicios de transporte.
* Hoteles.
* Compañías de crédito.
* Telemercadeo.
* Servicios de salud.
* Otros servicios.

2.5. BENEFICIOS DERIVADOS DEL SERVICIO VPN

Las telecomunicaciones son esenciales e indispensables para la conducción de los negocios de las compañías. Por eso es importante destacar los beneficios que VPN ofrece a cada uno de los participantes del servicio.

2.5.1. BENEFICIOS PARA EL USUARIO DEL SERVICIO

- ***Conveniencia:***

  VPN hace más fácil y gestionable cualquier comunicación que el usuario final desea realizar tanto dentro como fuera de la red.

- ***Acceso a múltiples puntos de la red:***

  El usuario final puede acceder todos los puntos que conforman la red virtual de su empresa, sin importar el sitio donde éstos se encuentren. Con las redes privadas el acceso esta limitado al número de sitios que la empresa puede interconectar, y a su ubicación. Con VPN es posible lograr una cobertura casi total de la red y presentarla al usuario como si estuviera ubicada toda en el mismo sitio.

- ***Rapidez y facilidad para acceder diversa información:***

  Independientemente de la ubicación de los puntos de una empresa, VPN le presenta al usuario final una sola y única red. Los diferentes tipos de llamadas que se pueden realizar y las características de identificación de usuarios, permiten acceder a la información que se encuentra en la red desde sitios ubicados dentro y fuera de ella.

- ***Marcación uniforme:***

  Los usuarios finales cuentan con un plan de marcación único definido por el operador del servicio VPN, para cada suscriptor. El plan de marcación es uniforme dentro de la red virtual de cada empresa, independientemente de la ubicación física o geográfica de cada uno de los puntos.

- ***Confiabilidad para las redes de las compañías:***

  En caso de que se presenten problemas durante una comunicación, debidos al enlace utilizado, la red pública conmutada permite el reenrutamiento de la información sin costos adicionales. Esto garantiza que el usuario final pueda llevar a cabo su comunicación sin que se vea afectada por problemas en las líneas o en los equipos de transmisión responsabilidad del operador, incrementando la confiabilidad de las comunicaciones.

2.5.2. BENEFICIOS PARA EL SUSCRIPTOR DEL SERVICIO

- ***Reducción de costos*:**

  - Reducción del capital de inversión. Las empresas no necesitan hacer inversiones adicionales en equipos como en el caso de las redes privadas, ya que se utiliza la red pública para enrutar las llamadas entre los diferentes puntos de los clientes.
  - Ahorro en gastos telefónicos. Se consiguen gracias al descuento por uso masivo, por el abandono de las líneas arrendadas poco usadas y sin rentabilidad, y en algunos países por la reducción de costos en el uso de la larga distancia.
  - Los suscriptores necesitan menos personal de mantenimiento y soporte para sus redes, lo cual supone un ahorro de gastos considerable. Esto se logra ya que la gestión de tráfico para el encaminamiento alternativo automático lo realiza la RTPC.

- ***Flexibilidad :***

  - Mayor flexibilidad por el uso de la RTPC. Las líneas dedicadas tienen mayores limitaciones en cuanto a capacidad de tráfico y disponen de menos posibilidades de encaminamiento alternativo que la RTPC.
  - Permite supervisión de las llamadas para evitar fraudes. Los usuarios pueden controlar y observar con gran flexibilidad los costos que se originan en su VPN.

  Además de esto, VPN ofrece flexibilidad para el suscriptor en diferentes áreas:

  - En precios, permitiendo negociar contratos y descuentos, de acuerdo con los requerimientos específicos de los usuarios.
  - En la oportunidad de llevar todas las locaciones, particularmente los sitios más pequeños, hasta dentro de la red (on-net).
  - En la capacidad para adicionar o quitar nuevas locaciones. El suscriptor puede adicionar o quitar rápidamente conexiones de la red, mejorando la administración y el control sobre toda la organización. Esto significa, que la red se convierte en una parte integral de los negocios, no sólo en un mecanismo de transporte. Anteriormente la introducción de una nueva locación implicaba cambios y un rediseño necesario de la red. Con VPN, las comunicaciones a las nuevas locaciones pueden ser modificadas en muy poco tiempo. Esto permite que las llamadas sean redireccionadas, y que los sitios sean borrados o establecidos simple y rápidamente.
  - En ofrecer los medios para soportar las necesidades de los trabajadores que permanentemente se están trasladando de un sitio a otro y que ha adquirido una gran importancia para las organizaciones de ventas y servicios. La flexibilidad de las tarjetas de llamada y el desarrollo de los accesos celulares a VPN serán significativos para incrementar su uso en el futuro.

  VPN provee una mejor combinación de costo y flexibilidad que cualquier otro servicio, mejorando su eficiencia en comunicaciones.

En la Fig. 2.1 se puede observar la posición de VPN en una relación costo - flexibilidad, comparado con los servicios de RTPC y de líneas dedicadas. El atractivo de VPN se incrementa a medida que se mejora la ubicuidad del servicio, por lo que resultan puntos de conmutación más pequeños desde la RTPC hasta VPN, incrementándose a su vez la relación costo-efectividad en el ámbito global.

VPN ayuda a las empresas a mejorar dos factores vitales para el éxito como son su eficiencia y su efectividad.

- ***Eficiencia***

  - Red híbrida. Los usuarios no tienen que abandonar su estructura de red existente al utilizar VPN, sino que pueden establecer una red híbrida combinando las líneas arrendadas (Ll - Leased lines) con ella. Así, por ejemplo, es posible usar Lls para una alta carga básica entre dos filiales y VPN como mecanismo de desborde y de comunicación con otras filiales.
  - Mejor utilización de los recursos. Las inversiones realizadas por las telcos, permiten que los usuarios tengan un rápido acceso a las nuevas tecnologías y se beneficien de los servicios y de las ventajas de red que se ofrecen basados en ellas. Además, no tienen que estar atados a equipos propios que pueden dejarlos rezagados en corto tiempo, debido a los rápidos avances que en materia de comunicaciones se están presentando a nivel mundial.

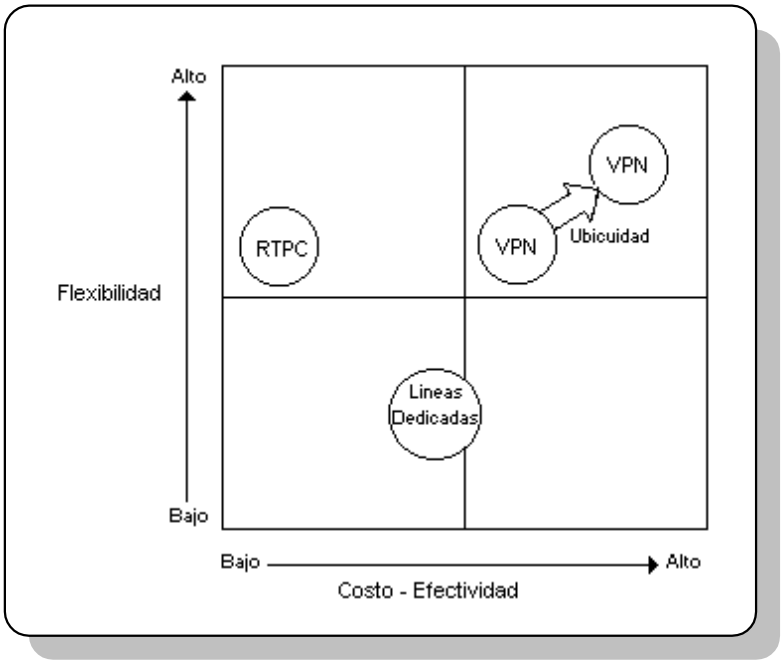


Fig. 2.1. VPN respondiendo a las necesidades de comunicación de las empresas

- Mejores métodos de controlar costos. Gracias a la utilización de las características de facturación de VPN, se puede obtener un control detallado del tráfico causado en cada uno de los puntos de la red.
- Mejores niveles de soporte y funcionalidad. A través del uso de VPN, los usuarios no sólo reducen sus costos sino que también obtienen un servicio mejor soportado y con mayor funcionalidad. En la Fig. 2.2 se comparan VPN, redes privadas de líneas arrendadas y RTPC en términos de la funcionalidad que ofrecen y del soporte que es proporcionado por las telcos.

  La funcionalidad y el soporte para redes privadas basado en líneas arrendadas son proporcionados por los mismos usuarios. Esto lo logran contratando sus propios asesores en comunicaciones e invirtiendo en sus propios equipos de redes privadas.

  VPN, por otro lado, ofrece los equipos y la experiencia necesarios para que el usuario no tenga que invertir en ellos, al mismo tiempo que provee un mejor nivel de funcionalidad.

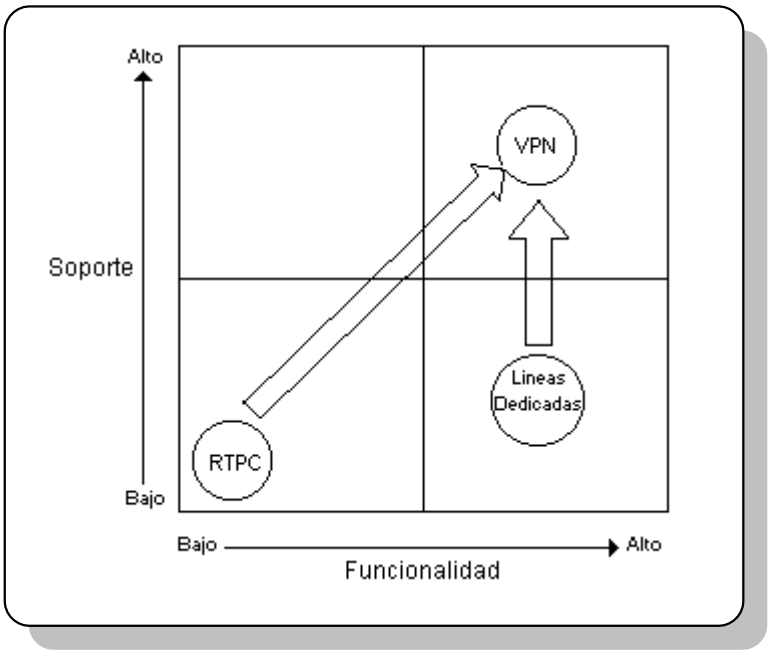


Fig. 2.2. Valor de VPN contra otros productos

- ***Efectividad***

VPN incrementa la efectividad de las comunicaciones de las compañías ya que directamente ayuda a mejorar la respuesta y la flexibilidad de su núcleo de negocios.

Esto se alcanza:

- Proporcionando a las empresas la flexibilidad y rapidez para adicionar y remover puntos.

- Permitiendo a los empleados de las empresas acceso a la red y a todas sus facilidades, independientemente del punto donde se encuentren (Las redes privadas de líneas arrendadas sólo sirven a los puntos más grandes).

- Ofreciendo características de red amplia, lo cual permite a los empleados efectuar sus funciones más efectivamente (las redes privadas cuentan con una gran variación en la uniformidad de sus características, las cuales están frecuentemente restringidas a puntos individuales).

- ***Características avanzadas***

  - Un plan de numeración común. Corresponde a uno de los principales beneficios que VPN puede proporcionar a sus usuarios. Se determina un plan de numeración privado para todos los miembros de una VPN, en el cual también se definen números que permiten acceder a la red y salir de ella, desde y hacia la RTPC, respectivamente. La red es transparente a sus usuarios, permitiendo que todas las llamadas siempre sean completadas y que los números de teléfono puedan ser cambiados de sitio dependiendo de las necesidades de los usuarios finales.

  - Las responsabilidades del manejo de la red son transferidas al operador del servicio (planeación, instalación y mantenimiento).

  - La administración de la red puede ser realizada parcialmente por el cliente, o totalmente por el operador del servicio. A través de una terminal de operador el cliente puede ser guiado en sus tareas de administración.

  - Los datos de VPN son administrados de forma centralizada.

  - VPN puede prestar los servicios tanto de voz conmutada como de datos conmutados.

2.5.3. BENEFICIOS PARA EL OPERADOR / PROVEEDOR DEL SERVICIO

- Ofrece una reducción significativa en los costos de provisión de la red, comparado con las líneas arrendadas. Mientras que las líneas arrendadas tienen que ser aprovisionadas y mantenidas como entidades separadas, VPN usa los recursos comunes de la red. La simplificación en operaciones, administración y mantenimiento de VPN conduce a un considerable ahorro en los costos - más que sólo un ahorro en ancho de banda de transmisión.

- Suministra a las compañías de telecomunicaciones (operador / proveedor) los elementos externos de las redes privadas. Las compañías no necesitan gastar en asesorías, equipos, ni mantenimiento, para correr complejas redes de líneas arrendadas. Ahora estos gastos son desviados a las compañías operadoras de telecomunicaciones.
- Fácil ampliación con nuevas facilidades. La arquitectura de RI permite ampliar las funciones básicas de VPN adicionándole en cualquier momento nuevas y específicas facilidades.
- Incremento de su participación en el mercado. VPN permite obtener y disfrutar los lucrativos negocios de los clientes corporativos cubriendo todas sus necesidades de comunicaciones. VPN también permite a las compañías de telecomunicaciones extender su participación en el mercado a través de las fronteras nacionales.
- Alternativa competitiva contra otros mercados, como el mercado de las PABX. Con el servicio VPN, el operador de red puede ofrecer a sus clientes una relación precio / rendimiento atractiva, lo cual, como compensación, evita que los abonados al servicio se cambien a redes de otros operadores.
- Mejora del servicio a los clientes, por el rápido despliegue de recursos.
- Aumento de los ingresos, por una rápida prestación de los servicios.

2.6. CARACTERISTICAS DEL SERVICIO VPN

Los desarrollos tecnológicos en diferentes áreas (como en equipos PBX, multiplexores inteligentes y sistemas de administración de redes) han permitido la introducción de características avanzadas sobre redes corporativas. Estas características pueden estar disponibles para todos los clientes (grandes, medianos, pequeños) gracias a la utilización de las Redes Privadas Virtuales. Con el esquema actual esto no es posible ya que las características son proporcionadas desde los propios equipos del cliente, es decir, desde el extremo de la red; mientras que con VPN, son suministradas desde el centro, el corazón mismo de la red.

Las características de VPN ofrecidas a los usuarios son diferentes dependiendo de la compañía de telecomunicaciones (telco) que brinde el servicio, al igual que la clasificación que se haga de las mismas. Sin embargo, se definirá un grupo estándar de características, diferenciadas por el nivel de flexibilidad que la telco puede ofrecer y por la personalización realizada para cada usuario.

En la *Tabla 2.1*. se pueden definir algunos puntos básicos que permiten comparar los beneficios de estos dos esquemas.

Las características de VPN se pueden dividir en cuatro categorías, las cuales son:

- *Características de Grupo Cerrado de Usuarios*, las cuales utilizan la capacidad de VPN para buscar información guardada en las bases de datos relacionadas específicamente con cada grupo cerrado de usuarios. Estos incluyen planes privados de numeración, enrutamiento preferido, códigos de autorización, filtrado de llamadas, entre otros.
- *Características de Gestión*, las cuales ofrecen a los usuarios gestión de configuración, gestión de costos y monitoreo de desempeño.
- *Características relacionadas con RDSI*, las cuales están asociadas con acceso RDSI e incluyen datos conmutados, despliegue de la línea ID llamante, despliegue de nombre llamante y selección de llamada por llamada.
- *Características manejadas por los eventos*, las cuales ocurren después de que un cierto evento ha tenido lugar. Estos incluyen reenrutamiento por congestión, transferencia de llamadas, anuncios de terminación, entre otros.

	Características proporcionadas desde el centro	**Características suministradas desde la periferia**
Disponibilidad de características	Disponible para todos los sitios sin importar su tamaño, método de acceso o facilidad de emisión de mensajes de administración de la red.	Sólo disponible para grandes sitios donde se puede contar con circuitos arrendados y sofisticados sistemas de gestión y administración de equipos.
Costo de las características	Dependiendo de las necesidades del usuario, pueden ser pagadas selectivamente.	Pagado como una parte del costo del capital de los equipos.
Nuevas características	No es necesario actualizar los equipos de los clientes.	Es necesario hacer actualizaciones de hardware y/o software.
Provisión y administración de las características	Responsabilidad del operador. El usuario no necesita incrementar sus conocimientos con la introducción de nuevas características.	Responsabilidad del usuario. Debe mantener un grupo de conocimientos apropiado para las características utilizadas.

Tabla 2.1. Provisión de características - Centro contra periferia.

2.6.1. CARACTERISTICAS DE GRUPO CERRADO DE USUARIOS

La implementación de este conjunto de características se basa en la habilidad de la red para buscar y actuar sobre información guardada en las bases de datos de la red. Las características más comunes ofrecidas en esta categoría se describen a continuación:

- **Plan de Numeración Privado (PNP)**. Cada grupo VPN tiene su propio plan de numeración privado. El plan de numeración de una VPN proporciona un esquema de numeración uniforme para todos los puntos de una organización a lo ancho del mundo, es decir, que puede estar conformado por planes de numeración nacionales e internacionales. Un plan de numeración es la más básica, y al mismo tiempo, la más importante característica de VPN. Un PNP ofrece los siguientes beneficios a los usuarios:
  - La compañía puede mantener un sencillo directorio interno para todos sus puntos, a través del mundo.
  - Las personas pueden retener sus números aunque alguna oficina sea relocalizada.
  - Los largos números internacionales son evitados. Esto, junto al hecho de que el Sistema de Señalización por Canal Común No.7 CCS7 (Common Channel Signaling System No. 7) es usado para propósitos de señalización, significa que las llamadas internacionales pueden ser originadas muy rápidamente.

- **Marcación abreviada.** Cada VPN tiene su propia lista de marcación abreviada. Un usuario VPN puede marcar un número abreviado (ABD) para comunicarse con un abonado dentro o fuera de la red. VPN automáticamente conecta la llamada cuando reconoce códigos abreviados. Esta característica permite ahorrar tiempo durante el levantamiento de la llamada.

- **Abonados ubicados en la red (ON - NET).** Un abonado **on-net** corresponde a un usuario final, suscrito a la VPN y que tiene facilidad de marcación abreviada de acuerdo a un plan de numeración uniforme.

- **Abonados ubicados fuera de la red (OFF - NET).** Un abonado **off-net** corresponde a un usuario final que no está suscrito a la VPN.

- **Abonados de Acceso remoto**. Corresponden a usuarios finales que accedan la VPN por marcación, usando un abonado de la red pública conmutada. Pueden ser considerados como abonados Off-Net (por no encontrarse dentro de la VPN) que están autorizados para acceder a la Red Privada Virtual desde un terminal que no se encuentra dentro de ella.

  Después de la validación, el usuario tiene los mismos derechos que si estuviera llamando desde un punto dentro de la VPN, por lo que se conocen **como Abonados Virtuales On-net**. Cuentan con números de la RTPC y con números de marcación abreviada de la VPN.

- **Enrutamiento preferido.** Los usuarios pueden especificar las rutas preferidas para sus llamadas, particularmente para llamadas internacionales y de larga distancia. Por ejemplo, un usuario puede especificar que sus llamadas transatlánticas sean enrutadas sobre cables ópticos como una prioridad y que las rutas satelitales sean usadas como una opción alternativa o de contingencia. Los beneficios para los usuarios son:

- Consistente calidad del servicio sobre cada llamada.
- Rutas alternativas y de contingencia disponibles para todos los usuarios.
- Ahorro de costos para las compañías, que previamente han pagado por sus propios circuitos dedicados de contingencia, o baja utilización de sus redes ya que han escogido implementar diversos enrutamientos.

- **Códigos de autorización.** Los códigos de autorización permiten realizar la identificación del abonado que llama y la clase del servicio para los usuarios de la VPN. Si la identificación no puede ser hecha por otros medios, el mismo código de autorización puede ser usado para originar llamadas on-net y off-net para propósitos de tarifación y de verificación de la clase de servicio. De igual forma, el código de autorización puede ser utilizado para anular las restricciones del servicio y el bloqueo sobre ciertos números.

- **Clase de Servicio.** La clase de servicio es determinada por la identificación automática del número (ANI)[1], el código de autorización o el grupo al que pertenece el usuario. Las clases de servicio derivadas de un código de autorización tienen prioridad sobre otras clases de servicio derivadas de otros medios. Las clases de servicio identifican las restricciones de acceso y las restricciones a las facilidades de red:
  - Las *restricciones de acceso* incluyen acceso a llamadas off-net, acceso a partes de la VPN y acceso a números específicos.
  - Las *restricciones a las facilidades de red* permiten o restringen el acceso a ciertas características de la red para ciertos usuarios o grupos de usuarios.

  Son posibles también restricciones de hora, día de la semana o año, y podrían ser implementadas por estación, localidad y por códigos de autorización. Estas restricciones pueden ser usadas para prevenir el uso no autorizado de VPN.

- **Anular la Clase de Servicio.** Permite a un usuario VPN anular el tratamiento de una clase de servicio preasignado a un equipo terminal, durante la duración de la llamada, entrando un código de autorización. Los registros de llamada deben reflejar todos los datos relevantes de la llamada, a ser cargados al código de autorización del usuario más que a la estación de origen.

- **Filtrado de llamadas.** Es un conjunto de características que determinan la elegibilidad de una llamada para ser completada, basada en la información de la clase del servicio asociado con el usuario, la estación, o el grupo de enlace.

[1] *ANI (Identificación Automática del Número* - Automatic Number Identification): Número utilizado por una compañía telefónica para determinar que abonado ha originado una llamada. Para efectos de facturación, enrutamiento de la llamada o tratamiento especial de la misma.

- **Código de Bloqueo.** El código de bloqueo evita que algunos usuarios, grupos, o puntos de la red accedan a ciertos servicios de VPN. Para ello se utilizan diferentes clases de restricciones de acceso a los servicios como son los códigos de área, códigos de centrales y países. Esto se realiza haciendo una traslación de los dígitos marcados y comparando los resultados con la clase de servicio permitido. Las llamadas bloqueadas son interceptadas y conectadas a la red apropiada de anuncios grabados.

2.6.2. CARACTERISTICAS DE GESTION

El uso de sofisticados sistemas de gestión de red se ha convertido en una necesidad para la eficiente operación de redes privadas basadas en líneas arrendadas. Esto se debe a la creciente dificultad para operar y planear las redes, principalmente debido a:

* La incrementada complejidad y flexibilidad de los equipos, particularmente para comunicación de datos.
* La proliferación de equipos y sistemas en redes corporativas.
* La incrementada sofisticación de operaciones como resultado de la integración de voz y datos al nivel de transmisión.
* La creciente necesidad de herramientas especializadas.
* La proliferación de aplicaciones de redes.

Muchas corporaciones grandes han acumulado considerables propiedades de telecomunicaciones y el costo de operación de sus redes se ha convertido en un significativo punto del presupuesto.

Existe una incrementada tendencia hacia outsourcing[2]. Actualmente, las corporaciones "no quieren tener su propia compañía de teléfonos". Ellos prefieren concentrarse en su núcleo de negocios. Al mismo tiempo, los negocios de muchas corporaciones dependen en buena cantidad, de comunicaciones confiables.

VPN es capaz de encarar muchos de estos problemas:

* Reduciendo los equipos requeridos en las premisas de los clientes.
* Removiendo la obligación de monitorear y encontrar fallas en los componentes de la red.
* Reduciendo la necesidad de personal (staff) de operaciones altamente capacitado.
* Removiendo las dificultades en planear y desarrollar la red corporativa.

[2] *Outsourcing :* Término empleado para definir un acuerdo en el que una compañía proveedora se compromete a proporcionar a su cliente los servicios o procedimientos que actualmente el cliente está supliendo internamente.

Simultáneamente, VPN incrementa el control sobre los servicios de comunicaciones de las corporaciones. Los principales elementos de las características de gestión de VPN son control de configuración, control de costos y monitoreo de desempeño.

- **Control de configuración**. Este control generalmente es proporcionado desde un terminal propio del usuario el cual se interconecta con el equipo de la telco. Los principales aspectos del control de configuración son las habilidades para:
  - Controlar los recursos de la red. Esto permite al usuario incrementar o decrementar la capacidad de su propia red.
  - Adicionar, borrar y cambiar números privados y sus atributos.
  - Adicionar, borrar y cambiar accesos y códigos de autorización.

  Adicionalmente, se cuenta con reportes de gestión sofisticados. Estos incluyen información sobre uso e incrementos de tráfico, picos de tráfico y patrones de tráfico.

- **Control de costos**. Esta facilidad proporciona reportes de facturación ajustados a las necesidades de los usuarios. Las facturas personalizadas pueden ser preparadas para toda una corporación, regiones individuales, puntos individuales, funciones individuales o usuarios individuales.

- **Monitoreo de desempeño**. Esta facilidad ofrece a los usuarios la habilidad para monitorear y verificar la correcta operación de su red virtual, proporcionando la confidencialidad que muchas compañías requieren.

2.6.3. CARACTERISTICAS RELACIONADAS CON RDSI

Estas características se encuentran generalmente disponibles para los usuarios que tienen acceso RDSI a la VPN. Incluyen:

- **Servicio Integrado Digital Conmutado (RDSI BE).** Habilita el uso de líneas de acceso (conectividad digital) para integrar servicios de voz, datos, imágenes y video al equipo de usuario VPN. El operador de red además de proveer conectividad por medio de interfaces digitales RDSI, lo puede hacer por medio de enlaces T1 o E1.

- **Despliegue de línea llamante.** La cual muestra el número del abonado que origina la llamada. Esta facilidad puede ser interfazada con las facilidades de la base de datos propia del usuario, para mejorar el servicio. Por ejemplo, si el abonado llamante es un cliente, entonces el conteo de detalles puede ser desplegado sobre una pantalla a medida que transcurre la llamada.

- **Despliegue del nombre de la red.** Permite que el nombre del abonado llamante sea desplegado sobre el aparato receptor.

2.6.4. CARACTERISTICAS MANEJADAS POR LOS EVENTOS

Estas características se presentan cuando un evento particular ha ocurrido o cuando ciertos criterios que han sido definidos de antemano se presentan. Algunos ejemplos de este tipo de características son:

- **Destino alterno para llamada ocupada / no contestada.** El usuario puede reenrutar llamadas VPN si el destino al que se llama está ocupado o no contesta dentro de un período de tiempo.

- **Reenrutamiento por congestión.** Se asigna una ruta alterna al mismo destino cuando la primera ruta seleccionada está congestionada. Se solicitará el permiso del usuario para realizar el reenrutamiento.

- **Transferencia de llamada.** Una llamada que llegue a un destino puede ser transferida a otro lugar por el encargado de dicho destino.

- **Anuncios de mensajes grabados.** Se pueden tener mensajes de anuncios grabados dentro de la red. La grabación será asignada a un número on-net y será accesible por estaciones on-net y off-net. La longitud máxima del anuncio es de 3 minutos. Una llamada a un anuncio será respondida dentro de los 5 primeros repiques, después de los cuales el acceso al anuncio será permitido.

- **Anuncios de terminación.** Una llamada puede ser terminada por una máquina de anuncios grabados en vez de la línea del usuario.

- **Operadores.** Los operadores permiten que los usuarios obtengan algunos de los siguientes servicios:
  - Ayuda a los usuarios cuando tienen problemas de marcación y permanece en la línea hasta que la llamada ha sido completada.
  - Verifica los códigos de autorización dados verbalmente por abonados que acceden a la VPN desde puntos on-net y off-net. Una vez el código ha sido verificado, el operador establece la llamada solicitada por el abonado.
  - Un usuario VPN puede llamar al operador VPN marcando un número especial para reportar un robo o pérdida del código de autorización, para obtener el valor de su cuenta y para reportar interrupciones en sus llamadas o transmisión insatisfactoria, entre otros.

Con la utilización de las Redes Inteligentes, muchas características especializadas y personalizadas pueden ser creadas fácilmente en esta categoría.

2.7. SERVICIOS VPN

Aunque el primer servicio de redes virtuales fue introducido por France Telecom en 1975, no fue sino hasta mediados de los 80s cuando VPN logró una extensa aceptación, después de que fue introducido en los Estados Unidos. Desde entonces, el ***servicio de Voz Conmutada*** logró ganarse la confianza de las empresas de telecomunicaciones más grandes en el mundo.

En 1991 debido al éxito de las Redes Privadas Virtuales de voz, las compañías de telecomunicaciones centraron su atención en desarrollar ***servicios virtuales de Datos Conmutados***. El objetivo era lograr los mismos niveles de confianza obtenidos por la voz a mediados de los 80s.

2.7.1. SERVICIO DE VOZ CONMUTADA

El servicio de voz conmutada soporta conexiones para voz o datos análogos superiores a 9.6Kbps y soporta llamadas iniciadas por abonados on-net para ser conectados a todos los abonados on-net y off-net, por medio de marcación directa de estación a estación. Las llamadas también pueden ser iniciadas desde un abonado off-net.

El servicio de voz conmutada interconecta los siguientes tipos de equipo terminal:

- Líneas telefónicas simples.
- Sistemas telefónicos multilíneas.
- Estaciones Centrex.
- Centrales privadas (PBXs) electromecánicas, análogas y digitales, RDSI de acceso básico y de acceso primario.
- Equipos terminales de datos.
- Equipos terminales digitales T1.
- Aparatos de facsímil del grupo I, II y III del UIT-T.
- Equipos de seguridad de voz y de datos.
- Otros equipos usados para conexión de redes públicas conmutadas y privadas conmutadas.

El servicio de voz conmutada también provee interconectividad de red entre la VPN y la red pública conmutada.

De las características de VPN mencionadas anteriormente, las más importantes utilizadas por el servicio, son el plan de numeración privado y los anuncios de mensajes grabados.

2.7.2. SERVICIOS DE DATOS CONMUTADOS

Los requerimientos de transmisión de datos se han incrementado rápidamente durante la última década, multiplicándose el número de aplicaciones e incrementando el porcentaje invertido en comunicaciones de datos de una empresa del 30% hace 10 años, a más del 60% actualmente. Estos factores han contribuido al desarrollo de aplicaciones conmutadas y a la necesidad de conexiones conmutadas de alta velocidad.

El servicio de datos conmutados provee un servicio de conmutación de circuitos síncrono, dúplex, totalmente digital, de entrega punto a punto con velocidades de 56, 64, 384Kbps. Es usado para soportar estaciones de trabajo (workstations), computadores host, computadores personales, terminales y otros equipos de oficina.

Generalmente, los usuarios utilizan las nuevas VPNs de datos conmutados como un suplemento a sus propias redes de datos y no como un sustituto. Su utilización es atractiva para usuarios con aplicaciones de respaldo, no críticas, y aplicaciones donde el tiempo empleado iniciando y soportando la comunicación no son un problema.

Aplicaciones críticas, como la nómina de la empresa, u otras aplicaciones que requieren altos niveles de seguridad, continúan siendo enviadas a través de enlaces privados. Otras aplicaciones, como aplicaciones de ingeniería y de manufactura como por ejemplo Cad-Cam, gráficas y diseños, las cuales requieren una continua conexión en línea seguirán trabajando con líneas dedicadas, mientras los nuevos desarrollos pueden asegurar la confiabilidad, disponibilidad y seguridad necesarias para migrar a ellas.

2.8. ARQUITECTURAS DE RED

En la *Fig. 2.3.* se puede observar el camino evolutivo seguido en el ámbito mundial, para la implementación de las diferentes arquitecturas de red y para el surgimiento de las Redes Inteligentes.

VPN puede ser implementado como:

- Un servicio integrado con la Red Telefónica Pública Conmutada (RTPC).
- Un servicio soportado por una Red Overlay (*Red Paralela*) distinta a la RTPC.
- Wide Área Centrex *(WAC - Centrex de Área Ancha)* el cual es un sub-grupo de VPN y que puede ser soportado por redes integradas o por redes overlay.
- Un servicio independiente sobre una plataforma de RI.

En la *Tabla 2.2.* se presenta una comparación de las características de cada una de las arquitecturas de red. La selección del método que se debe aplicar para implementar una Red Privada Virtual, depende en gran parte de la rapidez con que una compañía necesite proveer el servicio y por otro lado de las características que cumplan con las expectativas de dicha compañía.

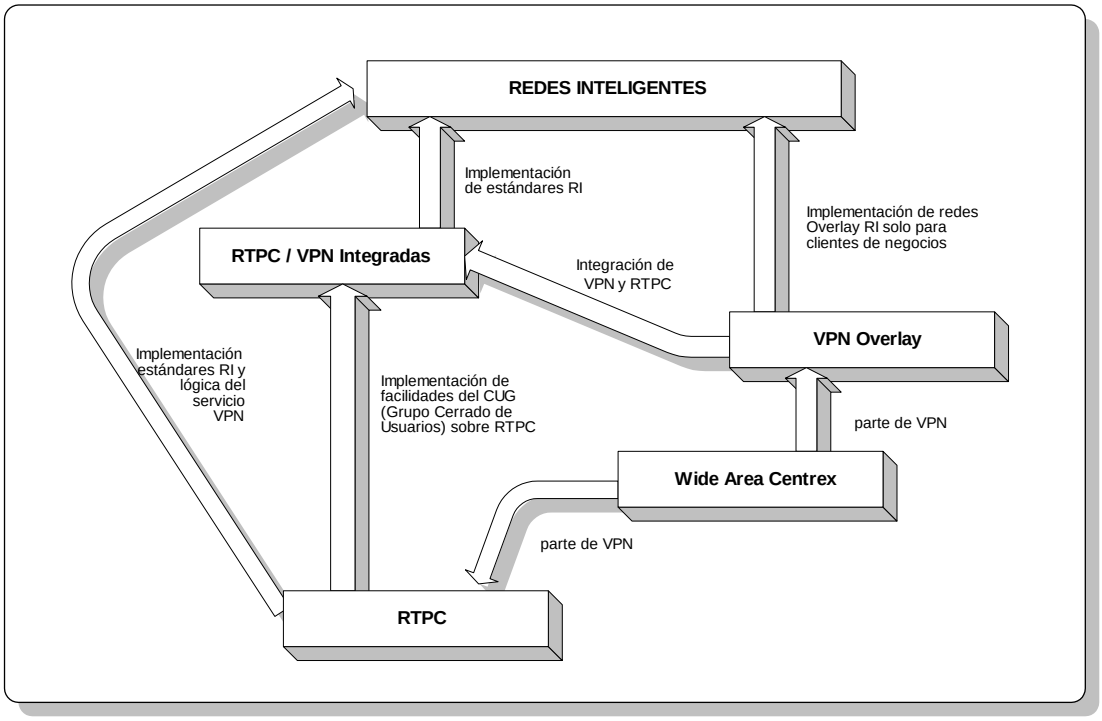


Fig. 2.3. Camino en la evolución de las redes

	Redes Integradas	Redes Overlay	Wide Area Centrex	Redes Inteligentes
Velocidad de implementación del servicio VPN	_	+	=	++
Compatibilidad con infraestructura existente	++	_	=	_
Evolución hacia las Redes Inteligentes	+	_	=	
Facilidad de acceso	++	_	=	++
Costos de la red	+	_	+	+
Responsabilidad ante los clientes corporativos	_ _	++	+	++
Velocidad de respuesta a las presiones competitivas	_	++	+	++
Acceso a bases de datos, actualización, mantenimiento, etc.	_	+	=	++
TOTAL	+	++	=	+++++ +++++

Tipo : + Relativamente mejor - Relativamente peor = No tiene impacto

Tabla 2.2. Comparación de las Arquitecturas de Red

2.8.1. REDES INTEGRADAS

Se definen Redes Integradas como aquellas en las que el servicio VPN puede ser ofrecido sobre una Red Pública Conmutada después de realizar algunas actualizaciones.

Para implementar VPN sobre una RTPC, una telco necesita:

- Ser capaz de implementar la funcionalidad de VPN sobre sus centrales digitales.
- Ser capaz de implementar y acceder bases de datos de red distribuidas y centralizadas.
- Estar avanzada en sus programas de digitalización de centrales locales.
- Haber alcanzado un elevado nivel de penetración de la señalización por canal común dentro de la red.

En estas redes el acceso al servicio VPN es compartido con la RTPC, por lo que el servicio está siempre disponible.

Las redes integradas ofrecen los siguientes beneficios a las telcos:

- Instalaciones (oficinas, sedes, sucursales, puntos de venta, fábricas, etc.) de una empresa de todos los tamaños pueden ser conectadas a VPN. Este será el principal servicio diferenciador para las compañías de telecomunicaciones en un mercado competitivo.
- El camino evolutivo hacia la estandarización de VPN va más recto que el de otras arquitecturas.
- El uso de recursos de red es optimizado, ya que se comparte la misma infraestructura de red tanto para la RTPC, como para el servicio VPN.
- No son necesarias inversiones en nuevos conocimientos ni en el mantenimiento de la infraestructura.

