UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERIA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACIÓN DE SERVICIO DE VOZ SOBRE IP SOPORTADO POR UNA RED PRIVADA VIRTUAL PARA EMPRESA DE TELEFONÍA MÓVIL

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO ELECTRÓNICO

PRESENTADO POR:

MILTON CALLAÑAUPA GONZALES

PROMOCIÓN
1997 – II

LIMA – PERU
2002

A mi familia por su apoyo y confianza.

IMPLEMENTACIÓN DE SERVICIO DE VOZ SOBRE IP SOPORTADO POR UNA RED PRIVADA VIRTUAL PARA EMPRESA DE TELEFONÍA MÓVIL

SUMARIO

El desarrollo de las telecomunicaciones y la globalización del mercado, exige a las empresas ser mas competentes, esto significa ofrecer servicios y soluciones de alta calidad, amplia cobertura a costos reducidos, esto solo se puede conseguir promoviendo una cultura de eficiencia, En una empresa de Telefonía Móvil los costos de interconexión y el uso eficiente del Ancho de banda son importantes para lograr estos objetivos.

En este informe, brindaremos los detalles de la implementación de una alternativa de acceso a la red celular de una empresa de telefonía móvil para sus clientes corporativos, permitiéndoles de esta manera un mejor manejo de sus costos por tráfico hacia teléfonos celulares de la empresa de telefonía móvil.

Se emplea tecnología de voz sobre IP para comprimir la voz y optimizar el ancho de banda, se utiliza como medio de transporte una Red Privada Virtual que soporta protocolo MPLS (Multi Protocol Label Switching) con el cual se logra obtener un alto desempeño para el envío de paquetes a través de la red y permite aplicar conceptos de QoS (Calidad de Servicio).

ÍNDICE

PRÓLOGO

El mercado de telefonía móvil esta pasando por un momento de interesante desarrollo, con la llegada de una nuevos operadores de telefonía, los operadores sienten la necesidad de desarrollar nuevas vías para incrementar el negocio.

El presente proyecto tiene como objetivo revisar y aprovechar la disponibilidad de tecnologías para la transmisión de voz sobre redes de datos, las cuales abren un abanico de posibilidades para la convergencia de ambos mundos

En este sentido se plantea una solución que mejorará la calidad de un servicio prestado por una empresa de telefonía móvil, reducirá costos de interconexión y sentará las bases tecnológicas para que la empresa se convierta en un Proveedor de servicios de telefonía por Internet (PSTI).

La solución propone enrutar las llamadas a celulares generadas por un cliente-empresa a través de una conexión de datos a la red celular utilizando tecnología de voz sobre IP. La red de datos a emplear será una Red Privada Virtual implementada con tecnología MPLS (Multi Protocol Label switching) que permite optimizar el desempeño del envío de paquetes

a través de la red y hace posible implementar modelos de QoS(calidad de servicio).

Desde hace tiempo, los responsables de comunicaciones de las empresas tienen en mente la posibilidad de utilizar su infraestructura de datos, para el transporte del tráfico de voz interno de la empresa. No obstante, es la aparición de nuevos estándares, así como la mejora y abaratamiento de las tecnologías de compresión de voz, lo que está provocando finalmente su implantación.

La telefonía IP conjuga dos mundos históricamente separados: la transmisión de voz y la de datos. Se trata de transportar la voz, previamente convertida a datos, entre dos puntos distantes. Esto posibilitaría utilizar las redes de datos para efectuar las llamadas telefónicas, y yendo un poco más allá, desarrollar una única red que se encargue de cursar todo tipo de comunicación, ya sea vocal o de datos.

Es evidente que el hecho de tener una red en vez de dos, es beneficioso para cualquier operador que ofrezca ambos servicios, véase gastos inferiores de mantenimiento, personal cualificado en una sola tecnología.

CAPÍTULO I

ANTECEDENTES

1.1 Situación Actual

Las empresas de telefonía se ven obligadas a pagar un costo de interconexión pactado al operador que recepciona las llamadas fijo – móvil (land to movil) por el servicio de culminación de llamada . Este costo es cargado al cliente, incrementando el costo del tráfico, este costo se podría suprimir si la empresa de TM implantará una red de voz propia, pero es casi imposible por lo elevado de los costos de equipamiento, operación y mantenimiento.

Con la llegada de nuevos operadores de telefonía Móvil y el desarrollo de las tecnologías, la competencia en el mercado ya no se basa en ofrecer mayor cobertura del servicio de voz o mejor calidad de voz, la competencia se esta dando en el desarrollo de servicios de valor agregado y las redes de datos tienen que ver mucho con el desarrollo de servicios. Tal vez no sea negocio para la compañía de TM implementar una red de voz, pero si lo

sería implementar una red de datos donde se pueda ofrecer servicios de voz y otros servicios de valor agregado.

1.2 Determinación de necesidades

Existen clientes que pudieron invertir conjuntamente con la empresa de TM en la renta enlaces PRI o E1 para interconectar sus negocios con la red de TM y así reducir sus costos en llamadas fijo-móvil, justamente estos clientes VIP generan aproximadamente el 40% del trafico fijo-móvil, este tráfico representa un porcentaje importante y un elevado costo por interconexión. Pero fueron incrementándose y se complicaba cada vez mas las labores de operación y mantenimiento.

Gracias al desarrollo y reducción de costos de la tecnología VOIP (voz sobre ip) resultó viable la implantación de un sistema de interconexión VOIP utilizando los servicios de la RPV (Red Privada Virtual) que ofrece una compañía de telecomunicaciones local, mas adelante se explicará al detalle el análisis previo para determinar la tecnología mas adecuada a utilizar.

CAPÍTULO II

FUNDAMENTOS TECNOLÓGICOS

2.1 Generalidades de Voz sobre IP

El crecimiento y fuerte implantación de las redes IP, tanto en local como en remoto, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que permitan la calidad de servicio en redes IP, han creado un entorno donde es posible transmitir telefonía sobre IP.

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

La telefonía sobre IP abre un espacio muy importante dentro del universo que es Internet. Es la posibilidad de estar comunicados a costos más bajos dentro de las empresas y fuera de ellas, es la puerta de entrada de nuevos servicios apenas imaginados y es la forma de combinar una página de presentación de Web con la atención en vivo y en directo desde un call center, entre muchas otras prestaciones.

Voz sobre IP es la habilidad de transmitir información de llamadas telefónicas sobre una red IP con funcionalidades similares a las encontradas en el sistema de telefonía tradicional.

2.1.1 Redes de voz Vs. Redes de datos

Las redes desarrolladas a lo largo de los años para transmitir las conversaciones vocales, se basaban en el concepto de conmutación de circuitos, o sea, la realización de una comunicación requiere el establecimiento de un circuito físico durante el tiempo que dura ésta, lo que significa que los recursos que intervienen en la realización de una llamada no pueden ser utilizados en otra hasta que la primera no finalice, incluso durante los silencios que se suceden dentro de una conversación típica.

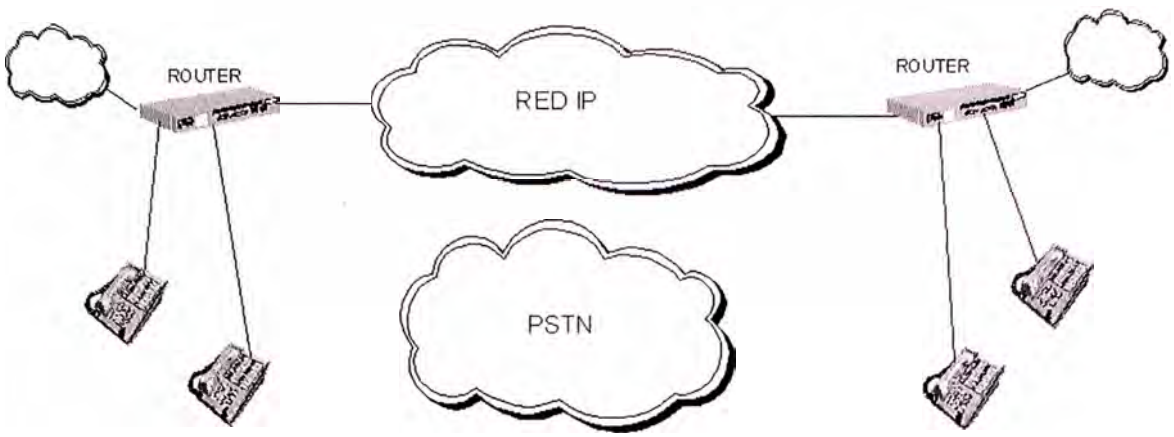


Fig. 1 Diagrama de red de voz vs. red de datos

En contraposición a esto tenemos las redes de datos, basadas en el concepto de conmutación de paquetes, o sea, una misma comunicación sigue diferentes caminos entre origen y destino durante el tiempo que dura, lo que significa que los recursos que intervienen en una conexión pueden ser utilizados por otras conexiones que se efectúen al mismo tiempo.

Es obvio que el segundo tipo de redes proporciona a los operadores una relación ingreso / recursos mayor, es decir, con la misma cantidad de inversión en infraestructura de red, obtiene mayores ingresos con las redes de conmutación de paquetes, pues puede prestar más servicio a sus clientes. Otra posibilidad sería que prestará más calidad de servicio, velocidad de transmisión, por el mismo precio.

Pero bueno, si las redes de conmutación de paquetes son tan buenas, ¿por qué no se utilizan ya para las llamadas telefónicas? Bueno, este tipo de redes también tiene desventajas. Transportan la información dividida en paquetes, por lo que una conexión suele consistir en la transmisión de más de un paquete. Estos paquetes pueden perderse, y además no hay una

garantía sobre el tiempo que tardarán en llegar de un extremo al otro de la comunicación.

2.1.2. La telefonía tradicional hasta ahora

Lo que tenemos hasta hoy es una red de acceso, que incluye el cableado desde el hogar del abonado hasta las centrales locales y el equipamiento necesario, y una red de transporte, que incluye las centrales de rango superior y los enlaces de comunicaciones que las unen. La comunicación se lleva a cabo por conmutación de circuitos.

Como ya hemos indicado anteriormente todos los recursos destinados a intervenir en el desarrollo de una conversación telefónica no pueden ser utilizados por otra llamada hasta que la primera no finaliza.

2.1.3 La telefonía vocal con IP

En la telefonía IP el cambio fundamental se produce en la red de transporte: ahora esta tarea es llevada a cabo por una red basada en el protocolo IP, de conmutación de paquetes, por ejemplo Internet. En cuanto a la red de acceso, puede ser la misma que en el caso anterior, físicamente hablando (bucle de abonado).

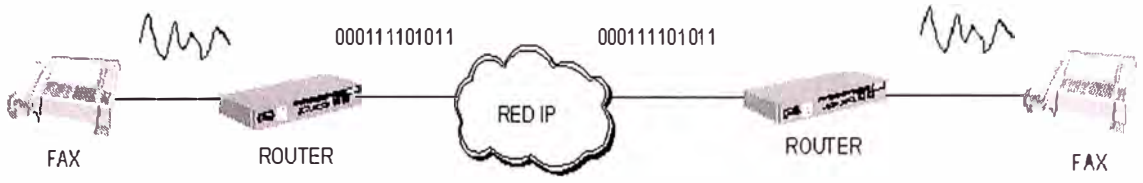


Fig. 2 Diagrama de empaquetamiento de la voz en IP

Los elementos necesarios para que se puedan realizar llamadas vocales a través de una red IP dependen en gran medida de qué terminal se utiliza en ambos extremos de la conversación. Estos pueden ser terminales IP o no IP.

Entre los primeros está el teléfono IP, un ordenador multimedia, un fax IP, entre los segundos está un teléfono convencional, un fax convencional, Los primeros son capaces de entregar a su salida la conversación telefónica en formato de paquetes IP, además de ser parte de propia red IP, mientas que los segundos no, por lo que necesitan de un dispositivo intermedio que haga esto antes de conectarlos a la red IP de transporte.

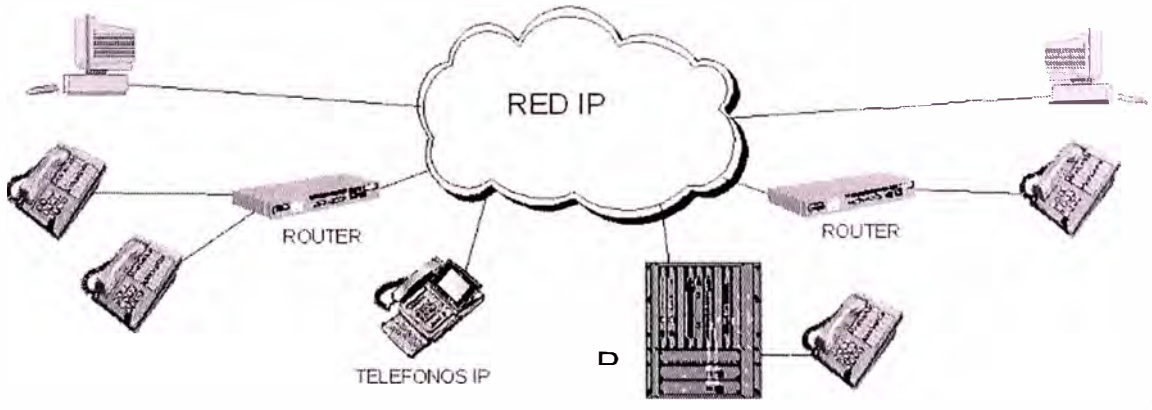


Fig. 3 Terminales IP y no IP en la red VoiP

Hay que señalar que en el caso de que uno o ambos extremos de la comunicación telefónica sean un terminal IP, es importante conocer de qué modo están conectados a Internet. Si es de forma permanente, se les puede llamar en cualquier momento. Si es de forma no permanente, por ejemplo, a través de un Proveedor de Acceso a Internet (PAI) vía módem, no se les puede llamar si en ese momento no están conectados a Internet.