Por otra parte, las redes integradas tienen un número de desventajas asociadas. Entre ellas:

- El mejoramiento y la personalización de los servicios se realiza lentamente ya que las tareas de actualización se deben realizar sobre toda la red.
- El grado de servicio puede no ser fácilmente diferenciado, por lo que es difícil dar valores a los clientes de negocios.

2.8.2. REDES OVERLAY

Las Redes Overlay, es decir, redes paralelas o redes separadas de la RTPC, son utilizadas en caso de que la infraestructura de una compañía de telecomunicaciones no sea ni fácil ni rápidamente adaptable para ofrecer el servicio VPN.

Estas redes son implementadas específicamente para proporcionar los servicios de VPN. Otros servicios diseñados para solucionar las necesidades de las compañías, (tales como, Correo Electrónico, Videoconferencia, Acceso Internet, etc.) pueden ser proporcionados por la misma red.

El acceso a la red es ofrecido a través de líneas dedicadas y es independiente del acceso RTPC de las telcos. La RTPC y las Redes Overlay generalmente se interconectan en los niveles superiores de la jerarquía de red.

La opción Overlay se selecciona cuando:

- La telco necesita introducir su servicio VPN rápidamente, pero su Red Pública Conmutada requiere modificaciones y mejoras que no pueden ser realizadas tan rápida ni fácilmente.
- La telco desea proporcionar una red para satisfacer las necesidades de los usuarios corporativos. Esta red puede ser utilizada para ofrecer un grado superior de servicio comparado con el que se puede obtener sobre la RTPC, y para que nuevos servicios puedan ser rápidamente implementados.
- La telco desea proteger las ganancias de su RTPC. Esto lo logra desanimando el uso de VPN a las compañías con pequeñas instalaciones, al incrementar el valor de las líneas dedicadas.
- La telco percibe un beneficio estratégico en seleccionar los equipos de un proveedor diferente a los de su RTPC.

La selección de una arquitectura Overlay también se ve influenciada por:

- La disponibilidad de una red de transmisión en fibra óptica con amplia capacidad para transportar el tráfico VPN a unos pocos centros de conmutación overlay.
- La disponibilidad de líneas dedicadas para los grandes clientes corporativos, las cuales pueden ser reasignadas para proporcionar acceso dedicado a VPN.

Las Redes Overlay se basan en la utilización de centrales de gran tamaño, las cuales tienden a estar ubicadas en posiciones estratégicas en los principales centros de negocios del país y hacen un uso óptimo de la capacidad de la red de transmisión.

El acceso dedicado es proporcionado a través de unidades concentradoras remotas, ubicadas en sitios cercanos a las instalaciones de los clientes (normalmente en puntos en las centrales locales). Las unidades multiplexoras pueden también ser colocadas en puntos de grandes clientes.

Las Redes Overlay ofrecen los siguientes beneficios a las telcos:

- El servicio puede ser implementado sin considerar el estado de la red existente. Esto generalmente es ventajoso en sitios donde: la red es compleja, se usan estándares propietarios, no es digitalizada y se usan equipos de una gran variedad de proveedores.

- Proporciona una plataforma para la telco desde la cual se puede ofrecer un grado superior de servicios para grandes clientes corporativos.
- Se requiere un grado mínimo de conocimientos para realizar el mantenimiento ya que la red se basa en un pequeño número de grandes conmutadores.
- Los enlaces de accesos dedicados VPN pueden ser usados para ofrecer otros servicios a los clientes corporativos (incluyendo líneas arrendadas).

Entre las desventajas de las Redes Overlay se pueden mencionar:

- La prestación de los servicios, ya que se requieren accesos dedicados para todas las instalaciones. Generalmente las telcos tienen en cuenta el valor de los negocios que pueden generar los clientes, antes de realizar las adecuaciones necesarias en todas sus instalaciones. Sin embargo, en la práctica resulta más costoso y lento proporcionar el servicio a puntos ubicados lejos de los principales centros de negocios.
- El uso de los recursos de la infraestructura de la red, los cuales no son optimizados tanto como podrían serlo. Las compañías de telecomunicaciones que hagan una mejor utilización de sus redes tendrán costos más bajos y por lo tanto tendrán una ventaja sobre sus competidores.

Una Red Overlay puede permanecer independiente de la red principal y retener su posición como la principal red en solucionar las necesidades de los clientes corporativos. Sin embargo, la importancia del acceso y las motivaciones para reducir sus costos, conducirán a las telcos hacia una sencilla arquitectura de Red Inteligente.

2.8.3. CENTREX Y CENTREX DE AREA ANCHA

Centrex es un servicio de las compañías de telecomunicaciones que elimina la necesidad de los clientes de poseer su propia PBX. El servicio es proporcionado conectando las extensiones del teléfono a un punto ubicado directamente en la central local. Centrex de Área Ancha (WAC - Wide Area Centrex) es una forma especial de Centrex, donde el servicio es ofrecido en distintos puntos de la compañía y un grupo cerrado de usuarios es mantenido a través de la red conmutada.

Centrex y WAC pueden ser usados como un elemento de una VPN. Por ejemplo, una VPN puede contener varios puntos equipados con PBXs y otros directamente conectados a Centrex. El grupo cerrado de usuarios es mantenido transparentemente a través de toda una red.

Centrex puede ser visto como uno de los componentes del portafolio de servicios de una compañía de telecomunicaciones para clientes corporativos, al lado de las soluciones basadas en PBX y los servicios de líneas arrendadas *(Fig. 2.4).* Los servicios de Centrex y WAC tienen un mercado muy limitado. Se utilizan sólo para grandes instalaciones, generalmente aquellas donde se trabaja con más de 1000 extensiones.

Las principales razones para que una telco implemente soluciones basadas en Centrex son:

- Completar su portafolio de productos ofrecidos a grandes clientes corporativos.
- Beneficiarse de las ganancias adicionales que previamente eran consumidas por los clientes en las PBXs y en su mantenimiento.
- Proteger las ganancias que podrían desviarse hacia otros operadores de redes.

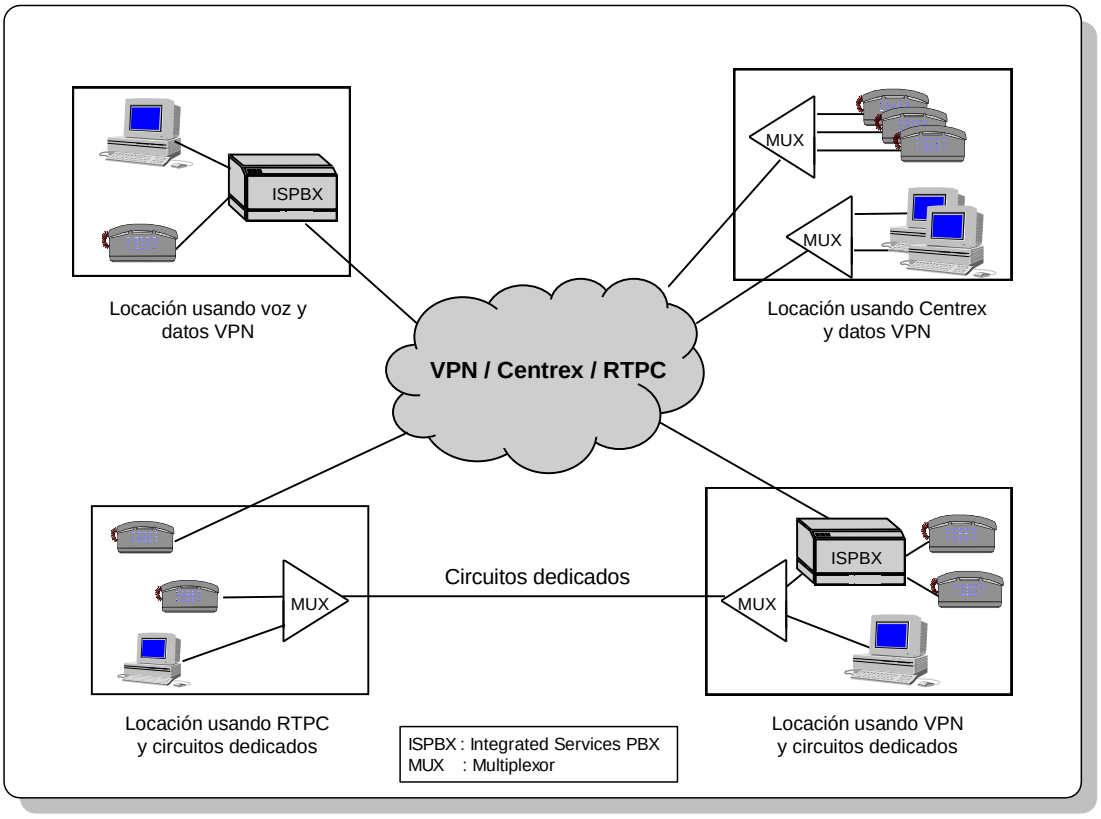


Fig. 2.4. Soluciones Híbridas VPN, RTPC, Centrex, Circuitos Dedicados

Las soluciones Centrex pueden ser integradas con la RTPC (p.e. un conmutador proporciona tanto las funciones RTPC como las funciones de Centrex) o implementadas como una red overlay.

2.8.4. REDES INTELIGENTES

El servicio de Red Privada Virtual corresponde al principal servicio de Redes Inteligentes para usuarios corporativos. La característica más importante de la arquitectura de RI es su independencia tanto del mecanismo de acceso usado, como de los servicios específicos que son ofrecidos. Esto significa que la lógica del servicio es independiente de la lógica de la llamada.

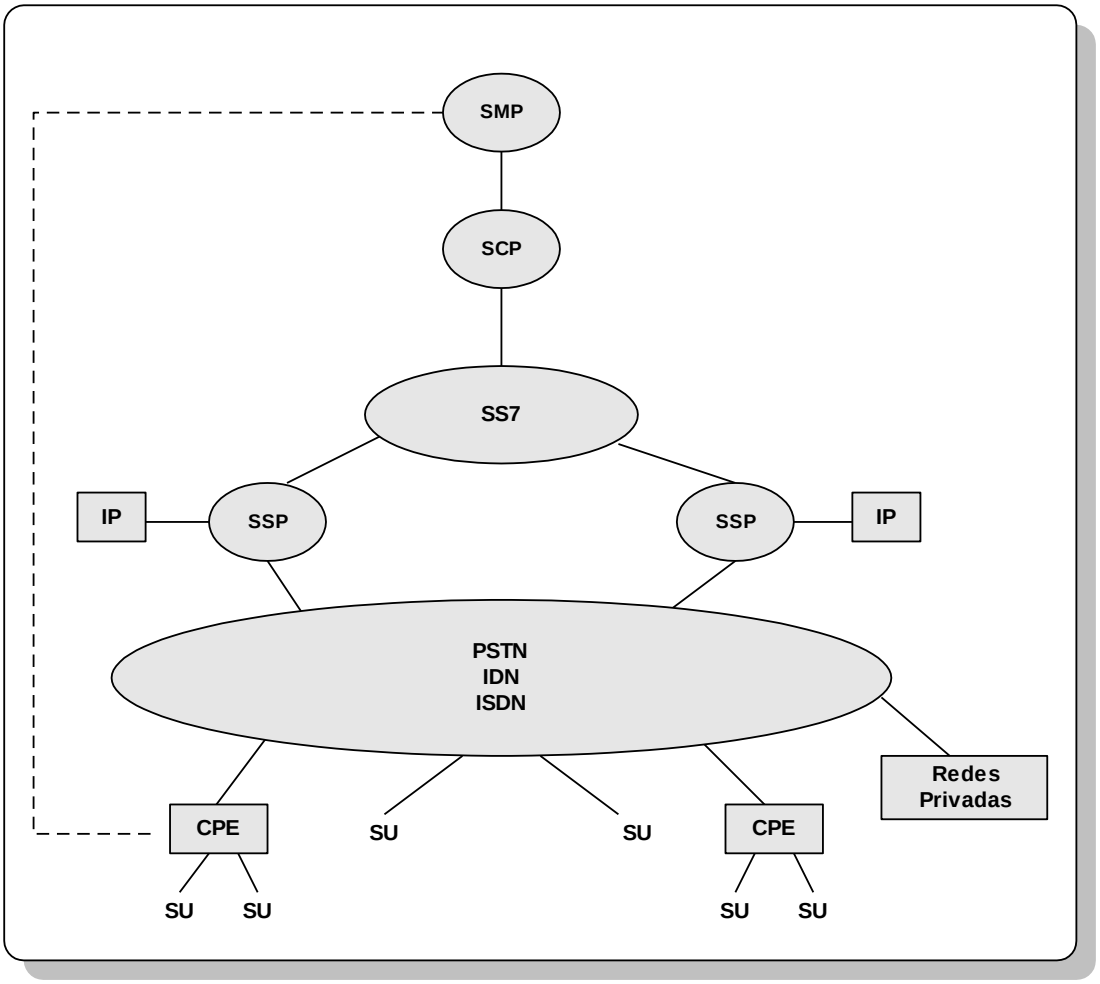
La RI permite a las compañías de telecomunicaciones:

- Crear nuevos servicios rápidamente y personalizarlos según las necesidades de los usuarios. Esto es posible gracias a la utilización de plataformas estandarizadas, genéricas y cuya programación es independiente de los servicios.
- Introducir fácilmente nuevas tecnologías en la red, debido a que la lógica del servicio es independiente de los elementos de red.
- Reducir los costos para el desarrollo de sistemas y software, y eliminar la necesidad de construir interfaces entre diferentes productos y arquitecturas.
- Proveer la oportunidad para una verdadera independencia tanto para los componentes de red como para los elementos de servicio.

La arquitectura de RI está basada en un número de componentes bien definidos como son (*Fig. 2.5.*):

- Punto de Conmutación de Servicios (Service Conmutadoring Point - SSP).
- Punto de Control de Servicios (Service Control Point – SCP).
- Punto de Transferencia de Señalización (Signal Transfer Point - STP).
- Periférico Inteligente (Intelligent Peripheral - *IP*).
- Sistema de Gestión de Servicios (Service Management System - SMS).
- Ambiente de Creación de Servicios (Service Creation Enviroment - SCE).

La meta a largo plazo de los diferentes operadores de telecomunicaciones siempre fue desarrollar su propia Red Inteligente, ya que el servicio VPN se podía proporcionar mejor a través de esta plataforma. Por tal motivo el presente trabajo se enfoca en el funcionamiento del servicio VPN dentro de una arquitectura de Red Inteligente.



SMP	:	Punto de Gestión del Servicio *(Service Management Point)*
SCP	:	Punto de Control del Servicio *(Service Control Point)*
SSP	:	Punto de Conmutación del Servicio *(Service Conmutadoring Point)*
SS7	:	Sistema de Señalización No.7 *(Signaling System No.7)*
IP	:	Periférico Inteligente *(Intelligent Peripheral)*
PSTN	:	Red Telefónica Pública Conmutada *(Public Switched Telephony Network)*
IDN	:	Red Digital Integrada *(Integrated Digital Network)*
ISDN	:	Red Digital de Servicios Integrados *(Integrated Service Digital Network)*
CPE	:	Equipo Local del Cliente *(Customer Premises Equipment)*
SU	:	Usuario del Servicio *(Service User)*

Fig. 2.5. Componentes de la Red Inteligente

3. SERVICIO VPN SOBRE REDES INTELIGENTES

En este capítulo se presenta un estudio detallado del servicio Red Privada Virtual, desde el punto de vista de las Redes Inteligentes.

Se incluye la descripción de las principales características del servicio, los diferentes métodos de acceso, los tipos de llamadas, el esquema de numeración y algunos procedimientos para el funcionamiento del servicio en una arquitectura de Red Inteligente.

3.1. ESTANDARIZACION DEL SERVICIO VPN SOBRE RI

Para realizar la especificación del servicio de Red Privada Virtual se utiliza el Modelo Conceptual de RI, el cual es la base para el diseño y la descripción de la arquitectura de Red Inteligente y de los servicios dentro de ella.

El Modelo Conceptual de RI se encuentra definido en la recomendación Q.1201 de la UIT-T y está formado por el Plano de Servicios, el Plano Funcional Global, el Plano Funcional Distribuido y el Plano Físico. El Plano de Servicios incluye la definición de los servicios y los describe en términos de una o más Características de Servicio (Service Features).

En la Recomendación Q.1201 también se describe la normalización de las Redes Inteligentes en una serie de etapas, llamadas Conjuntos de Capacidades (CS – Capability Sets) de RI, como concepto arquitectural para la creación y prestación de servicios. Cada nuevo CS amplía los aspectos definidos en el CS anterior.

A continuación se presenta la definición del servicio Red Privada Virtual a partir de cada uno de los Conjuntos de Capacidades y las adiciones en características de servicios hechas por cada nuevo Conjunto de Capacidades.

3.1.1. CONJUNTO DE CAPACIDADES 1 (CS-1)

Es la primera etapa normalizada de la Red Inteligente, formada por las Recomendaciones Q.121x de la UIT-T aprobadas en Marzo de 1993 y reeditadas en 1995 con el nombre de CS-1R.

Soporta servicios de telecomunicaciones en un solo extremo y con un solo punto de control. El punto de control de servicio (SCP) es invocado en la fase de establecimiento o de terminación de la llamada y no durante la fase de conexión activa de la misma.

A continuación se presentan las definiciones textuales previstas por el CS-1 para el servicio VPN, las cuales no son necesariamente coherentes entre sí y posteriormente se presentan las características del servicio asociadas al mismo.

3.1.1.1. Descripción del Servicio VPN

Descripción No. 1 :

" Este servicio permite establecer una red privada utilizando recursos de red pública. Las líneas de abonado, conectadas en distintas conmutaciones de red, constituyen una centralita automática privada virtual e incluyen varias capacidades de centralita, como el plan de numeración privado, la transferencia de llamadas y la retención de llamadas.

En forma optativa pueden atribuirse a cada usuario privado una clase de servicio o derechos y privilegios especiales. Otra opción consiste en que el usuario privado tenga acceso desde su red privada a cualquier punto de la red, conservando, previa autenticación, su clase de servicio o sus derechos y privilegios especiales".

Descripción No. 2:

" Este servicio permite el uso de recursos de la red pública para proporcionar capacidades de red privada sin utilizar necesariamente recursos de red especiales. Las líneas de abonado conectadas con distintas conmutaciones de la red, constituyen una red privada virtual que puede incluir capacidades de red privada, como restricciones de marcación, plan de numeración privado, retención, transferencia de llamadas, etc.

Un PNP puede proporcionar a un grupo de usuarios la capacidad de efectuar llamadas utilizando secuencias de dígitos que tienen estructuras y significados distintos a los proporcionados por el plan de numeración público; otra posibilidad es que la VPN utilice las secuencias de dígitos, las estructuras y el significado del plan de numeración público".

Descripción No. 3 :

" El servicio VPN permite a un abonado definir y utilizar un plan de numeración privado para comunicar a través de una o más redes entre interfaces de acceso de usuario designados. Una PNP proporciona a un grupo de usuarios la capacidad de efectuar llamadas utilizando secuencias de dígitos que tienen estructuras y significados distintos a los proporcionados por el plan de numeración público".

3.1.1.2. Descripción de las Características de Servicio del CS-1

Cada servicio está relacionado con un grupo de características del servicio previstas por el CS-1, las cuales pueden ser primordiales (fundamentales para el servicio) o pueden ser opcionales (mejoran el servicio).

En la *Tabla 3.1.* se exponen todas las características que se pueden definir para conformar el servicio VPN.

CARACTERISTICAS DEL SERVICIO DEFINIDAS EN EL CS-1 PARA VPN		
Marcación abreviada	ABD	O
Asistencia	ATT	O
Autenticación	AUTC	O
Código de Autorización	AUTZ	O
Distribución de Llamadas	CD	O
Retención de Llamadas con Anuncio	CHA	O
Consignación de Llamadas	LOG	O
Cola de Llamadas	QUE	O
Transferencia de Llamadas	TRA	O
Grupo cerrado de usuarios	CUG	O
Llamadas en consulta	COC	O
Gestión del perfil de abonado	CPM	O
Anuncio grabado especial	CRA	O
Tono de llamada especial	CRG	O
Desviación "Sígame"	FMD	O
Acceso fuera de la red	OFA	O
Llamadas fuera de la red	ONC	O
Avisador de Número de Origen	OUP	O
Plan de Numeración Privado	PNP	P
Encaminamiento cronodependiente	TDR	O

P: Primordial O: Opcional.

Tabla 3.1. Características de servicio del CS-1 que definen VPN

Marcación abreviada (“Abbreviated Dialling” - ABD)

Descripción No.1:

“Esta característica permite definir números de marcación abreviada en un servicio VPN. Para los usuarios del VPN, los números de marcación abreviada no están sujetos a restricciones de llamada, por ejemplo, un usuario VPN tal vez no pueda tener acceso a la característica de servicio de llamada fuera de la red, pero puede alcanzar el número fuera de red mediante esta característica”.

Descripción No.2:

“Es una característica que permite definir secuencias de dígitos de marcación abreviada para representar la secuencia de dígitos de marcación real, esto es, una secuencia de dos dígitos puede representar una secuencia completa de marcación para un plan de numeración privado o público”.

Descripción No.3:

“Esta característica de servicio es una característica de línea de origen que permite a los abonados empresariales marcar el teléfono de otros abonados de su sociedad utilizando un número reducido, incluso en el caso en que la línea del usuario llamante y la línea del usuario llamado estén servidas por distintas conmutaciones”.

Asistencia (“Attendant” - ATT)

“Esta característica de servicio permite a los usuarios VPN tener acceso a una posición de asistencia dentro de la VPN a fin de proporcionar información de servicio VPN (por ejemplo, números VPN). Puede tenerse acceso a la asistencia marcando un código de acceso especial”.

Autenticación (“Authentication” - AUTC)

“Esta característica de servicio permite verificar si se autoriza al usuario a ejercer ciertas opciones en una red telefónica. En otras palabras, la petición efectuada por el usuario es auténtica y debe concederse”.

Código de autorización (“Authorization Code” - AUTZ)

“Esta característica de servicio permite al usuario VPN anular las restricciones de llamada de la estación VPN desde la que se efectúa la llamada. Pueden asignarse distintos conjuntos de privilegios de llamada a diferentes códigos de autorización y múltiples usuarios pueden compartir un determinado código de autorización”.

Distribución de llamadas (“Call Distribution” - CD)

“Esta característica de servicio permite al usuario servido especificar el porcentaje de llamadas que ha de distribuirse entre dos o más destinos. También pueden aplicarse otros criterios a la distribución de llamadas dirigidas a cada destino”.

Retención de llamadas con anuncio (“Call Hold with Announcement” - CHA)

“La característica de servicio de retención de llamada con anuncio permite al abonado colocar una llamada en retención con las opciones de difundir música o anuncios especiales a la parte retenida”.

Consignación de llamadas (“Call Logging” - LOG)

“Esta característica de servicio permite establecer un registro cada vez que se recibe una llamada en un número telefónico especificado”.

Cola de llamadas (“Call Queuing” - QUE)

Descripción No.1:

“Esta característica de servicio permite al usuario servido colocar en cola las llamadas que se encuentran con un destino ocupado y conectarlas tan pronto como se detecta la situación de libre. Una vez incorporado a la cola, el abonado llamante oye un anuncio inicial que le informa de que se responderá la llamada cuando esté disponible la línea”.

Descripción No.2:

“Es una característica de servicio que permite al abonado en el caso de que la llamada encuentre un elemento desencadenante terminal, como en la situación de ocupado o el sonido de un número determinado de tonos, introducir la llamada en una cola, enviando un anuncio especial a la parte llamante”.

Transferencia de llamadas (“Call Transfer” - TRA)

“La característica de servicio de transferencia de llamadas permite al abonado colocar una llamada en retención y transferir la llamada a otro emplazamiento”.

Grupo cerrado de usuarios (“Closed User Group” - CUG)

“Esta característica de servicio permite al usuario ser miembro de un conjunto de usuarios VPN que están normalmente autorizados a realizar y/o recibir llamadas sólo dentro del grupo. Un usuario puede pertenecer a más de un CUG. Así, un CUG puede definirse en el sentido de que ciertos usuarios puedan efectuar llamadas hacia fuera del CUG o recibir llamadas desde dentro del CUG, o ambas posibilidades”.

Llamadas en consulta (“Consultation Calling” - COC)

“La característica de servicio de llamada en consulta permite a un abonado situar en retención a una llamada a fin de iniciar una nueva llamada para consultar”.

Gestión del perfil de abonado (“Customer Profile Management” - CPM)

“Esta característica de servicio permite al abonado gestionar en tiempo real su perfil de servicio, esto es, los destinos terminales, los anuncios grabados que han de escucharse, la distribución de las llamadas, etc.”

Anuncio grabado especial ("Customised Recorded Announcement" - CRA)

"Esta característica de servicio permite dirigir una llamada a un anuncio de terminación (adaptado al abonado) en lugar de a una línea de abonado. El usuario servido puede definir distintos anuncios para las llamadas infructuosas por diferentes motivos (por ejemplo, la persona llama fuera de las horas de oficina, todas las líneas están ocupadas)".

Tono de llamada especial ("Customised ringing" - CRG)

"Esta característica de servicio permite al abonado atribuir un tono de llamada distinto a una lista de partes llamantes".

Desviación "Sígame" ("Follow-Me-Diversion" - FMD)

Descripción No.1:

"Esta característica de servicio permite a un usuario VPN modificar el número de encaminamiento de su código VPN por intermedio de un teléfono DTMF. El número actualizado puede ser otro código VPN o un número RTPC".

Descripción No.2:

"Gracias a esta característica de servicio, un usuario puede registrar las llamadas entrantes en cualquier acceso terminal. Una vez registradas, todas las llamadas entrantes dirigidas al usuario se presentarán a ese acceso terminal. Un registro de las llamadas entrantes anulará cualquier registro previo. Varios usuarios pueden registrar simultáneamente las llamadas entrantes dirigidas al mismo acceso terminal. El usuario puede también eliminar explícitamente el registro de las llamadas entrantes".

Acceso fuera de red ("Off-Net- Access" - OFA)

"Esta característica de servicio permite a un usuario VPN tener acceso a su VPN desde cualquier estación que no sea VPN de la red telefónica pública con conmutación utilizando un número de identificación personal (PIN). Pueden asignarse distintos conjuntos de privilegios de llamada a diferentes PIN y múltiples usuarios pueden compartir un PIN determinado".

Llamadas fuera de red ("Off-Net-Calling" - ONC)

"Esta característica de servicio permite al usuario llamar fuera de la red VPN. También se consideran fuera de la red las llamadas dirigidas por un VPN a otro".

Avisador de usuario de origen (“Originating User Prompter” - OUP)

Descripción No.1:

“Esta característica de servicio permite al usuario servido proporcionar un anuncio que pedirá al llamante que marque un dígito o una serie de dígitos por medio de un teléfono de doble tono en multifrecuencia (“Dual-Tone Multi-Frequency” - DTMF) o un generador. Los dígitos recogidos proporcionarán información adicional que puede utilizarse para el encaminamiento directo o como verificación de seguridad durante el tratamiento de la llamada”.

Descripción No.2:

“Esta característica de servicio permite dirigir a la parte llamada un anuncio especial, en el que se le puede pedir que marque una numeración adicional (por ejemplo, por intermedio del DTMF) o una instrucción vocal, que utilizará la lógica de servicio para continuar el tratamiento de la llamada”.

Plan de numeración privado (“Private Numbering Plan” - PNP)

“Esta característica de servicio permite al abonado mantener un plan de numeración dentro de su red privada, que es distinto del plan de numeración público”.

Encaminamiento cronodependiente (“Time Dependent Routing” -TDR)

Descripción No.1:

“Esta característica de servicio permite al abonado aceptar o rechazar una llamada y, en caso de aceptación, encaminar esta llamada conforme a la hora, el día de la semana y la fecha”.

Descripción No.2:

“Es una característica de servicio que permite al usuario servido aplicar distintos tratamientos de la llamada basándose en la hora del día, el día de la semana, el día del año, días festivos, etc.”

3.1.2. CONJUNTO DE CAPACIDADES 2 (CS-2)

El Conjunto de Capacidades 2 de RI, es la segunda etapa normalizada de la Red Inteligente, formada por las Recomendaciones Q.122x de la UIT-T aprobadas en Septiembre de 1997.

En el CS-2 de RI se han identificado tres tipos de servicios: servicios de telecomunicación, servicios de gestión de servicios y servicios de creación de servicios. Los dos últimos tipos de servicios se presentan por primera vez en el CS-2 de RI.

El CS-2 adiciona soporte para movilidad (independencia del acceso del usuario e independencia del terminal) y servicios de banda ancha y facilita la interconexión de servicios inteligentes a través de múltiples proveedores de servicios.

CS-2 introduce "Manejo de Participantes en la llamada" (Call Party Handling), que es la capacidad para adicionar y retirar participantes de una llamada en la mitad de la llamada.

En el grupo de servicios de telecomunicaciones definidos por el CS-2, se especifica el servicio de Red Virtual Global (GVNS), el cual es una extensión del servicio de Red Privada Virtual definido por el CS-1.

3.1.2.1. Descripción del Servicio GVNS

El Servicio de Red Virtual Global (GVNS, global virtual network service) es un servicio de Red Privada Virtual conmutada global sustentada por múltiples redes (por ejemplo, ofrecida a los clientes por la RTPC y/o la RDSI).

El estándar CS-2 habilita a las VPNs conmutadas de circuitos para que se extiendan a múltiples países y redes de operadores. Un número de características de CS-2 soportan los servicios de interconexión. Estos protocolos incluyen la capacidad para enrutar números de cobro revertido automático (toll-free freephone), comunicación de información de tasación e identificación de operadores involucrados en la llamada a través de múltiples redes, entre otros.

3.1.2.2. Descripción de las Características de Servicio del CS-2

El conjunto previsto de características de servicios de telecomunicación del CS-2 de RI, está compuesto por 64 características, de las cuales aproximadamente 25 pueden ser definidas para conformar el servicio GVNS. (Ver *Tabla 3.2.*)

A continuación se presenta la definición de algunas de las características de servicio que conforman el servicio GVNS. Las definiciones de las características de servicio que no aparecen a continuación, pueden ser encontradas en la Recomendación Q.1221 de la UIT-T "Introducción al Conjunto de Capacidades 2 de Red Inteligente".

Autenticación de usuario ("User Authentication" - UAUT)

Esta característica confirma la identidad del usuario a la red y la identidad de la red al usuario. UAUT se efectúa durante interacciones entre la red y un usuario.

UAUT supone que se intercambia información apropiada entre la red y el usuario. El usuario tiene que proporcionar sus datos de autenticación a través del terminal o por un

dispositivo de acceso, que transmite los datos a la red y establece una conexión entre la red y el usuario.

CARACTERISTICAS DEL SERVICIO DEFINIDAS EN EL CS-2 PARA GVNS	
Autenticación de usuario	UAUT
Registro de usuario	UREG
Respuesta segura	SANSW
Nueva llamada antes de la liberación	FO
Autorización de origen (de la llamada) flexible	FOA
Autorización de terminación (de la llamada) flexible	FTA
Retención de llamada	HOLD
Recuperación de llamada	CRET
Transferencia de llamada	CT
Alternación de llamadas	CTOG
Tasación por uso de característica	FUC
Servicios a petición	SOD
Identificación de servicio entre redes	INSI
Indicador de tasa entre redes, hacia delante	INRI-F
Indicador de tasa entre redes, hacia atrás	INRI-B
Tasación flexible en tiempo real	RTFR
Identificación de empresa de telecomunicaciones de origen	OCI
Identificación de empresa de telecomunicaciones de destino	OTC
Selección de facilidad especial	SFS
Encaminamiento de llamada personalizado con red pública	CCR-PU
Encaminamiento de llamada personalizado con clientes	CCR-CU
Encaminamiento de llamada personalizado con red privada	CCR-PR
Interrogación de perfil de servicio entre redes	ISPI
Modificación de perfil de servicio entre redes	ISPM
Transferencia de perfil de servicio entre redes	ISPT

Tabla 3.2. Características de servicio del CS-2 que definen GVNS

UAUT supone el uso de algoritmos de seguridad para comprobar la validez de la información proporcionada por el usuario. Una vez efectuada la validación, la red visitada pudiera mantener el seguimiento del usuario autenticado para evitar el uso múltiple de UAUT.

Una Red VPN debería garantizar que múltiples llamadas de acceso conmutadas utilizando el mismo perfil de autorización de usuario no estén en progreso simultáneamente, siendo esto un indicador de la presencia de fraude.

Autorización de origen (de una llamada) flexible ("Flexible (call) origination authorization" – FOA)

La característica FOA puede tener efecto inmediatamente antes de que un conmutador RI autorice el origen de la llamada, durante el proceso de establecimiento de la llamada. Un algoritmo personalizado, proporcionado por el proveedor de la red o por el abonado, puede determinar si se debe originar o no la llamada.

Si la llamada no está autorizada por el algoritmo personalizado RI, se termina el intento de llamada. Si la llamada está autorizada por el algoritmo personalizado RI, dependiendo del perfil del abonado a la característica, el procesamiento de la llamada puede prescindir de la autorización basada en el conmutador o puede continuar con la autorización basada en el conmutador.

La característica FOA puede ser utilizada por servicios de movilidad personal y de terminal, para proporcionar la capacidad de autorización cuando un conmutador impone restricciones a la autorización de hacer una llamada. Estas restricciones podrían ser la consecuencia de una característica de cribado de llamadas basada en el conmutador, en nombre del abonado "titular" de una línea de acceso dada.

Existe la posibilidad de que un usuario móvil pueda transitar a esta línea de acceso, en cuyo momento es posible que haya que suprimir las restricciones.

Autorización de terminación (de llamada) flexible ("Flexible call termination authorization" – FTA)

La característica FTA puede tener efecto inmediatamente antes de que un conmutador RI autorice la terminación de la llamada, durante el proceso de establecimiento de la llamada. Un algoritmo personalizado, proporcionado por el proveedor de red o por el abonado, puede determinar si se debe autorizar o no la llamada.

Si la llamada no está autorizada por el algoritmo personalizado RI, se termina el intento de llamada. Si la llamada está autorizada por el algoritmo personalizado RI, de acuerdo con el perfil del abonado a la característica, el procesamiento de la llamada puede prescindir de la autorización basada en el conmutador o puede continuar con la autorización basada en el conmutador.

La característica FTA puede ser usada por servicios de movilidad personal y del terminal para proporcionar la capacidad de autorización cuando un conmutador impone restricciones a la autorización de terminación de llamada. Estas restricciones podrían ser la consecuencia de una característica de cribado de llamadas basada en el computador, en nombre del abonado "titular" de una línea de acceso dada. Existe la posibilidad de que un usuario móvil pueda transitar a esta línea de acceso, en cuyo momento es posible que haya que suprimir las restricciones.

FOA y FTA ocurren en cualquier tiempo antes del punto cuando un conmutador RI autorizaría un intento de llamada. Estas características permiten a un proveedor de servicios o a un usuario empresarial definir algoritmos personalizados no estandarizados.

Respuesta segura ("Secure answering" - SANSW)

La respuesta segura es una característica por la cual el abonado / usuario del servicio requiere que las llamadas entrantes no puedan ser respondidas a menos que la parte que responde se autentique satisfactoriamente primero como el abonado deseado.

El uso de esta características se relaciona estrictamente con los requisitos de privacidad del abonado / usuario de un servicio; aunque se ha considerado solamente en la descripción de UPT, podría ser útil también para otros servicios, por ejemplo, Cobro Revertido Automático, Red Privada Virtual y UMTS.

Encaminamiento de llamada personalizado con redes públicas ("Customised call routing with public networks" - CCR-PU)

Esta característica de servicio permite a una red pública acceder a otras redes públicas para información de procesamiento y encaminamiento de la llamada. De acuerdo con las necesidades del abonado, la red pública accesada determina el destino apropiado de cada llamada entrante, que podrá ser un número telefónico local, nacional o internacional.

Esta acción permanecerá bajo el control único de la red pública accesada, que proporciona la actualización conveniente, así como la confidencialidad. La característica de servicio CCR puede ser proporcionada como una característica del activador de origen o de destino.

Encaminamiento de llamada personalizado con clientes ("Customised call routing with customers" - CCR-CU)

Esta característica de servicio permite a la red pública acceder a sistemas de clientes para información de procesamiento y encaminamiento de la llamada. El sistema accesado (que puede ser una red privada, simple base de datos, centralita automática privada, o un terminal) determina el destino apropiado de cada llamada entrante, que podrá ser un número telefónico local, nacional o internacional.