2.2 Protocolo H.323

Es un protocolo para multimedia que provee las bases para trafico de audio, video y datos sobre una red IP,

Esta basado en protocolos de capa 3 y 4 (TCP, UDP, IP)

Es independiente de la topología de la red, la red puede estar conformada por hubs, routers, switches, accesos remotos, etc.

Cubre varios estándares y recomendaciones de ITU: H.225(Q.931), H.245, G.711, G.729, etc.

Voz sobre IP sigue en su mayoría, el estándar H.323 creado por ITU, H.323 describe los terminales y otros elementos que proveen servicios de comunicación multimedia sobre una red de paquetes.

Estos elementos pueden proveer audio en tiempo real (voz), video y datos, H.323 define 4 tipos de elementos:

Terminales, Gateways, Gatekeeper y Multipoint Control Unit (MCUs).

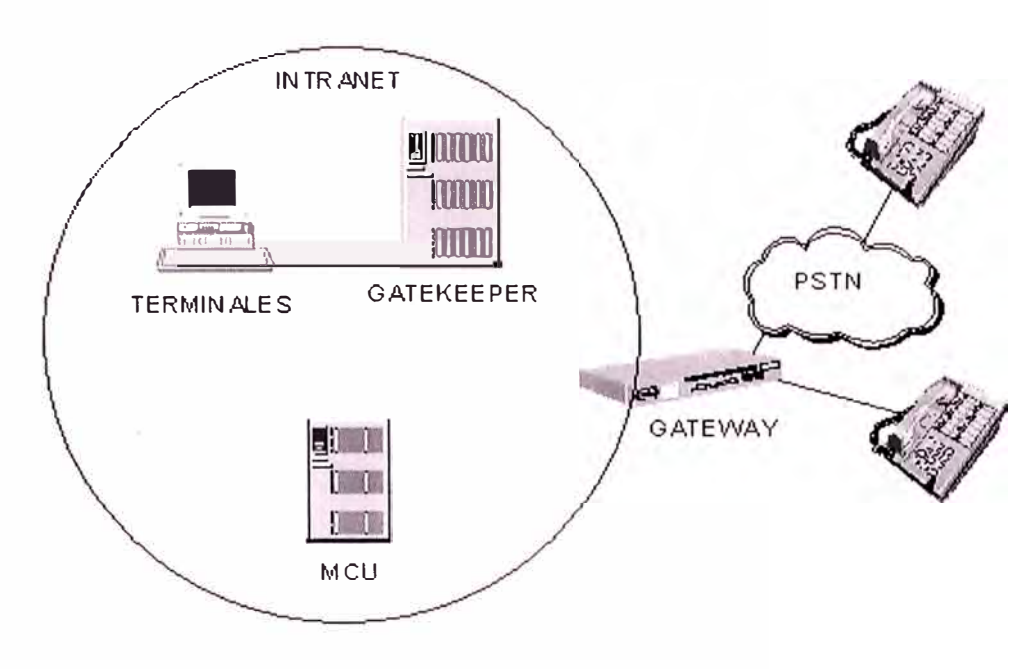


Fig. 4 Elementos definidos por el protocolo H.323

2.2.1 Puente o Gateway

El Gateway es el elemento encargado de hacer de puente entre la red telefónica convencional (RTB o PSTN) y la red IP. Cuando un teléfono convencional trata de hacer una llamada IP, alguien tiene que encargarse de convertir la señal analógica en un caudal de paquetes IP, y viceversa. Esta es una de las funciones del Gateway, que también ofrece una manera de que un dispositivo no IP pueda comunicarse con otro IP. Por una parte

conecta a una central telefónica, y por la otra a una red IP. Otra de sus funciones es realizar la compresión y empaquetamiento de la voz.

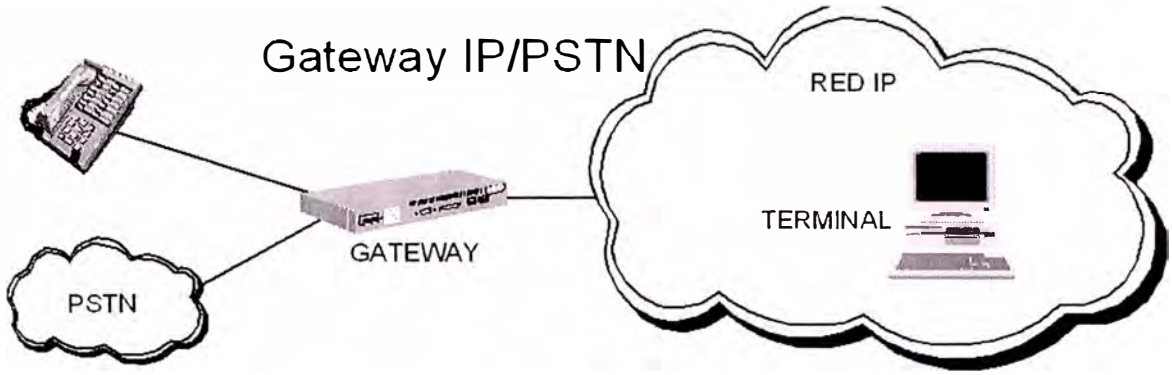


Fig. 5 Gateway IP / RTB (PSTN)

2.2.2 Controlador de conferencias Gatekeeper

El Gatekeeper actúa en conjunción con varios Gateways, y se encarga de realizar tareas de autenticación de usuarios, control de ancho de banda, encaminamiento IP, Es el cerebro de la red de telefonía IP. No todos los sistemas utilizados por los PSTIs son compatibles (Gateway, Gatekeeper) entre sí. Este ha sido uno de los motivos que ha impedido que la telefonía IP se haya extendido con mayor rapidez. Actualmente esto se está corrigiendo, y casi todos los sistemas están basados en el protocolo H.323.

2.2.3 Unidad de control Multipunto (MCU)

Multipoint control unit, provee el control para soportar conferencias entre tres o más elementos, es opcional. Puede ser un dispositivo stand – alone como una PC o integrado en gateway, gatekeeper o terminal. Típicamente consiste de MC (Multipoint Controller) y MP (Multipoint Processor)

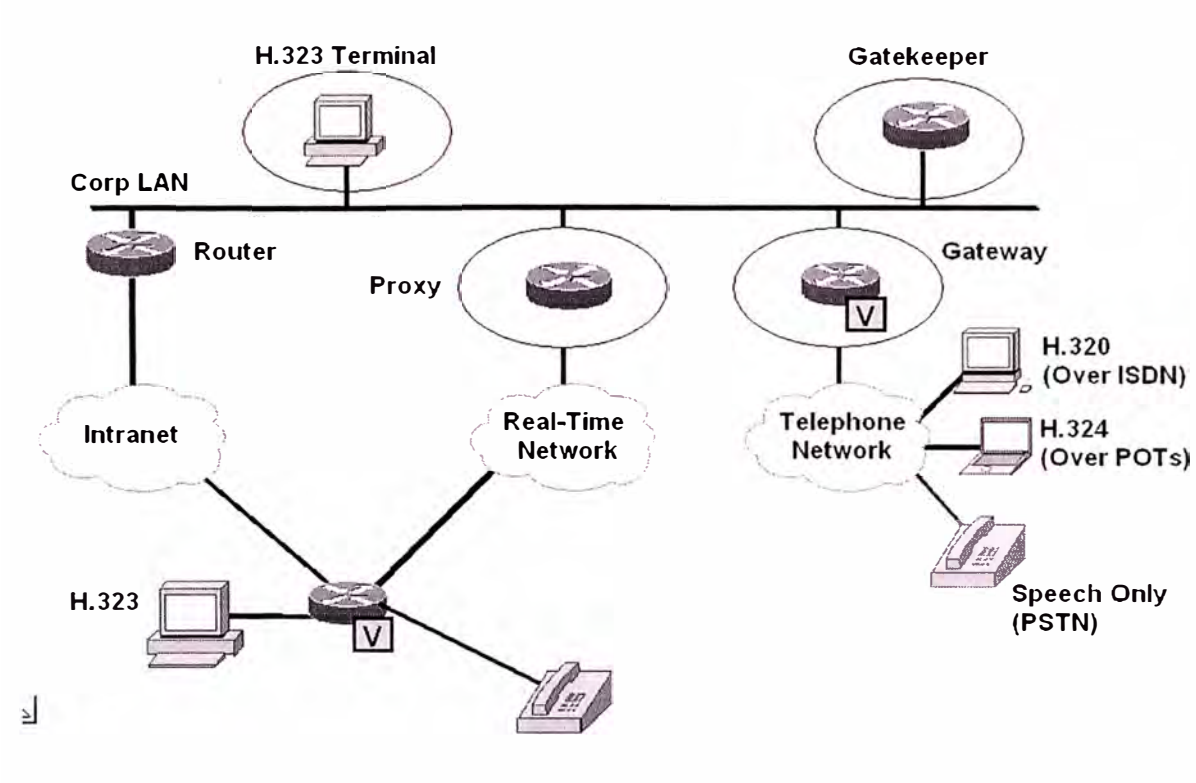


Fig. 6 Infraestructura en una red VoiP bajo protocolo H.323

El H.323 es la primera especificación completa bajo la cual, los productos desarrollados se pueden usar con el protocolo de transmisión más ampliamente difundido (IP). Existe tanto interés y expectación entorno al H.323 porque aparece en el momento más adecuado. Los administradores de redes tienen amplias redes ya instaladas y se sienten confortables con

las aplicaciones basadas en IP, tales como el acceso a la web. Además, los ordenadores personales son cada vez más potentes y, por lo tanto, capaces de manejar datos en tiempo real tales como voz y vídeo.

Varias compañías consultoras independientes predicen una rápida adopción del H.323

Un terminal H.323 es un extremo de la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323, gateway o unidad de control multipunto (MCU). Esta comunicación consta de señales de control, indicaciones, audio, imagen en color en movimiento y /o datos entre los dos terminales. Conforme a la especificación, un terminal H.323 puede proporcionar sólo voz, voz y datos, voz y vídeo, o voz, datos y vídeo.

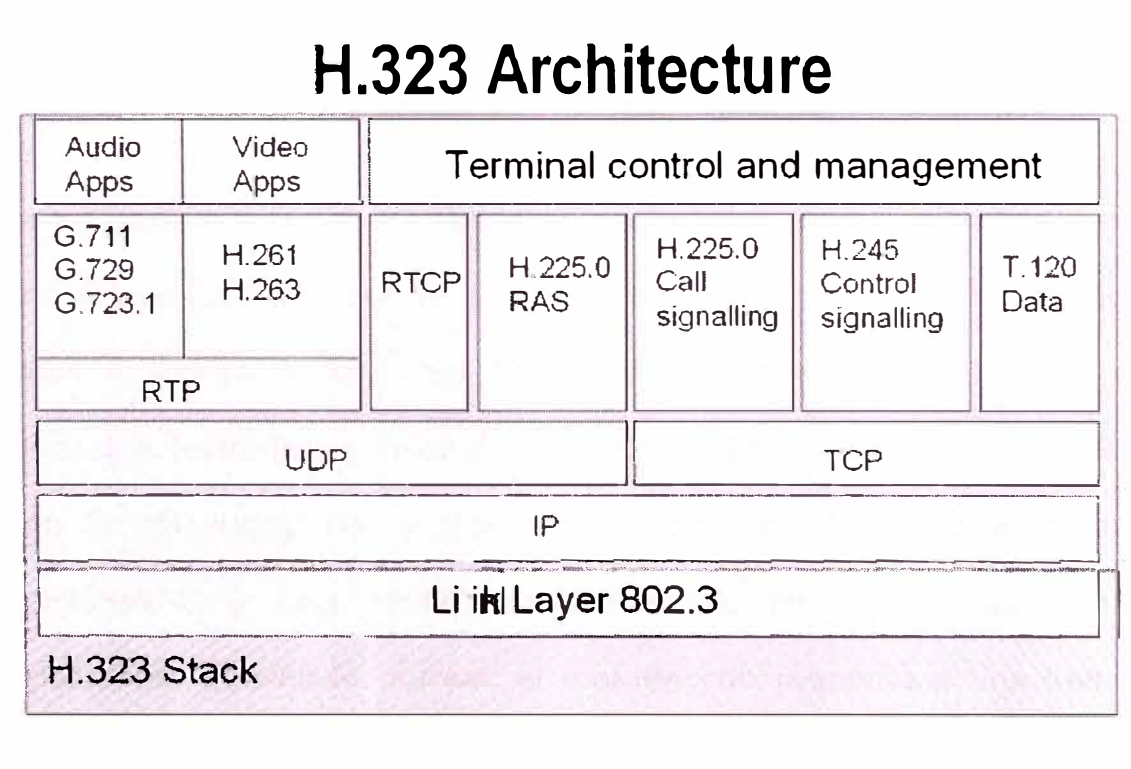


Fig. 7 Stack del protocolo H.323

2.3 Escenarios de Voz sobre IP

2.3.1 Llamadas teléfono a teléfono

En este caso tanto el origen como el destino necesitan ponerse en contacto con un Gateway. Supongamos que el teléfono A descuelga y solicita efectuar una llamada a B. El Gateway de A solicita información al Gatekeeper sobre como alcanzar a B, y éste le responde con la dirección IP del Gateway que da servicio a B. Entonces el Gateway de A convierte la señal analógica del teléfono A en un caudal de paquetes IP que encamina hacia el Gateway de B, el cuál va regenerando la señal analógica a partir del caudal de paquetes IP que recibe con destino al teléfono B. Fijaos como el Gateway de B se encarga de enviar la señal analógica al teléfono B.

Por tanto tenemos una comunicación telefónica convencional entre el teléfono A y el Gateway que le da servicio (Gateway A), una comunicación de datos a través de una red IP, entre el Gateway A y el B, y una comunicación telefónica convencional entre el Gateway que da servicio al teléfono B (Gateway B), y éste. Es decir, dos llamadas telefónicas convencionales, y una comunicación IP. Si las dos primeras son metropolitanas, que es lo normal, el margen con respecto a una llamada telefónica convencional de larga distancia o internacional, es muy grande.

Fig. 8 Esquema del escenario teléfono a teléfono analógico

2.3.2 Llamadas PC a teléfono o viceversa

En este caso sólo un extremo necesita ponerse en contacto con un Gateway. El PC debe contar con una aplicación que sea capaz de establecer y mantener una llamada telefónica. Supongamos que un ordenador A trata de llamar a un teléfono B. En primer lugar la aplicación telefónica de A ha de solicitar información al Gatekeeper, que le proporcionará la dirección IP del Gateway que da servicio a B. Entonces la aplicación telefónica de A establece una conexión de datos, a través de la Red IP, con el Gateway de B, el cuál va regenerando la señal analógica a partir del caudal de paquetes IP que recibe con destino al teléfono B. Fijaos como el Gateway de B se encarga de enviar la señal analógica al teléfono B.

Por tanto tenemos una comunicación de datos a través de una red IP, entre el ordenador A y el Gateway de B, y una comunicación telefónica

convencional entre el Gateway que da servicio al teléfono B (Gateway B), y éste. Es decir, una llamada telefónica convencional, y una comunicación IP. Si la primera es metropolitana, que es lo normal, el margen con respecto a una llamada telefónica convencional de larga distancia o internacional, es muy grande.

2.3.4 Llamadas PC a PC

En este caso la cosa cambia. Ambos ordenadores sólo necesitan tener instalada la misma aplicación encargada de gestionar la llamada telefónica, y estar conectados a la Red IP, Internet generalmente, para poder efectuar una llamada IP. Al fin y al cabo es como cualquier otra aplicación Internet, por ejemplo un chat.

Como se ha explicado Voz sobre IP puede ser implantado utilizando diversos equipos como se observa en la figura xx

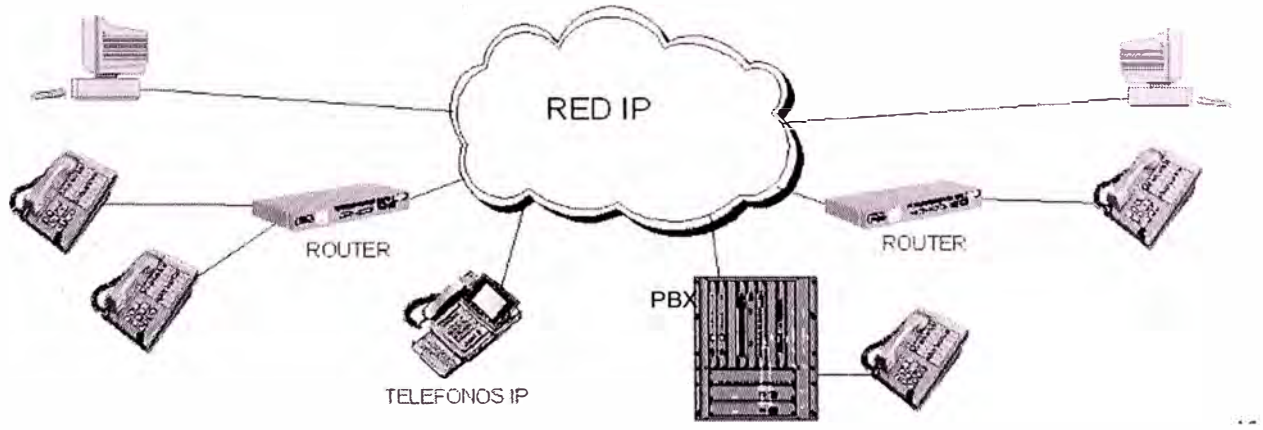


Fig. 9 Equipos utilizados en los diferentes escenarios de telefonía IP

2.3.5 Futuro de la Telefonía IP

En primer lugar tenemos al Proveedor de Servicios de Telefonía por Internet (PSTI, o ISTP en inglés). Proporciona servicio a un usuario conectado a Internet que quiere mantener una comunicación con un teléfono convencional, es decir, llamadas PC a teléfono. Cuenta con Gateways conectados a la red telefónica en diversos puntos por una parte, y a su propia red IP por otra. Cuando un usuario de PC solicita llamar a un teléfono normal, su red IP se hace cargo de llevar la comunicación hasta el Gateway que da servicio al teléfono de destino. Esto significa que para que los usuarios de PC de un PSTI puedan llamar a muchos países, éste necesita tener una gran cantidad de Gateway; Pues no. Conforme se van extendiendo los PSTI por todo el mundo, lo que se hace es establecer acuerdos económicos con otros PSTI, para intercambiar llamadas IP. Tú finalizas las llamadas que originan mis usuarios, y que tengan como destino teléfonos que tus Gateways cubren de forma local, y viceversa. En vez de llevar a cabo estos acuerdos bilaterales, lo que se suele hacer es trabajar con intermediarios, que tienen acuerdos con PSTI's de todo el mundo. Estos intermediarios son conocidos como Proveedores de Servicios de Clearinghouse (PSC, o CSP).

Con lo visto, no parece descabellado asegurar que el futuro de la telefonía pasa por las redes IP. Entonces, ¿qué pasa con los operadores tradicionales?, a no ser que no se den cuenta de que la telefonía IP no es

su competidor, sino su aliado. La mayoría de ellos han puesto en marcha proyectos de telefonía IP, y el que no lo haya hecho ya se puede dar prisa. Por el contrario existen nuevos operadores, que desde sus inicios han apostado fuerte por esta tecnología, y cuyo crecimiento está asegurado.

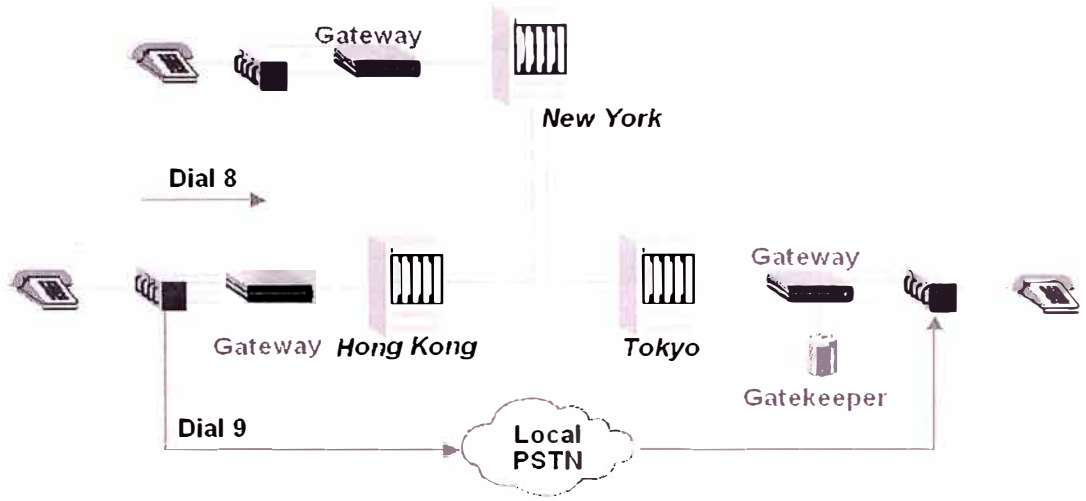


Fig.10 Evolución de las redes de telefonía IP

2.4 Redes Privadas Virtuales

2.4.1 Evolución de las Redes Privadas Virtuales

La evolución de las necesidades de conectividad ha hecho que de las redes privadas (PN) se haya generado la necesidad de evolucionar a redes privadas virtuales (VPN) y la necesidad de securizar estas ultimas y convertirlas en redes privadas virtuales seguras (SVPN) hace que las herramientas hardware para cifrado de datos sean periféricos de elevado interés. Se repasan las necesidades que han provocado estos cambios y los enfoques que aportan las soluciones hardware de cifrado. Se concluye con una apreciación acerca de sí la introducción de IPv6 hará que su necesidad aumente o disminuya.

Desde la aparición de las Redes Privadas (PN) estas se han revelado como un buen sistema para incrementar la productividad de la empresa, si bien esto ya no siempre es una realidad. El incremento del uso de la tecnología de las comunicaciones y su implantación en el ámbito global ha planteado una serie de problemas de gestión y de explotación que las Redes Privadas ya no siempre son capaces de soportar.

Como ejemplo de estos problemas podemos destacar la imposibilidad de proporcionar conectividad a todos los elementos que forman parte de la estructura de la empresa, como pueden ser los agentes comerciales, que

pueden necesitar una conexión desde emplazamientos móviles o remotos, o los tele trabajadores o cualquiera de los que formando parte de los recursos de la empresa, no se encuentran ubicados en las dependencias de la misma.

También, en una valoración desde el punto de vista optimización de la explotación hay que considerar la nada despreciable coste de las líneas y equipos de comunicación de datos cuando estas son privadas. Esto hace que no siempre se pueden mantener correctamente saturadas en su capacidad, puesto que o si se dimensionan al pico, se infrautilizan gran parte del tiempo con el derroche de recursos que ello comporta, o bien si se dimensionan al valle para disminuir su coste se incurre en el peligro de que se saturen en los momentos de trafico crítico.

Adicionalmente, el ya mencionado incremento de la conectividad en el ámbito global hace que sea un deseo lógico el disponer de medios de comunicación entre la empresa y sus clientes y proveedores, pero no siempre podemos disponer de herramientas que lo permitan, o bien las herramientas que se dispone en ambos lados de la comunicación no siempre son compatibles. Y no debe dejarse de lado los problemas de gestión interempresarial que suponen el ponerse de acuerdo en cuales son las políticas de gestión, explotación y mantenimiento de los recursos compartidos.

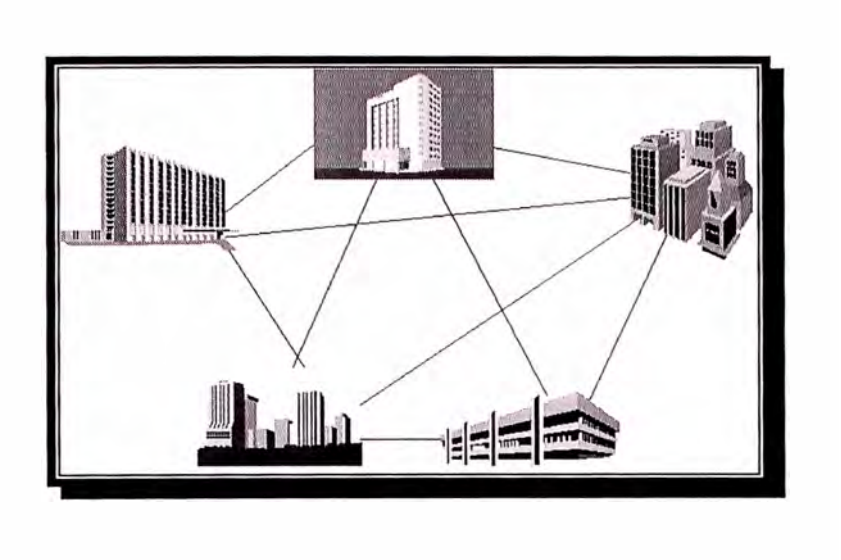


Fig. 11 Redes Privadas

Podemos concluir que los principales problemas que plantea una Red Privada “clásica” son dos:

La Red Privada nunca es lo suficientemente grande

La Red Privada nunca es lo suficientemente compatible

El conjunto de inconvenientes que se resumen en los dos corolarios anteriores han hecho que se volviera una necesidad el evolucionar a un sistema más distribuido para la interconexión de equipos computacionales. El nacimiento del concepto de Red Privada Virtual es la respuesta a esta necesidad de evolución.

La Red Privada Virtual, entendida como aquella que si bien a nivel lógico se puede ver como una única red privada, pero que a nivel físico es un conjunto de diferentes redes privadas que comparten una infraestructura

de datos subyacente de carácter publico ha venido a solucionar gran parte de los anteriores problemas, si bien a costa de generar otros nuevos, en su mayor parte directamente relacionados con el carácter publico de la infraestructura intermedia ya comentada.

La opción más lógica para interconectar redes privadas y formar entre ellas una red privada virtual que permita compartir recursos de comunicación y de datos es hacerlo a través de una red subyacente del mayor alcance posible, solucionando así el primero de los dos problemas, el de que el tamaño nunca es el suficiente. Para solucionar el segundo problema, el de que nunca se esta en un entorno suficientemente compatible, se debe escoger una red de alcance global cuyos protocolos de transmisión sean estándares reconocidos y seguidos.

Y una vez planteada como debe ser la red que permita transformar nuestro conjunto de redes privadas en una única red privada virtual, de alcance global y compatible, la elección es amén de lógica, prácticamente única. Internet es “la” red, es mundial y es compatible.

Por ultimo, cabe considerar la VPN de acceso remoto, en la cual se proporciona conectividad a la red corporativa a los usuarios remotos pero móviles, sin capacidad de disponer de una infraestructura de red estática.

Genéricamente, la filosofía de una VPN, si representáramos Internet por la esfera del mundo, tendría un aspecto topológico parecido al siguiente

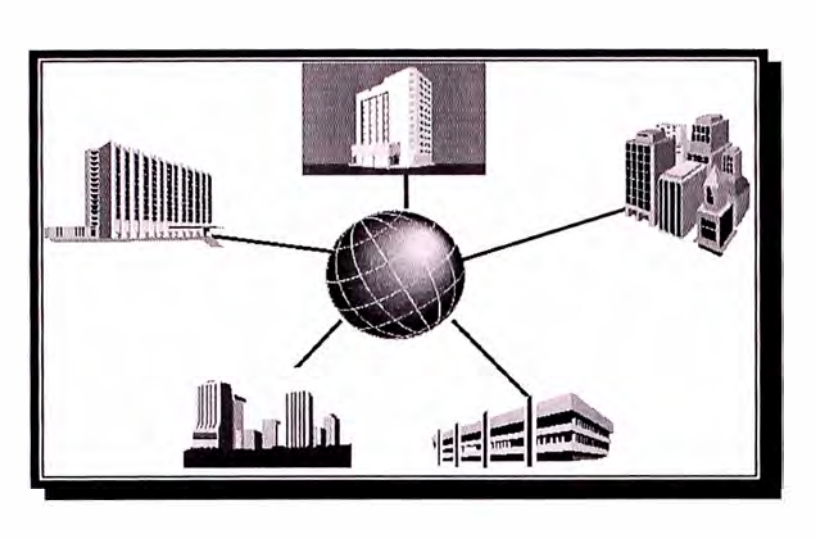


Fig. 12 Red Privada Virtual

Ahora bien, el hecho de que Internet sea la elección lógica para la consecución de una VPN también es la causa de que alguno de las ventajas de la red se conviertan en inconvenientes.