Esta acción permanecerá bajo el control único del sistema accesado, que proporciona la actualización conveniente, así como la confidencialidad. La característica de servicio CCR puede ser proporcionada como una característica del activador de origen o de destino.

La característica CCR permite a una red acceder otra red pública o privada para completar una llamada. La red accedida tiene entonces control completo de la llamada desde ese punto en adelante, teniendo en cuenta la actualización conveniente de otras características como reenvío de llamadas (call forwarding), cribado (screening), o enrutamiento definido de usuario (user-defined routing).

3.1.3. CONJUNTO DE CAPACIDADES 3 (CS-3)

El Conjunto de Capacidades 3 de RI, corresponde a la tercera etapa normalizada de la Red Inteligente, formada por las Recomendaciones Q.123x de la UIT-T aprobadas en Diciembre de 1999. A diferencia de los dos Conjuntos de Capacidades anteriores, el CS-3 no provee sustancialmente nuevas funcionalidades, sino una versión revisada de CS-2.

El CS-3 ofrece soporte para servicios mejorados de redes móviles y usuarios UPT sobre Redes de Banda Ancha y para la integración con RDSI-BA. Los servicios de banda ancha soportados son Conversación en Banda Ancha (p.e. videoconferencia de banda ancha, vigilancia por video, videotelefonía) y Recuperación de Banda Ancha (p.e. video a la carta).

Adicionalmente, el CS-3 permite el "Manejo de Participantes en la Llamada" en Redes de Banda Ancha, soporta servicios con múltiples puntos de control y aborda algunos aspectos básicos de la interoperabilidad de servicios y aplicaciones de Redes IP y servicios y características de Redes Inteligentes.

El CS-3 no ofrece definiciones para nuevos servicios, pero contiene nuevas características de servicio y capacidades de red que junto con las características de servicio definidas en el CS-2, sirven para identificar y verificar los servicios de referencia del CS-3 antes mencionados.

A continuación se presentan algunas características de servicio y capacidades de red que complementan los servicios VPN y GVNS definidos en CS-1 y CS-2.

3.1.3.1. Descripción de las Características de Servicio del CS-3

Las definiciones de las características de servicio presentadas en CS-3 son un poco diferentes de las proporcionadas en los Conjuntos de Capacidades anteriores y en la Recomendación Q.1290.

Las características de servicio describen la capacidad desde el punto de vista del usuario, y son aplicables no sólo a los usuarios finales del servicio sino también, a todos los usuarios de la red inteligente, entre los que se cuentan los operadores de red o los proveedores de servicios de red.

En la *Tabla 3.3.* se presentan las características de servicio relacionadas con el servicio de Red Privada Virtual. Se adiciona la columna "Usa NC" para indicar las Capacidades de Red (NC - *Network Capabilities*) requeridas para realizar dicha Característica de Servicio.

Tratamiento de selección de operador ("carrier selection handling" – CSHND)

En el caso de llamadas iniciadas en la RI y de llamadas iniciadas en el terminal que son tratadas en la RI, se podrá controlar la selección del operador. El control se puede hacer llamada por llamada, por abonado o por defecto. Esta característica es una extensión de una capacidad del CS-2 RI.

CARACTERISTICAS DE SERVICIO DEFINIDAS EN EL CS-3		
Nombre	**Referencia**	**Usa NC**
Tratamiento de selección de operador	CSHND	CAIDT
Indicador de servicio entre redes	INSIN	IEBSL
Interfaz con el nodo VPN	VPNNI	VPNNO VPNCO

Tabla 3.3. Características de servicio del CS-3

Indicador de servicio entre redes ("inter-network service indicator" – INSIN)

En una llamada entre redes, permite a la red destinataria recibir de la red originadora una indicación del servicio usado para la llamada recibida. No se especifica el contenido de indicador de servicio, lo que significa que el mecanismo exige acuerdo mutuo o se puede crear en un dominio.

Interfaz con el nodo VPN ("VPN node interface" - VPNNI)

Las redes privadas (por ejemplo, PBX) pueden intercambiar información VPN por medio de la señalización de la red pública (a través del mecanismo de transporte de protocolo de aplicación de la ISUP). Los proveedores de servicio vigilarán y controlarán el uso de esta capacidad.

La red privada puede terminar el contexto PINX (PBX) VPN y proporcionar la funcionalidad PINX (PBX) pasarela de salida, según la funcionalidad que soporta (o que debe llegar a) la parte llamada o, por ejemplo, el tipo de abono.

3.1.3.2. Descripción de las Capacidades de Red del CS-3

Las Capacidades de Red describen capacidades que permiten el acceso y el control de servicios basados en la red. Estas capacidades son descritas desde el punto de vista de la red. Por ejemplo, si un usuario desea dejar un mensaje a un abonado que no contesta el teléfono (característica de servicio), entonces la red tendrá la capacidad de conectar un anuncio a una llamada (capacidad de red).

Las capacidades de red del CS-3 soportan el conjunto de servicios de referencia y las características de servicio del CS-3. Estas capacidades se pueden usar también para soportar otros servicios que pueden, o no, estar normalizados por el UIT-T.

En la *Tabla 3.4.* se presentan las Capacidades de Red relacionadas con el servicio de Red Privada Virtual. Se adiciona la columna "Usada por SF/BS" para indicar las características de servicio (SF, service features) y los servicios básicos (BS, benchmark services) realizados por esa capacidad de red.

CAPACIDADES DE RED DEFINIDAS EN EL CS-3		
Nombre	**Referencia**	**Usa NC**
Transferencia de identificación de operador	CAIDT	CSHND
Intercambio de información entre programas de lógica de servicio	IEBSL	INSIN
Notificación red privada virtual	VPNNO	VPNNI
Control de VPN	VPNCO	VPNNI

Tabla 3.4. Capacidades de red del CS-3

Transferencia de identificación de operador ("carrier identification transfer" – CSHND)

Cuando la red solicita a la RI el soporte de establecimiento de conexión, y cuando la RI le pide a la red que establezca la conexión, se podrá transferir cierta información de identificación de operador. Esta capacidad ya existe en el CS-2, pero es una mejora derivada de la mejora de la ISUP.

Intercambio de información entre programas de lógica de servicio ("information exchange between service logic programs" – CRCDR)

Esta capacidad posibilita el intercambio de información entre diferentes programas de lógica de servicio (SLP), que se invocan uno a continuación del otro en la llamada. Los SLP pueden estar ubicados en SCP diferentes, y también SSP diferentes pueden invocarlos.

No se supone que los SLP tengan conocimiento de que hay otros funcionando, pero pueden mandar información genérica hacia delante o hacia atrás en caso de que otro SLP esté activo y sea capaz de entender la información. Esto se puede usar en la información de interacción (por ejemplo, cuando se prohíben redireccionamiento o reenvío de llamada) o en la información de tasación (por ejemplo, cuando se invoca el servicio con recargo una vez autorizada la tarjeta de crédito).

Notificación red privada virtual ("VPN notification" – VPNNO)

Una SSF podrá notificar a la SCF, que proporciona un servicio red privada virtual (VPN, virtual private network) por red inteligente, que el uso de la capacidad de red de transportar las mejoras de señalización PSS1 (conocido como Q.SIG) con respecto a la llamada básica está presente en el mensaje de petición de llamada recibida.

Control de VPN ("VPN control" – VPNCO)

Una SCF que proporciona el servicio red privada virtual (VPN) por RI podrá ordenar a la SSF que prohíba o permita la utilización de la capacidad de red de transportar las mejoras

de señalización PSS1 con respecto a la llamada básica. Si se usa este control, la VPN con PSS1 APM se termina correctamente y la SCF y la SSF cooperarán para proporcionar la funcionalidad PINX (PBX) pasarela de salida según los flujos de información PSS1. Si este control no se utiliza, la funcionalidad por defecto es Transit PBX.

3.1.4. CONJUNTO DE CAPACIDADES 4 (CS-4)

El Conjunto de Capacidades 4 corresponde a la cuarta etapa normalizada de la Red Inteligente, formada por las Recomendaciones Q.124x de la UIT-T aprobadas en Septiembre de 2001.

Esta versión mejora las características CS-3 existentes. Ofrece avanzada Portabilidad de Número, Movilidad, Banda Ancha y se enfoca principalmente en el soporte de RI para VoIP y para interoperabilidad con redes IP.

El nuevo CS-4 habilita una variedad de servicios básicos (p.e. High Quality Audio, High Bandwith Audio) y servicios suplementarios (p.e. Llamada en espera, Grupo Cerrado de Usuarios, Transferencia de llamadas) existentes, definidos por la UIT-T, para ahora ser proporcionados a clientes de VoIP, con la flexibilidad necesaria para adicionar nuevos ser vicios que puedan llegar a estar disponibles en el futuro.

El CS-4 cubre muchos aspectos de la interoperabilidad entre servicios y aplicaciones de redes IP y servicios y características de RI. Estos aspectos incluyen el acceso de capacidades de RI desde Gatekeepers H.323, Servidores Proxy SIP/SDP y Servidores de Llamadas (Call Servers) basados en la arquitectura H.248, Funciones de Control de Gateway, Soporte de señalización para servicios de Internet, APIs (Interfaz de Programa de Aplicación – *Application Program Interface*) basados en plataformas CORBA (Arquitectura común para gestores de solicitudes a objetos) y JAVA (lenguaje de programación orientado a objetos) y funcionalidad de Softswitch.

Con relación al servicio VPN, el CS-4 incluye solamente una característica de servicio (SCUGC) y una capacidad de red (CUGC) que definen que los programas de la Lógica de Servicio pueden influenciar la ejecución de los servicios CUG (Grupo Cerrado de Usuarios).

3.2. EJECUCION DEL SERVICIO

La operación básica de una Red Privada Virtual no es compleja. El servicio VPN es implementado usando una base de datos provista por el operador de la red, localizada en los SCPs y llamada Base de Datos del Servicio Comercial *(Business Service DataBases - BSDB).* En la *Fig. 3.1.* se pueden observar las entidades físicas de la Red Inteligente

implicadas y cada uno de los pasos básicos en la ejecución del Servicio Red Privada Virtual.

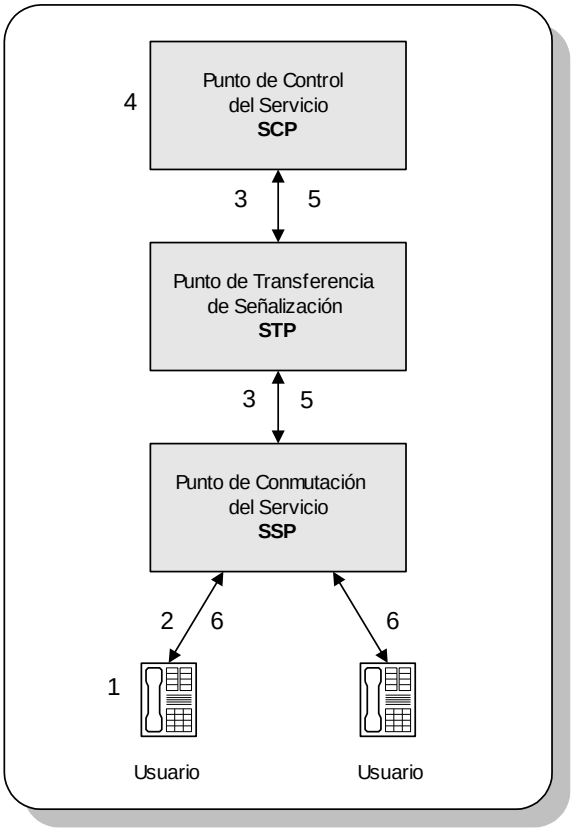


Fig. 3.1. Entidades Físicas relacionadas con la Ejecución del Servicio

1. Cuando se origina una llamada VPN la red pública identifica la llamada como destinada a la Red Privada Virtual. Esto se puede hacer mediante:
    - Identificación de la línea donde se origina la llamada cuando el equipo local del cliente (CPE - *Customer Premises Equipment*) es descolgado.
    - Marcación de un Código de Acceso al Servicio (SAC - *Service Access Code*).
    - Marcación de un número específico por parte de un usuario de acceso remoto.

2. La central que da acceso al usuario detecta que la llamada efectivamente corresponde a una solicitud para el servicio VPN y se comunica con la central más cercana equipada adecuadamente con un SSP para que él decida que hacer con la llamada.

3. El SSP suspende el procesamiento normal de la llamada y envía una pregunta al SCP solicitando instrucciones para el procesamiento de la llamada. Algunos de los datos enviados en el mensaje de pregunta y que serán utilizados como clave para la búsqueda, son:

- El código de acceso marcado.
- La línea identificada.
- Identificación Automática de Número *(ANI - Automatic Number Identification).*
- El Número de Identificación Personal *(PIN - Personal Identification Number).*

4. El SCP consulta la base de datos de la VPN (BSDB), en la cual se almacenan las características particulares del servicio para los clientes individuales, codificadas como *Registros de procesamiento de la llamada (CPRs).* Por seguridad, la base de datos BSDB debe ser desplegada en parejas. Cada BSDB de la pareja contiene el mismo conjunto de registros CPRs, pero el STP enruta las llamadas con cierta dirección de origen a una BSDB y las llamadas con otra dirección de origen, a la otra BSDB. Si una BSDB falla, los STPs redireccionan el tráfico a la otra BSDB. Los datos en las BSDBs de los SCPs son administrados por el SMS.

5. El SCP envía un mensaje de respuesta al SSP indicando si la llamada debe ser o no completada, con la siguiente información:
   - Información de enrutamiento para el establecimiento de la llamada. Esto a su vez puede incluir:
     - Información sobre rutas preferidas y alternativas.
     - Destino alternativo dependiendo de la hora, del día o del mes.
   - Información hacia adelante de la llamada.
   - Información de carga y opciones de facturación para clientes particulares.
   - Información para identificar cualquier restricción sobre la llamada o sobre los números llamados.
   - Códigos de autorización para acceso a facilidades especiales.

6. El SSP recibe las respuestas del SCP y enruta la llamada al número de destino definido por el SCP. La llamada es cargada según su duración a ratas específicas obtenidas desde la base de datos analizada.

Las técnicas de señalización por canal común se utilizan para transferir la información relacionada con la llamada entre los conmutadores involucrados en el proceso, así como con la máquina de la base de datos. CCS7 es el sistema de señalización estándar aceptado para este propósito.

3.3. TIPOS DE LLAMADAS EN UNA VPN

Los diferentes tipos de llamadas VPN que se pueden soportar se presentan en la *Fig. 3.2.* La nube interior representa el servicio VPN ofrecido sobre una arquitectura de Red Inteligente y la nube exterior representa la red RTPC / RDSI que sirve de red de acceso para los usuarios del servicio.

Los símbolos de teléfono en la nube interior representan la líneas On-net de la VPN. Todas las líneas en la RTPC / RDSI que no son líneas On-net de la VPN, se denominan líneas Off-net (fuera de la red).

3.3.1. LLAMADA ON-NET – ON-NET

Corresponde a una llamada de un miembro VPN a otro miembro VPN de su propio grupo (On-net hacia On-net). Se origina desde un teléfono o PABX definido como parte de la VPN y el usuario marca un número privado. El SSP detecta que se está haciendo una llamada VPN y consulta al SCP para que le traduzca el número marcado de acuerdo con el plan de numeración privado. El SCP devuelve el número de teléfono normal relacionado con el número privado junto con información sobre como facturar la llamada.

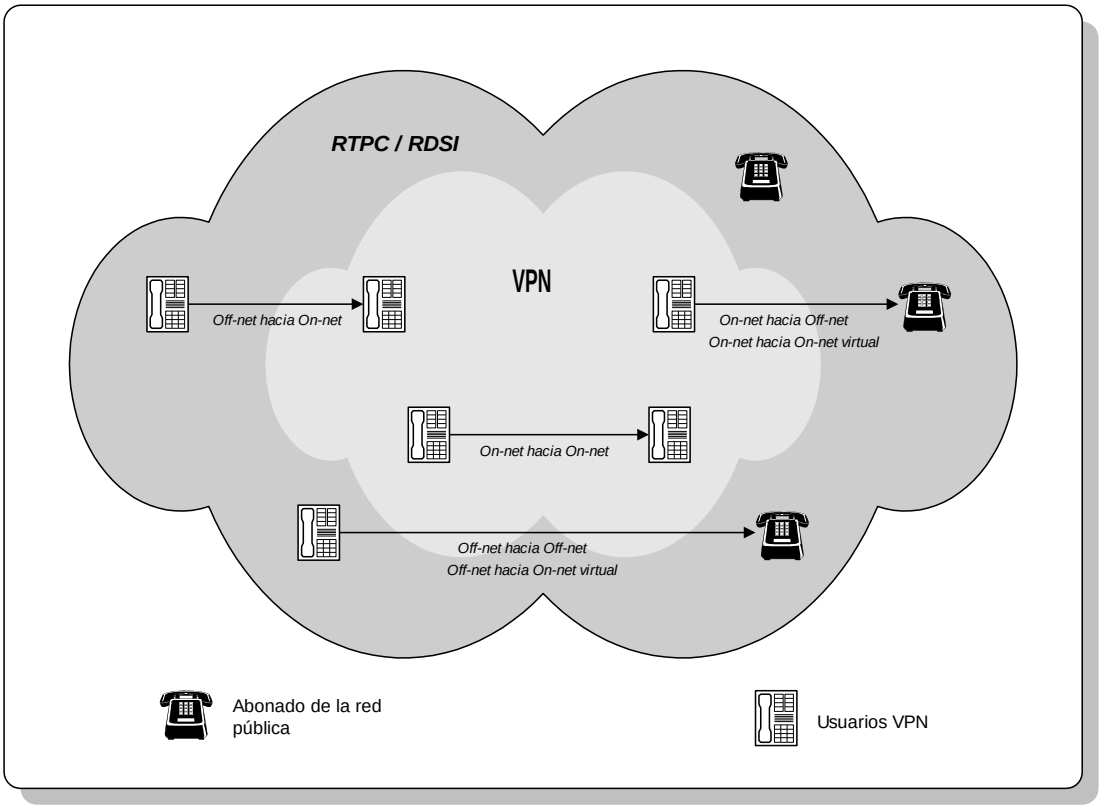


Fig. 3.2. Tipos de Llamadas

3.3.2. LLAMADA ON-NET – OFF-NET

La llamada se hace desde un terminal (teléfono o PABX) definido como parte de la VPN. El usuario marca un código de acceso para la línea externa y luego el número de teléfono externo. El SSP detecta que se está haciendo una llamada VPN y consulta al SCP. Este determina que no es necesaria la traducción del número.

3.3.3. LLAMADA OFF-NET – ON-NET

Una línea on-net puede ser accesada desde una línea off-net en la red pública, después de la autenticación del abonado llamante como usuario VPN. Esta identificación se realiza introduciendo el número del Plan de Numeración Privado (PNP) que tiene asignado y el Número de Identificación Personal (PIN) que lo identifica como un Abonado de Acceso Remoto.

La llamada se hace desde cualquier teléfono que no pertenece a la VPN. El usuario marca un código de acceso y luego el número con el que desea la conexión. De ahí en adelante, la llamada se trata igual que en los casos de llamadas On-net – On-net.

La línea RTPC / RDSI utilizada queda libre de tasas, cargándose el valor de la llamada al abonado del servicio VPN.

3.3.4. LLAMADA OFF-NET – OFF-NET

Un usuario VPN usando una línea off-net en la red pública puede cursar llamadas salientes VPN después de realizar el proceso de autenticación del abonado llamante.

Durante la conexión, la línea RTPC / RDSI se maneja como una línea On-net a través del árbol de enrutamiento de la VPN y la llamada se comporta igual que una llamada On-net – Off-net.

Los usuarios VPN que cuentan con números de la red pública conmutada y números de marcación abreviada del plan de numeración de la red VPN, se conocen como ***Abonados de Acceso Remoto, o Abonados virtuales On-net.*** Tanto los *abonados On-net* como los *abonados Off-net* pueden llamar a los *Abonados virtuales On-net* marcando un número del plan de numeración de VPN.

3.4. METODOS DE ACCESO

Una compañía de telecomunicaciones puede ofrecer una combinación de métodos de acceso a sus clientes, aunque esto depende en gran medida de la arquitectura que se haya adoptado para soportar el servicio.

Los principales métodos de acceso utilizados para originar y finalizar llamadas VPN, a través de una arquitectura de Red Inteligente, son las Líneas Dedicadas (Líneas Privadas) y las Líneas no Dedicadas (Líneas Dial-up Públicas). También se utilizan, pero en menor escala, las Líneas de Grupo Comercial (usadas principalmente por la arquitectura Centrex) y las Líneas de Conexión Directa.

3.4.1. LINEAS DEDICADAS

Las Líneas Dedicadas o Líneas Privadas se utilizan para conectar las instalaciones de los clientes a la VPN. Estas líneas son líneas conmutadas generalmente digitales y pueden ser líneas sencillas (por ejemplo, líneas de una PBX o de una central terminal) o líneas de acceso RDSI tipo primario.

El tráfico RTPC normalmente es soportado por enlaces diferentes a los del tráfico VPN. Sin embargo, en algunas circunstancias, una sola línea dedicada puede soportar llamadas públicas locales así como llamadas VPN, siendo necesario que el tráfico RTPC saliente sea filtrado en la central local (Ver *Fig. 3.3*.).

En caso que el proveedor de la red de acceso sea diferente del proveedor de la red VPN, el proveedor de la red de acceso puede autenticar la identidad de la locación llamante o del usuario final y pasar esta información al proveedor de la red VPN a través de un protocolo de señalización de canal común (SS7 – Signaling System Number 7) asociado con el grupo de troncales conectando las redes.

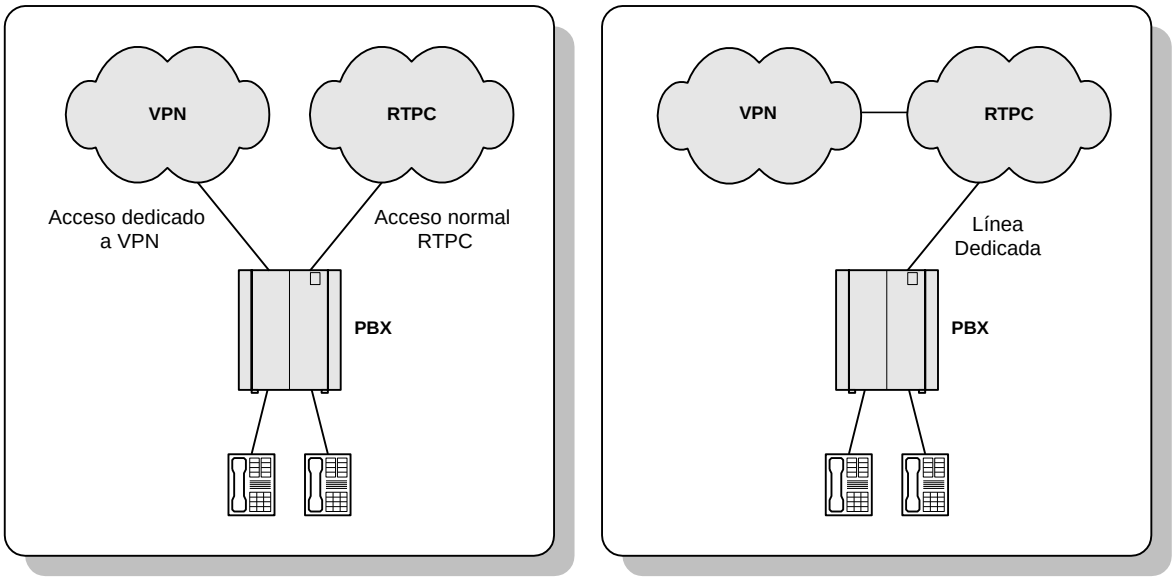


Fig. 3.3. Acceso Dedicado

Los accesos dedicados se utilizan en particular:

- En instalaciones de grandes clientes, donde debido al gran volumen de tráfico, las líneas dedicadas son justificables.
- Para servicio internacional, donde el servicio nacional no es ofrecido y las líneas dedicadas deben transportar el tráfico directamente hasta la entrada internacional.
- En los sitios donde el servicio local y el servicio de larga distancia son prestados por diferentes operadores. En este caso, el enlace al acceso dedicado lo proporciona la compañía de teléfonos local y es terminado sobre el **Punto de Acceso VPN** del portador de larga distancia. Un *Punto de Acceso VPN* (POP - Point of Presence)**,** corresponde a un conmutador que provee la interfaz entre una red VPN y una red

pública. Esto significa, que al menos un *Número de Llamada* (DN - Directory Number) debe ser asignado en una red pública para hacer el enrutamiento de una llamada privada dentro de una red pública.

Los accesos dedicados son utilizados también en las redes Overlay, donde una nueva infraestructura de red ha sido implementada para soportar el servicio VPN tanto de voz como de datos. Las líneas dedicadas de acceso para este tipo de redes pueden ser líneas de acceso RDSI tipo primario, o enlaces a una red de datos Frame Relay, IP o ATM. La relación de VPN con las redes de datos será explicada en el Capítulo 4.

3.4.2. LINEAS NO DEDICADAS

Es una forma de acceso usada por usuarios que realizan llamadas desde teléfonos que no pertenece a la VPN (llamadas off-net, abonados de acceso remoto) o para sitios pequeños de una compañía donde no se justifica arrendar líneas dedicadas.

La PBX o el usuario marcan un prefijo especial que identifica la llamada como VPN, en este momento se adelanta la llamada sobre el *Punto de Acceso VPN* de la compañía de telecomunicaciones seleccionada, como se puede ver en la *Fig. 3.4.* Se le indica entonces a la persona que llama que marque un código de autorización especial.

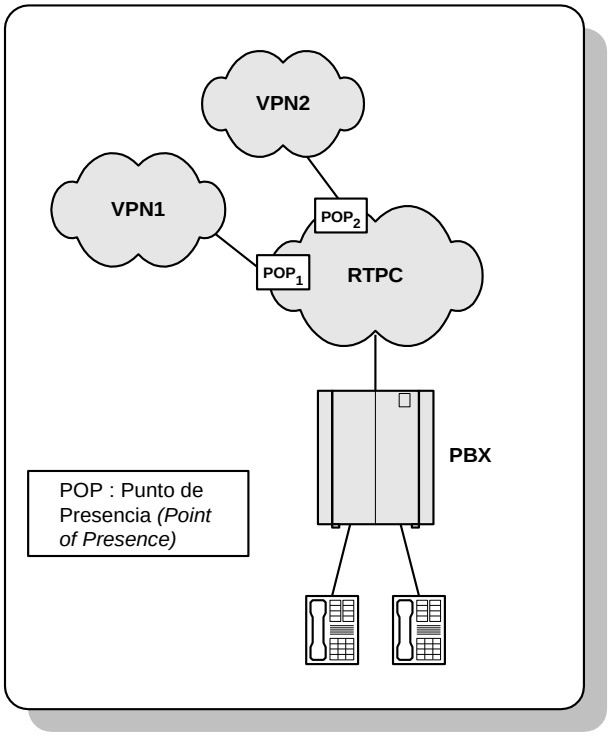


Fig. 3.4. Acceso Indirecto

Se presentan dos formas especiales de acceso indirecto, que pueden ser brindadas por el suscriptor del servicio a sus usuarios:

- *Acceso 800* - Las llamadas desde localizaciones off-net son cargadas a la cuenta de la compañía. La persona que llama marca un número 800 especial, seguido por el código de acceso apropiado y el código de autorización, y de este modo gana acceso a la VPN.
- *Acceso por Tarjeta de Llamada (Calling Card Access)* - Las llamadas desde teléfonos públicos son cargadas a la cuenta de la persona que llama. La tarjeta de llamada también puede almacenar los códigos de autorización y de acceso necesarios, evitando a la persona que llama marcar una larga secuencia de dígitos.

3.4.3. LINEAS DE UN GRUPO COMERCIAL

Un Grupo Comercial puede conformar su propia Red Privada Virtual o hacer parte de una red general. Se determina un plan de numeración para el grupo comercial; así, cuando un abonado realiza una llamada por una línea de un grupo comercial utiliza un prefijo que le ha sido asignado para indicar que es una llamada VPN (por ejemplo, marcando un “8”).

Dentro de esta categoría se puede considerar el servicio CENTREX, que como ya se explicó, integra las características de los conmutadores privados dentro de la red telefónica pública, permitiendo crear grupos de trabajo.

3.4.4. LINEAS POR CONEXION DIRECTA

El operador de la red puede asignar ciertas líneas de conexión directa a la VPN, las cuales habilitan la llamada con sólo descolgar el teléfono o el terminal que esté siendo utilizado. Estas líneas pueden ser asignadas dentro de un grupo comercial.

3.4.5. OTROS ACCESOS

Conexión con PBX

El servicio VPN convierte un número específico de un suscriptor PBX a un adecuado número PBX sobre la red pública. Por consiguiente el PBX debe ser capaz de distinguir una llamada VPN de una llamada por Conexión Directa a Extensiones *(DID - Direct Inward Dialling)* separando las rutas entrantes de la PBX.

El servicio DID, ofrecido sobre la Red Telefónica Pública Conmutada, permite efectuar llamadas sin pasar por una operadora; cada extensión se comporta como una línea telefónica convencional aumentando la capacidad de atención a las llamadas entrantes de

la empresa. El PBX puede recibir llamadas VPN y enrutarlas a una estación destino a través de otra ruta.

La *Fig. 3.5.* permite verificar la diferencia entre una llamada VPN a un suscriptor PBX y una llamada por Conexión Directa a Extensiones (DID) a un suscriptor PBX.

En el primer caso el número 4567 marcado por el usuario de la VPN, corresponde a un número del Plan de Numeración Privado asignado por la Red Privada Virtual a la que pertenece, ya sea en el ámbito local, nacional e internacional. La PBX debe ser capaz de reconocer el número PNP (Plan de Numeración Privado) y enrutar la llamada hasta la extensión asociada con dicho número.

En el caso de una llamada DID al 321-4567 un abonado que no pertenece a la VPN, utiliza un número asignado por la compañía de telecomunicaciones local a una extensión de la PBX, por lo que no es necesario pasar por la operadora.

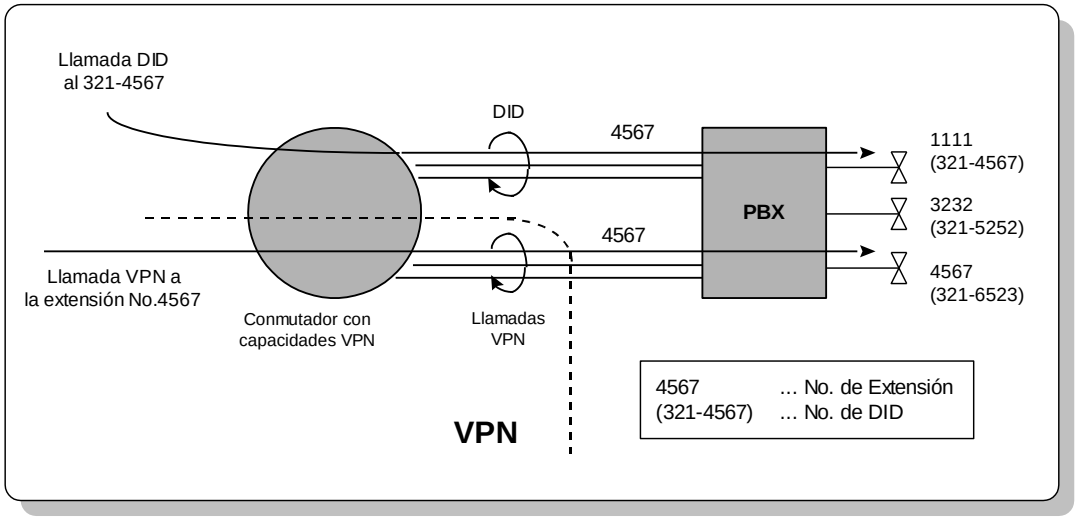


Fig. 3.5. Conexión con PBX

Acceso desde conmutadores no SSP

Los usuarios pueden obtener acceso a través de conmutadores que no cuentan con capacidades SSP (no pertenecen a la VPN) y marcar el código de acceso VPN definido para la red pública. Cuando esto ocurre el conmutador no-SSP determina que es una llamada VPN y la enruta al SSP más cercano. El SSP se encarga de realizar la validación con el SCP para determinar si el abonado llamante puede establecer conexión con algún miembro de la VPN y de allí en adelante se considera como una llamada correspondiente a la Red Privada Virtual.

En la *Fig. 3.6.* se pueden observar los diferentes métodos de acceso que pueden ser utilizados para originar y finalizar llamadas VPN y que fueron explicados anteriormente.

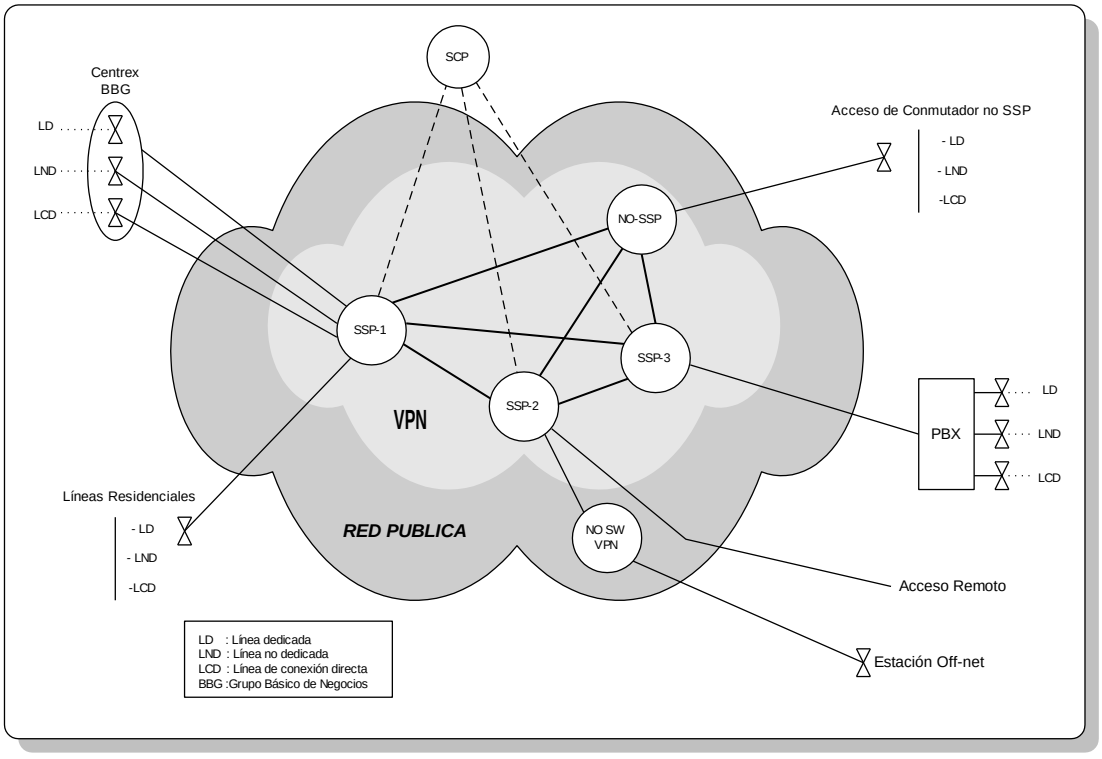


Fig. 3.6. Configuración de VPN

3.5 NUMERACION Y MARCACION

3.5.1 ACCESO AL SERVICIO VPN

Se puede acceder al servicio VPN a través de RDSI/RTPC marcando un número de llamada el cual consta de:

- Código de servicio VPN (3 a 4 dígitos), también se lo puede encontrar como Código de Acceso a la Red VPN.
- Código de identificación VPN (2 a 4 dígitos). Si el usuario pertenece a más de un grupo VPN, el indicador de red privada debe ser marcado.
- Número PNP correspondiente al número asignado al abonado llamado *(Called Party Number - CdPN).*
- Código de Acceso Remoto VPN (Plan de marcación de la red pública), por ejemplo, un código de 1 a 10 dígitos.

El acceso al servicio desde líneas off-net es permitido de una manera similar pero es necesario proporcionar información adicional para propósitos de autenticación:

- Número PNP y PIN del abonado llamante.