El hecho de que Internet este accesible a todo el mundo, a la vez que ha promovido un crecimiento explosivo de las capacidades de comunicación personal y ha proporcionado un método fácil de acceso a recursos informáticos públicos pero distantes, también se ha convertido en un método fácil de acceso a recursos informáticos distantes, pero privados.

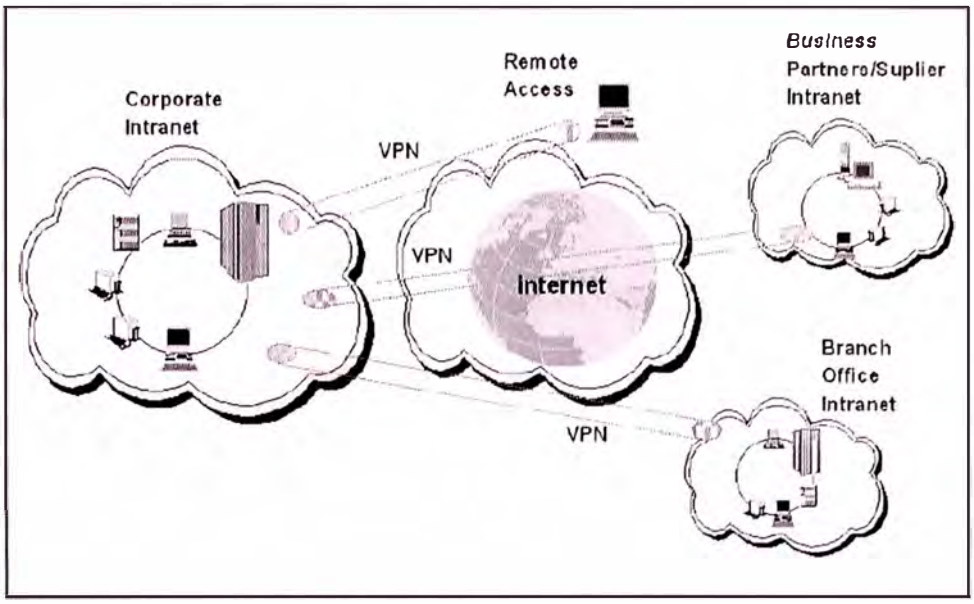


Fig. 13 Alcance de las redes privadas virtuales

Es decir, la empresa que para aumentar su productividad opte por el establecimiento de una VPN entre sus usuarios locales, remotos y móviles, a la vez que pone sus recursos a disposición de los usuarios autorizados, corre el riesgo de ponerlos al alcance de usuarios no autorizados con los riesgos que ello conlleva.

Es lógico pues que la evolución de las redes privadas virtuales (VPN) sea hacia las redes privadas virtuales seguras (SVPN). Para proporcionar comunicaciones seguras, un sistema debe ser capaz de proporcionar siete puntos principales, como son:

Confidencialidad: Debe proteger el valor de la información

Integridad: Debe proporcionar protección de la veracidad de la información

Autenticación: Debe proporcionar confianza en el origen de la información

No repudiación: Debe asegurar la capacidad de acceder al servicio

Identificación : Debe asegurar la identidad de los usuarios

Control de Acceso: Debe permitir el control de acceso a la información y los recursos

Viabilidad: Debe asegurar la recepción de la información.

El objetivo de las SVPN es, pues, mediante las técnicas que fueren necesarias, conseguir proporcionar comunicaciones seguras a los usuarios a través de proporcionar inmunidad a las amenazas que se devengan de los tipos clásicos de ataques.

También es viable considerar el ataque de modificación de la información como un ataque de interceptación del flujo de datos en paralelo con un ataque de generación de la información, pero esta división en cuatro tipos de ataques es la mas ampliamente aceptada en los ámbitos de la protección de datos, y es la que se va a mantener en este documento.

2.4.2 Las Redes Privadas Virtuales en la actualidad y el futuro.

En general el cambio que sufren estas estructuras va parejo a las nuevas necesidades de las organizaciones con respecto a sus comunicaciones en un entorno cada vez más globalizado en el que las empresas necesitan tener una presencia extendida en un ámbito de

competencia feroz donde aprovechar cualquier ventaja que la tecnología aporte constituye un factor decisivo de éxito (y al contrario de fracaso).

Por una parte la seguridad se convierte en una exigencia ineludible. Si un sistema no es seguro no es útil y por ello se han diseñado mecanismos y estrategias que aporten el nivel de seguridad necesario.

Por otra parte la calidad a todos los niveles (capacidad, fiabilidad etc.) de los canales de comunicación públicos soporte de las VPN va cambiando respecto a lo acostumbrado hasta ahora; tanto por la propia infraestructura de estas redes de nueva generación como por los proveedores de acceso a las mismas. La internet que hemos sufrido: lenta, endeble e impredecible tiene sus días contados, al menos en el entorno profesional.

Pero además, las redes son mucho más grandes y heterogéneas, requiriéndose comunicar un mayor número de usuarios y ubicaciones pertenecientes, ya no sólo a una única organización, sino a todos los agentes de un proceso (por ejemplo clientes, proveedores y empleados en sus distintas posibilidades de ubicación -fijas y móviles- que componen un mismo proceso de negocio). Es por ello que no vale con garantizar la seguridad o la calidad en el servicio en el interior de una organización, sino que es necesario asegurar estos valores en el nuevo entorno requerido.

Fruto de todos estos cambios surgen las Redes Privadas Virtuales de Gran Escala (Large Scale VPN, LSV o LSVPN) en las que no sólo hablamos de un tamaño mayor (centenares de ubicaciones y miles de usuarios) sino de unos requerimientos mejorados en todas las facetas mencionadas y otras propias de estas estructuras de mayor tamaño y criticidad para las organizaciones que las emplean.

El objetivo de esta ponencia es exponer en grandes líneas los factores claves de esta nueva situación.

2.4.3 Ventajas y desventajas de las VPNs

Las VPNs reducen sustancialmente los costos y son fáciles de usar, pero es necesario indicar que las redes privadas virtuales implican costos, requisitos organizacionales y cargas de trabajo al personal de sistemas adicionales para una organización, pero que son sopesados al obtener ahorros en el costo, al utilizar una red pública en vez de una instalación de línea rentada y la facilidad de utilizar dicha red con el fin de hacer negocios.

Estos beneficios se orientan a áreas independientes y podemos indicarlos de la siguiente manera:

Cargos de telecomunicaciones

Líneas rentadas

Números 800

Administración

Equipo de acceso remoto por marcación

Facilidad de mantenimiento

Diseños de administración de red simplificada

Pese a los beneficios potenciales que pueden lograrse en necesario observar mucho cuidado en su diseño e implementación.

Ahorra y reduce los costo del servicio telefónico de larga distancia, al eliminar muchos de los dispositivos asociados con la infraestructura de telecomunicaciones de las líneas rentadas.

También reducción del tiempo que el personal de sistemas de la corporación invierte en la administración y mantenimiento de los dispositivos al eliminar dispositivos como las líneas rentadas y el equipo costoso de acceso remoto, significando un ahorro en el rango de 60 a 80 por ciento., esta cantidad es deducida eliminando el número de líneas de acceso de una corporación típica, junto con una número estimado de líneas rentadas, y multiplicando el resultado por el número de usuarios que acceden al equipo. Por consiguiente el mantenimiento y el soporte para estos dispositivos no serán necesarios, así que se estima adicionalmente el número de horas eliminadas que se necesitaron para el soporte y calcular un ahorro en los costes. Estas estadísticas financieras incluyen el equipo actual, la línea de

telecomunicación y la estructura de soporte. Por lo tanto, el mayor impacto de la tecnología VPN en los ahorros en el costo se originan al eliminar los cargos incurridos durante las condiciones de trabajo normal dentro del escenario de línea rentada regular. Otras consideraciones para la eliminación son las siguientes:

Líneas rentadas

Líneas por marcación

Equipo de acceso por marcación

Tiempo que invierte para configurar el equipo del usuario final.

Tiempo que invierte para mantener el equipo del usuario final.

Contratos de mantenimiento del equipo

Equipo PBX (propiedad del cliente)

Servidor de autenticación por marcación

Números 800

Enlaces ATM o Frame costosos

Conexiones ISDN

Soporte para IP, DNS y flujo de enrutamiento

2.4.4 Diseño de una VPN

La VPN es benéfica, desde el punto de vista de diseño arquitectónico, flexibilidad y mantenimiento, la necesidad de un diseño WAN complejo, de

cálculos de desempeño de enlace, ajustes en el tamaño de los conductores de ancho de banda y redundancia, ya no representan un problema para una organización, ya que la principal preocupación es la conexión a internet de su proveedor PSI local, quién manejará todos los problemas asociados con su conexión, se supero el inconveniente de diseñar e instalar líneas rentadas en ciertas ubicaciones, considerando el tiempo de inactividad, enlaces redundantes y los problemas de ampliación y desempeño, con el limitante que las líneas rentadas no son ampliables fácilmente y son caras, por lo que el administrador de una red típica WAN sobre líneas rentadas debe tener en cuenta el flujo de tráfico entre departamentos ubicados en distintos puntos geográficos, edificios, ciudades, cuentas de accesos de usuarios remotos por marcación y carga adicional de instalar enlaces redundantes para prevenir fallas de la comunicación con el enlace principal

Con la arquitectura VPN, el trabajo de reduce ya que solo se requiere una conexión a internet, el PSI se encarga del transporte, aspectos asociados con las redundancias y los atributos de tolerancia frente a fallas. Ahora la red WAN puede ser escalable, redundante y estar basada en normas (TCP/IP), y soportar capacidades de administración distribuidas, lo principal entonces será considerar el ancho de banda correcto para el PSI, examinar los patrones de tráfico en las redes y estimar el porcentaje de tráfico necesario para acceso a internet e incluso hacerse un análisis de tendencias para estimar la cantidad necesaria en el futuro, para con estos

datos decidir si que quiere tener un conducto de ancho de banda actualizado.

La Administración centralizada, es una característica sólida como un excelente mecanismo par solucionar problemas, ya que simplifica los procesos de mantenimiento y la solución de problemas de infraestructura de la VPN, elimina exceso de personal y reduce las cargas de administración gracias a la posibilidad de administración remota

2.4.5 Beneficios de la VPN para el usuario final.

En la actualidad los negocios deben ir en busca del cliente indistintamente de la zona geográfica en la que este ubicado, por lo que el acceso a la red debe estar disponible a todo momento, con el acceso a través del PSI y la tecnología VPN y debido a la compatibilidad con diferentes protocolos de red superada gracias a Internet, hoy en día esto es técnicamente posible.

- **Reducción de costos**

Con Internet, se paga solo el tiempo en línea, que generalmente significa una llamada local, y la cuota mensual respectiva, eliminando de este modo los costos por cargos telefónicos de larga distancia en el caso de tener oficinas remotas y/o sucursales. Con líneas rentadas, retransmisión de

tramas u otra infraestructura se paga aún si no se esta utilizando el conducto (tiempo de inactividad)

- **Accesos a Datos**

Las VPN ofrecen al usuario remoto diferentes tipos de acceso hacia la organización, a través de diferentes aplicaciones, utilizando internet como si fuera su red local y conectarse al servidor a través de cualquier servicio deseado.

- **Asignación de prioridad de tráfico**

Ya que las VPN ofrecen acceso a una extranet, a una Intranet o servidores internos de una organización, es posible decidir que sólo se permita pasar libremente cierto tipo de tráfico, con el fin de conservar el ancho de banda, mientras que el otro tipo de tráfico quede en cola de espera según su importancia.

2.4.6 Beneficios de un alcance global.

Con internet se obtiene el acceso global, cualquier usuario en el planeta, puede conectarse a la LAN de su compañía, siempre que exista un proveedor de TSI en esa área, permitiendo a la compañía tener presencia en todo el mundo.

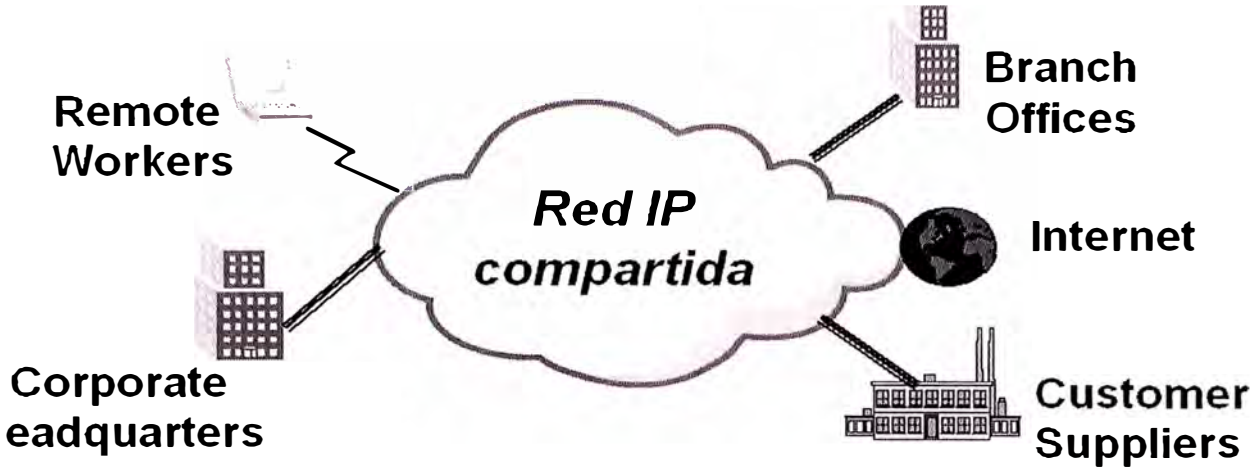


Fig. 14 Acceso global de las VPN

- **Teleconferencias**

Actualmente pese a la demanda, esta tecnología no es muy usada sobre internet, pero dado que seguirá creciendo los PSI deberán poder proporcionarla y quienes ofrezcan garantías de calidad de servicio entre varias ciudades importantes del mundo, ahorrando tiempo y dinero se volverán un socio de esa compañía.

- **Telefonía IP**

La teleconferencia, todavía tiene mayor demanda que la telefonía IP, pero es sin duda un servicio de rápido crecimiento que demandará el mismo tipo de garantía de calidad de servicio y significará significativos ahorros al poder utilizar a internet como un medio de comunicación en las llamadas diarias.

2.4.7 Ventaja competitiva de las VPN

Las VPN ofrecen una ventaja competitiva, que conforme mas organizaciones comiencen a usar VPN y se conecten a Internet, la ventaja se dará en términos de confiabilidad, latencia y características adicionales ofrecidas por la VPN, además mientras más PSI ofrezcan características de tecnología internet adicionales, más compañías demandarán estas características, lo cual incrementará su ventaja competitiva.

- **Costos de la tecnología VPN.**

A pesar del ahorro en la implementación de las VPN hay costos adicionales que deben considerarse:

Infraestructura de red del PSI

Equipo de VPN

Costos de mantenimiento

Licencias

Aspecto legal de la compatibilidad con el año 2000

Costos de la solidez del cifrado

Administración

Personal de seguridad

Servicio de ayuda para resolver problemas

- **Costos de telecomunicaciones adicionales.**

Estos elementos incurren en desembolsos de recursos financieros para implementar esta tecnología, pero también pueden ahorrarle mucho dinero a la compañía.

2.4.8 Infraestructura de red del proveedor de servicios IP

La compañía en caso de una falla importante del enlace a internet, deberá tener ya sea un enlace secundario a los PSI o algún tipo de equipo de acceso remoto para dirigir los negocios.

Los ahorros en el costo asociados con las VPN no toman en consideración estos factores, pero esta situación debe planearse para protegerse oportunamente

- **Equipo de VPN**

Si se quiere añadir una configuración independiente o algún tipo de equipo, como servidor RADIUS de autenticación de usuarios ¿donde será colocado?, o equipo para acceso remoto (RAS), es necesario considerar que otro tipo de hardware y software se puede añadir, y multiplicarlos por el número de sitios que se tiene para tener un aproximado de los costos capitales

- **Costos de mantenimiento**

Como cualquier otro equipo, es probable costos de mantenimiento por hardware, software o ambos, que deben incluir actualizaciones gratuitas para interoperabilidad con las futuras normas de seguridad IPSec, PPTP, y L2TP para la VPN de internet.

Cada proveedor ofrecerá contratos de mantenimiento variables, y la preocupación será el tiempo de inactividad, ¿cuánto demora en reparar o reemplazar un equipo y a que precio?, atención de 4 a 24 horas inclusive fines de semana.

- **Licencias**

Según el producto, y de acuerdo al proveedor, las licencias significarán el número de usuarios simultáneamente conectados al dispositivo de red, o tal vez una cuota de licencia simple a un enrutador, esto seria conveniente porque permite conexiones VPN ilimitadas, también puede basar las licencias en el número de túneles creados, por lo que si se tiene claro la utilidad de la VPN, se puede calcular el número de usuarios finales, túneles, etc necesarios.

- **Administración**

Debe haber un responsable de la supervisión y mantenimiento de la VPN, ya sea la organización o el PSI, de ser administrado por el PSI, este se incluye en la tarifa por el servicio, por lo general las actualizaciones normales y/o correcciones se manejan vía telefónica si el dispositivo VPN es

un dispositivo de sistema operativo UNIX o un tipo de enrutador. Con los dispositivos de hardware existe un disco flexible que se carga en el dispositivo y al momento de encender el hardware se instalará la nueva revisión, si los dispositivos están en lugares distantes será necesario administrarlos en forma remota.

- **Tipos de accesos requeridos**

En banda, se puede crear un túnel de administración cerrado entre los dispositivos de la VPN, para la administración remota desde internet.

Fuera de banda, esta configuración coloca un módem de cifrado en los puertos de consola de los dispositivos VPN en diferentes ubicaciones.
Se requiere tener esta configuración en caso de que no pueda tener acceso en banda al dispositivo VPN. De instalarse un dispositivo en forma remota e involuntariamente se deniega el acceso en banda, se habrá perdido la conectividad a este dispositivo, por lo que se hace uso de módems de cifrado para que se comuniquen con los módem de cifrados instalados, bloqueando cualquier llamada entrante de otros módems.

- **Personal de seguridad**

Este costo adicional será uno de los mayores desembolsos de la organización, respecto a recursos técnicos y financieros requeridos para implementar y vigilar la tecnología VPN. Se necesitará algunos técnicos que

se responsabilicen de definir las políticas de seguridad de la organización y que actualicen los cambios a esta política.

Si la organización implementa esta tecnología personalmente estar claros de los algoritmos de cifrado más sólidos disponibles, autenticación de usuarios, se usará servidor RADIUS, firmas digitales o autoridades emisoras de certificados para la autenticación, etc, si la VPN es administrada por un PSI, la organización deberá decidir las políticas de seguridad corporativas y el PSI las implementará

- **Costos adicionales de telecomunicaciones**

Adicionalmente a los costos asociados con la implementación de la tecnología VPN, existen costos directos en los que la organización incurrirá con el servicio telefónico

- **Larga Distancia**

Los usuarios marcan a un PSI y con una cuota mensual de conexión a internet pueden conducir todos sus negocios en forma gratuita, ya que la llamada no tiene costo, sin embargo, hay una diferencia en las tarifas entre llamadas de larga distancia de estado a estado y llamadas de larga distancia interestatales, por lo que si el usuario remoto tiene que marcar a un PSI y establecer una conexión, podrán incurrir en cargos de larga distancia

interestatales, si la compañía telefónica no maneja todas las centrales locales.

- **Garantías de calidad de servicio**

La calidad de servicio es un proceso en el cual los conmutadores y los enrutadores instalan recursos para mover datos en forma rápida y confiable, intentando cubrir algunos de los atributos siguientes:

Definir los retrasos

Inestabilidad

Límites de pérdida de celdas/paquetes

Seguridad

Ancho de banda con base en aplicaciones

Especificar los retrasos aceptables

Descartar rangos

Añadir ancho de banda, soluciona fácilmente el problema, pero es caro y no todas las aplicaciones lo necesitan, por lo que la QoS ayuda a definir un esquema de asignación de prioridades, donde las aplicaciones que consumen mayor ancho de banda obtendrán los servicios que necesitan y las aplicaciones de uso menos intensivo también.

- **Contratos a nivel de servicio**

- **Tiempo de actividad de la red**

El tiempo de actividad de la red es el tiempo real que la red esta **activa** y disponible para **pasar** tráfico. La red podría estar activa pero ser incapaz de pasar tráfico. En el nivel de enlace de datos, un dispositivo podría reportarle que está activo, pero la capa de red del mismo, la capa real que reenvía su tráfico, podría no estar en funcionamiento, por lo que la red está inactiva y no fluirá ningún tráfico, esto podría ocurrir en un enrutador con una tabla de enrutamiento incompleta o incorrecta, Si el enrutador del proveedor, el responsable de pasar su tráfico tiene su tabla de enrutamiento corrompida, su tráfico puedo enviarse de regreso a la organización o simplemente detenerse. Se debe esperar entonces que el PSI indique un tiempo de actividad disponible del rango del 90 al 99.9 por ciento.

- **Ancho de banda**

Podría significar el ancho de bando del conducto hacia el proveedor, o el ancho de banda de banda disponible sobre la columna vertebral del PSI, en este caso generalmente es bastante grande estando en el rango de terabits por segundo(un terabit es 10^{12} o 1,000,000,000,000 de bits por segundo) esto gracias a la tecnología de red óptica síncrona (SONET) que utiliza rayos de luz como portadores, pero esta tecnología esta siendo aplicada primero a la columna vertebral de Internet, en consecuencia, pese a poder atravesar el país en un segundo, todavía podría llevar 3 o 4 segundos

alcanzar su destino final, debido a que está saliendo de la columna vertebral de sonet y entrando a un enlace mas lento.

- **Latencia**

Es el concepto que explica el retraso del establecimiento inicial del enlace en la comunicación entre puntos. Las conexiones de la red atravesarán dos, tres o varias columnas vertebrales del PSI.

Este problemas es intentado resolver por los PSI, siendo la mejor solución trabajar en conjunto estableciendo contratos entre ellos para que puedan ofrecer garantías de latencia sus clientes

Concluyendo:

Ahorros de la VPN = [(costos eliminados) – (costos adicionales) + (ventaja competitiva)]

Donde:

Costos eliminados se refieren a la eliminación de los servicios, lo cual genera ahorros para su organización, y costos adicionales se refiere a los costos en que se incurre cuando se añaden características tales como la redundancia y la tolerancia frente a las fallas.

Costos eliminados:

Líneas rentadas

Líneas por marcación

Equipo de acceso por marcación

Tiempo que invierte el personal para configurar el equipo del usuario final

Tiempo que invierte el personal para mantener el equipo del usuario final

Equipo PBX (propiedad del cliente)

Servidor de autenticación por marcación

Sistemas UPS para equipo de marcación

Números 800

Costosos enlaces ATM o por tramas

Conexiones ISDN

Soporte para IP, DNS y enrutamiento

Costos adicionales:

- Equipo de VPN
- Costos de mantenimiento
- Licencias
- Asuntos relativos a la solidez del cifrado
- Administración
- Capacidades de supervisión en banda y fuera de banda
- Personal de seguridad
- Servicio de ayuda para resolver problemas
- Larga distancia
- Número 800
- Contratos de Calidad de servicio.

2.4.9 ARQUITECTURAS DE LAS VPN's.

La seguridad de una VPN se basa en un dispositivo de hardware, en su sistema operativo, en la solidez del algoritmo de cifrado utilizado en la tecnología VPN y en la infraestructura de administración de claves que tiene instalada. Además de estos elementos debe validar a la autoridad emisora de certificados en la que ha decidido confiar como una fuente autorizada.

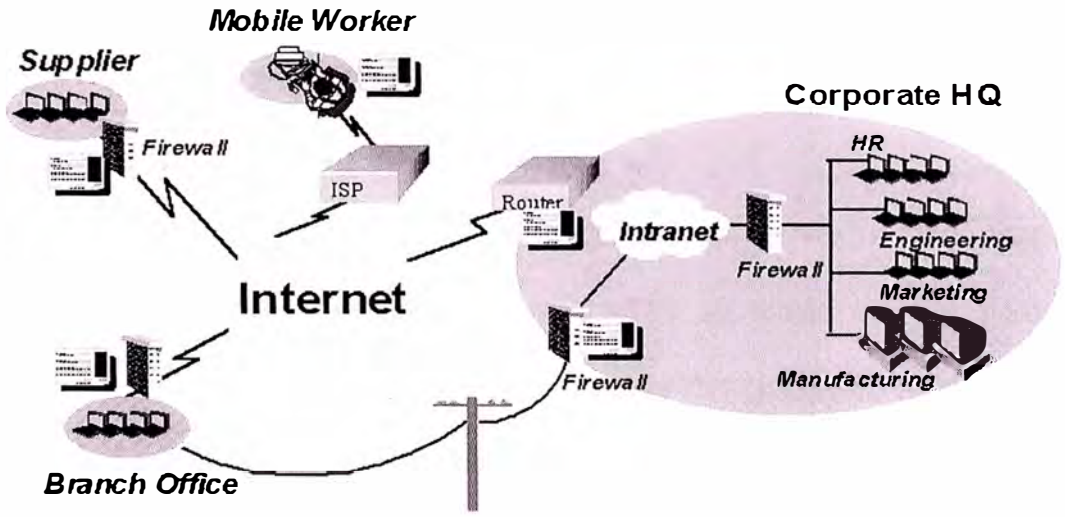


Fig.16 VPN para empresa global

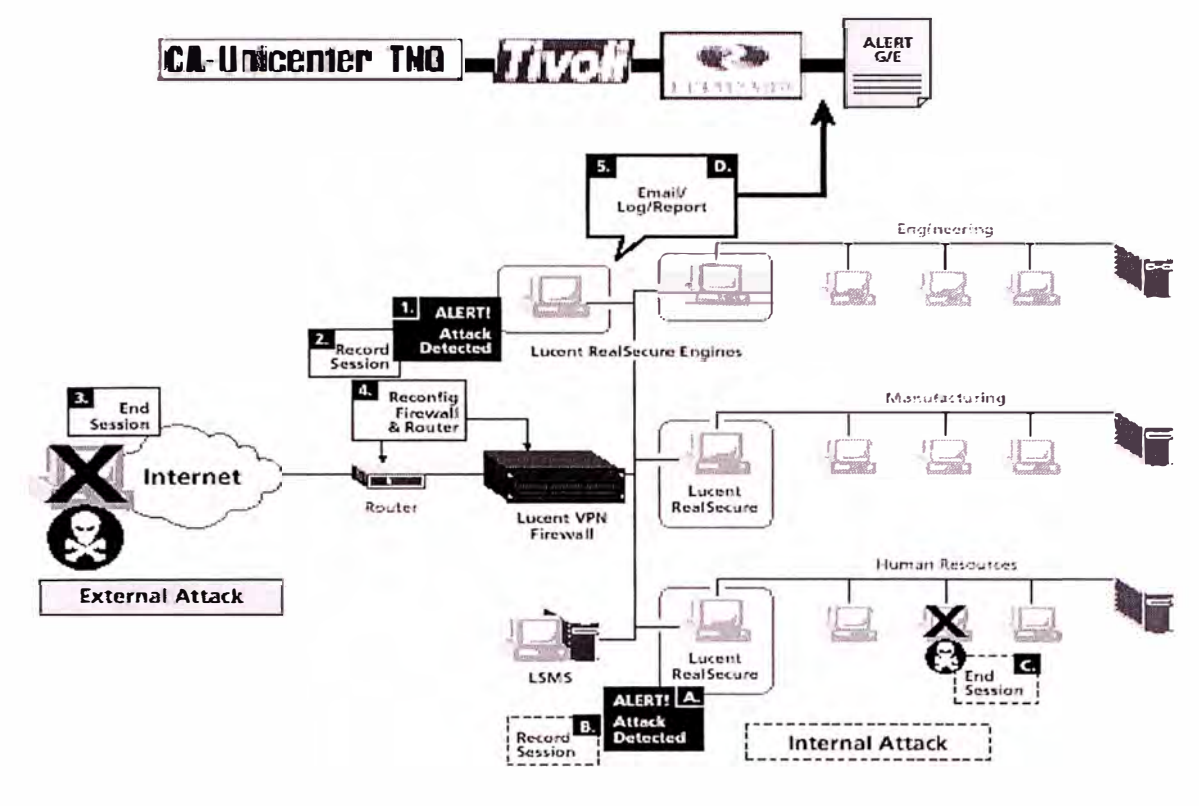


Fig. 17 VPN para comercio global.