En el caso de un grupo comercial, se define un plan de marcación específico de numeración:

- Código de Acceso VPN al Grupo Comercial

3.5.2 PLAN DE NUMERACION PRIVADO

Un número PNP consta de los números decimales 0 a 9. A la hora de crear una VPN, el suscriptor al servicio puede decidir si desea aplicar uno de los siguientes planes de numeración:

- **Plan de numeración uniforme (longitud completa): 2 a 10 dígitos.**
- **Plan de numeración abreviado (números abreviados): 1 a 9 dígitos.**

Todos los números de llamada PNP de longitud completa y todos los números PNP abreviados deben tener la misma longitud, respectivamente, la cual se puede especificar para cada abonado al servicio. Estos números de llamada tienen la misma importancia, es decir, donde se pueda emplear un número de llamada de longitud completa en el plan de numeración, se puede utilizar también un número abreviado. No es necesario que todos los números de llamada abreviados empiecen con la misma cifra. Sin embargo, no se soporta ambigüedad (por ejemplo, 123 como un número abreviado y 1234567 como un número completo).

Además de números de llamada privados para acceder a las líneas internas de la red o líneas de la red virtual, el abonado al servicio tiene que definir "números clave" especiales (códigos) para utilizar otros tipos de llamada VPN. Como estos números también forman parte del plan de numeración privado, tienen que cumplir las condiciones de un número abreviado o de un número completo:

- **"Número clave de salida de la red", código de escape fuera de la red.**
  Este número facilita el acceso del plan de numeración privado al plan de numeración público, o sea, al marcar dicho número, el usuario de la VPN puede marcar un número de llamada público y establecer una comunicación con una línea fuera de la red.

- **"Número clave hacia la red", código de acceso remoto.**
  Este número permite el acceso desde la red pública a la VPN, o sea, al marcar este número y tras la autenticación del abonado que llama, éste obtiene acceso a la VPN. El abonado que llama puede marcar ahora los números del plan de numeración privado. Los números clave de salida de la red y de acceso a la misma pueden ser idénticos.

3.5.3. PROCEDIMIENTO DE MARCACION

En la siguiente descripción, se explica el flujo de información entre el usuario (------) y los anuncios o tonos enviados por el SSP << ----- >>.

1. **Línea dedicada**
   (Número del abonado llamado).
2. **Líneas no dedicadas**
   (Código de acceso a la red VPN) + << Anuncio / Tono >> + (Número del abonado llamado).
3. **Línea del Grupo Comercial**
   (Código de acceso VPN al grupo comercial) + (Número del abonado llamado).
4. **Acceso Remoto**
   (Código de acceso remoto VPN) + << Anuncio / Tono >> + (Número de Llamada de la estación on-net del abonado llamante + PIN) + << Anuncio / Tono>> + (Número del abonado llamado).
5. **Línea de conexión directa**
   El abonado llamante puede originar una llamada VPN a una estación destino predefinida para comenzar a hablar sin necesidad de marcar.

En el ANEXO A se puede observar un ejemplo de un PLAN DE NUMERACION PRIVADO y su aplicación para cada uno de los diferentes tipos de llamadas.

3.6. PROCEDIMIENTOS VPN

3.6.1. SUSCRIPCION AL SERVICIO

Un cliente (Suscriptor del servicio) que desee configurar una VPN debe suscribirse al servicio con el proveedor del mismo. El plan de numeración “on-net”, establecimiento de enrutamientos y suscripciones adicionales del servicio deben ser acordadas entre ambas partes. Después de que la VPN se encuentre en operación, el usuario del servicio debe ser capaz de manejar su propia VPN para extender los acuerdos realizados previamente con el proveedor del servicio.

3.6.2. ACTIVACION / DESACTIVACION / REGISTRO

Después de realizados los acuerdos entre el proveedor y el usuario, el proveedor proporciona el registro inicial de los datos del perfil del suscriptor del servicio en la red, especificando la fecha y hora tanto del inicio como de la finalización de la disponibilidad del grupo VPN.

Los objetos del perfil del usuario están definidos por dos tipos de atributos:

- Atributos bajo la exclusiva responsabilidad del proveedor del servicio (p.e. parámetros de enrutamiento, carga y facturación)

- Atributos que pueden ser modificados tanto por el proveedor como por el suscriptor del servicio (p.e. plan de numeración, marcación abreviada, passwords de seguridad y PIN, parámetros de filtrado y clases de servicios).

El suscriptor puede, por medio de un acceso al SMP (Service Management Point), acceder los objetos específicos del servicio relacionados con su perfil. El acceso al suscriptor del servicio a los cambios a objetos del perfil está sujeto a un chequeo de autorización y a un procedimiento de validación de su acción sobre el objeto.

Cuando el grupo VPN es activado, la persona encargada de la operación en el usuario puede empezar la configuración de la red privada (es decir, asignación de los números privados a los miembros de su VPN).

Datos y parámetros relacionados con el servicio.

Adicionalmente a los datos requeridos para realizar una llamada normal, los siguientes datos y parámetros son necesarios para la definición del servicio y de las funciones de manejo de las llamadas:

- Plan de numeración VPN.
- Número “on-net” de la organización.
- Número “on-net” asociado con usuarios finales del servicio.
- Plan de enrutamiento de las llamadas.
- Localización física (localización en la red pública) de los nodos que conforman la red VPN.
- Opciones de suscripción comunes de VPN; tratamiento del sobreflujo de tráfico, conexión a troncales dedicadas, enrutamiento de punto de origen.
- Suscripciones de los usuarios finales; códigos para ignorar restricciones, códigos de cuenta, niveles de restricción de las llamadas.
- Tipos de líneas de acceso; principales características e identificaciones.
- Listado de los códigos de identificación con sus respectivas ubicaciones, listado de todos los códigos usados, niveles de restricciones definidos para el suscriptor del servicio, etc.
- Puntos privados de entrada y salida de la red.
- Características de los usuarios finales las cuales pueden influir en el escenario de la llamada (es decir, suscriptor RDSI, suscriptor analógico).

3.6.3. ELIMINACION

El suscriptor del servicio puede directamente o a través de su proveedor del servicio, eliminar los objetos bajo su responsabilidad para su grupo VPN.

3.6.4. TARIFICACION

El proceso de tarifación es muy similar para los diferentes tipos de llamadas, puesto que las llamadas off-net son cargadas al abonado que llama y no a la línea RTPC / RDSI desde la cual se origina la llamada.

3.6.4.1. SSP

El operador de la red provee un sistema para recibir, unir y organizar toda la información de tarifación para los servicios VPN. Los detalles de la llamada son identificados en el nivel más bajo de la llamada de origen, es decir, el número de abonado de origen, el número de localización o el código de autorización.

La identificación del abonado es provista por la identificación automática de marcadores externos (AIOD - Automatic Identification of Outward Dialling), la identificación automática del número (ANI) o un código de autorización. En el caso de la Red Digital de Servicios Integrados, se debe proveer la identificación del abonado, como se especifica en la recomendación Q.931 del CCITT.

Al completarse una llamada, el SSP produce un Registro de Contabilización Automático de Mensajes (*AMA - Automatic Message Accounting)* basado en el campo indicador de tarifación del SCP, el cual generalmente es manejado en el SCP.

Los detalles de la llamada incluyen:

- Número del abonado que llama.
- Fecha del mensaje.
- Hora del mensaje de origen.
- Longitud y duración del mensaje, medido en unidades de tiempo y/o facturación.
- Número llamado.
- Código de servicio VPN, indicando el tipo de servicio usado.
- Cargos de uso.

3.6.4.2. SCP

Generalmente el SCP no registra ninguna información de tarifación.

3.6.4.3. SMS

El SMS debe generar información sobre las actividades de sesión del suscriptor del servicio (actualizaciones, número de preguntas, solicitudes de reporte) para el operador de la red, de manera que se pueda generar la información de tarifación.

4. RELACION DE VPN CON OTRAS TECNOLOGIAS

Las telecomunicaciones modernas están entrando en una fase revolucionaria en el ámbito mundial, debido a su convergencia con las tecnologías de información. La tendencia a la integración busca unificar las soluciones existentes y brindar redes universales sobre las cuales los usuarios puedan transmitir voz, fax, datos y video.

Una Red Privada Virtual ha sido definida como *"un servicio diseñado para suministrar las características de una red privada, nacional e internacional, utilizando los recursos de la Red Telefónica Pública Conmutada".* Este concepto ha sido ampliado y trasladado al ambiente de comunicación de datos, en el que los usuarios corporativos pueden crear Redes Privadas Virtuales sobre redes de datos, tales como redes Internet, lo que les ofrece mayor flexibilidad y una mejor relación costo-efectividad que sus redes privadas basadas sobre circuitos arrendados.

En el presente capítulo se presenta una descripción de los diferentes tipos de Redes Privadas Virtuales de datos, con los protocolos y tecnologías que han hecho posible su implementación. Se introduce el tema de las Redes Privadas Virtuales de Banda Ancha, analizadas desde el punto de vista de las Redes ATM y desde el punto de vista de la Arquitectura TINA.

Adicionalmente, se presentan las principales consideraciones para la utilización de las Redes Privadas Virtuales sobre redes IP privadas o sobre Internet, las cuales se presentan como el principal servicio para la transmisión de datos a nivel corporativo en la presente década.

Finalmente, se introducen las Redes de Próxima Generación, las cuales proveen un ambiente de control común, unificado y flexible para soportar múltiples tipos de servicios y aplicaciones sobre múltiples tipos de redes de transporte; se explica su relación con las Redes Inteligentes y la prestación del servicio VPN integrando tanto las Redes Inteligentes como las Redes de Próxima Generación.

4.1. REDES PRIVADAS VIRTUALES DE DATOS

Con el fortalecimiento de las tecnologías de transmisión de datos, los proveedores de servicios encontraron que podían obtener mayores beneficios ofreciendo nuevos servicios de valor agregado a sus clientes, siendo uno de los más importantes para el ambiente corporativo el servicio de Red Privada Virtual.

En el ambiente de las redes de datos se presentan dos tipos de redes VPN. Las redes VPN orientadas a conexión (Connection-Oriented VPNs) y las redes VPN no orientadas a conexión (Connectionless VPNs).

4.1.1. REDES VPN ORIENTADAS A CONEXION

Las redes "Orientadas a Conexión" requieren el establecimiento de un camino extremo a extremo entre el origen y el destino antes de la transmisión de datos. La conexión puede ser creada a través de métodos administrativos o establecida dinámicamente a través de protocolos de señalización.

Entre los protocolos de datos que utilizan el método de comunicación orientado a conexión, y que han tenido gran influencia en las redes VPN, se encuentran X.25, Frame Relay, ATM y MPLS.

El primer concepto asociado con las Redes Privadas Virtuales en el mundo de datos se presentó con las redes **X.25**, en donde los usuarios podían conformar grupos de interés hacia o desde los cuales el acceso podía estar restringido. Estos grupos se llamaban Grupos Cerrados de Usuarios (CUG) y manejaban los mismos conceptos de las VPNs para las llamadas entrantes y salientes de la red. Sin embargo, X.25 fue una solución estrictamente de datos.

Frame Relay siguió a X.25 a finales de los 80s, permitiendo a las empresas crear redes corporativas de voz y datos, disminuyendo los costos operativos y los costos de telefonía de larga distancia, volviendo las redes mucho más rentables.

Las redes Frame Relay ofrecieron servicios de comunicaciones de datos a alta velocidad (de 64Kbps hasta 2Mbps) e impulsaron el concepto de transmisión de voz sobre redes de datos, utilizando técnicas de fragmentación, encapsulamiento y prioritización de paquetes, así como de administración de tráfico por congestión, permitiéndoles ofrecer una calidad de voz (Voz sobre Frame Relay) similar a la de las redes públicas de telefonía conmutada.

Como un valor agregado para sus clientes, las redes Frame Relay ofrecieron el servicio de Redes Privadas Virtuales, brindando a la red interna de telefonía de la compañía los beneficios mencionados en el Capitulo 1 para los usuarios y suscriptores.

Las redes Frame Relay y en general las redes de datos orientadas a conexión, pueden ser consideradas como "Redes Overlay" para la prestación del servicio VPN, tal como se mencionó en el Capítulo 1, sección 1.8.2.

ATM (Asynchronous Transfer Mode) fue el sucesor de Frame Relay, ofreciendo mejores anchos de banda de transmisión (hasta 155Mbps) y mejor Calidad de Servicio (QoS) que cualquier otra tecnología. Su capacidad multiservicio permite el transporte de voz, datos e imagen (videoconferencia), y la prestación de nuevos servicios multimedia.

ATM define el uso de paquetes de longitud fija (de 53 bytes), los cuales son llamados celdas, haciendo las comunicaciones más eficientes y permitiendo el uso de nodos de

conmutación a velocidades muy altas. De los 53 bytes, cinco son utilizados para información del encabezado (el direccionamiento necesario), y los restantes 48 se dedican a los datos del usuario. La prestación del servicio VPN sobre redes ATM dio origen a las Redes Privadas de Banda Ancha, las cuales serán explicadas más en detalle en la sección 4.2 del presente capítulo.

Un nuevo protocolo considerado como una mejora y posible reemplazo de ATM, es **MPLS** (Multiprotocol Label Switching). MPLS permite una fácil migración e integración de las redes IP, permitiéndoles adquirir características de protocolos orientados a conexión. Ofrece un mayor rendimiento al manejar conmutación en vez de enrutamiento entre los puntos intermedios de la comunicación y brinda capacidades de Clases de Servicio. Adicionalmente, cuenta con capacidades de enrutamiento dinámico y paquetes de tamaño variable entre otras características.

MPLS ofrece grandes facilidades para el desarrollo de las Redes Privadas Virtuales (VPN) ya que facilita la creación de canales privados permanentes, con garantías de servicio y codificación, sobre diversos tipos de tecnologías e implementaciones ya existentes.

De todas las tecnologías anteriores, se puede concluir que las VPNs orientadas a conexión garantizan la calidad del servicio y hacen posible transmitir sobre ellas diferentes protocolos de nivel de red (IP, IPX...), por lo que además de ser importantes para los clientes corporativos, están siendo utilizadas por los proveedores de servicios para la creación de sus redes de transporte (backbone).

A pesar de las ventajas mencionadas de las VPNs orientadas a conexión, una de sus principales desventajas para los clientes corporativos, es que su arquitectura es muy costosa, tanto en términos de aprovisionamiento, como de configuración y administración. El establecimiento de una VPN orientada a conexión típicamente toma un largo tiempo, requiere de mucha mano de obra y puede presentar problemas de escalabilidad en caso de requerirse una topología de malla total entre las locaciones de la empresa.

4.1.2. REDES VPN SIN CONEXION

Las limitaciones presentadas por las VPNs orientadas a conexión, forzaron a los Proveedores de Servicios a buscar una solución más flexible y rentable, que les permitiera ser más competitivos y ofrecer más beneficios a sus clientes corporativos. La solución la encontraron en las VPN sin conexión.

El término “sin conexión” o “no orientado a conexión” se refiere a un método de comunicación en el que cada componente de la comunicación es manejado separadamente por la red. El establecimiento de una red sin conexión no requiere el establecimiento de una conexión anterior a la comunicación de datos. El protocolo “sin conexión” más representativo, es IP.

En las VPN sin conexión, una VPN es una capa lógica sobre una red IP compartida que puede ser la Internet pública o una red privada con protocolos de enrutamiento IP, conocidas como **VPN IP.**

Una VPN IP segura, utiliza el concepto de un túnel encriptado implementado en los equipos corporativos conectados a la red IP. Un túnel puede existir en el nivel de enlace o en el nivel de red como una asociación entre dos puntos finales conectados a una red pública, lo que lo hace virtual. Ya que una red IP es no orientadas a conexión, los paquetes entre los nodos corporativos pueden tomar diferentes caminos dependiendo de las condiciones, tales como fallas del enlace o la configuración de los parámetros de enrutamiento.

Esta arquitectura tiene un número de ventajas fundamentales. Primero, los cambios de configuración a las VPN corporativas no requieren cambios en el núcleo de Internet. Segundo, ya que Internet es la red pública global, una VPN corporativa utilizando túneles puede ser implementada a través de múltiples redes de Proveedores de Servicio Internet (ISP).

Las VPN IP son consideradas hoy en día como el más grande generador de ganancias dentro de las redes IP. Para ilustrar la oportunidad de negocios, en la *Fig. 4.1.* se puede observar la proyección de crecimiento de los ingresos (en billones de dólares) relacionados con las redes VPN IP, en Estados Unidos hasta el año 2004.

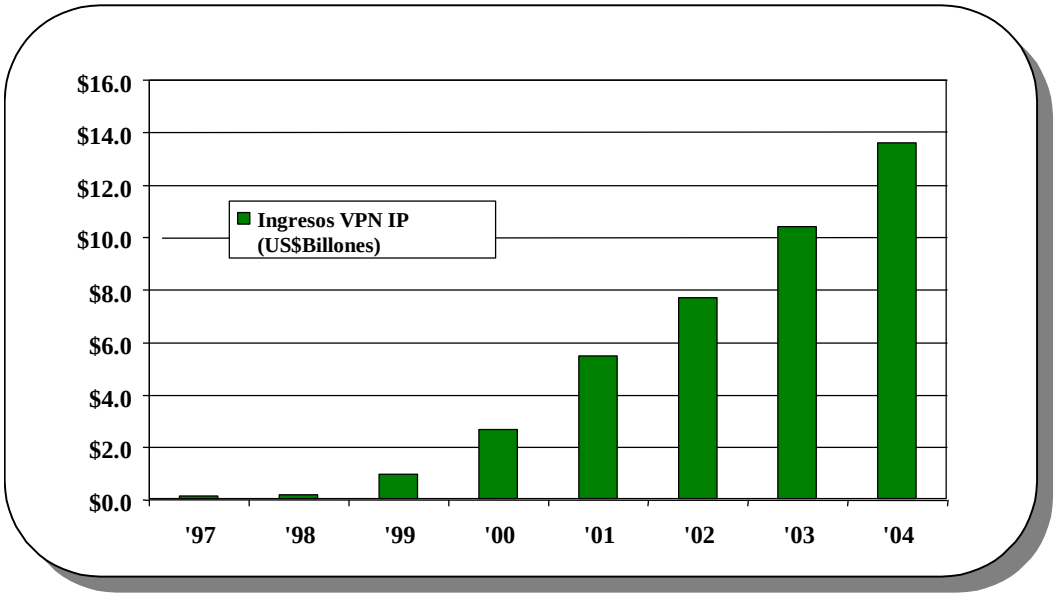


Fig. 4.1. Proyección de Ingresos para VPNs-IP, USA, 1997-2004

Más adelante en este capítulo se explicarán los diferentes tipos de redes VPN IP, los protocolos requeridos para su implementación y los aspectos de seguridad que se deben tener en cuenta.

4.2. REDES VPN DE BANDA ANCHA

El servicio de Red Privada Virtual de Banda Ancha (B-VPN) corresponde a una extensión del servicio VPN tradicional ofrecido sobre redes de Banda Ancha.

A continuación se presenta una descripción del servicio B-VPN bajo la arquitectura TINA definida por el Consorcio TINA-C. Este consorcio define el servicio de "Red Privada Virtual de Banda Ancha" como un servicio que amplia la capacidad de la VPN tradicional y que puede ser ofrecido de manera transparente, independientemente de la red de transporte, de la tecnología y de los equipos utilizados.

Posteriormente se presenta una explicación del funcionamiento del servicio de Red Privada Virtual, como un servicio corporativo de transmisión de voz, datos y video ofrecido por los proveedores de servicios con redes ATM.

4.2.1. B-VPN Y TINA

El Consorcio **TINA-C** (Telecommunications Information Networking Architecture Consorcium), formado por 46 operadores y proveedores de equipos de telecomunicaciones líderes en el mundo (1993-2000), definió una arquitectura de software abierta, orientada a objetos, diseñada para separar las aplicaciones de alto nivel de la infraestructura física subyacente de la red de telecomunicaciones. Esta arquitectura se conoce con el nombre de TINA.

El propósito de la arquitectura TINA es asegurar la interoperabilidad, portabilidad y reutilización de los componentes de software y la independencia de tecnologías especificas.

La arquitectura TINA está basada en un Ambiente de Procesamiento Distribuido (DPE) lo que permite que las características de control y administración sean distribuidas flexiblemente dentro de la red en vez de estar atadas a los concentradores en el centro de la misma. El DPE TINA está basado en la arquitectura CORBA desarrollada por el Grupo de Administración de Objetos (OMG). Una descripción más detallada de la tecnología CORBA y su relación con la evolución hacia las Redes Inteligentes Distribuidas se presenta en el ANEXO B.

TINA define un conjunto de interfaces de comunicación, llamadas Puntos de Referencia, que proveen una clara separación entre los papeles que deben realizar cada uno de los participantes de una solución (por ejemplo, entre el consumidor y el proveedor de conectividad). El cumplimiento con estos puntos de referencia garantiza la interoperabilidad entre productos TINA y permite a compañías nuevas y a compañías ya establecidas ampliar sus negocios con una máxima flexibilidad.

El Consorcio TINA-C seleccionó un grupo de servicios con el fin de validar y mejorar la arquitectura y especificaciones de TINA durante su etapa de desarrollo, a través de su

diseño, implementación y demostración. Uno de estos servicios fue la **Red Privada Virtual de Banda Ancha** (BVPN - *Broadband Virtual Private Network*).

El servicio Red Privada Virtual de Banda Ancha busca ampliar la capacidad de la VPN y su objetivo principal es suministrar a los usuarios una plataforma multi-servicio donde cada servicio suscrito sea ofrecido en una forma transparente y eficiente, sin importar las redes involucradas, marcas de equipo y tecnologías.

Este servicio está compuesto principalmente por:

- Una *red de transporte* que define la conectividad global para un cliente dado. Para las condiciones de este ejemplo, la red de transporte será una red ATM.

- Un *portafolio de servicios* ofrecidos sobre una red de transporte e integrados en una forma eficiente en términos de uso de ancho de banda, calidad del servicio, etc.

Los servicios incluidos en el portafolio cubren una gran variedad de servicios, en los cuales puede estar interesado un cliente, entre ellos: Interconexión de LANs, Video en demanda, Videoconferencia, Frame Relay, etc.

4.2.1.1. Características de BVPN

En la *Fig. 4.2.* se presentan los diferentes aspectos de BVPN, a través de una configuración de un cliente con 3 locaciones. En esta configuración, el servicio BVPN provee una red de transporte enlazando estos puntos. Esto permite a los clientes diseñar su propia red corporativa mientras utilizan los recursos de la red pública.

Una Red Privada Virtual de Banda Ancha está compuesta por un nivel de transporte de red y un nivel de servicio de red. Hay tantos niveles de servicios de red, como servicios sean descritos por el usuario. Todos estos niveles de red (transporte, servicios) son modelados del mismo modo: puntos de acceso y enlaces entre puntos de acceso.

El enlace es una vista abstracta de la conectividad ofrecida por la red. Un enlace en el nivel de transporte de red puede contener uno a varios enlaces en el nivel de servicio de red. Todo el interés del servicio BVPN reside en la integración de estos 2 niveles: lo cual permite optimizar recursos en el nivel de transporte de red (es decir, ancho de banda) y reducir los costos de uso en los niveles de servicios de red.

La *Fig. 4.2.* muestra la relación entre los niveles de servicio y transporte. El nivel de transporte está definido por 3 puntos de acceso (1 por cada sitio) y 3 enlaces entre los puntos de acceso. Estos puntos de acceso para los servicios de transporte son equivalentes a la interfaz UNI (Interfaz Usuario-Red – *User Network Interface*).

El nivel de Servicio 1 está definido por 3 puntos de acceso y 2 enlaces. El nivel de Servicio 2 está definido por 3 puntos de acceso y 3 enlaces. Sobre el nivel de transporte son multiplexados los niveles de Servicio 1 y Servicio 2.

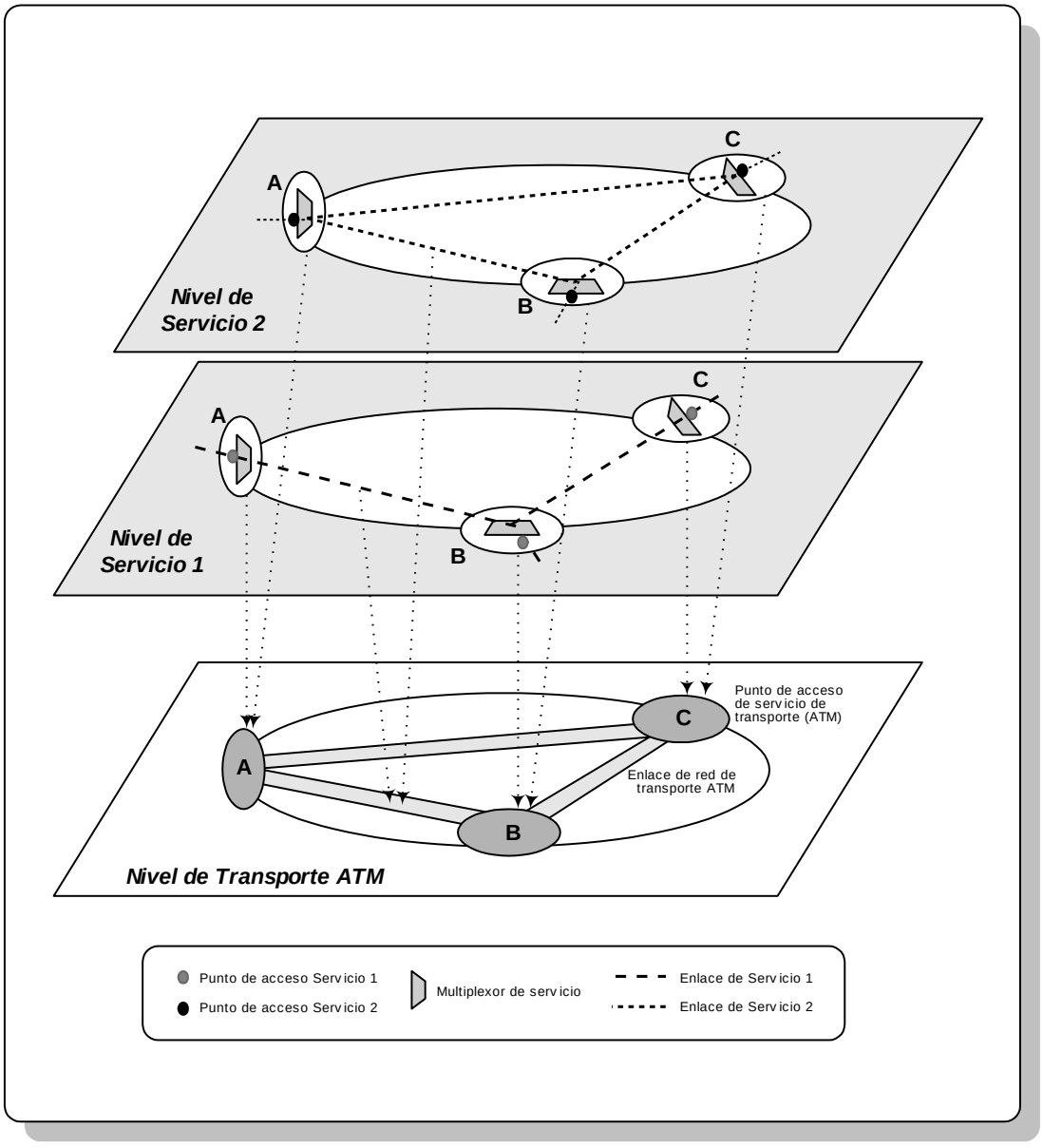


Fig. 4.2. BVPN compuesto de niveles de transporte y servicios

Esto significa que:

- Los enlaces en cada nivel de servicio son multiplexados dentro de los enlaces en el nivel de transporte.
- Los puntos de acceso en cada nivel de servicio son multiplexados dentro de los puntos de acceso en el nivel de transporte.

4.2.1.2. Participantes del Servicio

Tal como en el servicio VPN tradicional, en el servicio BVPN se encuentran involucrados los siguientes participantes:

- **Usuario del servicio BVPN.** Usa el servicio BVPN, es decir, utiliza el portafolio de servicios ofrecidos sobre la red de transporte. Sólo se relaciona con el proveedor del servicio BVPN.

- **Proveedor del servicio BVPN.** Proporciona al usuario del servicio BVPN la red de transporte y el portafolio de servicios a través de una integración de diferentes proveedores de servicios (proveedores de red, información, contenido). Esta integración le permite actuar como un agente de negocios (integrador de soluciones), es decir, una organización la cual ofrece a través de una única interfaz muchos servicios proporcionados por otras organizaciones. La red de transporte podría también ser ofrecida por un proveedor de servicios.

- **Proveedor de Servicios.** Proporciona un servicio particular para ser integrado dentro de un portafolio de servicios BVPN. Es posible que ofrezca sus servicios directamente a los usuarios, pero esto no es considerado en la configuración actual.

4.2.2. VPN Y ATM

ATM (Asynchronous Transfer Mode) es una tecnología de multiplexación y conmutación orientada a celdas, de alto rendimiento, que utiliza paquetes de longitud fija para transportar diferentes tipos de tráfico.

ATM puede transportar eficientemente voz, datos y video, con una excelente utilización del ancho de banda, simplificando la administración de la red y reduciendo los costos de comunicaciones.

El desarrollo de VPN sobre ATM es de gran importancia para los proveedores de servicios y operadores, ya que les permite adicionar valor a los servicios corporativos que ofrecen a sus clientes.

Sin embargo, solamente tiene sentido económicamente cambiar la infraestructura actual o implementar una infraestructura de red ATM si se puede demostrar que:

- Una amplia base ATM podría reducir las distancias de acceso y ofrecer la oportunidad de costos de acceso más bajos.
- La solución es rentable y la red es flexible.
- Puede ofrecer mejor integración de voz y datos.

4.2.2.1. Fundamentos ATM

En las redes ATM cada celda es de 53 bytes, de los cuales 5 bytes corresponden al encabezado y 48 bytes corresponden a la carga útil. El tamaño de celda fija garantiza que la información sensible a retardos, tal como voz o video no es afectada por largas tramas o paquetes de datos.

Los estándares ATM definen dos tipos de conexiones: Las Conexiones de Canal Virtual (VCC, *Virtual Channel Connection*), o también conocidas como Circuitos Virtuales (VC), las cuales corresponden a la unidad básica que transporta un sencillo flujo de celdas de usuario a usuario, y las Conexiones de Camino Virtual (VPC, *Virtual Path Connection*), cada una de las cuales agrupa un conjunto de VCs con los mismos puntos de terminación.

Una Conexión de Camino Virtual puede ser creada extremo a extremo a través de una red ATM con el fin de que todas las celdas que incluye sean enrutadas de la misma manera a través de la red ATM, permitiendo una más rápida recuperación en caso de fallas.

Una red ATM también puede utilizar Caminos Virtuales con el propósito de encapsular Circuitos Virtuales entre conmutadores ATM. Dos conmutadores ATM pueden tener muchas diferentes Conexiones de Canal Virtual entre ellos, perteneciendo a diferentes usuarios. Estas pueden ser encapsuladas por los 2 conmutadores en una Conexión de Camino Virtual. Esto permite crear el concepto de una Troncal Virtual entre los 2 conmutadores.

Los Circuitos Virtuales pueden ser configurados estáticamente como Circuitos Virtuales Permanentes (PVCs) o controlados dinámicamente vía señalización, como Circuitos Virtuales Conmutados (SVCs)

Como se puede observar en la Fig. 4.3. una red ATM está compuesta de una serie de conmutadores y dispositivos de acceso.

Los dispositivos de acceso están instalados en las locaciones de los clientes y pueden ser enrutadores, servidores o equipos multiservicio (integran voz, datos, video) con capacidades de acceso ATM.

Los conmutadores que conforman la red ATM pueden ser conmutadores de borde o conmutadores de centro. Los conmutadores de borde se encargan de establecer las conexiones con los dispositivos de acceso de los clientes y se conectan con otros tipos de redes, tales como redes Frame Relay (acceso con velocidades desde 64Kbps) y redes líneas dedicadas. Los conmutadores de centro, son conmutadores de mayor capacidad y se encargan únicamente del transporte y la conmutación dentro de la red.

ATM soporta dos tipos de interfaces: interfaz usuario-red (UNI) y la interfaz red-nodo (NNI). UNI proporciona la conexión entre un dispositivo de acceso ATM y un conmutador de la red ATM, mientras NNI permite la conexión entre dos conmutadores ATM de la misma red o de redes diferentes.

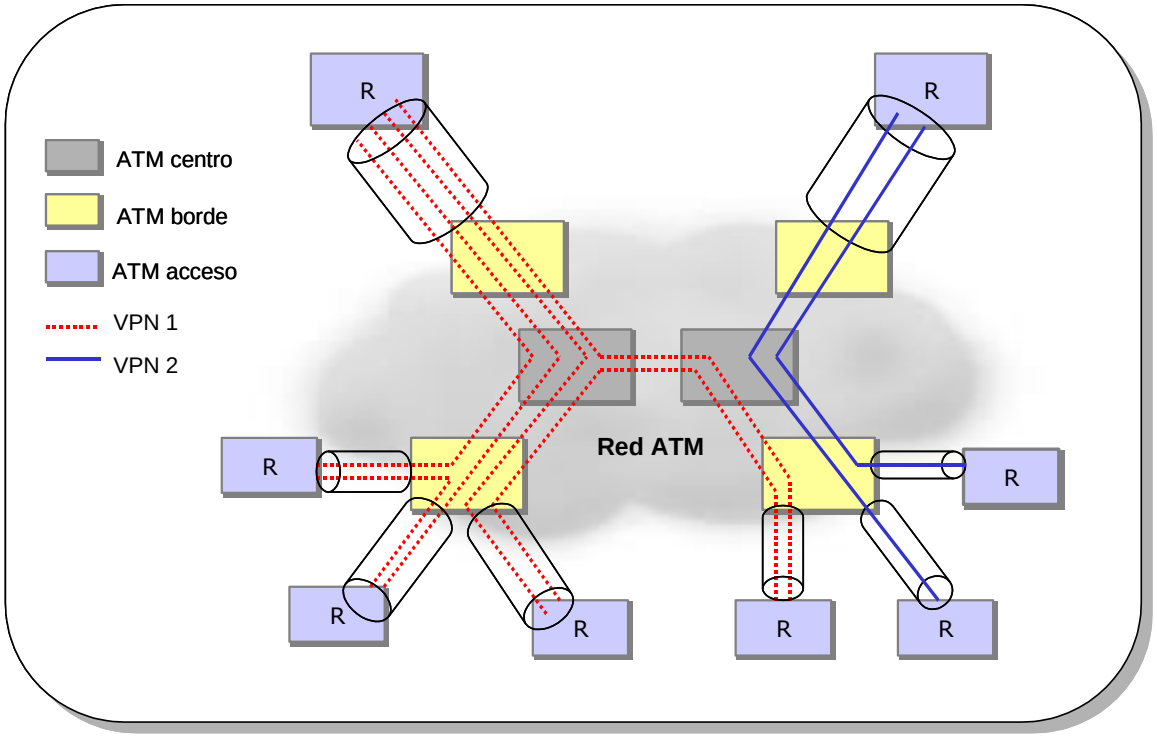


Fig. 4.3. Plataforma ATM

4.3. REDES VPN IP

Una Red Privada Virtual (VPN) IP se puede considerar como un método alternativo a una Red de Área Amplia (WAN) que utiliza Internet o una red IP privada, en vez de líneas privadas de datos arrendadas para conectar todas sus instalaciones.

Los beneficios que se obtienen al integrar las Redes Privadas a Internet son:

- Reducción en los costos de adquisición y operación de la red.
- Expansión de la red más fácilmente, adicionando Accesos Internet, en vez de una o más líneas arrendadas.
- Nivel de seguridad igual que con líneas arrendadas y superior al obtenido por una red conectada a Internet y protegido solamente por un Cortafuegos (Firewall).
- Alta calidad de servicio, igual que con líneas arrendadas.

Sin embargo, IP no fue concebido como un protocolo orientado a conexión, y por lo tanto no cuenta con mecanismos que puedan asegurar, por sí mismos, aspectos críticos como la seguridad o la calidad de servicio. La solución de estos problemas ha originado el desarrollo de nuevos protocolos de autenticación y encripción basados en IP, los cuales buscan que las comunicaciones sean seguras a través de la infraestructura pública.

En el ANEXO C se presenta una descripción detallada del funcionamiento de las Redes Privadas Virtuales sobre Internet, sus beneficios, aplicaciones, protocolos empleados, esquemas de seguridad implementados y su administración.

4.3.1. TIPOS DE VPN IP

Se conocen varios tipos de VPNs, las cuales son clasificadas a continuación desde un punto de vista funcional (los escenarios donde se utilizan las VPNs), y desde un punto de vista administrativo (los dominios administrativos donde se desarrollan las VPNs).

4.3.1.1. Clasificación Funcional

La clasificación de VPN en términos funcionales, refleja la manera en la que los clientes y las organizaciones utilizan las VPNs. Las VPNs pueden ser utilizadas para ofrecer las siguientes soluciones: la conexión de oficinas remotas, la marcación de usuarios remotos a una red corporativa, y la creación de una extranet para permitir a socios remotos el acceso a los recursos corporativos.

- **VPN Intranet**

  Una VPN Intranet conecta virtualmente oficinas remotas a las oficinas centrales de una corporación utilizando enlaces seguros a través de una infraestructura de acceso pública. El acceso a la Intranet es estrictamente limitado a aquellas redes o conexiones que son autenticadas.

  Diferentes niveles de acceso pueden ser asignados a diferentes sitios en la Intranet, dependiendo de su propósito. Las VPNs soportan confiabilidad y prioritización de aplicaciones de misión crítica que actualmente representan la utilización clásica de esta tecnología.

- **VPN Acceso Remoto**

  Una VPN puede ser desarrollada para proveer acceso a la Intranet de la empresa a usuarios remotos, trabajadores desde casa (home workers) y trabajadores móviles conectados por acceso conmutado (telecommuters). Una VPN de acceso remoto permite a los usuarios conectarse a los recursos corporativos desde cualquier lugar que ellos necesiten.

  Esta solución puede abarcar muchas tecnologías tales como líneas análogas, cable módems, RDSI, xDSL. Sin embargo, ya que los usuarios típicamente se conectan sobre conexiones de baja velocidad, las VPN de acceso remoto deben tener cuidado de requerimientos tales como calidad de servicio y confiabilidad. El principal requerimiento de seguridad es la autenticación de usuarios. Para esto, las VPNs deben incorporar un sistema de autenticación para evitar intrusos no autorizados, utilizando por ejemplo RADIUS (Remote Authorization Dial-In User Service).

- **VPN Extranet**

  El término “extranet” significa permitir el acceso seguro a una parte de una intranet corporativa a terceros, tales como clientes, socios, proveedores y vendedores externos.

  Una VPN Extranet utiliza una infraestructura compartida para construir conexiones dedicadas desde socios hasta recursos corporativos restringidos (por ejemplo una base de datos). Uniendo estos recursos a una VPN dedicada (a parte de la VPN Intranet), la corporación puede conceder acceso seguro a sus socios. La Intranet corporativa, es preservada de accesos no autorizados porque pertenece a una VPN diferente.

  Se requiere que los diversos socios cuenten con soluciones basadas en estándares para garantizar su interoperabilidad.

4.3.1.2. Clasificación Administrativa

Considerando el dominio administrativo en el que las VPNs son desarrolladas, se presentan dos tipos de VPNs IP: en la primera, todas las funciones VPN son implementadas en las premisas de los clientes y en la segunda, los proveedores de servicios que cuentan con el backbone IP se encargan de ofrecer todos los servicios VPN.

- **VPN basadas CPE**

  Todas las funciones VPN son implementadas en dispositivos CPE tales como cortafuegos y enrutadores WAN de borde, que son propiedad del cliente y se encuentran en sus oficinas.

  Estos equipos despliegan conectividad VPN entre los usuarios estableciendo conexiones directas y seguras con las entidades CPE en el otro lado de la red. Esta solución es llamada “orientada a conexión”. La red del proveedor no está involucrada con ninguna función en particular y es utilizada únicamente como red de transporte.

  La red, no reconoce el tipo de tráfico que se está transmitiendo: los paquetes VPN no se pueden distinguir de los paquetes normales de datos y la red los remite como cualquier otro paquete. Finalmente, según esta solución los asuntos relacionados con el establecimiento y administración de la VPN, solamente son importantes a los equipos del cliente.

- **VPN basadas Proveedor**

  Todas las funciones de la VPN, tales como configuración y administración, son delegadas al proveedor e implementadas en la red.

  Los usuarios no deben preocuparse de establecer un canal de comunicación con un usuario remoto, ellos solamente deben informar al proveedor que pertenecen a una red VPN particular y enviar el tráfico VPN al nodo de acceso del proveedor. Depende del proveedor transmitir los datos VPN generados por los usuarios VPN al destino apropiado (de una manera segura) dentro de una red virtual.

La principal ventaja de esta solución es que los clientes pueden reducir sus costos de soporte (equipos sin características especiales), mientras los proveedores pueden explotar nuevas fuentes de ingresos, como la prestación de algunos de los siguientes servicios de valor agregado: Comercio electrónico, Web hosting, hosting de aplicaciones, aplicaciones multimedia, entre otros.

4.3.2. SEGURIDAD EN VPN

Los clientes de VPN esperan generalmente que su red VPN ofrezca un nivel de seguridad que por lo menos sea equivalente al ofrecido por una configuración WAN privada. Proporcionar tal nivel de seguridad de una manera confiable, eficiente y rentable es una tarea compleja, que debe considerar los factores que se describen a continuación y que deben ser ofrecidos por todos los protocolos encargados de implementar una VPN:

- Privacidad: Implica que el tráfico VPN privado no debe ser accesible para entidades, sistemas o personas no autorizadas. Puede ser lograda a través del uso de encripción.

- Integridad: Garantiza que los datos no han sido alterados de ninguna manera desde su transmisión hasta su recepción. La integridad es generalmente lograda a través del uso de comprobación de paridad (checksums).

- Autenticación: Define mecanismos para verificar la identidad del remitente y receptor de la comunicación.

- No Repudiación: Protege al remitente y al receptor para que su contraparte no pueda posteriormente negar su participación en una transacción. También se conoce como Verificación de los Datos de Origen, y se logra con el uso de Firmas Digitales. Cuando las medidas de No-repudiación han sido tomadas, el receptor no puede negar haber recibido una transacción, ni el remitente puede negar haberla enviado.

4.3.3. PROTOCOLOS VPN IP

Para implementar una Red Privada Virtual sobre una red pública, se utiliza una técnica de creación de ***túneles*** virtuales, que existen solamente durante el intercambio de información. Esta técnica en inglés recibe el nombre de *tunneling*.

Cuando los datos se envían a través del túnel, la trama o el paquete se *encapsulan* dentro de otro paquete IP especial. En cuanto los datos alcanzan el extremo opuesto, son desencapsulados y procesados como si hubieran sido enviado desde un sistema de la misma LAN.

Existen varios protocolos de creación de túneles VPN, pero los 3 más importantes son: PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), y IPSec (IP Security).

La técnica de creación de túneles (tunneling) por sí misma no provee seguridad, por lo que es necesario combinarla con otros protocolos de autenticación y encripción de datos. Sin embargo, a diferencia de los demás protocolos, el protocolo IPSec fue desarrollado con todas las capacidades de seguridad necesarias para la transmisión de datos sobre redes públicas, tal como se explicará más adelante.

4.3.3.1. Point to Point Tunneling Protocol (PPTP)

PPTP es una tecnología de túnel multiprotocolo basada en el Protocolo PPP (PPP, *Point-to-Point Protocol*) y desarrollada por Microsoft, Ascend, 3Com, ECI Telematics y USRobotics.

PPTP encapsula las tramas PPP sobre el protocolo GRE (Generic Routing Encapsulation) de Cisco, lo que le permite transportar protocolos heredados como IPX y NETBEUI. Para la encripción de la información, utiliza el algoritmo MPPE (Microsoft´s Point to Point Encryption) de Microsoft.

El protocolo PPTP viene incorporado en los sistemas operativos Windows 95 DUN1.2, Windows 98, Windows 2000 y Windows NT4.0 lo que lo convierte en un estándar de facto para las empresas que utilizan computadores con sistemas operativos Microsoft.

PPTP puede ser utilizado para soportar usuarios por marcación (VPN Acceso Remoto), conexiones LAN to LAN (VPN Intranet) y en menor proporción conexiones de socios externos (VPN Extranet).

4.3.3.2. Layer 2 Tunneling Protocol (L2TP)

L2TP es un protocolo estándar de IETF (RFC 2611) que combina el protocolo PPTP y el protocolo L2F (Layer 2 Forwarding) desarrollado por Cisco.

Las diferencias principales con PPTP son que L2TP combina los canales de control y de datos y encapsula las tramas PPP sobre UDP. Esto permite que L2TP sea más utilizado para las soluciones VPN Extranet que PPTP ya que muchos firewalls no soportan GRE. Adicionalmente puede ser utilizado para ofrecer VPN Acceso Remoto y VPN Intranet.

L2TP soporta características de autenticación y de autorización, a través de la interoperabilidad con servidores RADIUS y TACACS+. Para encripción utiliza el protocolo estándar IPSec.

4.3.3.3. IP Security (IPSec)

IPSec definido por la IETF a través de las recomendaciones RFC 1825 hasta RFC 1829, es un protocolo abierto y basado en estándares que provee privacidad a los datos a través de la creación de túneles y de la encripción en el nivel de red.

IPSec es el protocolo más completo para la implementación de VPNs y fue diseñado para lograr comunicaciones seguras sobre Internet. Reduce la amenaza de ataques basado en el muestreo (spoofing) de direcciones IP y provee un medio estandarizado para garantizar integridad de los datos, autenticar una fuente de datos y garantizar la confidencialidad de la información, al mismo tiempo que maneja el problema de administración de claves.

IPSec es un conjunto de 3 protocolos de seguridad interrelacionados implementados sobre un paquete IP modificado, junto con una infraestructura que soporta distribución de claves y administración.

Los dos primeros protocolos involucrados en la transferencia de datos son: Authentication Header (AH) y Encapsulating Security Payload (ESP). El protocolo AH provee autenticación de fuente, verificación de la integridad de los datos y soporta mecanismos opcionales para prevenir réplicas de ataques, pero no provee confidencialidad. El protocolo ESP provee confidencialidad de los datos a través de encripción (DES, 3DES), y también puede proveer verificación de integridad de los datos, autenticación de fuente y un servicio anti-replicas. Un dispositivo con capacidades de IPSec puede configurar AH, ESP o ambos.

El tercer protocolo permite a IPSec resolver el difícil problema de la administración automática de llaves por sí mismo y se llama IKE (Internet Key Exchange). IKE proporciona un método estándar para negociar llaves de encriptamiento únicas para una sesión. Esta llave de encripción empleada para codificar la información en el túnel se puede renegociar y cambiar automáticamente durante la sesión.

IPSec puede ser utilizado para soportar redes VPN Intranet, VPN Extranet y VPN Acceso Remoto. Para esto, el protocolo debe estar instalado en los equipos encargados de originar y terminar el túnel.

Se puede concluir que la principal ventaja de IPsec es su alto grado de seguridad, sin embargo, presenta algunas desventajas: mayor complejidad para su instalación y administración y aún no se garantiza la interoperabilidad de los productos de distintos fabricantes.

4.4. COMPARACION VPN FR/ATM vs. VPN IP

En las tres secciones anteriores se han mencionado las principales características y aplicaciones de las redes VPN orientadas a conexión y de las redes VPN no orientadas a conexión. A continuación se presenta un análisis de las diferencias entre los dos tipos de redes y las consideraciones que se deben tener en cuenta para seleccionar la mejorar solución para una empresa.

4.4.1. VENTAJAS VPN FR/ATM SOBRE VPN IP

- **Confiabilidad y Seguridad:** Las principales ventajas de las redes VPN FR/ATM sobre las redes VPN IP, son la confiabilidad y la seguridad. Una VPN basada en IP construida sobre el Internet público usando servicios ofrecidos por varios ISPs puede no proveer una calidad aceptable.

- **Eficiencia de la Red:** Un resultado directo de tener que utilizar mecanismos de encripción en las redes VPN IP es el decremento en la eficiencia global de la red, lo que no ocurre en las redes FR/ATM.

  El encabezado requerido para la encripción, desencripción y el proceso de autorización hace que el uso de los recursos de red disponibles no sea tan óptimo. Si el protocolo VPN empleado es IPsec, se requiere mucha actividad de la CPU del equipo encargado de establecer una conexión, por lo que en caso que se desee manejar miles de conexiones activas por segundo, tal vez sólo se podrían crear unos cuantos centenares.

- **Calidad de Servicio:** Las características de calidad de servicio (QoS) y de administración de tráfico son generalmente superiores para redes Frame Relay y ATM que las manejadas por Internet público y muchos ISPs.

  Las redes VPN IP están sujetas a las numerosas limitaciones de Internet incluyendo consistencia, disponibilidad y seguridad. Adicionalmente, Internet no es capaz de soportar características de servicio de alto nivel, tal como prioritización del flujo de tráfico, un requerimiento crítico para los negocios que quieren prioritizar tráfico basado en aplicaciones como voz, y datos de misión crítica.

  Por consiguiente, un importante criterio al seleccionar un ISP es asegurarse que el rendimiento de su backbone IP sea comparable al de una alternativa Frame Relay o ATM.

4.4.2. VENTAJAS VPN IP SOBRE VPN FR/ATM

- **Ahorros en los usuarios de acceso remoto:** En redes FR/ATM el acceso remoto es manejado fuera de la red privada del cliente a través de conexiones con RAS usando la RPTC. Esto implica costos de larga distancia o de números 800, así como costos de equipos que se incrementarían a medida que el número de usuarios crece (p.e. actualización de puertos).

  Con una VPN de Acceso Remoto, los usuarios se conectan a Internet utilizando cuentas dial-up (por marcación) con una tarifa plana y un software cliente VPN instalado en su PC. Esto elimina la estructura de precios por minuto y las tarifas de la RTPC.

  Adicionalmente, como la conexión es a través de un ISP y no directamente a las oficinas principales de la empresa, el proveedor de servicio termina la llamada vía IP

en la oficina principal del cliente. Esto elimina la necesidad de utilizar RAS administrados por el cliente.

- **Ahorros en la conectividad Internacional:** Las redes FR/ATM han reducido en gran medida los costos de interconectar locaciones internacionales, comparado con redes de líneas privadas. Sin embargo, la estructura de precios por PVCs (FR) o VCs (ATM) y por puerto internacional, hacen que esta solución todavía sea muy costosa.

  Las VPN IP reducen los costos para operar en un ambiente internacional, ya que no es necesario utilizar PVCs/VCs.

  Adicionalmente, los usuarios internacionales de acceso remoto, contarían con cuentas de acceso por marcación de tarifa plana, eliminando los elevados costos por minuto.

- **Ahorros en la conectividad B2B (Business to Business):** Una VPN IP permite a socios, proveedores, etc., comunicarse de una manera segura con la cadena de aprovisionamiento a través de Internet. Comparado con soluciones tradicionales tales como Redes de Valor Agregado (VAN – Value added networks) o FR/ATM, los ahorros son significativos al no tener que pagar por conectividad directa con otros. Las VANs cobran un valor adicional a los miembros de la cadena de aprovisionamiento por conectarse a la red de alto rendimiento. FR requiere que cada locación tenga su propio puerto así como PVCs a los sitios que requieren comunicaciones directas, creando una red en malla con todos los interesados.

- **Comunicaciones punto a punto:** La conectividad VPN IP Intranet es un área donde las VPNs IP pueden no generar costos mensuales más bajos para las empresas, en comparación con FR – principalmente cuando se comparan redes pequeñas o redes que no utilizan mucha conexión en malla. FR está ampliamente extendido y sus costos han bajado significativamente.

  Las VPN IP empiezan a mostrar ahorros significativos sobre FR en corporaciones que requieran una arquitectura altamente conectada en malla. En este caso los costos de los PVCs se incrementan en comparación con la malla libre de las redes VPN IP.

  En la *Fig. 4.4* se presenta una comparación de los diferentes medios de conectividad utilizados por las empresas para sus comunicaciones Intranet, según un estudio del Yankee Group. Para el año 2003 la participación en el mercado de las redes VPN IP crecerá fuertemente comparado con el año 2001, mientras que las redes FR, líneas dedicadas y dial-up disminuirán su participación en el mismo periodo de tiempo. Sin embargo la participación de las redes FR seguirá siendo aún mayor que las redes VPN IP. *(Fuente: The Yankee Group 2001 Enterprise Communications Survey)*

- **Administración y Control Simplificado:** En general, una VPN IP es un ambiente global más simple para administrar y mantener, comparado con las redes FR/ATM. FR requiere que la empresa conozca los flujos de tráfico y requerimientos específicos de ancho de banda para utilizar eficientemente el ambiente de PVCs. Esto puede ser complejo en grandes redes.

Las redes VPN IP son también más flexibles manejando cambios (p.e. adicionando removiendo usuarios, nuevos sitios, socios, etc.).

Para adicionar una nueva locación a la red, con VPN IP se requiere comprar el acceso Internet e instalar un dispositivo VPN. Si el acceso Internet ya existe solo es necesario instalar el dispositivo VPN para habilitar la funcionalidad de seguridad en la comunicación. Para adicionar una nueva locación a la red, con FR se requiere además del acceso y el equipo CPE, que el proveedor del servicio aprovisione el puerto FR y los PVCs.

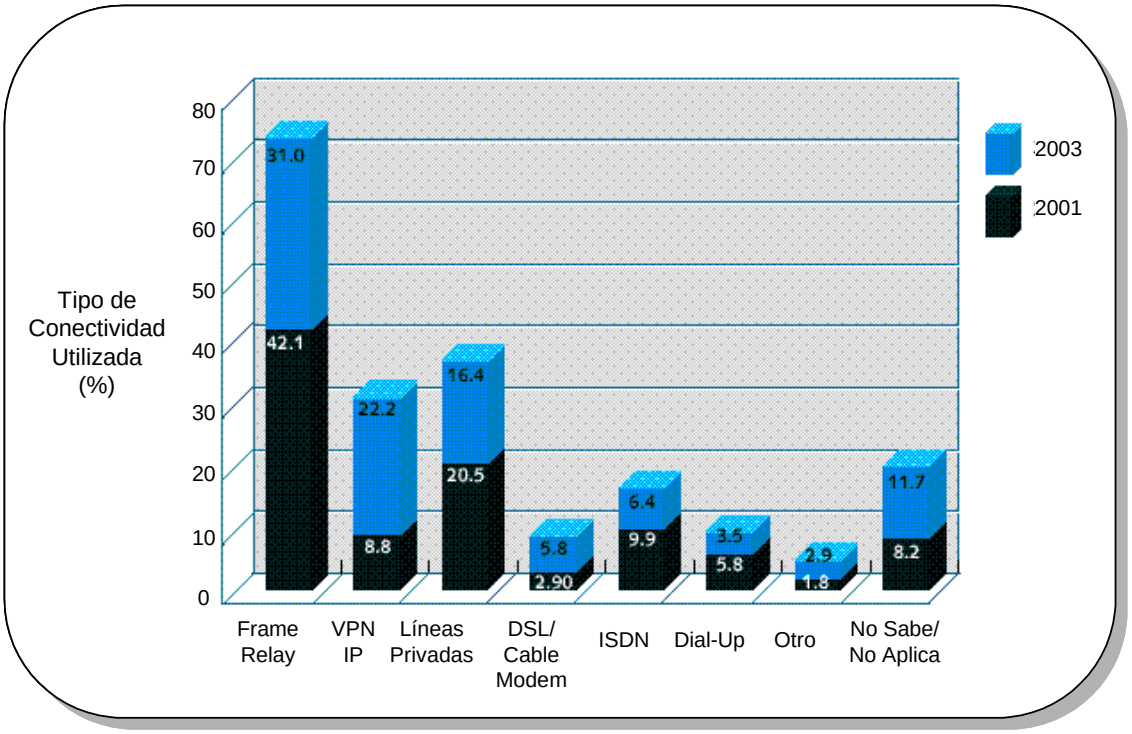


Fig. 4.4. Medios de Conectividad Intranet en Redes Corporativas

4.4.3. EJEMPLO COMPARATIVO

A continuación se presenta un ejemplo comparando las dos soluciones. En la *Fig. 4.5* se observa una VPN FR/ATM, con H sitios concentradores y B sitios remotos conectados con enrutadores (R) a través de conexiones virtuales (PVCs / VCs). Para el ejemplo se considera que cada sitio remoto se conecta a dos sitios concentradores y que los sitios concentradores están completamente conectados en malla.

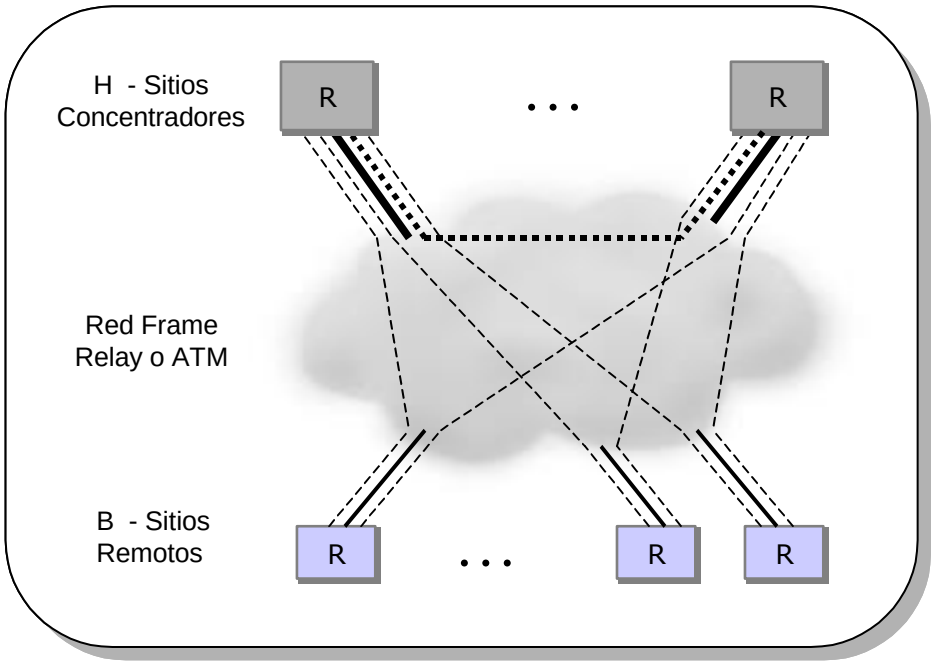


Fig. 4.5. VPN orientada a conexión

En la *Fig. 4.6.* se presenta una red VPN IP con el mismo número de sitios concentradores y sitios remotos que la red VPN FR/ATM. Para la red VPN IP se requiere adicionar equipos de encripción o entunelamiento, representados en el gráfico por los cuadros marcadas con O (Overlay).

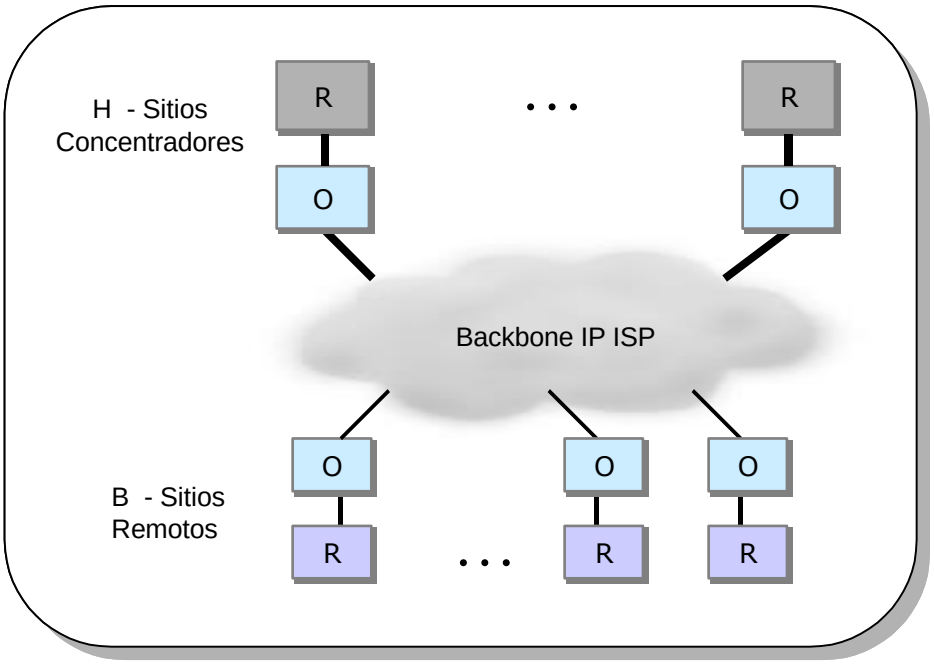


Fig. 4.6. VPN no orientadas a conexión

Los dos modelos consideran que los sitios remotos se conectan a la red utilizando enlaces de última milla n x 64Kbps en el caso FR y velocidades T1/E1 o superiores en el caso ATM. Los sitios concentradores se conectan utilizando enlaces de mayor capacidad con el fin de concentrar el tráfico proveniente de los enlaces remotos. Así mismo, en el caso de la red VPN FR/ATM, los PVCs/VCs conectando los sitios concentradores son de mayor velocidad que los que conectan los sitios remotos con los sitios concentradores (esto se representa con las líneas punteadas en la Fig. 4.5).

En cualquiera de los dos modelos los clientes deben considerar dos tipos de costos: los costos de capital (inversión inicial) y los cargos mensuales recurrentes.

En los costos de capital deben incluir el valor de los enrutadores o equipos CPE para cada sitio, así como la instalación del enlace local con el proveedor del servicio (última milla).

Para la solución VPN IP se requiere adicionar costos de equipos de seguridad (encripción o entunelamiento), así como otros costos por concepto de licenciamiento, administración de red y configuración e instalación inicial, lo que hace la inversión inicial en las redes VPN IP superior a la inversión con las redes VPN FR/ATM.

Los equipos pueden ser adquiridos por los clientes o pueden ser alquilados como parte del servicio ofrecido por el proveedor (outsourcing).

Las dos alternativas tienen cargos mensuales por los enlaces locales y cargos por puerto de conexión a la red. Sin embargo, los cargos por puerto para el servicio FR/ATM son diferentes que para un servicio IP con un Acuerdo de Nivel de Servicio (SLA – Service Level Agreement) garantizado por el ISP o el proveedor de la red IP.

La alternativa orientada a conexión adicionalmente tiene cargos mensuales por Circuitos Virtuales (PVCs o VCs), con altas velocidades soportando las conexiones de malla total entre los concentradores y con bajas velocidades usadas para la interconexión entre los concentradores y los sitios remotos. Cada proveedor maneja una estructura de precios diferente y en muchas ocasiones para las redes VPN FR/ATM le presentan a sus clientes un único valor mensual por el enlace local, por el puerto y por el Circuito Virtual.

Si una porción significativa del tráfico se mueve entre un gran número de sitios remotos a unos pocos sitios concentradores, entonces una VPN orientada a conexión es más económica.

A medida que el número de sitios concentradores se incrementa, el valor de la solución VPN FR/ATM se va volviendo mayor que el de la solución VPN IP. Esto ocurre porque se requieren más PVCs para conectar los sitios remotos a los concentradores y porque el costo inicial para la solución VPN IP (que es superior al de la solución VPN FR/ATM) es repartido entre más nodos.

Otra consideración que se debe hacer, es respecto al manejo del tráfico. En una red VPN FR/ATM si el diseño de la red es en estrella o en malla parcial, el tráfico que fluye entre sitios remotos o desde un sitio remoto hacia Internet debe realizar dos saltos pasando por

los sitios concentradores. Para que el tráfico realice un solo salto sería necesario crear un diseño de malla total, lo cual incrementaría considerablemente el valor global de la solución.

A diferencia de la solución VPN FR/ATM, la característica no orientada a conexión de las redes VPN IP permite que el tráfico viaje hacia su destino realizando un único salto. Este diseño se considera inherentemente de malla total y tiene un costo de capital constante e independiente de los patrones de tráfico.

Las redes VPN FR/ATM no se utilizan para proveer una solución de Acceso Remoto y son demasiado costosas para las VPN Extranet, por lo que en ambos casos las redes VPN IP son ideales.

Como conclusión en el caso de las VPN Intranet, las redes FR/ATM son ideales cuando la configuración de tráfico de la empresa es en estrella o en una pequeña malla parcial o cuando los requerimientos de seguridad, calidad y confiabilidad son muy altos; y las redes VPN IP son ideales cuando la configuración de tráfico en la empresa requiere una conexión en malla total o cuando la empresa desea manejar en una sola red todas sus aplicaciones (Intranet, Extranet, Acceso Remoto).

4.5. REDES DE PROXIMA GENERACION (NGN)

Las Redes de Próxima Generación (NGN – *Next Generation Networks*) son definidas como redes de telecomunicaciones abiertas, basadas en paquetes que emplean nuevas técnicas de señalización, administración, control y procesamiento distribuido para proveer todos los tipos de servicios, desde servicios básicos de telefonía de voz hasta avanzados servicios multimedia de banda ancha.

La meta principal de las Redes NGN es proveer un ambiente de control común, unificado y flexible que pueda soportar múltiples tipos de servicios y aplicaciones sobre múltiples tipos de redes de transporte.

La base fundamental de las redes NGN es su naturaleza distribuida en niveles funcionales, donde los elementos de transporte (p.e. enrutadores, conmutadores y gateways) y de conmutación de paquetes están lógicamente y físicamente separados del control de la llamada y del servicio y de la creación y ejecución de los servicios.

Algunas de las características y requisitos que deben cumplir las Redes NGN son:

- Utilizar interfaces abiertas para conectar cada uno de los niveles funcionales, permitiendo una fácil integración e interoperabilidad, convirtiéndola en una arquitectura abierta y flexible, independiente de los fabricantes de equipos.
- Ofrecer una red común para manejar la conmutación y el transporte para todos los tipos de tráfico, incluyendo voz, datos y multimedia, minimizando los costos operativos y habilitando la rápida introducción de nuevos servicios a través de la red.

- Permitir la conexión con redes heredadas (redes TDM y redes de paquetes existentes), protegiendo al máximo las inversiones realizadas.
- Cumplir con los 5 requisitos de las redes de los proveedores de servicios (conocidas como “Carrier-Class”): escalabilidad, rendimiento y calidad de servicio, seguridad, multi-capacidad y gestionabilidad.
- Ofrecer características y niveles de calidad iguales o superiores a los ofrecidos por las redes RTPC para las comunicaciones de voz.
- Permitir a los usuarios finales el manejo de datos paquetizados, incluyendo Voz (VoATM, VoIP), datos y servicios multimedia, directamente desde la red de acceso usando tecnologías de banda ancha, tales como DSL, Cable módem, LMDS, RDSI.
- Optimizar la conmutación de la red IP (DiffServ, MPLS, RSVP) y soportar QoS.

Sin embargo existen factores económicos y de negocios muy fuertes que limitaran la migración hacia las Redes de Próxima Generación en un corto plazo, estos son:

- El reemplazo total de la infraestructura de RTPC existente (instalar nuevo equipo, probarlo y migrar el tráfico y los clientes existentes) es muy poco probable, en primer lugar porque no sería viable financieramente, y en segundo lugar porque sería una tarea difícil de lograr en un corto periodo de tiempo.

- La red de acceso migrará muy lentamente empezando con clientes corporativos de gran tamaño. Entre el 70% y el 95% de todos los clientes continuarán utilizando servicios de líneas telefónicas análogas, ya que los clientes residenciales y pequeños y medianos negocios no necesitaran servicios de datos y video avanzados, o al menos serán incapaces de pagar el incremento en el costo de conectividad de alta velocidad a sus casas u oficinas.

Como conclusión, no es posible definir una recomendación general de como y cuando migrar una red. La estrategia para migrar a NGN dependerá de las condiciones de la red instalada, los requerimientos de los clientes que el operador este atacando, y de los planes de expansión futuros del operador de red.

En el ANEXO B se presenta la evolución tecnológica desde las Redes Públicas Básicas de Telefonía incluyendo las Redes Inteligentes, pasando por las Redes de Datos hasta llegar a las Redes de Próxima Generación.

4.5.1. ARQUITECTURA DE LAS REDES NGN

La arquitectura de las Redes NGN se basa en tres niveles fundamentales de red (Ver *Fig. 4.7)* que separan la conmutación de paquetes y los elementos de transporte (es decir, enrutadores, conmutadores, gateways) del control de la sesión y de la creación y ejecución de los servicios, tal como lo hacen las Redes Inteligentes.

4.5.1.1. Nivel de Red

El primer nivel es el nivel de RED o de conmutación física, el cual abarca las redes de acceso, la red de backbone y la red de conmutación. Este nivel es el encargado de transportar los diferentes tipos de tráfico (voz, datos, multimedia) y de proveer conectividad de un extremo a otro de la red.

El nivel de RED está compuesto por **Media Gateways** que proporcionan conversión de RTPC a IP y otros elementos del nivel de transporte físico tales como adaptadores de terminales, conmutadores RTPC, enrutadores IP, conmutadores ATM y conmutadores Multi-Servicio que residen en la red. Estos últimos han tenido una gran acogida entre los operadores, ya que se encargan de concentrar en un solo equipo diferentes tipos de redes de acceso.

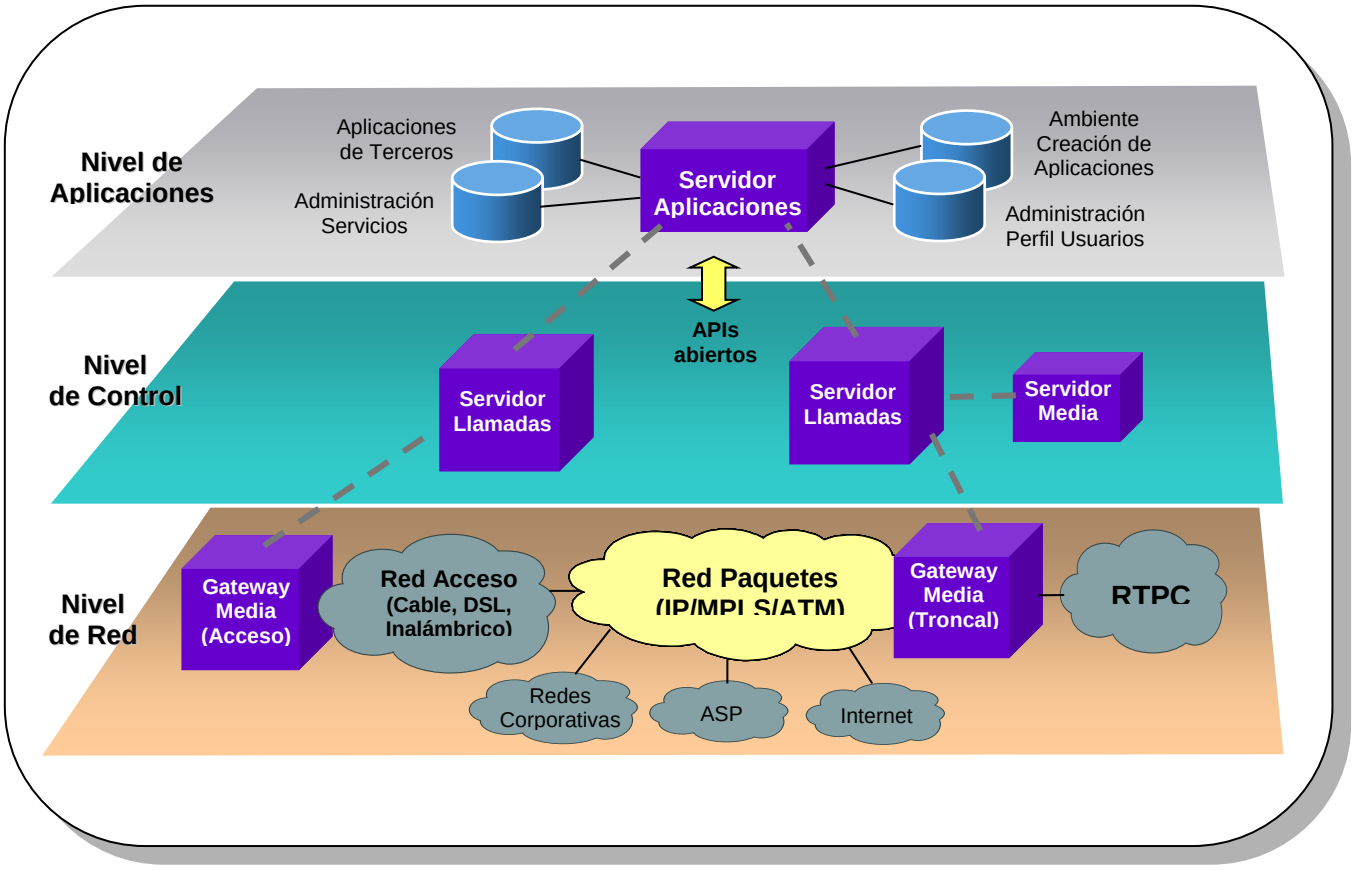


Fig. 4.7. Arquitectura en 3 niveles de las Redes NGN

- Los **Media Gateways** se encargan de convertir un tipo de tráfico proporcionado en un tipo de red al formato requerido en otro tipo de red (en el caso de la telefonía, se encargan de adaptar la voz proveniente de los circuitos conmutados, a la red de paquetes(IP, ATM)). Se utilizan como interfaces ya sea con los dispositivos de usuario final (Gateways Residenciales) con redes de acceso (Gateway de Acceso), o

con la RTPC (Gateways de Troncales). Contiene equipos para manipulación del tráfico, tales como canceladores de eco, generadores de tono, codificadores, entre otros.