Para usar la VPN en el comercio global, se debe recordar que la seguridad detrás de la solidez de una VPN se basa en las políticas de cifrado tanto del gobierno emisor como en las del gobierno receptor. Por lo tanto, se tendría que dar los pasos necesarios para mantener los datos seguros cumpliendo las leyes de cada país.

- **VPN en una extranet.**

La VPN de extranet es un servidor Web, así que todas las características de seguridad que se aplican a los servidores web se aplican también a una VPN de extranet.

Si no se puede utilizar el software de cifrado más sólido disponible debido a las normas gubernamentales, utilice el software de cifrado más sólido de uso interno y alguna otra de solidez de cifrado de uso internacional.

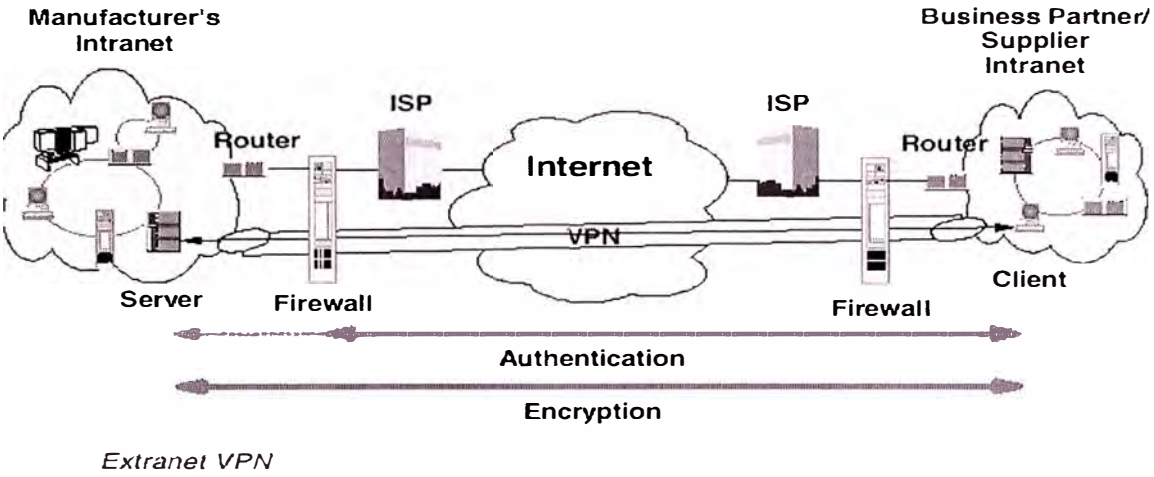


Fig. 18 Esquema de una VPN en una extranet

2.4.10 Tecnologías VPN

Algunas de ellas son:

Proporcionadas por los proveedores de servicios de red.

Basadas en firewalls.

Basadas en cajas negras.

Basadas en acceso remoto/routers.

Según las aplicaciones.

De servicios múltiples.

Basadas en software.

- **VPN proporcionada por un proveedor de servicio de red.**

En este caso el ISP puede instalar un switch PPTP frontal en sus oficinas, el cual creará en forma automática los túneles VPN para su tráfico. El destino final de las comunicaciones descifrará los paquetes y entregará los datos a su anfitrión. También se podría agregar un firewall a este tipo de ambiente, por lo general justo enfrente de un dispositivo de red o entre ellos. De manera similar a la vieja forma de instalar una zona desmilitarizada DMZ, el router interno se conectan a un puerto del firewall, el otro puerto del firewall se conecta al router externo y el puerto serial del router externo se conectar al ISP. También debe encargarse de asuntos tales como el direccionamiento IP, el enrutamiento y el correo.

Seguridad

Se debe contratar en muchos casos un equipo de seguridad externo para formular las políticas de seguridad y hacer que el ISP la implemente.

Control de cambios

Se debe tener claro quién hace los cambios en el control de la política de acceso y cuanto tiempo toma implementar estos cambios.

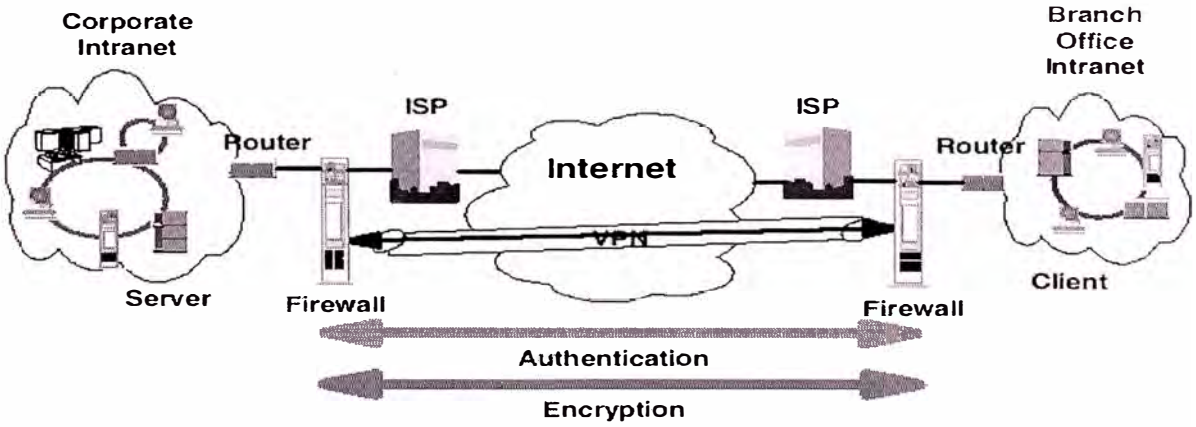
Autorización

Se debe conocer si la base de datos esta en el dispositivo VPN del proveedor o en algún servidor interno bajo nuestro control. Se debe tener

acceso inmediato a la base de datos para revocar privilegios de acceso que cuente con una manera de conectar a su proveedor en forma inmediata para llevar a cabo esta tarea.

Administración de claves

Las claves generadas y administradas deben de guardarse en un lugar seguro, no sólo para propósitos de seguridad sino también para recuperarlas. Estas incluyen claves públicas, claves de dispositivo y cualquier certificado del cual sea responsable. Las claves de cifrado para el túnel también deben de ser capaces de reproducirse en caso que el dispositivo VPN falle y se requiera un nuevo dispositivo.



Branch office VPN

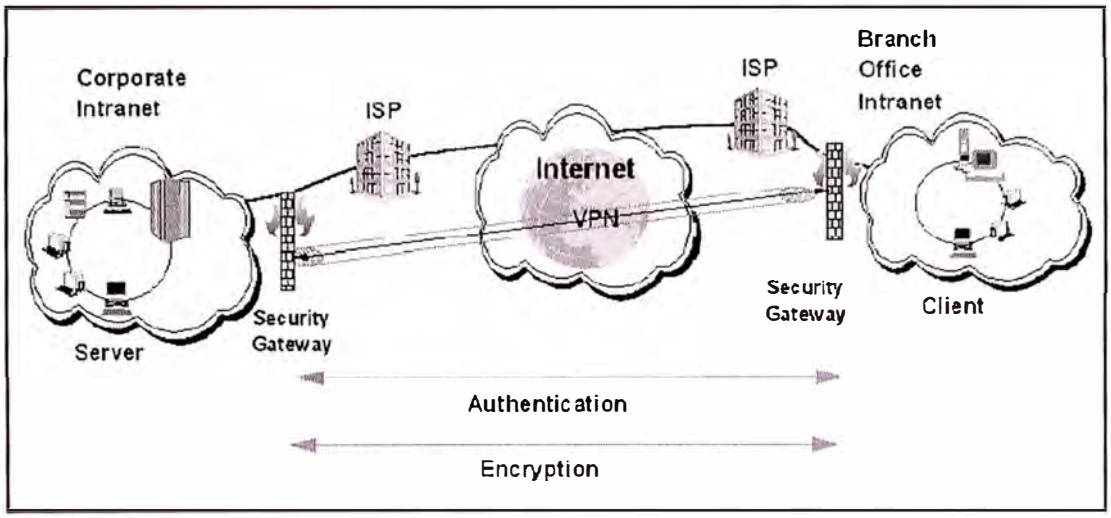
Fig. 19 VPN ofrecida por un proveedor de servicios IP

- **VPN basadas en firewall.**

El firewall requerida de un software de cifrado. Un aspecto importante de la seguridad es el sistema operativo subyacente. Como no existe un dispositivo 100 por ciento seguro, si se crea una VPN en ese dispositivo, hay que asegurarse que el sistema operativo subyacente sea seguro. La tecnología VPN debería ubicarse en el nivel más bajo de la pila OSI. Entre más arriba se encuentre en la pila, se presentarán mayores oportunidades de que ocurran intrusiones en la seguridad de las capas inferiores de las que depende.

Se debe decidir que tipo de protocolo se desea utilizar: L2F, PPTP, L2TP o IPSec.

Añadir tecnología a un firewall, se refiere únicamente a un firewall de inspección de estados (stateful packet inspection). De la misma manera que la tecnología VPN se ejecuta en los niveles más bajos de la pila OSI, el firewall debe hacerlo o puede caer en problemas de desempeño importantes. Un proxy firewall se ejecuta en el nivel 7, el nivel de aplicaciones del modelo OSI, y el firewall de filtrado de paquetes también tiene que examinar el paquete completo cada vez que pasa. Un firewall de inspección de estados se ejecuta en los niveles 2 y 3. Debido a este requerimiento de procesamiento, sólo se debe añadir tecnología de VPN a un firewall de inspección de estados.



Branch Office Connection Network

Fig. 20 Diagrama de una VPN basada en firewalls

- **VPN basadas en caja negra.**

Una caja negra se trata básicamente de un dispositivo cargado con software de cifrado para crear un túnel de VPN. Algunas cajas negras vienen con software que se ejecuta en un equipo cliente de escritorio para ayudar a administrar ese dispositivo, u otras pueden configurarse a través de un explorador web. Estos dispositivos de cifrado de hardware son más veloces que los tipos de software , ya que crean túneles más rápidos bajo demanda y ejecutan el proceso de cifrado con mayor rapidez. Aunque no todos ofrecen una característica de administración centralizada, y por lo general no soportan el acceso a sí mismos, es necesario enviar estos accesos a una base de datos para consultas. También se requiere otro servidor si se desea llevar a cabo la autenticación, aunque algunos dispositivos permiten añadir dispositivos si se desea.

Con la mayoría de instalaciones de caja negra es posible que se requiera un firewall independiente, aunque algunos proveedores están incorporando VPN de caja negra con capacidad de firewall.

El dispositivo VPN de caja negra se sitúa detrás del firewall. Aunque también puede situarse a un lado del mismo. El firewall proporciona seguridad a la empresa, pero no provee seguridad para los datos. Asimismo, el dispositivo VPN brindará seguridad a los datos pero no a la empresa.

- **VPN basadas en router**

Existen dos tipos de VPN basadas en router. En uno de ellos el software se añade al router para permitir que el proceso de cifrado ocurra. En el segundo método se inserta una tarjeta externa de otro proveedor en el mismo chasis que el router. Este método esta diseñado para endosar el proceso de cifrado del CPU del router a la tarjeta adicional.

Se debe tener en cuenta que el desempeño de las VPN basadas en router puede ser un problema, debido a la adición de un proceso de cifrado al proceso de enrutamiento, se agrega una carga más pesada al router, especialmente si éste está manejando una gran cantidad de rutas o implementando un algoritmo de enrutamiento intensivo.