4.5.1.2. Nivel de Control de Servicios

Sobre la capa de Red, está el nivel de CONTROL de Servicios, el cual administra el control de la llamada y la creación de servicios en la red. Es independiente de la tecnología utilizada en la conectividad de la red, lo que minimiza el impacto de introducir nuevas o mejoradas tecnologías de transporte.

En este nivel se separa el control de la sesión de acceso (funciones relacionadas con acceso, p.e. autenticación, suscripción), de la sesión de servicio (fase de utilización de un servicio) y de la sesión de comunicaciones (visión de recursos relacionados con conexión necesarios para el desarrollo de un servicio particular), permitiendo que cada tipo de sesión sea tratado independientemente de las otras sesiones.

Así, múltiples sesiones de servicio pueden ser iniciadas desde una única sesión de acceso. Así mismo, las sesiones de comunicaciones pueden ser tratadas separadamente de la sesión total del servicio del que hacen parte (es decir, permitiendo separar el control de conectividad del control de la llamada).

Adicionalmente este nivel se encarga de hacer la conexión entre los niveles de Red y de Aplicación, permitiendo a los servicios ser definidos en el nivel de aplicación independientemente de las tecnologías de transporte y conectividad utilizadas para soportar dichos servicios.

En este nivel se incluyen elementos conocidos como Call Servers y Media Servers.

- Un **Call Server** provee control de la llamada de acuerdo con un modelo de llamada, se encarga del manejo de la señalización y del control de los Media Gateways. También provee una interfaz (p.e. un protocolo estándar o un API abierto) hacia los Servidores de Aplicaciones ubicados en el Nivel de Aplicaciones, para habilitar los servicios y controlar las políticas (p.e. políticas de QoS personalizadas, políticas de AAA, etc.).

  Múltiples Call Servers podrían cooperar para manejar una llamada sencilla. Los Call Servers más conocidos son: **Gatekeepers H.323**, **Call Manager, Call Agents, SIP Proxy Servers y Softswitch**.

- Un **Media Server** habilita la interacción entre los abonados llamantes y las aplicaciones mediante diferentes funciones, tal como provisión de tono para marcar o anuncios. Otras funciones más avanzadas de estos servicios, podrían ser respuesta de voz interactiva y la conversión texto-a-voz o voz-a-texto.

La base fundamental del Nivel de Control es el Ambiente de Procesamiento Distribuido (DPE), el cual es la unión invisible que permite la interacción entre los niveles de transporte y aplicación en la NGN. El DPE ofrece una infraestructura de software para soportar el desarrollo e implementación de aplicaciones distribuidas en las redes NGN.

Así, la inteligencia de la red puede ser distribuida a las localizaciones más convenientes dentro de la red o, si es apropiado, al CPE. Por ejemplo, la inteligencia de la red podría residir en servidores de propósito general corriendo los componentes necesarios para un servicio particular, sobre servidores que realizan funciones específicas (por ejemplo, Puntos de Control de Servicio [SCPs], Periféricos Inteligentes, y Nodos de Servicio en un ambiente AIN), o en los dispositivos de borde cerca del cliente. Las capacidades funcionales no estarán más atadas a los elementos físicos de la red.

La Red de Señalización SS7 es la aproximación más cercana a un DPE en una red actual de telecomunicaciones tradicional. Por lo tanto el DPE en NGN heredará las funciones de alto nivel de las redes SS7 actuales y adicionará muchas más funcionalidades para satisfacer los requerimientos de los servicios de banda ancha de la próxima generación.

4.5.1.3. Nivel de Aplicaciones

Este nivel corresponde al nivel de aplicación de la torre OSI, y es donde los servicios son definidos y desde donde se maneja toda la inteligencia de la red.

Una cualidad esencial de las redes NGN, es su trabajo con arquitecturas e interfaces abiertas en el Nivel de Aplicación. Un ambiente de desarrollo abierto basado en APIs abiertos, permitirá a los desarrolladores de aplicaciones de telecomunicaciones, a los proveedores de servicios e inclusive a los usuarios finales, crear e introducir nuevas aplicaciones rápidamente y transparentemente. En el ANEXO B se presenta la descripción de los principales protocolos que están siendo utilizados para la implementación de APIs abiertos.

Con la separación de este nivel, se agiliza la introducción de nuevos servicios dando a los proveedores de servicios más control sobre el proceso de introducción de servicios y permitiendo la reutilización de componentes de aplicaciones existentes.

En este nivel se encuentran Servidores de Aplicaciones (Application Server), y Servidores de Características (Feature Server)

- Un **Servidor de Aplicaciones** se encarga de introducir, ejecutar, controlar y administrar servicios avanzados. Los Servidores de Aplicaciones deben interactuar con los Call Servers y otros recursos controlados, a través de protocolos o APIs abiertos.

  Entre los servicios controlados se incluyen: enrutamiento y contabilización de llamadas, protección de llamadas, políticas para AAA y QoS, grupos cerrados de usuarios, entre otros.

  Las principales funciones que deben realizar son: manejo del Ambiente de Ejecución de la Lógica del Servicio (SLEE – Service Logic Execution Environment), administración del ciclo de vida del servicio, soporte para desarrollo de políticas y servicios por medio de APIs, administración del sistema y servicio, soporte de mecanismos de registro.

4.5.2. SERVICIO VPN HIBRIDO CON LAS REDES NGN

Las redes NGN permiten ofrecer avanzados servicios, sin importar donde están ubicados los usuarios, cuales terminales están utilizando o la red de acceso a la que están conectados. Esta nueva clase de servicios tiene que ser desarrollada en varios ambientes de red: redes fijas (RTPC, Red Inteligente, RDSI, xDSL), redes móviles (GPRS, 3G-UMTS) e Internet.

Más que reemplazar las plataformas de telecomunicaciones anteriores, las redes NGN buscan reutilizar y aprovechar los sistemas heredados existentes (tal como las Redes Inteligentes) y extender la prestación de los servicios que se ofrecían sobre dichas redes (p.e. VPN).

Para lograr una suave migración desde servicio RI hasta servicios NGN, se requiere:

- Desarrollar APIs abiertos para comunicar el Servidor de Aplicaciones (Application Server)con SCPs de diferentes vendedores, ya que cada fabricante de RI cuenta con sus propias herramientas de creación y uso de la lógica de servicio.

- Proveer en la red NGN entidades que actúen como un SSF para un SCF supervisor, como por ejemplo el Servidor de Llamadas (Call Server). Estas entidades deben ser capaces de mapear mensajes INAP a sus protocolos soportados (p.e. H.323, H.248, SIP).

En la Fig. 4.8 se presenta la integración entre una red NGN y una Red Inteligente, considerando el protocolo SIP como el protocolo de señalización entre los terminales y los elementos de red (Call Server y Media Gateways) y entre los elementos de red.

SIP es un protocolo de control del nivel de aplicación que puede establecer, modificar y terminar sesiones o llamadas multimedia. SIP maneja principalmente los mecanismos de establecimiento (set-up) y cuelgue (tear down) de la llamada y es independiente de la transmisión de flujos de información entre el llamador y el receptor.

SIP está siendo estandarizado por el IETF y está surgiendo dentro de los cuerpos de estandarización como la tecnología habilitadora para proveer el soporte de señalización en las Redes de Próxima Generación, en especial en los grupos de desarrollo de aplicaciones móviles como 3GPP (*Third Generation Partnership Project*), donde toda la señalización de las llamadas multimedia IP será desarrollada a través de este protocolo.

Sobre la arquitectura presentada en la *Fig. 4.8* es posible implementar una amplia variedad de servicios. Uno de los más importantes es el servicio VPN.

4.5.2.1. Características del servicio VPN híbrido

En el servicio VPN sobre redes híbridas las llamadas pueden ser originadas y terminadas sobre la Red Inteligente y también sobre la Red NGN. Los usuarios de la VPN pueden utilizar como terminales para establecer la comunicación: computadores, teléfonos IP (SIP, H.323, MGCP), terminales UMTS o teléfonos convencionales.

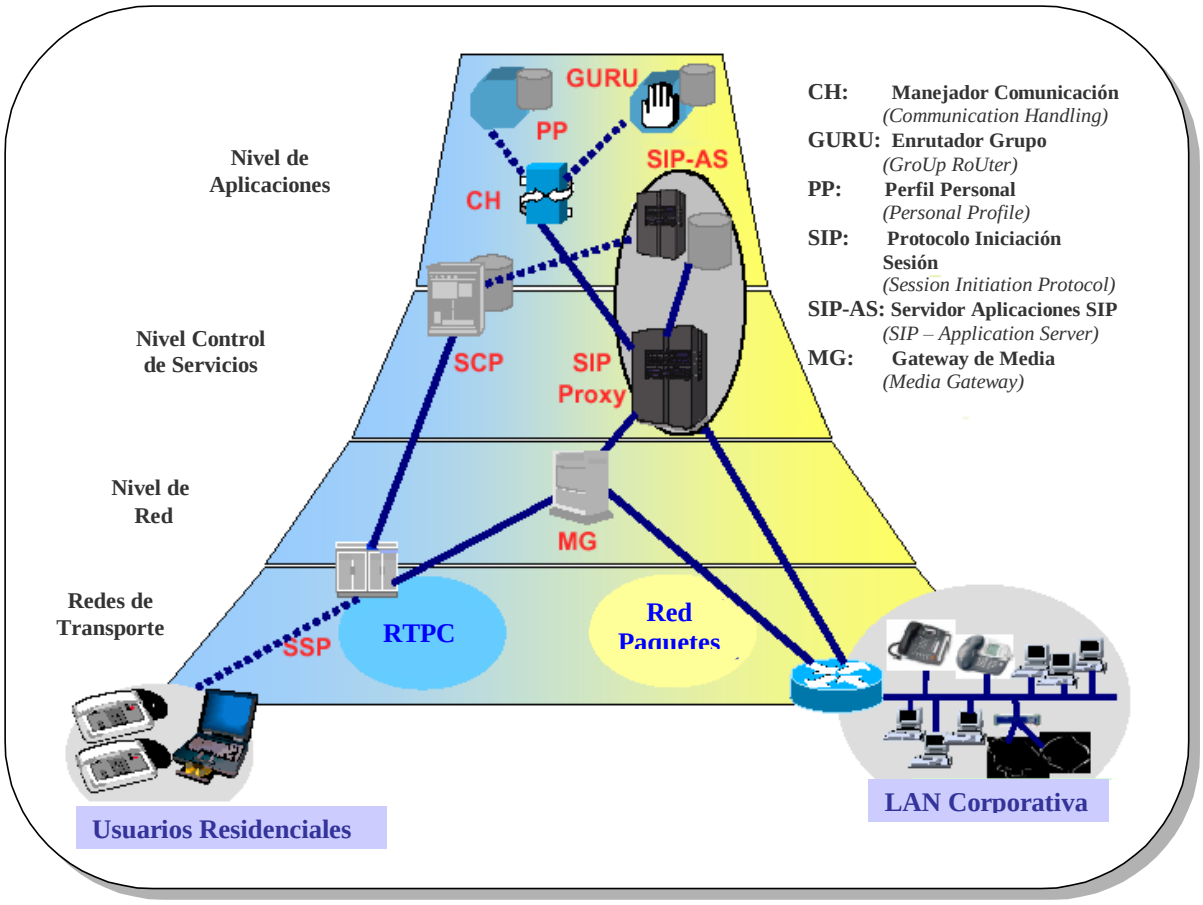


Fig. 4.8. Integración Red Inteligente – Redes de Próxima Generación

En el servicio VPN híbrido los usuarios cuentan con las características de servicio descritas en el Capítulo 2 para el servicio VPN sobre Redes Inteligentes. Entre las principales características se destacan: Plan de Numeración Privado (número o nombre lógico), Grupo Cerrado de Usuarios, Marcación Abreviada, Gestión de Perfil de Abonado, Filtrado de Llamadas Entrantes, Filtrado Llamadas Salientes, Llamadas dentro de la red (On-net) y Llamadas Fuera de la Red (Off-net).

A continuación se mencionan los diferentes escenarios que se pueden presentar al originar y terminar llamadas, dentro y fuera de la red, desde diferentes tipos de terminales (IP o teléfonos convencionales).

- **Llamadas On-net.** El usuario llamado es un miembro de la VPN: el "número marcado" puede ser un número o un nombre lógico, dependiendo del tipo de terminal utilizado. Los posibles escenarios presentados son:

  - *Llamada IP a IP:* Un usuario A miembro de la VPN registrado sobre un terminal IP llama a otro usuario B de la VPN. La lógica del servicio verifica que B está registrado sobre un terminal IP. En ese caso la llamada es una llamada de VoIP. El usuario A llama al usuario B con un nombre / número lógico que será trasladado a la dirección IP del terminal donde el usuario B está registrado.

  - *Llamada IP a RTPC:* Un usuario A miembro de la VPN registrado sobre un terminal IP, llama a otro usuario B de la VPN registrados sobre un teléfono de la RTPC. La lógica traslada el nombre / número lógico usado por el usuario A para llamar al usuario B y detecta que B está registrado sobre un teléfono RTPC.

    La lógica chequea si el usuario A está autorizado para llamar a un teléfono RTPC y al usuario B o a un teléfono y verifica como B quiere manejar las llamadas entrantes desde A (p.e. enrutarlas a un teléfono IP). La lógica enruta la llamada a la RTPC a través de un gateway de voz y monitorea su terminación.

  - *Llamada RTPC a IP:* Un usuario A miembro de la VPN, registrado sobre un teléfono RTPC, llama a un usuario B de la VPN registrado sobre un terminal IP. La línea de teléfono está registrada como una línea de la VPN.

    El usuario A marca un código de acceso y el número VPN que identifica al usuario B. La lógica, impulsada por los componentes de la Red Inteligente, enruta la llamada a la red IP, a través de un gateway de voz, y monitorea su terminación. La lógica podría verificar las reglas del usuario A para llamadas salientes y las reglas del usuario B para llamadas entrantes.

- **Llamadas Off-Net.** El usuario llamado no es un miembro de la VPN. El "número marcado" es un número de la RTPC predefinido con un código específico (p.e. "0").

  - *Llamada IP a RTPC:* Un usuario A miembro de la VPN, registrado sobre un terminal IP, llama a un usuario B externo a la VPN, marcando un número RTPC. La lógica detecta si el usuario A está autorizado para realizar llamadas RTPC externas (diferentes clases de llamadas podrían ser definidas: Llamadas internacionales, llamadas nacionales, llamadas locales, etc.). En caso de una llamada autorizada, la lógica enruta la llamada hacia la RTPC a través de un gateway de voz y monitorea su terminación.

  - *Llamada RTPC a RTPC:* Un usuario A miembro de la VPN, registrado sobre un teléfono RTPC, llama a un usuario B externo a la VPN, marcando un número RTPC. En este escenario la Red Inteligente se encarga de todo el procesamiento de la llamada.

- **Llamadas de Acceso Remoto.** El usuario que origina la llamada es un miembro de la VPN, pero se encuentra fuera de la VPN.

- Un usuario A miembro de la VPN, se encuentra en su casa o en cualquier otro lugar fuera de la VPN y llama a un usuario B. El usuario A debe marcar un número de Red Inteligente para acceder la VPN y ser identificado como un usuario VPN con permisos para realizar llamadas de Acceso Remoto. Después de ser identificado como miembro de la VPN, la lógica considera que el usuario está dentro de la VPN y procesa las llamadas de igual manera que en los casos On-net y Off-net.

4.5.2.2. Ejecución del Servicio VPN Híbrido.

La *Fig. 4.9* describe el flujo de llamada para una llamada On-Net originada desde un teléfono RTPC. Un usuario A miembro de la VPN registrado sobre un teléfono RTPC origina una llamada hacia un usuario B miembro de la VPN registrado sobre un terminal IP.

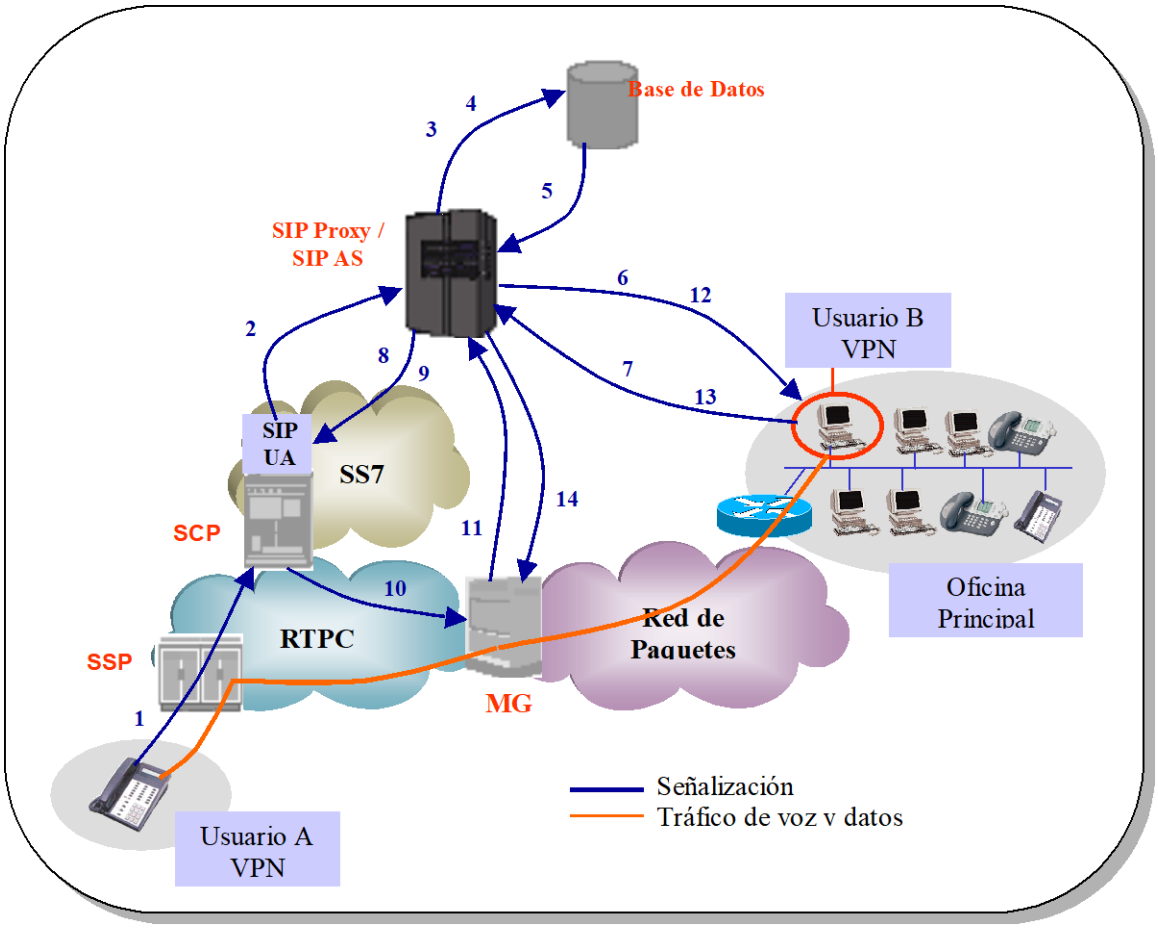


Fig. 4.9. Llamada On-net originada desde un terminal RTPC

En la *Fig. 4.9* se puede observar como la tecnología SIP puede ser utilizada para la interoperabilidad entre la arquitectura IP y la arquitectura de RI tradicional. El elemento principal en la arquitectura es el Servidor de Aplicaciones SIP programable (SIP AS), que

para el ejemplo se comporta también como un Servidor SIP Proxy (SIP Proxy/AS). Esto significa que se unifican en un equipo el Servidor de Llamadas (Call Server) y el Servidor de Aplicaciones (Application Server) mostrados en la *Fig. 4.8.*

El SSP y el SCP corresponden a los elementos de red habituales de un sistema de Red Inteligente. Sobre el SCP aparece una caja definida como SIP-UA, Agente de Usuario SIP (SIP – User Agent), el cual habilita al SCP para interactuar con el SIP Proxy/AS. El SIP-UA se implementa sobre un SCP comercial utilizando un ambiente de desarrollo propietario (requerimiento indispensable para interoperabilidad).

La señalización SIP (entre SCP y SIP AS) es transportada sobre una conexión TCP-IP. Un Gateway de Media (SIP-MG) conecta la RTPC y la red de paquetes en el nivel de transporte y se comunica con el SIP Proxy/AS para enrutar las llamadas. En este caso la señalización es transportada sobre UDP.

A continuación se presenta la ejecución del servicio paso a paso:

1. El usuario A miembro de la VPN marca el numero del usuario B miembro de la VPN. El SSP contacta al SCP para solicitar información del procesamiento de la llamada.
2. El SIP-UA (sobre el SCP) se comunica con el SIP Proxy/AS para que envíe un requerimiento al usuario final.
3. El SIP Proxy/AS verifica el perfil del usuario A para determinar si el usuario tiene autorización para realizar esta llamada (Filtrado de Llamadas Salientes) y verifica el perfil del usuario B para determinar como desea el usuario manejar la llamada (Filtrado de Llamadas Entrantes).
4. El SIP Proxy/AS traslada el número llamado.
5. La dirección IP del computador asociado es retornada al SIP Proxy/AS y este empieza el monitoreo de la llamada.
6. El SIP Proxy/AS hace una invitación al computador del usuario B. Este paso establece la sesión en el nivel de señalización pero la comunicación está suspendida.
7. El usuario B acepta la llamada y el computador envía una repuesta afirmativa al SIP Proxy/AS.
8. El SIP Proxy/AS envía la respuesta afirmativa al SCP (en respuesta al requerimiento del paso 2).
9. El SIP Proxy/AS envía una notificación al SCP para informar acerca del resultado de la invitación.
10. El SCP selecciona un Gateway de Media (MG) (que se encargará de la conversión de voz a paquetes) e instruye al SSP para enrutar la llamada hacia el MG y para aplicar el plan de cobro apropiado.

11. El MG envía un requerimiento al SIP Proxy/AS (con el apropiado SDP) para que envíe una nueva invitación al computador del usuario B. El SIP Proxy/AS identifica la llamada en estado de espera y recupera la información relevante.

12. El SIP Proxy/AS envía la nueva invitación al computador del usuario B, incluyendo el SDP del Gateway de Media (MG).

13. El computador del usuario B modifica los parámetros de la llamada con la información SDP y envía una respuesta positiva al SIP Proxy/AS aceptando la llamada.

14. El SIP Proxy/AS envía la respuesta con la información relacionada con el usuario B al Gateway de Media (SIP-MG). El MG establece el camino (enruta la llamada) entre los usuarios A y B y se inicia la comunicación.

5. APLICACION DEL SERVICIO VPN

En los capítulos anteriores se han presentado las principales características y beneficios que obtienen las empresas al implementar Redes Privadas Virtuales de voz y Redes Privadas Virtuales de datos, como un medio para optimizar sus sistemas de comunicaciones en el ámbito global y disminuir considerablemente sus gastos.

Estas ventajas deben ser evaluadas en los más altos niveles administrativos, ya que la implementación de una VPN puede generar traumatismos, debido a los cambios tecnológicos que es necesario realizar, a la nueva cultura informática que se debe implantar, a la reducción del personal de asesoría y administración de la red de comunicaciones delegada ahora en gran parte al proveedor del servicio.

En este capítulo se mencionan algunos aspectos que deben ser tenidos en cuenta a la hora de implementar una Red Privada Virtual. Así como un análisis de la situación actual del mercado de cada una de las tendencias en VPNs mencionadas en los capítulos 3 y 4 y algunas consideraciones para decidir cuando implementar cada una de ellas.

Adicionalmente se presentan ejemplos de operadores internacionales que actualmente están ofreciendo el servicio VPN de voz en el mundo, un análisis de los problemas que impidieron su implementación en Colombia y finalmente una perspectiva del futuro de las VPNs en Colombia

5.1. PLANEACION E IMPLEMENTACION DE UNA VPN

5.1.1. FACTORES DETERMINANTES DE LAS VPNS

Los constantes y rápidos cambios tecnológicos han permitido a las empresas desarrollar una gran variedad de servicios y aplicaciones que les permitan ser competitivas en sus propios mercados.

A la par con el incremento de las necesidades de las empresas, las compañías prestadoras de servicios de telecomunicaciones han ampliado el rango de opciones disponibles, siendo cada vez más difícil seleccionar el servicio y la tecnología que más se adecuen a dichas necesidades. Las opciones varían desde líneas dedicadas, Red Telefónica Pública Conmutada (RTPC), Centrex de Área Ancha (WAC), Redes Privadas Virtuales de voz y de datos, hasta Outsourcing.

La decisión del sistema de comunicaciones que se debe emplear se ve influenciada no sólo por el nivel de servicio que se desea obtener, sino también por el capital de inversión que la empresa este dispuesta a realizar. Aunque todas las empresas cuentan con

diferentes necesidades, servicios y equipos, cada una de ellas le da un valor diferente a los factores que influyen en la determinación de la mejor solución.

Algunos de estos factores son (Ver *Fig.5.1*):

- Características de sus comunicaciones.
- Tipo de necesidades de sus negocios.
- Patrones de tráfico.
- Topología de la red existente.
- Extensión geográfica de la organización.
- Disponibilidad de equipos y servicios.
- Prioridades de gestión.
- Necesidades del usuario final.
- Aplicaciones.
- Prioridades operacionales.

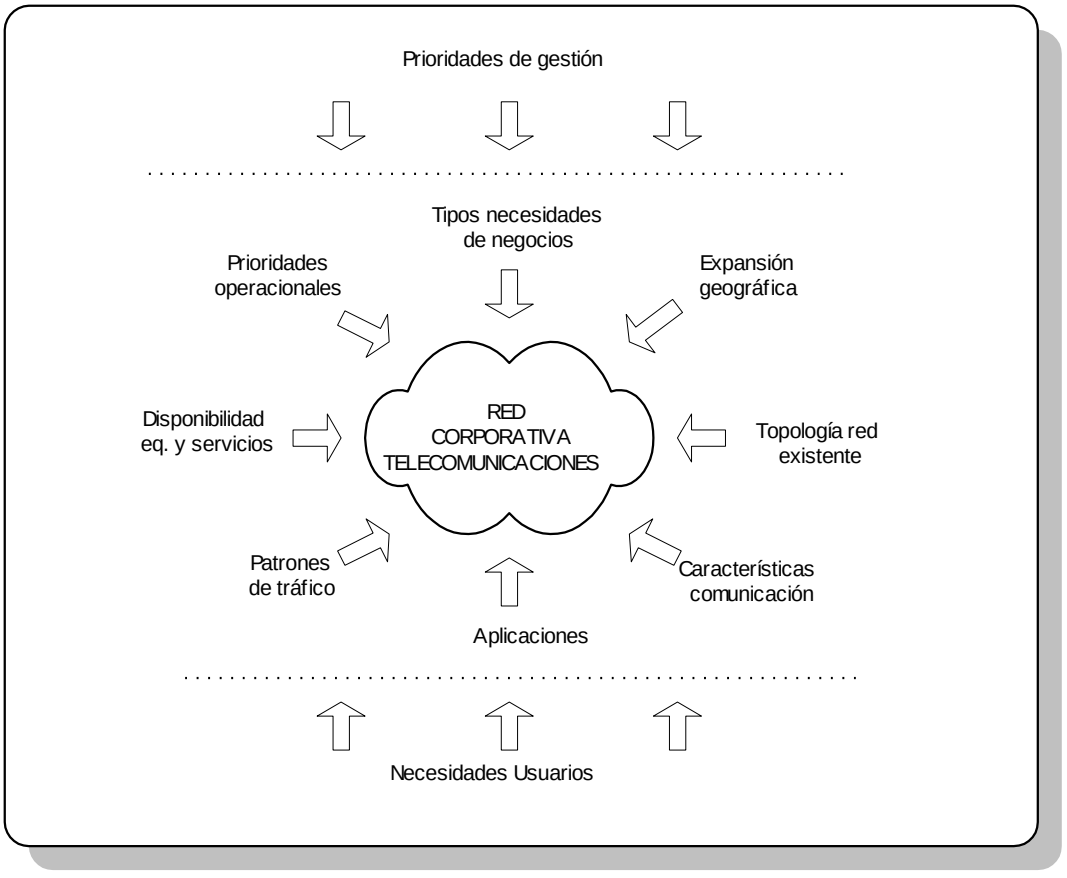


Fig. 5.1. Fuerzas que influyen en las soluciones de Redes

5.1.2. RECOMENDACIONES PARA IMPLEMENTAR UNA VPN

Como resultado de la experiencia que se ha tenido en el ámbito mundial, los administradores de telecomunicaciones ofrecen a los nuevos usuarios en todo el mundo

algunas consideraciones que se deben tener en cuenta al implementar una Red Privada Virtual, independientemente de la arquitectura de red seleccionada.

- **Buena planeación.**

  Es necesario invertir bastante tiempo en la etapa de planeación. Como herramientas para tomar una decisión se debe contar, entre otros, con un análisis detallado de tráfico y el estudio de los patrones de tráfico que maneja la compañía. Si la justificación de una red VPN no se hace basada en un análisis sólido y seguro, se pueden cometer muchas equivocaciones, y no aprovechar al máximo el servicio.

- **Estar preparado para manejar un "mar de información".**

  Los usuarios que deben seleccionar un operador para manejar su red de comunicaciones, se enfrentan con una gran cantidad de información. El estudio de dicha información debe realizarse minuciosamente y debe permitir establecer comparaciones y seleccionar lo que más se adecue a las necesidades de la empresa.

- **Emplear un correcto esquema de numeración.**

  Se debe tener mucho cuidado en seleccionar un correcto esquema de numeración. Por ejemplo, en caso de que se presenten conflictos con los códigos de marcación en la área pública o con un sistema existente de numeración en una PBX, requiere tiempo ordenar la confusión y la compañía terminará haciendo ajustes los cuales dejarán un esquema final de numeración mucho menos que el ideal.

- **Usar avanzada tecnología de PBX.**

  Se recomienda que la tecnología de PBX dentro de una compañía para conectar una red virtual debe ser "la más sofisticada que esté disponible, para que el usuario pueda realmente tomar ventajas de funcionalidades virtuales y RDSI futuras". Debe ser capaz de desarrollar todas las ventajas de VPN, de reconocer llamadas on-net, manejar señalización fuera de banda y forzar reenrutamientos on-net.

- **Evaluar la tecnología de conmutación de la empresa de telecomunicaciones.**

  Una de las principales razones para que el servicio VPN sea confiable se debe al alto nivel tecnológico instalado por los operadores para prestar el servicio. No todas las telcos han adoptado los niveles de tecnología de conmutación encontrados en otras partes del mundo. Por esto, es necesario verificar la tecnología utilizada y si los equipos son capaces de proporcionar el rendimiento que realmente se espera de ellos.

- **Poner atención a los aspectos culturales y organizacionales de la implementación.**

  Es importante poner atención a los miembros de la organización y a sus preocupaciones sobre la implementación de VPN. Esto no sólo aplica a la forma como se emplea la tecnología, sino también a las preocupaciones entre los asesores de telecomunicaciones respecto a la redundancia posible. La experiencia ha

demostrado que si se presta cuidado en la familiarización de los procesos en los niveles operacionales, esto animará una rápida aceptación de VPN a todo lo ancho de la compañía.

- **Manejar contratos flexibles.**

  Los usuarios pequeños, en particular, están interesados en cerrar contratos a largo plazo, esto puede ser desventajoso ya que les impide tomar ventajas de próximas reducciones de precios en el mercado, lo cual puede ocurrir después de que el contrato sea firmado.

5.2. CONSIDERACIONES PARA SELECCIONAR UNA VPN

5.2.1. COMPORTAMIENTO DE LAS VPNS EN EL MERCADO ACTUAL

La relación entre los diferentes tipos de redes VPNs de voz y datos y su participación en el mercado, se puede analizar desde el punto de vista del "Ciclo de Vida de la Tecnología" descrito por Geoffrey A. Moore, autor de los libros "Cruzando el Abismo" *(Crossing the Chasm)* y "Dentro del tornado" *(Inside the tornado)*. (Ver *Fig. 5.2.*)

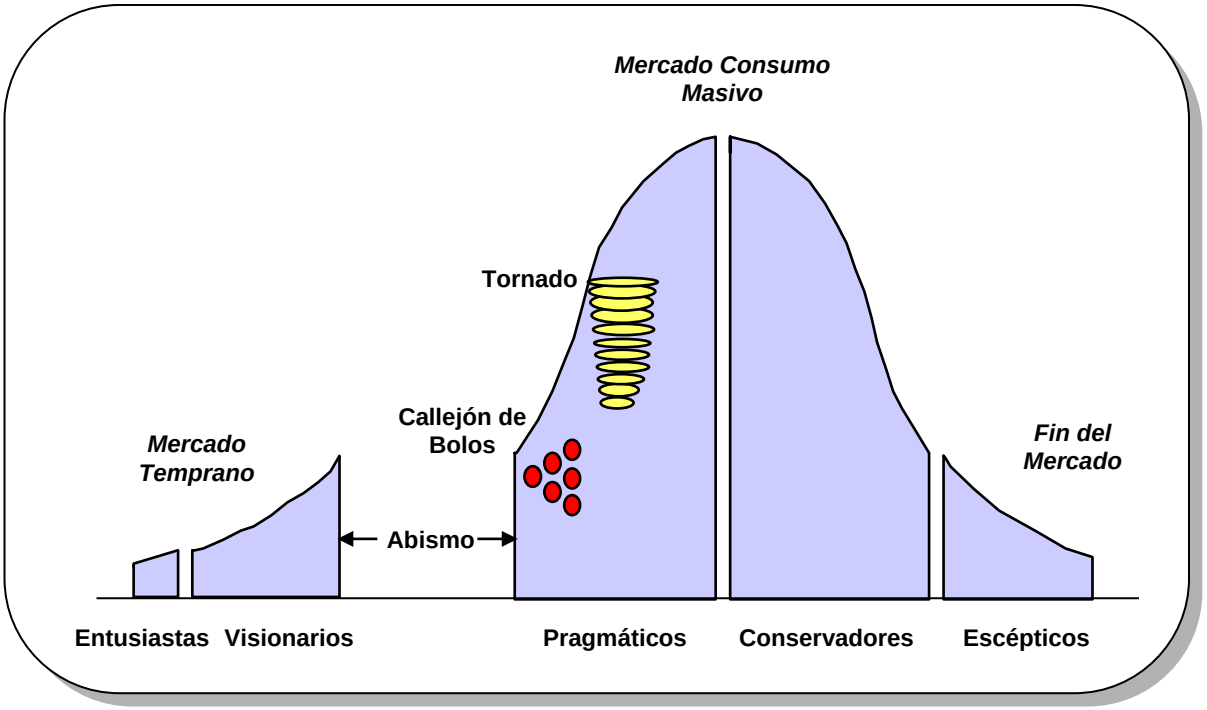


Fig. 5.2. Ciclo de Vida de Adopción de la Tecnología

El ciclo comienza con un pequeño grupo de entusiastas y visionarios que apoyan la innovación y quieren ser los primeros en adoptar la nueva tecnología. Cada nueva

tecnología encuentra un punto crítico en el ciclo de la adopción del mercado, llamado Abismo (chasm). En este momento, los pragmáticos necesitan ver las grandes ventajas de adoptar una nueva tecnología antes de decidir cambiar una tecnología que ya está entregando beneficios.

Una vez la tecnología pasa la prueba de adopción del mercado, al satisfacer las necesidades de un nicho específico del mercado, los pragmáticos aceptan la nueva tecnología y se inicia la fase de callejón de bolos (bowling alley). A medida que más nichos son penetrados, la tecnología va ganando impulso y se entra en la etapa de tornado.

Las redes **VPNs IP**, están empezando a entrar a la etapa del tornado. El tornado es un periodo en el que el mercado masivo adopta rápidamente el nuevo paradigma. En esta etapa el precio viene a ser extremadamente importante. Una vez el supercrecimiento del tornado pasa, la tecnología se mueve a la fase de Mercado de Consumo Masivo (mainstream market), donde la oferta y la demanda encuentran el equilibrio.

FR y **ATM** ya cruzaron sus abismos y las fases de callejones de bolos y tornado, y han entrado en las fases conservativas y escépticas. Las tasas de crecimiento de los ingresos han estado decreciendo, aunque los resultados aún son positivos, puesto que ya han capturado muchos de los mercados que podían penetrar.

Por otro lado, los mercados para **VPNs de voz** son relativamente planos e inclusive están declinando en algunas regiones del mundo. Esta tecnología se está acercando a la fase final del mercado. El mercado ve el producto maduro y como un artículo de consumo (commodity), por lo que solamente el precio es el principal factor de decisión.

5.2.2. ELECCIÓN ENTRE VPNS DE VOZ Y VPNS DE DATOS

Las necesidades y requerimientos de los usuarios, así como el tipo de tráfico determinarán la mejor solución a la hora de implementar una VPN.

Las redes de datos son completamente indispensables para los usuarios corporativos hoy en día, ya sea basadas en redes dedicadas, redes FR, redes ATM o redes IP. Por esto una de las principales decisiones que deben tomar las empresas en el momento de implementar su red de comunicaciones, es la manera de manejar su tráfico telefónico tanto interno como externo.

Las dos opciones entre las que deben elegir son (1) la transmisión de la voz sobre paquetes utilizando una red de datos (VoFR, VoATM, VoIP), o (2) transportar la voz sobre circuitos utilizando servicios avanzados tal como el servicio VPN de voz.

En el caso de la transmisión de voz sobre paquetes, las empresas instalan equipos que se encargan de la compresión de voz y de su conversión en paquetes que luego son transportados a través de los enlaces de sus redes privadas de datos (FR, ATM, IP). Esta solución ha sido muy utilizada por las empresas en los últimos años a través de

redes Frame Relay y ATM. Como se mencionó en la sección anterior, estas tecnologías ya superaron la fase de Mercado de Consumo Masivo.

La transmisión de voz también puede realizarse sobre redes IP, sin embargo la utilización del servicio VPN IP explicado en el Capítulo 4, todavía debe madurar mucho antes de lograr una gran participación en el mercado (Fase de tornado). Adicionalmente, de los 3 tipos de redes VPN IP mencionados en el capítulo 4 solamente las redes VPN IP Intranet podrían ofrecer una buena solución de transmisión de voz a los clientes corporativos. Se debe recordar que las redes VPN IP Intranet se comportan igual que las redes VPN FR/ATM.

A pesar de la fuerte acogida de la transmisión de voz sobre paquetes, existen razones muy importantes por las cuales las redes VPN de voz continúan teniendo una gran acogida en muchos países en el mundo, (ver ejemplos en la sección 5.4):

- Si la empresa maneja volúmenes de tráfico muy altos entre sus oficinas, la solución de voz sobre paquetes sería demasiado costosa por los equipos y el ancho de banda necesario para transmitir las llamadas simultáneas. A diferencia de esto, con las redes VPN de voz la empresa podría negociar muy buenos acuerdos de precios por volumen de tráfico de LDN y LDI con el proveedor del servicio.

- Si la empresa maneja muchas llamadas a diferentes destinos internacionales (no necesariamente oficinas corporativas), puede obtener descuentos especiales en las tarifas de LDI utilizando el servicio VPN de voz.

- Si la empresa cuenta con una gran cantidad de usuarios remotos (móviles o trabajadores en casa), las redes VPNs de voz les permiten realizar llamadas off-net con cargo a la VPN obteniendo descuentos significativos. Esto no se puede lograr a través de una red corporativa de datos.

- Si la empresa pertenece a una asociación o agrupación especial de empresas, podrían crear una red VPN de voz, obteniendo precios especiales y un plan de numeración privado. Generalmente en este tipo de asociaciones las empresas quieren mantener sus redes de datos independientes, por lo que el servicio de red privada no es una solución adecuada.

- Si la empresa cuenta con equipos de datos que no ha terminado de depreciar puede manejar una estructura paralela para voz y para datos.

Todas las razones mencionadas para utilizar las VPNs de voz son razones económicas, y esto se debe a la madurez de la tecnología. Aunque esta solución ya se está acercando a la fase de Fin de Mercado, faltan aún varios años para que las nuevas soluciones sobre redes de datos puedan reemplazarlas y aún así no lo harían completamente.

La introducción al mercado de las Redes de Próxima Generación, que apenas están en su fase de Mercado Temprano, brindarán una completa interoperabilidad entre los servicios de la red de circuitos y la red de paquetes, por lo que garantizará la permanencia de los servicios VPNs de voz por mucho más tiempo.

5.3. VPNS EN COLOMBIA

Antes de la apertura de las telecomunicaciones en Colombia el único operador de LDN y LDI era TELECOM y debido a que el alcance del servicio VPN implica cobertura nacional e internacional, los operadores locales que contaban con Redes Inteligentes (Emcatel, EEPPM y ETB) estaban obligados a interconectarse con Telecom para hacer la terminación de las llamadas.

Sin embargo se presentaron grandes problemas para la interconexión de las redes que solamente hasta este año están siendo solucionados y que han hecho que el único operador de Redes Inteligentes que ofrezca el servicio en el país, desde hace algún tiempo, sea TELECOM.

5.3.1. PROBLEMAS DE IMPLEMENTACION DEL SERVICIO VPN DE VOZ

- **Problemas Regulatorios – Señalización**

  El Ministerio de Telecomunicaciones de Colombia cuando expidió las dos versiones de la norma nacional de SS7 (la cual esta basada en la UIT), solamente definió los parámetros para protocolos MTP e ISUP.

  "En el Sistema de Señalización por Canal Común N.º 7 Colombiano (SSC7), la interconexión entre operadores se realizará únicamente a nivel de la parte de usuario RDSI (ISUP)" (Capítulo 1 Pág.8 – Norma Nacional SSC7 de 1988)

  Esto significa que nunca se expidió una norma para definir los servicios de usuario (parte de usuario y parte de aplicación) del protocolo SS7 requeridos por la Red Inteligente (TCAP e INAP).

  Aunque los operadores podían ponerse de acuerdo para establecer la interoperabilidad, no lo hicieron porque (1) era un trabajo dispendioso definir acuerdos de par en par y (2) como no era obligatorio por norma, por decisión de competencia ninguno estaba interesado en facilitar el negocio a los otros.

  Sin embargo la Comisión de Regulación de Telecomunicaciones expidió el 4 de enero de 2002 la *Resolución 469 de 2002*, por medio de la cual se modifica la resolución CRT 087 de 1997 y se expide un Régimen Unificado de Interconexión (RUDI), con el cual se hace exigible la interconexión entre operadores y se libera la utilización de la norma de señalización.

  Artículo 4.2.1.1. – Derecho a la Interconexión: Todos los operadores tienen el derecho a solicitar y a que se les otorgue interconexión, acceso a servicios adicionales a la interconexión, a redes de otros operadores que los primeros requieran para la adecuada prestación de sus servicios.

Artículo 4.2.1.12. – Señalización: Los operadores de servicios de Telecomunicaciones están en libertad de negociar con los demás operadores la adopción de la norma de señalización que resulte más apropiada para efectos de la interconexión entre sus redes.

A pesar que jurídicamente ya no hay restricciones para la interoperabilidad, sería necesario que los operadores de RI superen los problemas técnicos (interconexión de redes) y comerciales (acuerdos ínter administrativos) con los demás operadores antes de que sea viable pensar en la prestación del servicio VPN.

- **Problemas Regulatorios - Numeración**

En el anterior Plan de Numeración Nacional la RI estaba prevista con numeración 9XXXXX, pero para los operadores locales estos números solamente tenían aplicación local, y muchas empresas necesitaban aplicación nacional, y más aún, persistía el problema de la larga distancia.

Después de la entrada de Orbitel y ETB al mercado de Larga Distancia Nacional e Internacional la situación de los operadores locales para negociar la terminación de larga distancia se hizo más fácil, sin embargo, todavía se necesitaba demasiado esfuerzo comercial, y un acuerdo de interconexión con cada uno de ellos para que la llamada fuera enrutada. Legalmente los servicios de RI no eran considerados servicios de telefonía básica, por lo que los operadores no estaban obligados a enrutar estas llamadas sin previo acuerdo entre ellos. Con la resolución 469 de 2002 los operadores están obligados a permitir la interconexión.

El nuevo Plan de Numeración Nacional expedido por el Ministerio de Telecomunicaciones a través del *Decreto 25 del 11 de enero de 2002*, define en su Artículo 28 la nueva Numeración para Servicios. Los servicios de RI definidos son Cobro Revertido y Tarifa con Prima. Con este nuevo plan los operadores locales de Red Inteligente ya no tienen problemas para manejar su numeración a nivel nacional. Adicionalmente, en el futuro con la portabilidad de número la numeración ya no estaría atada a operadores específicos.

- **Problemas de Prestación del Servicio - Marcación**

El nuevo plan de numeración exige la utilización de un Número Nacional Significativo, N(S)N, de 10 dígitos, por lo que la numeración para cada operador estaría muy restringida y la ventaja de marcación abreviada del Plan de Numeración Privado no podría ser ofrecida a los usuarios.

Se podría presentar una solución para la marcación abreviada, pero únicamente para los usuarios corporativos en cuyas oficinas los PBXs puedan ser programados para reconocer el número RI y adicionar el código de acceso al número abreviado marcado por el usuario.

- **Problemas de Prestación del Servicio - Facturación**

  Si un usuario desea realizar una llamada de LDI, el operador local de RI, debe entregar la llamada al operador internacional. En este momento el operador internacional no distingue si el usuario es de RI y le hace la facturación al operador local. Cuando el operador local recibe la facturación debe entrar a su sistema para conciliar las llamadas y determinar si la llamada fue realizada a través de la RI.

  Este proceso es sencillo si las llamadas fueron originadas sobre líneas dedicadas (On-Net) pero en el caso de las llamadas de Acceso Remoto (off-net) el operador debe al final del mes decidir cuales llamadas se originaron con código de acceso a la RI y cuáles fueron llamadas normales. En otros países la solución a este problema se da mediante la utilización de Tarjetas VPN, similares a las tarjetas prepago con lo que las llamadas son automáticamente cargadas a la VPN.

- **Problemas de Comercialización y Mercadeo del Servicio**

  Además de todos los problemas de interoperabilidad y de prestación del servicio mencionados, los operadores colombianos han fallado en la forma de concebir y comercializar los productos. Los usuarios corporativos prefieren hacer sus propias redes privadas con operadores de datos (FR, IP) y transportar su tráfico corporativo a través de conmutación de paquetes.

  Recomendación de estrategia de entrada al mercado: Los operadores de telefonía de LDN y LDI podrían recuperar el tráfico telefónico que están perdiendo con operadores de datos, ofreciendo paquetes atractivos de servicios avanzados de telefonía, incluyendo el servicio VPN con tarifas muy reducidas. Con esta solución los usuarios no tendrían que comprar o alquilar equipos de compresión y digitalización de la voz, ni pagar ancho de banda adicional por la transmisión de los canales de voz (11Kbps aproximadamente por cada canal de voz).

5.3.2. OPERADORES DEL SERVICIO VPN EN COLOMBIA

Actualmente en el país los siguientes operadores cuentan con Redes Inteligentes:

- Operadores Telefonía Local: EMCATEL y EEPPM.
- Operadores Telefonía LDN y LDI: ORBITEL y TELECOM..
- Operadores Telefonía Local, LDN y LDI: ETB.

Como ya se mencionó en la sección anterior aunque los problemas regulatorios ya están siendo superados, aún se presentan problemas técnicos y comerciales que hacen que el servicio VPN de voz no sea considerado como un buen negocio con posibilidades de ser implementado por los operadores con Redes Inteligentes en Colombia.

- **EMCATEL**

  Cuentan con el servicio disponible en su Red Inteligente, sin embargo no es viable debido a los siguientes problemas: (1) interconexión con otros operadores para lograr cobertura nacional e internacional, (2) problemas de facturación mencionados en la sección anterior, (3) no hay muchos clientes que puedan aprovechar el servicio y estos clientes prefieren utilizan servicios dedicados o servicios de redes de datos (tienen acuerdos con EMTELCO para ofrecer estos servicios a nivel nacional).

- **EEPPM**

  Cuentan con el servicio disponible sobre su Red Inteligente y les parece muy interesante. Sin embargo al hacer el análisis de los Casos de Negocios no le ven viabilidad comercial ya que el alcance principal del servicio es nacional y tendrían que hacer alianzas con operadores nacionales para la terminación del tráfico. No obstante no lo han descartado por completo y si algún cliente estuviera interesado en el servicio lo podrían prestar. Cuentan con la red de EMTELCO, de la cual son dueños en un 99% para ofrecer los servicios de datos a nivel nacional.

- **ORBITEL**

  Tienen la posibilidad técnica de ofrecer el servicio sobre su Red Inteligente, pero consideran que no es un buen negocio ya que el mercado objetivo es muy limitado y ya ha solucionado sus problemas de comunicaciones utilizando redes de datos. Adicionalmente tendrían que llegar a los clientes a través de enlaces digitales demasiado costosos.

- **TELECOM**

  Ofrecen el servicio VPN de voz sobre su Red Inteligente a sus grandes clientes, pero no como un servicio de la red pública sino como un servicio privado. Esto se debe a que no pueden ofrecer enlaces conmutados en las principales ciudades y la conexión se debe realizar a través de enlaces digitales dedicados (E1s) desde el PBX hasta la Red de Telecom.

  La gran difusión de las redes VPNs de datos y las limitaciones en el acceso de los clientes, han hecho que en el último año la mayoría de sus clientes haya migrado hacia redes de datos con transmisión de voz sobre paquetes ofrecidas por TELECOM y que el servicio VPN de voz sea cada vez menos utilizado.

- **ETB**

  Cuentan con el servicio disponible en su Red Inteligente, pero a pesar de que podrían ofrecer accesos conmutados y accesos dedicados, así como llamadas on-net y off-net, han decidido no lanzarlo al mercado por dos razones principales: (1) Plan de numeración muy restringido y (2) competiría con su servicio de PBX corporativo que es muy rentable. Adicionalmente, están empezando a ofrecer soluciones de redes de datos a nivel nacional.

5.4. VPNS EN EL MUNDO

A diferencia de la situación presentada en Colombia, en muchos países del mundo las redes VPN de voz tuvieron una gran acogida entre los usuarios corporativos y aún cuentan con un gran potencial de negocios para los años venideros.

A continuación se presenta la descripción de los servicios VPN de voz de Telmex en México y Embratel en Brasil; dos de las empresas de telecomunicaciones más grandes de Latinoamérica y del mundo.

Adicionalmente, en el ANEXO D se presentan ejemplos de las VPNs de voz de operadores como AT&T en USA, Alestra en México, Vodafone y Retevisión en España, entre otros. Todos los ejemplos mencionados utilizan Redes Inteligentes.

5.4.1. TELMEX – MEXICO

TELMEX es la empresa líder de telecomunicaciones en México, y figura entre los 20 principales operadores en el mundo. Ofrece servicios de telefonía local, larga distancia nacional e internacional, acceso a Internet y transmisión de datos. Su red es 100% digital y cuenta con más de 67 mil kilómetros de Fibra óptica. En 1998 recibió licencias para telefonía inalámbrica fija y móvil y servicios PCS.

Telmex ofrece a sus clientes empresariales una amplia gama de servicios, dependiendo del tamaño de la empresa:

- Microempresas
- Pequeñas y Medianas Empresas
- Grandes Empresas (Financiero, Industria, Servicios, Gobierno y Turismo)

Los servicios de VPN de voz y redes de datos son ofrecidos para las grandes empresas. Dependiendo de las características mencionadas en la sección anterior sus clientes eligen el tipo de servicio que más les favorece:

- LADA VPNet: Permite la creación de una red corporativa de voz entre las instalaciones de los clientes utilizando la infraestructura de red pública y la Red Inteligente de Telmex.
- Red Uninet: Permite la creación de una red corporativa de datos entre dos o más puntos utilizando enlaces dedicados o las redes FR o IP de Telmex.

Según el Ing. Javier Sánchez, Subdirector de Ventas del Departamento de Industria de Telmex, el servicio **LADA VPNet** ha sido ofrecido desde hace aproximadamente 5 años y está siendo utilizado por entre el 80% y el 90% de todas las grandes empresas. Entre ellas se encuentran: Cemex, Coca Cola, Sabrita, Wall Mart, Palacio de Hierro, cadenas hoteleras, aerolíneas, entre muchas otras.

Adicionalmente, el Ing. Sánchez considera que a pesar de la facilidad de transmitir voz sobre las redes de datos, el servicio LADA VPNet continuará siendo utilizado durante al menos 2 o 3 años más, principalmente por las siguientes razones:

- Se requiere una gran cantidad de líneas telefónicas simultáneas, lo que haría la solución de datos en equipos y en ancho de banda demasiado costosa.
- El esquema tarifario basado en consumo de minutos es muy rentable comparado con el alquiler o compra de equipos para compresión de canales de voz. Además no han terminado de depreciar sus actuales equipos de datos.
- Obtención de los descuentos por manejar llamadas de usuarios móviles y llamadas internacionales no lograrían el volumen de tráfico requerido mensualmente.

El servicio LADA VPNet está disponible para empresas que cuentan con dos o más sitios de Larga Distancia con un consumo mínimo de 40,000 minutos mensuales de Larga Distancia Nacional o Internacional. En caso de que en seis meses consecutivos el Cliente no cumpla con el consumo mínimo mensual de 40,000 minutos, Telmex aplicará automáticamente la mejor tarifa de larga distancia para tráfico público conmutado de acuerdo a su consumo mensual.

Además de la cobertura nacional el servicio ofrece cobertura internacional a través de las alianzas definidas por Telmex con operadores internaciones.

LADA VPNet permite originar llamadas desde la red (on-net), así como desde la red pública conmutada a través de la tarjeta LADA VpNet (off-net) y terminarlas dentro (on-net) o fuera de la red (off-net). Adicionalmente servicio de operadora, control de llamadas, facturación detallada, enrutamiento alternativo, manejo de códigos de autorización, línea rápida (hot-line), entre muchos otros servicios.

A través de las funciones Lada VpNet el cliente controla y administra sus telecomunicaciones de acuerdo a sus requerimientos en cualquier parte del país (Ver *Fig. 5.3.*)

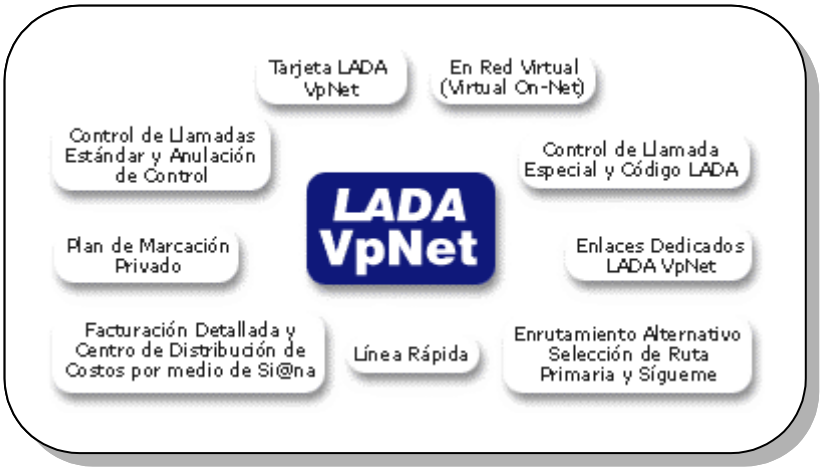


Fig. 5.3. Características del servicio LADA VpNet de Telmex

En el ANEXO D se presenta una explicación más detallada del servicio así como el esquema Tarifario de Telmex para la RED LADA VpNet (RLVPN). Los precios presentados fueron tomados del Libro Tarifario de Telmex (Sección 5) publicado en la página Web de la "Comisión Federal de Telecomunicaciones" (COFETEL) de México (http://www.cft.gob.mx/html/4_tar/telmex/indice.html) y están vigentes a partir del 08 de junio de 2002.

5.4.2. EMBRATEL – BRASIL

Embratel es el principal operador de telefonía de Larga Distancia Nacional e Internacional en el Brasil; surgió en 1998 de la privatización de Telebras monopolio del estado y fue adquirido por WorldCom. Ofrece servicios de telefonía básica de LDN y LDI, servicios avanzados de telefonía, transmisión de datos sobre redes FR, ATM e IP-VPN, acceso a Internet, radio y televisión, entre otros. Implementó la plataforma de Red Inteligente a principios de 2001.

Embratel ofrece a sus clientes empresariales tanto VPNs de voz como VPNs de datos, entre las cuales elegir dependiendo de las características mencionadas en la sección anterior:

- Servicios Avanzados de Telefonía: VipNet (Redes Privadas Virtuales).
- Servicios de Red Conmutados: FastNet (FR), ATMnet.
- Servicios de Internet: Business IP VPN.

VipNet es un servicio de Red Privada Virtual de voz, conocido también como Voice VPN (Virtual Private Network), que atiende oficinas no sólo en el Brasil sino también en el exterior.

El servicio VipNet había sido ofrecido por más de 3 años sobre una Red Integrada con la red pública, sin embargo el 26 de Marzo de 2002 fue lanzado el nuevo servicio migrado a la nueva plataforma de Red Inteligente de Embratel, instalada a principios de 2001 y sobre la cual ya estaban habilitados otros servicios como número 0800.

De acuerdo con el Gerente General de Servicios de Telefonía para el mercado corporativo de Embratel, Leonollo Patitucci, el nuevo producto tiene un mercado de 8.000 clientes potenciales.

El VipNet en la Plataforma de Red Inteligente permite realizar llamadas on-net y off-net, administrando con seguridad tanto el tráfico inter-corporativo como el extra-corporativo. Los clientes pueden contar con diversas facilidades soportadas por la Red Inteligente, tales como el plan de numeración privado y acceso remoto a la red VipNet, adquiriendo mayor agilidad en la comunicación y reduciendo costos de telefonía.

El nuevo servicio ofrece acceso a la red por medio de código especial y contraseña; discado abreviado con apenas tres dígitos; tarifas especiales para llamadas corporativas; restricción de llamadas por destinos predefinidos; informes de gestión de las llamadas por

centros de costos; y mensajes de navegación para orientación de los usuarios en la utilización de las instalaciones.

La conexión al servicio se realiza a través de enlaces digitales directos entre cada PABX del cliente y la Red Inteligente de Embratel, garantizando confiabilidad y seguridad en la comunicación.

Entre los precios definidos por el nuevo servicio VipNet sobre RI (Marzo 2002) se encuentran:

- Enlaces nacionales (LDN):
  - R$ 0,08/minuto entre ciudades a menos de 50Km. ($68 Pesos Colombianos aproximadamente).
  - R$ 0,18/minuto para ciudades distantes más de 50 Km. ($153 Pesos Colombianos aproximadamente).
  - El descuento por volumen - entre 25% y 30% - se aplica a clientes con cuentas superiores a R$ 50 mil.
- Enlaces internacionales (LDI):
  - EUA y Canadá - R$ 0,59 fuera de la red ($500 Pesos Col.); R$ 0,50 dentro de la red ($424 Pesos Col.)
  - Europa, Mercosur y Japón - R$ 0,89 fuera de la red ($755 Pesos Col.); R$ 0,71 dentro de la red ($602 Pesos Col.)
  - Demás países - tarifa de R$ 0,99 ($840 Pesos Col.)
  - El descuento por volumen – entre 25% y 30% - se aplica a clientes con cuentas superiores a R$ 35 mil.

La nueva etapa de VipNet sobre RI será la migración para la Red de Próxima Generación (NGN) de Embratel. Se trata de una plataforma basada en conmutación de paquetes soportada por el protocolo IP y que permite la interoperabilidad de las plataformas, sin necesidad de reemplazar los equipos existentes. Con esta nueva integración los clientes contarán con interoperabilidad de servicios entre la red pública y la red de paquetes.

En el ANEXO D se presenta una explicación más detallada del servicio VipNet y varios ejemplos de clientes que cuentan actualmente con el servicio en Brasil.

6. MANUAL DE USUARIO

Este capítulo presenta todos los aspectos relacionados con la operación del software de animación gráfica “Red Privada Virtual – VPN”. Esta herramienta guiará al usuario a través de los beneficios y características del servicio Red Privada Virtual, e incluye una demostración de la Ejecución del Servicio en cada uno de los tipos de llamadas disponibles.

6.1. ASPECTOS GENERALES

Este software se ejecuta en el entorno Windows; así que para su manejo sólo es necesario un conocimiento mínimo de este sistema operativo.

Ya que el ambiente gráfico se presenta de una manera general, los usuarios pueden usar este tutor de una manera muy fácil y amigable. En este capítulo se presenta la explicación para cada una de las opciones disponibles en el tutor.

6.2. REQUERIMIENTOS

6.2.1. REQUERIMIENTOS SOFTWARE

- Windows 95 o superiores.
- Navegador de Internet que soporte lenguaje html (se recomienda Microsoft Internet Explorer 4.0 o superiores).

6.2.2. REQUERIMIENTOS HARDWARE

- Procesador 80486 o superior.
- Memoria RAM: 32MB o superior.
- Disco Duro con capacidad de 10MB (solo si se desea copiar el tutor al PC).
- Monitor SVGA o superior.
- Resolución del monitor recomendada: 1200 x 768 pixels.
- CD-ROM 4x

6.3. INSTALACION

No es necesario instalar el programa para ejecutarlo. Para la ejecución del tutor se deben seguir los siguientes pasos:

- Insertar el CD (en el drive D o E) que contiene el software del tutor del servicio Red Privada Virtual.
- Entrar a Windows y escoger la opción EJECUTAR (RUN) del menú ARCHIVO del Administrador de Programas.
- Escribir "D:\vpn.html". Reemplace "D" por la letra del drive CD-ROM si es diferente.
- Presione OK o la tecla ENTRAR

6.4. DESCRIPCION DEL PROGRAMA

Después de ejecutar el programa desde el archivo "vpn.html", aparece la *"ventana principal del programa"* que se muestra en la *Fig. 6.1*.

Fig. 6.1. Ventana principal del programa

La parte superior de la pantalla, que incluye el escudo de la Universidad del Cauca y el título del programa, permanece siempre fija mientras el usuario navega.

Los dos botones que aparecen en la parte inferior de la pantalla se enlazan con las dos áreas en las que se encuentra dividido el programa: el área de tutor y el área de demostración.

El *área de tutor* resume los temas más importantes analizados en el presente trabajo de grado, permitiendo al usuario conocer de una manera didáctica las principales características de las redes VPN y su evolución por las Redes Inteligentes, las redes de datos y las redes de Próxima Generación.

El *área de demostración* presenta la ejecución del servicio considerando una red privada virtual internacional, ofrecida por un operador de red, y el funcionamiento de los diferentes tipos de llamadas.

Los siguientes son algunos comentarios generales del programa:

- Para poder pasar de un área a otra del programa es necesario regresar a la *ventana principal del programa*, la cual se puede alcanzar desde cualquier ventana interna a través del botón “Inicio”.

- La utilización del programa es muy sencilla; simplemente se debe presionar cualquiera de los botones del menú para acceder a más información sobre algún tópico.

- El cursor cambia de forma cuando encuentra una opción que invoca un enlace adicional de contenido (texto en color rojo). La forma más natural del cursor es una “flecha” que se convierte en un “dedo índice” cuando encuentra un enlace.

6.4.1. DESCRIPCION DEL AREA DE TUTOR

El área de tutor presenta los temas más importantes de las redes VPN permitiendo al usuario conocer el tema profundamente de una manera práctica y didáctica.

Al seleccionar el botón “Tutor” se llega a la ventana presentada en la *Fig. 6.2.*, en la cual se incluyen 14 nuevos botones:

Fig. 6.2. Ventana principal del tutor

Presenta la definición de las Redes Privadas Virtuales.

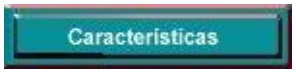
Explica los participantes que interactúan en la prestación del servicio VPN.

Analiza los tipos de compañías y sectores económicos que se ven beneficiados con la utilización del servicio VPN.

Expone los principales beneficios obtenidos por los usuarios al utilizar el servicio VPN.

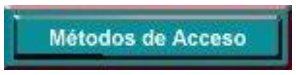
Presenta los principales beneficios obtenidos por las compañías que implementan el servicio VPN.

Explica los principales beneficios obtenidos por los operadores de telecomunicaciones al ofrecer el servicio VPN a sus clientes



Define un grupo estándar de características del servicio VPN, diferenciadas por el nivel de flexibilidad que el operador puede ofrecer y por la personalización realizada por cada usuario.

Expone las diferentes arquitecturas de red implementadas por los operadores de telecomunicaciones en el mundo, para ofrecer las características y beneficios del servicio VPN a sus clientes.



Presenta los principales métodos de acceso utilizados por los usuarios para originar y terminar llamadas VPN, a través de las diferentes arquitecturas de red, pero especialmente sobre la Red Inteligente.

Menciona los diferentes tipos de llamada que se pueden realizar en una VPN.

Explica algunos de los principales aspectos de la operación del servicio VPN, como son: el acceso al servicio, el plan de numeración privado y el procedimiento de marcación.

Describe la evolución del servicio VPN al ambiente de las redes de datos, dando origen a las redes VPN orientadas a conexión y a las redes VPN sin conexión.

Presenta la descripción y principales características de las nuevas redes VPN IP, que se están convirtiendo en la solución corporativa más importante de esta década.

Introduce las Redes de Próxima Generación y presenta su integración con las Redes Inteligentes para ofrecer un servicio VPN híbrido.

6.4.2. DESCRIPCION DEL AREA DE DEMOSTRACION

El área de demostración presenta un ejemplo de la ejecución del servicio VPN ofrecido por un operador de telecomunicaciones (no real) con presencia en Colombia, Venezuela y Estados Unidos.

Para el ejemplo se considera la solución más sencilla en la que el operador cuenta con una infraestructura de Red Inteligente instalada en sus países de cobertura. Generalmente, la solución real es ofrecida por un operador nacional a través de acuerdos con operadores de otros países que cuentan con una infraestructura similar de Red Inteligente y que ofrecen el servicio VPN.

Al seleccionar el botón “Demo” en la *ventana principal del programa* se llega a la ventana presentada en la *Fig. 6.3*.

Como se explicó anteriormente el botón “Inicio” regresa a la *ventana principal del programa* permitiendo acceder al área de tutor.

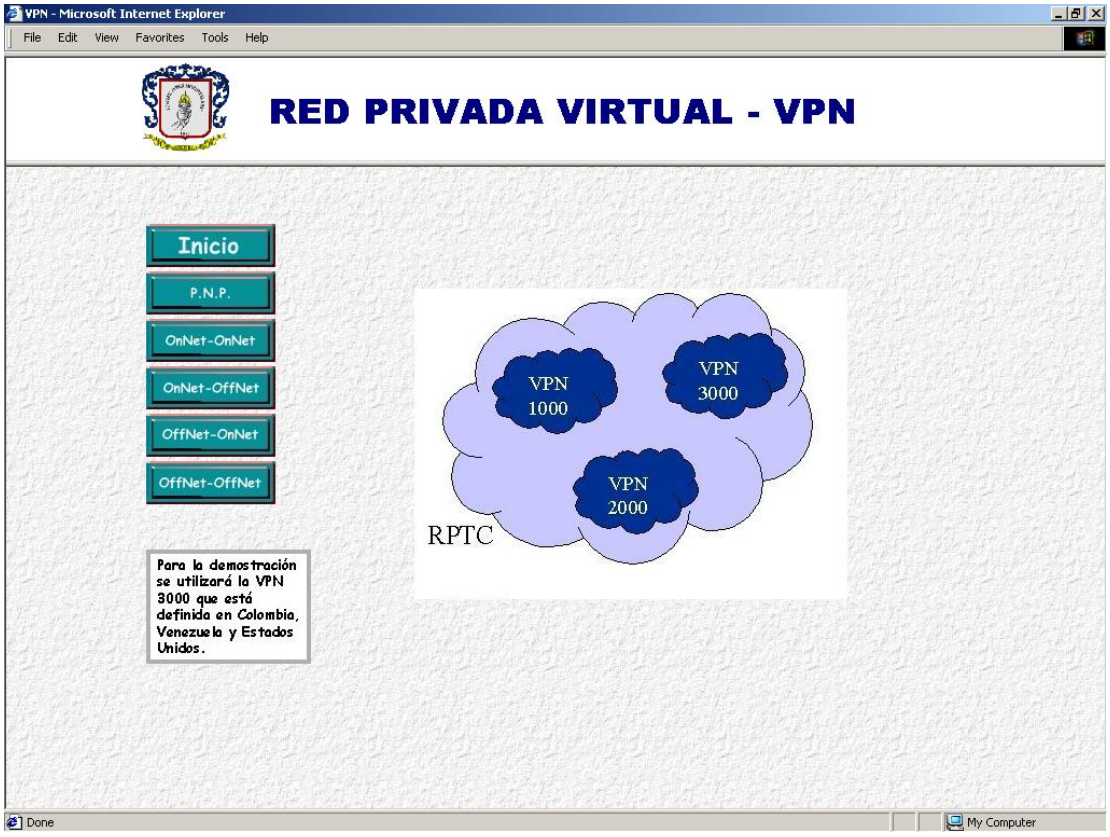


Fig. 6.3. Ventana principal de la demostración

En el gráfico aparece una nube representando la Red Pública del operador de telecomunicaciones, en la cual se encuentran definidas las VPNs 1000, 2000 y 3000. La VPN 3000 será utilizada para el ejemplo.

El cuadro de texto que aparece en las ventanas de la demostración explica el contenido del gráfico.

En esta ventana aparecen 5 nuevos botones:

Presenta el Plan de Numeración Privado definida para la VPN 3000 con presencia en Colombia, Venezuela y Estados Unidos.

Presenta la ejecución del servicio para una llamada On-Net – On-Net.

Presenta la ejecución del servicio para una llamada On-Net – Off-Net.

Presenta la ejecución del servicio para una llamada Off-Net – On-Net.

Presenta la ejecución del servicio para una llamada Off-Net – Off-Net.

En todas las ventanas asociadas con estos botones, aparecerá el botón “Demo” que al presionarlo regresará a la *ventana principal de la demostración*.

6.4.2.1. Descripción de la Ventana P.N.P.

En la *Fig. 6.4.* se presenta la ventana del Plan de Numeración Privado definido para la VPN 3000, utilizada como ejemplo en la demostración.

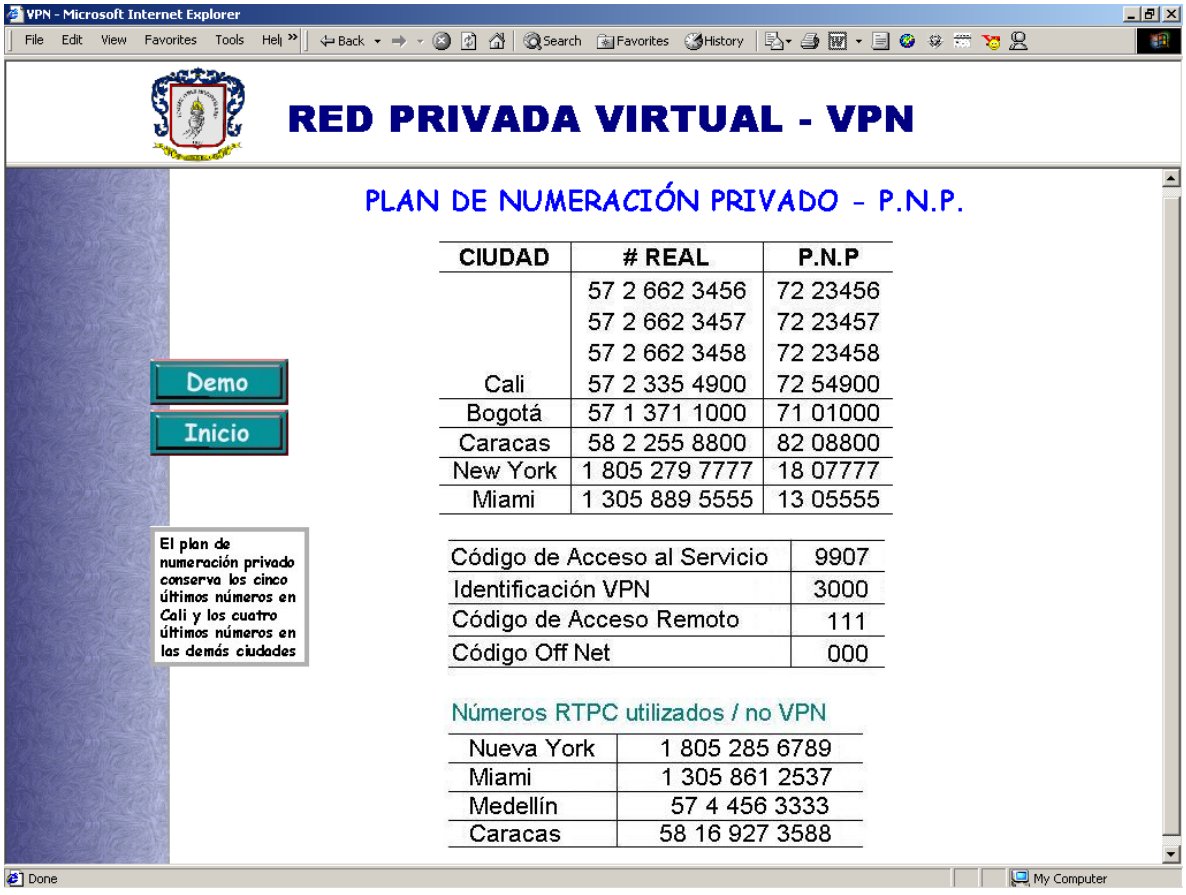


Fig. 6.4. Ventana del Plan de Numeración Privado

Como se explica en el tutor en la sección Numeración y Marcación, existen dos tipos de planes de numeración. Para el ejemplo se utiliza un “plan de numeración uniforme” de 7 dígitos para identificar las líneas internas de la red virtual, y se utiliza un “plan de numeración abreviado” de 3 dígitos para el Código de Acceso Remoto y el Código Off-net.