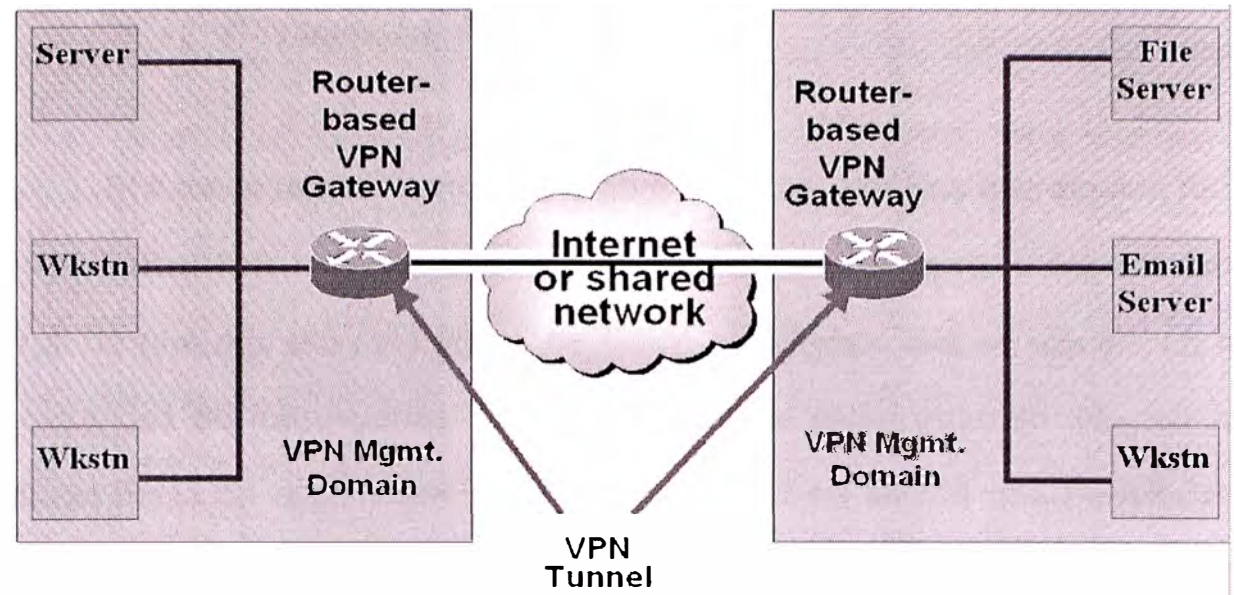


Fig. 21 VPN basada en routers

Hay que considerar si el router implementará autenticación de usuarios o para hacerlo necesitará un dispositivo independiente que sea compatible con él.

Existen dos inquietudes con las VPN basadas en router:

Interoperabilidad

Si desea conectarse a las VPN de los proveedores, su ruteador y el ruteador de los proveedores trabajan en conjunto y crean las VPN.

Encapsulamiento

Algunos fabricantes de routers sólo cifran y no encapsulan, como va a transportar protocolos que no son IP, como IPX o SNA.

- **VPN basadas en acceso remoto**

El acceso remoto como su nombre lo indica, significa que alguien fuera está tratando de crear un flujo de paquetes de cifrado hacia su organización. Así de una manera más literal, se aplica al software que se ejecuta en las máquinas de los usuarios remotos, las cuales están tratando de crear un túnel hacia su organización y a un dispositivo en su red que permita esa conexión. Este túnel podría venir de Internet, pero también podría venir de una línea conmutada, una línea ISDN o una red X.25.

Bajo este esquema el software que se ejecuta en una máquina remota en alguna parte y esa máquina intenta establecer una conexión a través de un túnel cifrado al servidor interno de la compañía o desde una línea de acceso conmutado como ISDN hacia un servidor de autenticación.

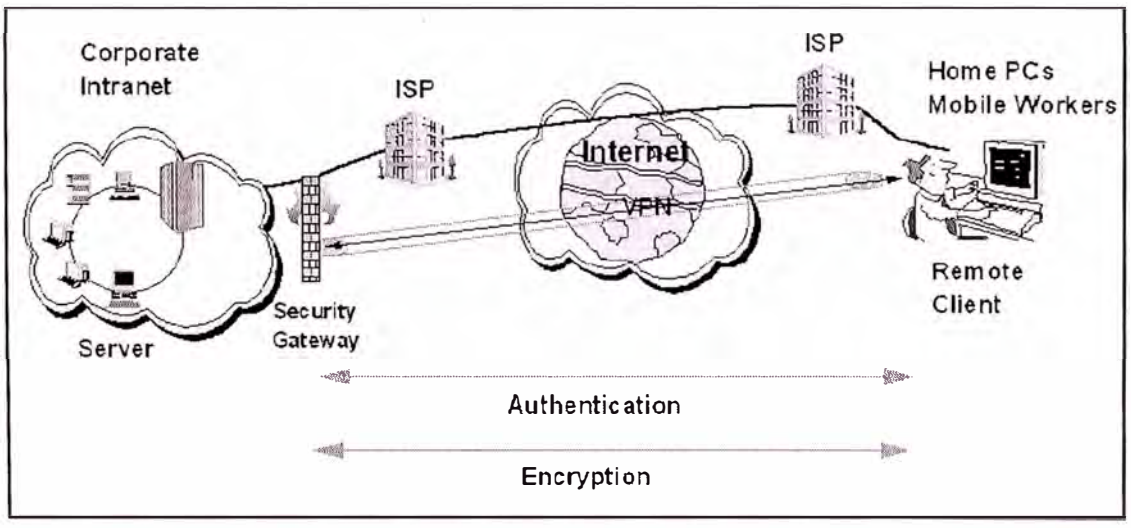


Fig. 23 VPN basada en accesos remotos

Un servidor de acceso instalado en su red, ya sea un router, un firewall, una caja negra o un servidor de autenticación independiente, concede el acceso.

- **VPN basados en aplicaciones (API)**

Por lo general, en las comunicaciones cliente / servidor el cliente solicita un servicio específico a un servidor en un puerto específico. El servidor responde al cliente con la información necesaria y se lleva a cabo la comunicación. Ahora, con las aplicaciones más nuevas, como la telefonía IP y las teleconferencias, cuando se hace una conexión para una aplicación específica en un puerto determinado, la respuesta que el servidor envía de regreso llega a varios puertos. Esto nos conduce a considerar una arquitectura de VPN llamada kit de herramientas proxy para VPN.

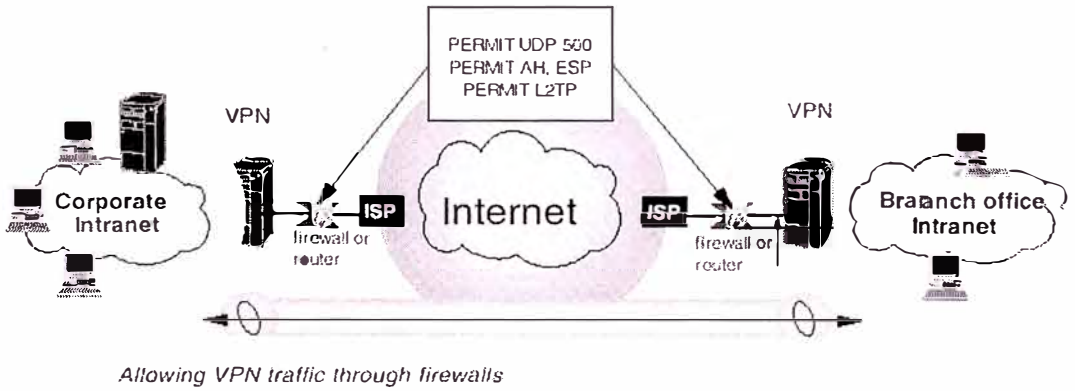


Fig. 24 Seguridad en VPNs basadas en firewall

Cuando se requiere desarrollar una aplicación nueva que necesitará soporte de cifrado sobre varios puertos individuales TCP/UDP que se requiere abrir, la mejor forma es tener algún tipo de API que pueda escribirse en el dispositivo VPN, la cual le permitiría escribir la funcionabilidad que necesita. A esto se le llama kit de herramientas de API para VPN.

- **VPN con aplicaciones de múltiples servicios**

Se esta comenzando a generar aplicaciones múltiples de propósitos que puedan residir en los dispositivos VPN basados en firewall.
Las aplicaciones de múltiples servicios para VPN son la filtración del contenido web y la revisión antivirus.

La filtración de contenido web se añade a su dispositivo de firewall / VPN para permitir ver que clase de sitios web están visitando sus usuarios internos.

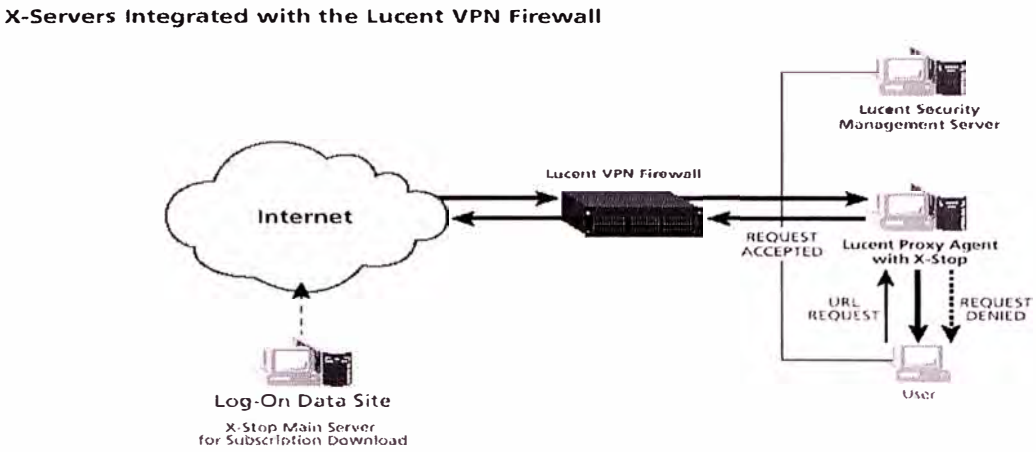


Fig. 25 Implementación de VPNs con Firewalls

El software antivirus, el cual puede cargarse en el propio dispositivo o endosarse a otro servidor.

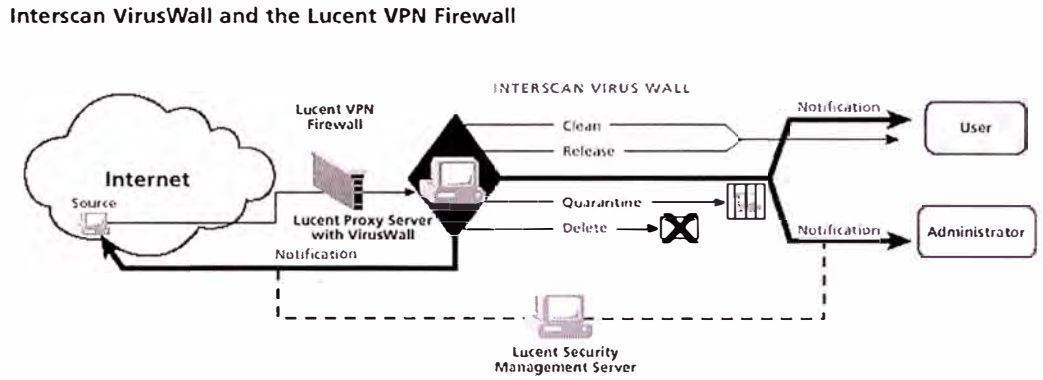


Fig. 26 Seguridad en las VPNs basadas en firewall

- **VPN basadas en software**

Una VPN basada en software básicamente es un programa para establecer túneles o cifrado a otro anfitrión. Por lo general se utiliza desde

un cliente a un servidor. Cuando se selecciona un software un VPN de software se necesitará tener procesos de administración de claves adecuados y posiblemente una autoridad emisora de certificados. Con firewall / VPN a firewall / VPN, las únicas claves que se necesitan son de VPN a VPN. Esto significa que el tráfico en la red interna se descifra, así que sólo necesita las claves para los dispositivos VPN. Pero en el caso de cliente a servidor, cada estación posiblemente podría tener su propio par de claves privadas / pública.

Certificación / compatibilidad.

ICSA certifica los productos de los proveedores de IPSec.

La compatibilidad también es importante desde el punto de vista de seguridad. Si se selecciona IPSec, la solución no estará completa, la otra mitad es la administración de claves o el Intercambio de claves de Internet (IKE). Con el propósito de contar con una solución de tecnología VPN completamente compatible, se necesita ambos. IPSec cifrará y firmará los paquetes, pero IKE negociará el intercambio de claves entre los dispositivos terminales.

2.4.11 SEGURIDAD EN LAS LSVPN.

Ya se ha mencionado con anterioridad, la seguridad es un requerimiento básico en cualquier VPN, en las LSVPN esta necesidad por supuesto se incrementa.

En cuanto a las áreas principales de la seguridad de una comunicación telemática, se obviarán en este documento otros factores necesarios para centrarnos en la seguridad en el canal de comunicación que es la parte distintiva característica de las VPN.

Al hablar de seguridad en el canal se suele pensar sólo en el atributo de la confidencialidad de la información pero existen otros valores como la garantía de integridad de la información transmitida, la autenticación de las partes integrantes (y el no repudio) que deben ser igualmente contemplados.

Los siguientes protocolos y sistemas son comúnmente usados para proveer varios niveles de seguridad en una red de computadoras. A continuación se hará una revisión breve de las tecnologías de seguridad disponibles hoy en día y comúnmente usadas, quienes dan confidencialidad, y algunos de los cuales son aplicables para VPNs:

IP Packet Filtering.

Network Address Translation (NAT).

IP Security Architecture (IPSec)

SOCKS

Secure Sockets Layer (SSL)

Application proxies.

Firewalls.

Kerberos, RADIUS, y otros sistemas de autenticación.

Antivirus, inspección y detección de intrusos en el sistema.

La siguiente figura ilustra donde se ubican las soluciones de seguridad dentro de las capas TCP/IP.