Los números de Código de Acceso al Servicio e Identificación VPN no pertenecen al plan de numeración privado, sino que corresponden a números del plan de numeración de la Red Telefónica Pública.

Los números RTPC especificados en esta ventana, corresponden a números que no pertenecen a la VPN, pero que son utilizados en la demostración para originar llamadas off-net (1805 2856789 y 1305 8612537) y para terminar llamadas off-net (574 4563333 y 5816 9273588).

6.4.2.2. Descripción de las Ventanas de Llamadas

En la demostración se presentan los cuatro tipos de llamadas que se pueden realizar en una VPN. Los números origen y destino de las llamadas corresponden a números especificados en el Plan de Numeración Privado.

En la *Fig. 6.5.* y en la *Fig. 6.6.* se presentan dos ejemplos de ventanas de llamadas, la primera para una llamada On-Net – On-Net y la segunda para una llamada On-Net – Off-Net.

En todas las ventanas de ejecución del servicio se encuentran:

- El título correspondiente al tipo de llamada que se está ejecutando especificando los números de teléfonos involucrados.
- El gráfico representando un paso en la ejecución del servicio.
- Un cuadro de texto con la explicación del paso que se está ejecutando.

En casi todas las ventanas se presentan dos nuevos botones:

Va al paso anterior en la ejecución del servicio. No aparece en la primera ventana de ejecución del servicio de una llamada.

Va al paso siguiente en la ejecución del servicio. No aparece en la ventana final de ejecución del servicio de una llamada.

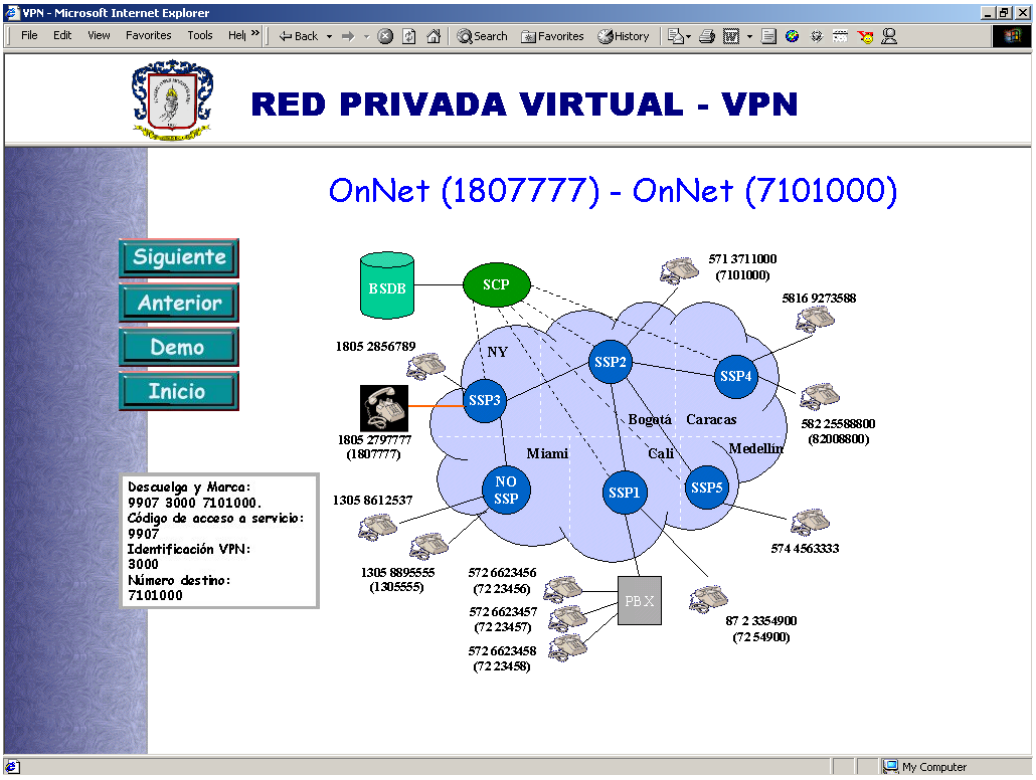


Fig. 6.5. Ventana Tipo de Llamada On-Net – On-Net

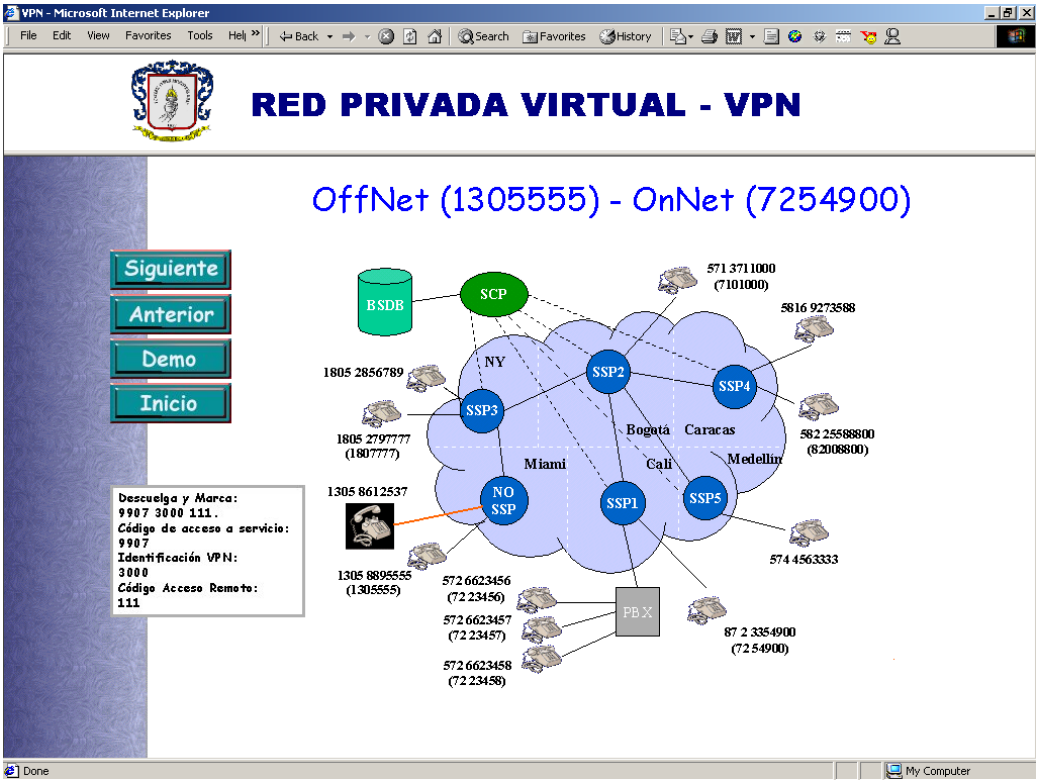


Fig. 6.6. Ventana Tipo de Llamada Off-Net – On-Net

7. CONCLUSIONES

- Con el incremento de la competencia y la demanda por nuevos servicios, los proveedores de servicios de telecomunicaciones, deben cada día ser más ágiles que sus competidores y construir redes más flexibles que les permitan ofrecer nuevas soluciones tan rápido como sus clientes las requieran.

- El servicio de Red Privada Virtual es uno de los principales servicios para clientes corporativos, que explota lo mejor de las redes públicas existentes de los operadores de telecomunicaciones y brinda a las empresas grandes beneficios tales como la disminución de costos, gran flexibilidad, eficiencia y efectividad.

- La arquitectura de red ideal para implementar el servicio VPN es la Red Inteligente, ya que hace un máximo aprovechamiento de todas las características del servicio. Sin embargo, también puede ser ofrecido sobre redes integradas, redes paralelas y redes Centrex y Centrex de Banda Ancha.

- Las VPN a pesar de ofrecer grandes beneficios a las empresas, afectan toda su organización, al pasar gran parte del control y administración de su red de telecomunicaciones a un operador, generando en muchos casos medidas críticas, tales como despido de personal, cambios tecnológicos y adecuación cultural, que obligan a que la aprobación de su implementación sea tomada por altos niveles directivos.

- Las VPNs de voz han estado en el portafolio de productos de los proveedores de servicios durante muchos años, con muchas compañías de la lista “Fortune 1000” con contratos de 50 a 100 millones de dólares por año en todo el mundo. Sin embargo ya han entrado en una etapa relativamente plana de crecimiento, en la que cada vez menos clientes las implementan debido a las nuevas tecnologías en VPNs. En el caso de la base instalada, la mayoría de los clientes las seguirán utilizando en paralelo con las nuevas tecnologías, y migrándolas muy lentamente.

- Las redes VPN orientadas a conexión (Frame Relay y ATM) tuvieron una gran acogida por parte de los clientes, ya que ofrecían la posibilidad de conectar todas las oficinas de la empresa (Intranet) transportando no solamente voz, sino también datos y video, con una muy buena calidad y un muy buen manejo del ancho de banda. Aunque ya no crecen al mismo ritmo que antes, cuentan con la mayor participación del mercado y lo harán por muchos años más.

- Las redes VPN sin conexión (VPN IP) están siendo adoptadas muy rápidamente, ya que además de ofrecer conectividad WAN, permiten conectar usuarios de acceso remoto y socios de negocios (extranet), haciéndolas accesibles para organizaciones de todos los tipos y tamaños. La administración y la seguridad de una VPN son tareas

complejas, por lo que las empresas prefieren utilizar a los proveedores de servicios para que se encarguen de ellas.

- Considerando el ciclo de vida de la tecnología se puede concluir que, las redes VPNs de voz se están acercando a su etapa final del mercado, las VPNs orientadas a conexión (FR/ATM) ya superaron la etapa de Consumo Masivo pero aún continúan creciendo y las VPNs IP están empezando a entrar en la etapa de tornado o etapa de despegue y rápida adopción de la tecnología.

- Las Redes Inteligentes se han convertido en uno de los pilares fundamentales para el presente y el futuro de las redes de telecomunicaciones y su integración con tecnologías de Banda Ancha como ATM y Redes de Próxima Generación (NGN), ya que genera valor a los operadores de telecomunicaciones a través del desarrollo de un rango más amplio de servicios para los usuarios y sirve de mediador en la evolución de los servicios entre los dos mundos.

- Las Redes de Próxima Generación no buscan reemplazar las plataformas de telecomunicaciones existentes, sino utilizarlas y extender la prestación de sus servicios. Gracias a esto el servicio VPN puede ser ofrecido como un servicio híbrido aprovechando las ventajas y beneficios tanto de las Redes Inteligentes (se encargan de manejar la parte conmutada) como de las redes NGN (se encargan del manejo de la llamada sobre la red de paquetes - IP).

- Se debe tener presente que muchas veces los desarrollos tecnológicos van más rápido que los requerimientos del mercado, siendo este el caso de las redes NGN, las cuales se encuentran en una etapa de Mercado Temprano en el ciclo de vida de la tecnología, y a las que les faltan varios años antes de que entren a la etapa de rápida adopción de la tecnología.

- La entrada del servicio VPN en Colombia tuvo que enfrentar demasiados problemas que hicieron que el servicio nunca fuera desarrollado, excepto por Telecom, a pesar de que los operadores contaran con la infraestructura tecnológica para ofrecerlo. Los principales problemas se debieron a la falta de regulación para la interconexión entre los operadores, en cuanto al manejo de señalización, a los planes de numeración y a la obligación de realizar acuerdos inter-administrativos.

- A pesar de que en el 2002 fueron expedidas nuevas regulaciones que podrían resolver los problemas de interconexión, los operadores de telecomunicaciones que cuentan con plataformas de Redes Inteligentes, consideran que el servicio no es atractivo para ser implementado, principalmente porque el mercado es muy limitado y porque casi todos ellos cuentan con otras soluciones como son las redes de datos, por lo que tal vez el servicio nunca será implementado en nuestro país.

- A diferencia de lo ocurrido en Colombia, las experiencias completamente satisfactorias de prestación del servicio VPN en otros países del mundo, permite concluir que el servicio es ideal para operadores de telecomunicaciones que pueden ofrecer telefonía local, de larga distancia nacional e internacional, y para países en los que la

regulación (señalización, numeración) respecto a la interconexión de Redes Inteligentes se encuentre muy bien definida.

- Como conclusión final se puede decir que el servicio de Red Privada Virtual ha revolucionado las comunicaciones empresariales en todo el mundo, ocupando el lugar central del portafolio de servicios ofrecido por las compañías de telecomunicaciones a sus clientes corporativos, desde principios de los 90s con las VPNs de voz, pasando por los finales de los 90s con las VPNs FR/ATM y hasta esta nueva década con las VPN IP.

8. RECOMENDACIONES

- Las Redes Inteligentes fueron implementadas hace ya varios años en Colombia, sin embargo no ha sido posible lograr la interconexión de las mismas. Se recomienda continuar con el estudio de Interconexión de las RI en Colombia, incluyendo el nuevo Régimen Unificado de Interconexión (RUDI) y el nuevo Plan Nacional de Numeración expedidos en el 2002 y determinar los requerimientos necesarios para poder realizar la interconexión desde el punto de vista del nuevo marco legal.

- Al presenciar durante varios años la evolución del servicio VPN y mezclarlo con la experiencia laboral, se logró una visión mucho más completa de la aplicación de la tecnología en el mundo real, por lo que se recomienda realizar trabajos continuados de investigación sobre temas de importancia, tal como redes VPN IP, no sólo durante su etapa de introducción al mercado, sino también durante su evolución.

- En este trabajo de investigación se abordaron temas que merecen un estudio mucho más profundo y ameritan un trabajo de grado, entre estos temas se encuentran el estudio de la evolución de las redes inteligentes como plataforma para la introducción de las redes NGN, así como los aspectos que impulsaran su implementación en Colombia desde un punto de vista no solo teórico e investigativo, sino también desde un punto de vista práctico y real, analizando las diferentes empresas del sector y la viabilidad de su introducción en nuestro país.

- Sería importante mezclar el área académica con el sector productivo de las telecomunicaciones en nuestro país mediante la realización de proyectos enfocados en analizar y solucionar problemas reales de las empresas de telecomunicaciones en Colombia.

- Uno de los impulsores para la adopción de una nueva tecnología, es su utilidad real para los usuarios. Es muy importante introducir en los trabajos de investigación un análisis de la viabilidad comercial de los nuevos servicios y tecnologías en los diferentes mercados y principalmente en nuestro país (p.e. estudios de rentabilidad, estudios de mercado, análisis del marco regulatorio).

- Para que la facultad continúe a la vanguardia en la formación de profesionales en el mercado de las telecomunicaciones en Colombia, es importante que de acuerdo con la evolución y expectativas del mundo empresarial, se sigan adaptando y ofreciendo nuevas materias de énfasis y electivas especializadas.

- Como medio importante de consulta para los investigadores y en general para los interesados en el tema, la universidad debería divulgar los proyectos de grado publicando en Internet el resumen, objetivos y conclusiones de cada uno de ellos.

9. DESCRIPCION DE ANEXOS

ANEXO A. Presenta un ejemplo de un Plan de Numeración Privado y su aplicación para cada uno de los diferentes tipos de llamadas.

ANEXO B. Se presenta la evolución de las Redes Inteligentes, analizando su relación con Internet (Redes Híbridas), los principales protocolos que están siendo utilizados para la implementación de APIs abiertos (Redes Convergentes), las tecnologías CORBA y de Agentes Móviles (Redes Distribuidas) y la introducción de las Redes de Próxima Generación.

ANEXO C. Se presenta una descripción detallada del funcionamiento de las Redes Privadas Virtuales sobre Internet, sus beneficios, aplicaciones, protocolos empleados, esquemas de seguridad implementados y su administración.

ANEXO D. Se presentan ejemplos de las VPNs de voz de operadores como Telmex y Alestra en México, Embratel en Brasil, AT&T en USA, Vodafone y Retevisión en España, entre otros. Todos los ejemplos mencionados utilizan Redes Inteligentes.

ANEXO E. En este anexo se encuentra una explicación de como fue realizado el programa gráfico “Red Privada Virtual – VPN”, así como el código de cada una de las ventanas que componen el programa.

10. BIBLIOGRAFIA

3COM. Private Use of Public Networks for Enterprise Customers. 3COM Technical Papers, 1998. http://www.3com.com/technology/tech_net/white_papers/500649.html

ALLARD, Frank. Broadband virtual private network signaling. En: BT Technology Journal. Vol.16, No.2. Abril 1998. p. 112-119.

ANDREETTO, Alessandra. Service opportunities for next-gen networks. En: SEMINARIO EURESCOM SUMMIT 2001: 3G TECHNOLOGIES AND APPLICATIONS. Plenaria 1. Heidelberg, Alemania. Noviembre 2001.
www.eurescom.de/~pub/seminars/Summit2001/1-2-andreetto.pdf

BLACK, Uyless D. Voice over IP. New Jersey, USA: Prentice-Hall, Inc., 2000. ISBN 0-13-022463-4.

BRENNAN, Rob et al. Evolutionary trends in intelligent networks. En: IEEE Communications Magazine. Vol. 38, No. 6. Junio 2000. p. 86-93.

BURGOS, Jairo et al. Redes inteligentes: servicios y aplicaciones. Anexo 3. Trabajo de grado (Ingeniero en Electrónica). Universidad del Cauca. Facultad de Ingeniería Electrónica y Telecomunicaciones. Popayán, 1994.

CHATZIPAPADOPOULOS, Fotis; PERDIKEAS, Menelaos y VENIERIS Iakovos. Mobile agent and CORBA technologies in the broadband intelligent network. En: IEEE Communications Magazine. Vol. 38, No. 6. Junio 2000. p. 116-124.

CHIANG, Tsun-Chieh et al. IN services for converged (internet) telephony. En: IEEE Communications Magazine. Vol. 38, No. 6. Junio 2000. p. 108-115.

COMISION DE REGULACIÓN DE TELECOMUNICACIONES. Resolución 469 de 2002: por medio de la cual se modifica la resolución CRT 087 de 1997 y se expide un régimen unificado de interconexión – RUDI. Bogotá: CRT, 2002. 23 p.

COMMUNICATIONS INDUSTRY RESEARCHERS. Advanced intelligent networks: opportunities in network control for the Coming Decade (Executive Summary). Charlottesville, USA: CIR, 1998. http://www.cir-inc.com/reports/AIN/exec.html

COUTURIER, Alban y MAMPAEY, Marcel. Using TINA concepts for IN evolution. En: IEEE Communications Magazine. Vol. 38, No. 6. Junio 2000. p. 94-99.

CRIMI, Joseph. Next generation network (NGN) services. Telcordia Technologies, 2001. 11 p. http://www.telcordia.com/solutions/ngn/wp_crimi.pdf

DE SERRES, Yves y HEGARTY, Lawrence. Value-added services in the converged network. En: IEEE Communications Magazine. Vol. 39, No. 9. Septiembre 2001. p. 146-154.

DE TOURNEMIRE, Eric. Proposal for BVPN as service example. Status: Draft. TINA Consortium, 1995.

ERICSSON. Intelligent network and the service script concept. Ericsson, 1994.

EURESCOM. Project 909. Enabling Technologies for IN evolution and IN-internet integration. Heidelberg, Alemania: Eurescom, Marzo 2000. http://www.eurescom.de/public/projects/P900-series/p909/default.asp

_____. Project 1109. Next generation networks: the service offering standpoint. Heidelberg, Alemania: Eurescom, Noviembre 2001. http://www.eurescom.de/public/projects/P1100-series/P1109/default.asp

FINKELSTEIN, Mark et al. The future of the intelligent network. En: IEEE Communications Magazine. Vol. 38, No. 6. Junio 2000. p. 100-106.

FUJITSU LIMITED. Fetex-150: general service specification. Private virtual network (PVN). Fujistsu, 1990.

GLITHO, Roch y MAGEDANZ, Thomas. Guest editorial – intelligent networks in the new millennium. En: IEEE Communications Magazine. Vol. 38, No. 6. Junio 2000. p. 82.

HEYWOOD, Peter. The Dawn of the New VPN Era. En: Data Communications International. Septiembre 1995. http://www.data.com/Roundups/New_VPN_Era.html

ICM CONSORTIUM. Integrated communications management of broadband networks: Cap. 6 - vpn management. Heraklio, Grecia: The ICM Consortium, Crete University Press, 1996. p. 147-188. ISBN 960 524 006 8. www.ee.ucl.ac.uk/~dgriffin/papers/book/icmbook.html

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Documentación. Presentación de tesis, trabajos de grado y otros trabajos de investigación. Quinta actualización. Bogotá: ICONTEC, 2002.

LENAHAN, Grant. Next generation networks: a practical view of network evolution. Telcordia Technologies, 1999. 10 p. http://www.telcordia.com/newsroom/knowledgebase/papers/ngn_evolution.doc

LIPPIS, Nick. Internet VPDNs: Welcome to Tomorrow. Data Communications on the Web. Agosto, 1997. http://www.data.com/opinion/lippis/vpdn.html

MAGEDANZ, Thomas. Intelligent network evolution: impact of internet, CORBA, TINA and mobile agent technologies. En: CONFERENCIA TINA ´99. Tutorial P. Oahu, USA. 1999. www.tinac.com/conference/tina99/tutorial_p.pdf

McCARTHY, Clare y DARABI, Fash. VPN Services: Market Strategies. OVUM Reports. October 1995. http://ovum.com/pubs/vps.html

McDYSAN, David E. VPN application guide: real solutions for enterprise networks. Estados Unidos: Wiley Computer Publishing, 2000. ISBN 0-471-3717-0.

MENDLER, Camile. New carriers poised to break VPN stranglehold. Communications Week International. Vol. 194. Noviembre 1997.
http://www.totaltele.com/cwi/194/194news11.html

MINISTERIO DE COMUNICACIONES. Decreto 25 de 11 de enero de 2002: por el cual se adoptan los planes técnicos básicos y otras disposiciones. Bogotá, 2002. 16 p.

MODARRESSI, Abdi y MOHAN, Seshadri. Control and management in next-generation networks: challenges and opportunities. En: IEEE Communications Magazine. Vol. 38, No. 10. Octubre, 2000. p. 94-102.

_____. Guest editorial – advanced signaling and control in next-generation networks. En: IEEE Communications Magazine. Vol. 38, No. 10. Octubre, 2000. p. 92-93.

MOLONY, David. C&W pioneers global mobile VPN offering. En: Communications Week International. Vol. 211. Septiembre, 1998.
http://www.totaltele.com/cwi/211/211news1.html

NICOLL, Stéphane. Network convergence for the provision of IN services in the internet. Monografía (Maestría en Informática). Facultes Universitaires Notre-Dame de la Paix. Facultad de Informática. Namur, Bélgica, 2000-2001.

NORTHERN TELECOM. Virtual private networking with magellan. Nortel, 1994.

PAVÓN, Juan. Building Telecommunications Management Applications with CORBA. En: IEEE Communications Survey. Vol. 2, No. 2. Segundo trimestre, 1999.
http://www.comsoc.org/livepubs/surveys/public/2q99issue/pavon.html

SHIVA. Virtual private networking: the next revolution in corporate productivity. Shiva White Papers, 1998. http://www.shiva.com/remote/prodinfo/vpn/index.html

SIEMENS. Descripción de algunos servicios de Red Inteligente. Siemens AG, 1994.

SUN MICROSYSTEM. The JAIN APIs: integrated network APIs for the java platform. Palo Alto, USA: Sun Microsystem, 2002. http://java.sun.com/products/jain/

UIT-T. Recomendación Q.1211: introducción al conjunto de capacidades 1 de red inteligente. Helsinki: UIT, 1993.

UIT-T. Recomendación Q.1221: introducción al conjunto de capacidades 2 de red inteligente. Ginebra: UIT, 1997.

UIT-T. Recomendación Q.1231: introducción al conjunto de capacidades 3 de red inteligente. Ginebra: UIT, 1999.

UIT-T. Draft new ITU-T recommendation Q.1241: introduction to intelligent network capability set-4. Versión prepublicada: UIT, 2001.

UIT-T. Draft recommendation Q.1244: distributed functional plane for intelligent network capability set-4. Génova: UIT, 2001.

Otras páginas web de consulta:

www.att.com

www.cisco.com

www.clarent.com

www-comm.itsi.disa.mil:8006/in/in_itu.html

www.comsoc.org

www.crt.gov.co

www.embratel.com.br

www.ericsson.com

www.ietf.org

www.infosyssec.net/infosyssec/secvpn1.htm

www.lucent.com

www.mincomunicaciones.gov.co

www.ngn.com

www.nortelnetworks.com

www.siemens.com

www.telmex.com.mx

www.tina.com

11. GLOSARIO

3DES	Estándar de encripción triple de datos (*Third Data Encryption Standard*).
3G	Tercera generación de telefonía móvil celular (*Third Generation*).
3GPP	Proyecto de asociación para servicios de tercera generación (*Third Generation Partnership Project*).
AAA	Autenticación, autorización, contabilización (*Authentication, Authorization, Accounting*).
AUTZ	Código de autorización (*Authorization Code*).
ABD	Marcación abreviada (*Abbreviated Dialling).*
AH	Encabezado de autenticación (*Authentication Header*).
AIOD	Identificación automática de marcadores externos (*Automatic Identification of Outward Dialling*).
AMA	Registro de contabilización automático de mensajes (*Automatic Message Accounting).*
ANI	Identificación automática de número (*Automatic Number Identification).*
API	Interfaz de programa de aplicación *(Application Program Interface).*
ARPA	Agencia de proyectos e investigación avanzada (*Advanced Research and Projects Agency*).
AS	Servidor de aplicaciones (*Application Server*).
ASP	Proveedor de servicios de aplicaciones (*Application Service Provider*).
ATM	Modo de transferencia asíncrono (*Asynchronous Transfer Mode*).
ATT	Asistencia (*Attendant).*
AUTC	Autenticación (*Authentication).*
BBG	Grupo de negocios básico *(Basic Business Group).*
BGDP	Plan de marcación del grupo de negocios *(Business Group Dialing Plan).*
BSDB	Base de datos del servicio comercial *(Business Service DataBases).*
BVPN	Red privada virtual de banda ancha (*Broadband Virtual Private Network*).
Caller-IP	Identificación de abonado llamante (*caller-ID*).

CCS7	Sistema de señalización por canal común No.7 (*Common Channel Signaling System No. 7).*
CD	Distribución de llamadas *(Call Distribution).*
CdPN	Número de abonado llamado *(Called Party Number - CdPN).*
CENTREX	Conmutador de oficina central *(Central Office Exchange).*
CHA	Retención de llamadas con anuncio *(Call Hold with Announcement).*
COC	Llamadas en consulta *(Consultation Calling).*
CORBA	Arquitectura común para gestores de solicitudes a objetos *(Common Object Request Broker Architecture).*
CPE	Equipo local del cliente *(Customer Premises Equipment).*
CPM	Gestión del perfil de abonado *(Customer Profile Management).*
CPR	Registros de procesamiento de la llamada *(Call Processing Record).*
CRA	Anuncio grabado especial *(Customised Recorded Announcement).*
CRG	Tono de llamada especial *(Customised ringing).*
CS	Conjunto de capacidades (*Capability Set*).
CTI	Integración telefonía – computación *(Computer Telephony Integration).*
CUG	Grupo cerrado de usuarios *(Closed User Group).*
DES	Estándar de encripción de datos (*Data Encryption Standard*).
DID	Conexión directa a extensiones *(Direct Inward Dialling).*
DN	Número de llamada *(Directory Number).*
DPE	Ambiente de procesamiento distribuido (*Distributed Processing Environment*).
DSL	Línea de suscriptor digital (*Digital Subscriber Line*).
EPPMM	Empresas Públicas de Medellín.
ETB	Empresa de Teléfonos de Bogotá.
ESP	Carga útil de seguridad de encapsulamiento (*Encapsulating Security Payload*).
FMD	Desviación “sígame” *(Follow-Me-Diversion)*.
FR	Frame Relay.
FRAD	Dispositivo de acceso Frame Relay *(Frame Relay Access Device).*
Gateway	Sistema que une dos tipos de redes diferentes.
GPRS	Servicio general de paquetes vía radio (*General Packet Radio Service*).
GRE	Encapsulación genérica de enrutamiento. (*Generic Routing Encapsulation*).

GVNS	Servicio de red virtual global (*Global Virtual Network Service*).
IDN	Red digital integrada *(Integrated Digital Network).*
IETF	Fuerza de trabajo de ingenieria de Internet *(Internet Engineering Task Force).*
IKE	Intercambio de claves en Internet (*Internet Key Exchange*).
INAP	Parte de aplicación de red inteligente (*Intelligent Network Application Part*).
IP	Periférico inteligente *(Intelligent Peripheral).*
IP	Protocolo Internet *(Internet Protocol).*
IPSec	IP seguro *(IP Secure).*
IPX	Intercambio de paquetes de conexión de redes *(Internetwork packet Exchange).*
ISDN	Red digital de servicios integrados *(Integrated Service Digital Network).*
ISP	Proveedores de servicio Internet *(Internet Service Provider).*
ISPBX	PBX con capacidades RDSI *(Integrated Services Privated Branch Exchange).*
ISUP	Parte de usuario de la RDSI (*ISDN User Part*).
IXC	Operadores entre - centrales *(Inter-eXchange Carriers).*
JAVA	Lenguaje de programación orientado a objetos y desarrollado por Sun Microsystem.
L2F	Protocolo de reenvío de nivel 2 *(Layer 2 Forwarding).*
L2TP	Protocolo de creación de túneles de nivel 2 *(Layer 2 Tunneling Protocol).*
LAN	Redes de área local *(Local Area Network*).
LATAS	Áreas de acceso y de transporte local *(Local Access and Transport Areas).*
LCD	Línea conexión directa.
LDI	Larga distancia internacional.
LDN	Larga distancia nacional.
LEC	Operador de intercambio local (*Local Exchange Carrier*).
LD	Línea dedicada.
Lls	Líneas arrendadas (*Leased lines).*
LMDS	Sistema de distribución local multipunto (*Local Multipoint Distribution System*).
LND	Línea no dedicada.

LNP	Portabilidad de número local *(Local Number Portability).*
LOG	Consignación de llamadas *(Call Logging).*
MGCP	Protocolo de control de gateways de medio (*Media Gateway Control Protocol*).
MTP	Puerto de transferencia de mensajes (*Message Transfer Port*).
MUX	Multiplexor.
NC	Capacidades de red (*Network Capabilities).*
NGN	Redes de próxima generación (*Next Generation Networks*).
NNI	Interfaz red a red (*Network to Network Interface*).
OFA	Acceso fuera de red *(Off-Net- Access).*
OMG	Grupo de administración de objetos *(Object Management Group).*
ONC	Llamadas fuera de red *(Off-Net-Calling).*
OSI	Interconexión de sistemas abiertos *(Open System Interconnection).*
OUP	Avisador de usuario de origen *(Originating User Prompter).*
PABX	Central telefónica privada automática (*Private Automatic Branch Exchange*).
PAD	Dispositivo de acceso X.25 (*Packet Assembler Disassembler X.25*).
PBX	Central telefónica privada (*Private Branch Exchange*).
PIN	Número de identificación personal *(Personal Identification Number).*
PINT	Interconexión de redes PSTN e Internet *(PSTN / Internet Inter-Networking).*
PLMN	Red mundial pública móvil (*Public Land Mobile Network).*
PNDP	Plan de numeración de la red pública *(Public Network Dialing Plan).*
PNP	Plan de numeración privado *(Private Numbering Plan).*
POP	Punto de presencia *(POP - Point of Presence).*
PPP	Protocolo punto a punto (*Point to Point Protocol*).
PPTP	Protocolo de creación de túneles punto a punto *(Point to Point Tunneling Protocol).*
PSTN	Red telefónica pública conmutada *(Public Switched Telephony Network).*
PVC	Circuito virtual permanente (*Permanent Virtual Circuit*).
QoS	Calidad de servicio (*Quality of Service*).
QUE	Cola de llamadas *(Call Queuing).*
RADIUS	Servicio de autenticación de usuarios remotos por marcación (*Remote Authentication Dial-In User Service*).

RAM	Memoria de acceso aleatorio (*Random Access Memory*).
RAS	Servidor de acceso remoto *(Remote Access Server).*
RDSI	Red digital de servicios integrados.
RDSI-BA	Red digital de servicios integrados de banda ancha.
RDSI-BE	Red digital de servicios integrados de banda estrecha.
RI	Red inteligente.
RFC	Requerimiento de comentarios (*Request for Comments*).
RSPV	Protocolo de reserva de recursos (*Resource ReSerVation Protocol*).
RTPC	Red telefónica pública conmutada.
SAC	Código de acceso al servicio (*Service Access Code*).
SCE	Ambiente de creación de servicios *(Service Creation Enviroment).*
SCP	Punto de control de servicios *(Service Control Point).*
SIP	Protocolo de iniciación de sesión *(Session Initiation Protocol).*
SLA	Acuerdo de nivel de servicios (*Service Level Agreement*).
SLEE	Ambiente de ejecución de la lógica del servicio (*Service Logic Execution Environment*).
SMS	Sistema de gestión de servicios *(Service Management System)*.
SS7	Sistema de señalización número 7 (*Signaling System Number 7*).
SSP	Punto de conmutación de servicios *(Service Conmmuting Point).*
STP	Punto de transferencia de señalización *(Signal Transfer Point).*
SU	Usuario del servicio *(Service User).*
SVC	Circuito virtual conmutado (*Switched Virtual Circuit*).
TACACS	Sistema de control de acceso de controlador y acceso de terminal (*Terminal Access Controller Access Control System*).
TCAP	Parte de aplicación de las capacidades de transacción (*Transaction Capabilities Application Part*).
TDM	Multiplexación por división de tiempo (*Time División Multiplexing*).
TDR	Encaminamiento cronodependiente *(Time Dependent Routing).*
Telcos	Compañías de telecomunicaciones.
TINA	Arquitectura de red de información de telecomunicaciones *(Telecommunications Information Networking Architecture).*
TRA	Transferencia de llamadas *(Call Transfer).*
UDP	Protocolo datagrama de usuario (*User Datagram Protocol*).

UIT-T	Unión internacional de telecomunicaciones – Sector de Normalización de las telecomunicaciones *(International Telecommunication Union – Telecommunication)*.
UMTS	Sistema de telecomunicaciones móviles universales (*Universal Mobile Telecommunication System*).
UNI	Interfaz usuario – red (*User Network Interface*).
VAN	Redes de valor agregado *(Value added network).*
VC	Circuito virtual, conexión virtual, canal virtual (*Virtual Circuit, Virtual Connection, Virtual Channel*).
VCC	Conexión de canal virtual (*Virtual Channel Connection*).
VPC	Conexión de camino virtual (*Virtual Path Connection*).
VoATM	Voz sobre ATM (*Voice over ATM*).
VoFR	Voz sobre Frame Relay (*Voice over FR*).
VoIP	Voz sobre IP (*Voice over IP*).
VPN	Red privada virtual (*Virtual Private Network).*
WAC	Centrex de área ancha *(Wide Area Centrex).*
WAN	Redes de área extendida (*Wide Area Network*).