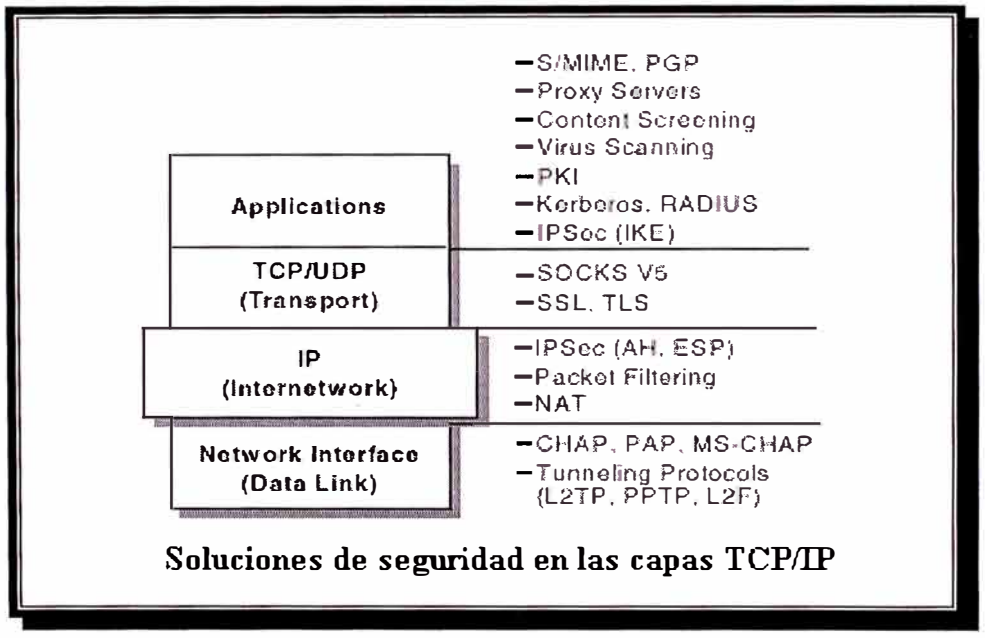
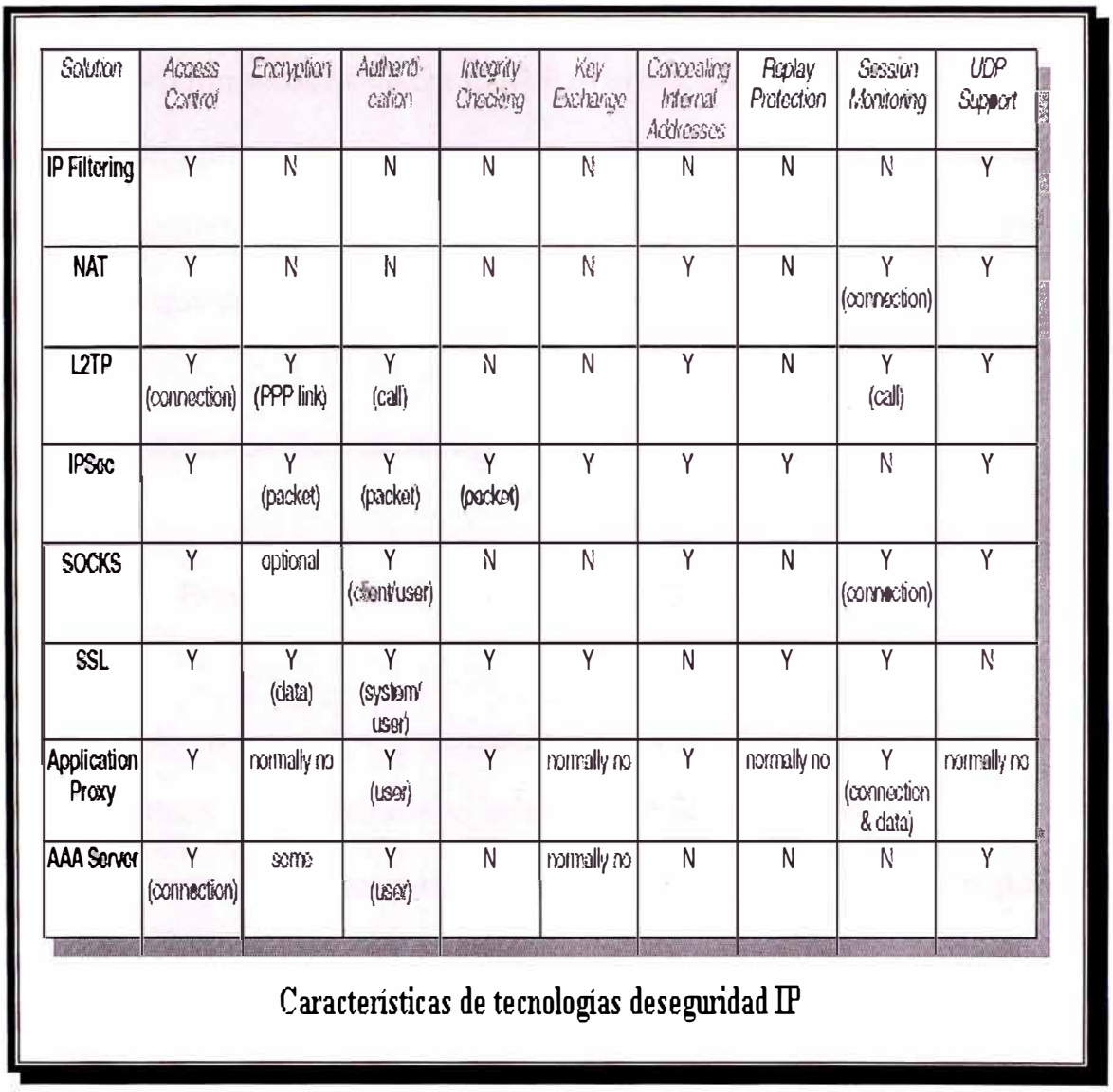


Fig. 27 Principales soluciones de seguridad en las capas TCP/IP

En la siguiente figura se muestra un resumen de las características de algunos de las soluciones de seguridad mencionados anteriormente y se compara entre ellos en un nivel específico de los requerimientos de un VPN.

Esto puede ayudar a alguien que necesita aconsejar una estrategia de seguridad para determinar que combinación de soluciones alcanzarán un nivel de protección.



Solution	Access Control	Encryption	Authentication	Integrity Checking	Key Exchange	Concealing Internal Addresses	Replay Protection	Session Monitoring	UDP Support
IP Filtering	Y	N	N	N	N	N	N	N	Y
NAT	Y	N	N	N	N	Y	N	Y (connection)	Y
L2TP	Y (connection)	Y (PPP link)	Y (call)	N	N	Y	N	Y (call)	Y
IPSec	Y	Y (packet)	Y (packet)	Y (packet)	Y	Y	Y	N	Y
SOCKS	Y	optional	Y (client/user)	N	N	Y	N	Y (connection)	Y
SSL	Y	Y (data)	Y (system/ user)	Y	Y	N	Y	Y	N
Application Proxy	Y	normally no	Y (user)	Y	normally no	Y	normally no	Y (connection & data)	normally no
AAA Server	Y (connection)	some	Y (user)	N	normally no	N	N	N	Y

Características de tecnologías deseguridad IP

Fig.28 Características de tecnologías de seguridad IP

Hasta hace muy poco tiempo los distintos fabricantes de Hardware y Software han usado distintas formas de securizar las comunicaciones de las VPN; propietarias en todo o en parte, pues aún usando estrategias de

dominio público (como por ejemplo el famoso algoritmo DES para encriptar) realizaban implementaciones propietarias que provocaban que los sistemas de seguridad de dos fabricantes distintos no pudieran comunicarse entre sí. Esta situación se acentúa en estructuras extranet donde se usa un medio común de comunicación para distintas entidades. En este entorno es difícil que una organización pueda imponer a otra su tecnología, y más cuando se trata de grandes empresas con homologaciones internacionales de los productos que pueden emplear.

2.4.12 Protocolos de tunneling

- **Protocolo Punto a Punto (PPP).**

Debido a que los protocolos de Nivel 2 dependen fuerte de las características originalmente especificadas para PPP, es importante examinar este protocolo más cercanamente. PPP fue diseñado para enviar datos a través de conexiones punto a punto dedicadas o conmutadas. PPP encapsula paquetes IP, IPX y NeBEUI dentro de tramas PPP y trasmite los paquetes PPP encapsulados a través de un enlace punto a punto. PPP es usado entre un cliente conmutado y un NAS.

Existen 3 fases distintas de negociación en una sesión conmutada PPP. Cada una de estas fases debe completarse satisfactoriamente antes que la conexión PPP esté listo para transferir datos del usuario.

Fase 1: Establecimiento del Enlace PPP

PPP usa Protocolo de Control de Enlace (LCP) para establecer, mantener y finalizar la conexión física. Durante la fase inicial del LCP, opciones de comunicación básica son seleccionadas. Durante la fase del establecimiento del enlace (Fase 1), protocolos de autenticación son seleccionados, pero estos no son implementados hasta la conexión de la fase de autenticación (Fase 2). Similarmente, durante el LCP, una decisión es hecha tal que los dos partes involucradas negociarán el uso de compresión y /o encriptación. La elección de compresión y algoritmo de encriptación elegida y otros detalles ocurren en la Fase 3.

Fase 2: Autenticación de Usuario

En la segunda fase, el cliente PC presenta las credenciales del usuario al servidor de acceso remoto. Un esquema de autenticación seguro proporciona protección contra ataques repetitivos que ocurren cuando una tercera parte monitorea una conexión satisfactoria y usa paquetes capturados para reproducir respuestas del cliente remoto tal que puedan conseguir una conexión autenticada.

La mayoría de implementaciones PPP proporcionan métodos de autenticación limitados, típicamente el Protocolo de Autenticación de Contraseña (PAP) y Protocolo de Autenticación por Negociación de Reto (CHAP).

Fase 3: Estableciendo el Protocolo de Nivel de Red

Una vez que la fase anterior es completada, el PPP invoca varios protocolos de control de red (NCP), que fueron seleccionados durante el establecimiento del enlace (Fase 1). Por ejemplo, durante esta fase el protocolo de control IP (IPCP) puede asignar una dirección dinámica para el usuario de acceso conmutado. Aquí también son negociados la compresión y la encriptación de datos.

Varios protocolos de red muy interesantes han sido desarrollados para uso en las VPNs. Estos protocolos continúan en competencia con cada otro para su aceptación en la industria.

- **Layer 2 Forwarding (L2F)**

L2F fue desarrollado por Cisco Systems al mismo tiempo que PPTP estuvo siendo desarrollado, es otro protocolo que habilita hosts remotos para acceder a la Intranet de una organización a través de la infraestructura pública, con seguridad.

Cisco propuso esta tecnología a la IETF para ser aprobada como estándar, y está definida en el RFC 2341.

Como con PPTP, L2F habilita acceso seguro a una red privada a través de una infraestructura pública mediante la construcción de un túnel a través de la red pública entre el cliente y el host. La diferencia entre PPTP y L2F es que L2F tunneling no es dependiente en IP; está habilitado para trabajar con otros protocolos de red nativos, como Frame Relay, ATM o FDI. Este servicio requiere sólo capacidad dial-up local reduciendo los costos de usuario y proveyendo el mismo nivel de seguridad encontrado en una red privada.

Un túnel L2F soporta más de una conexión, una limitación de PPTP. L2F está habilitado para hacer esto como conexiones se definan dentro del túnel. Esto es muy útil en situaciones donde más de un usuario es localizado en un lugar remoto, sólo una conexión dial-up es requerida. Alternativamente, si tunneling es usado sólo entre el POP y el gateway en la red interna, pocas conexiones son requeridas desde el ISP, reduciendo costos. Esto se puede apreciar en la siguiente figura.

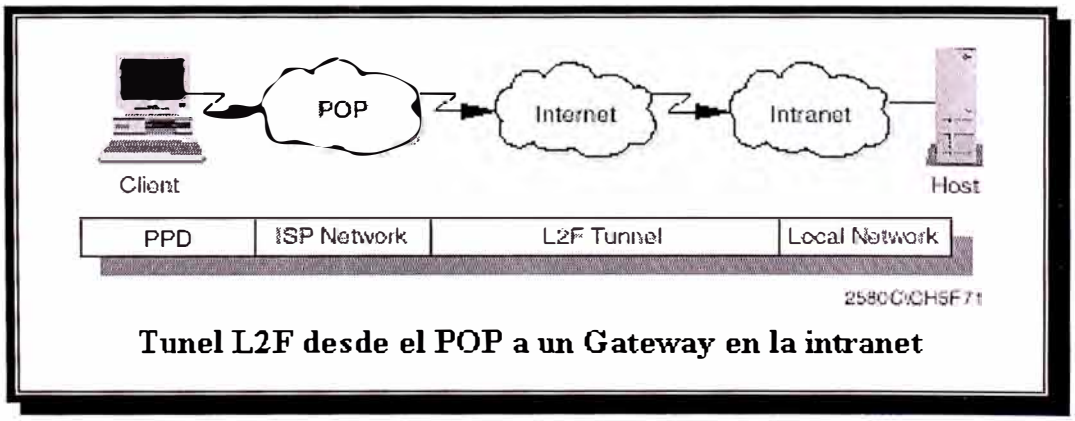


Fig. 29 Tunel L2F en conexión de una aplicación a Internet

L2F usa PPP para autenticación cliente, como hace PPTP, sin embargo, L2F también soporta TACACS+ y RADIUS para autenticación. Autenticación L2F comprende dos niveles, primero cuando el usuario remoto se conecta al POP del ISP, y luego cuando la conexión es realizada al gateway de la organización.

Con L2F, una VPN segura end-to-end puede ser creada y usada, es una solución confiable y escalable. Sin embargo, tiene algunas deficiencias que son dirigidas con L2TP.

- **Point-to-Point Tunneling Protocol (PPTP)**

El protocolo punto a punto (PPTP) se diseñó para permitir que los usuarios remotos marcaran a su ISP local y establecieran un túnel al servidor de la compañía.

Es un protocolo de autenticación y encriptación propietario de Microsoft. PPTP fue reemplazado por L2TP, pero Microsoft retiene PPTP como su camino de soporte VPNs en productos Microsoft Windows. PPTP usa RSA en vez de DES o 3DES para encriptación.

PPTP utiliza la infraestructura de protocolos existente para permitir una conexión por marcación, llamada PPP. Luego toma estos paquetes PPP y los encapsula dentro de un encabezado con Encapsulamiento para

enrutamiento genérico (GRE). Los payloads de la trama PPP encapsulada pueden ser encriptadas y /o comprimidas.

En el siguiente gráfico se muestra el datagrama creado por PPTP, con cada nivel representando una encapsulación dentro de la capa previa.

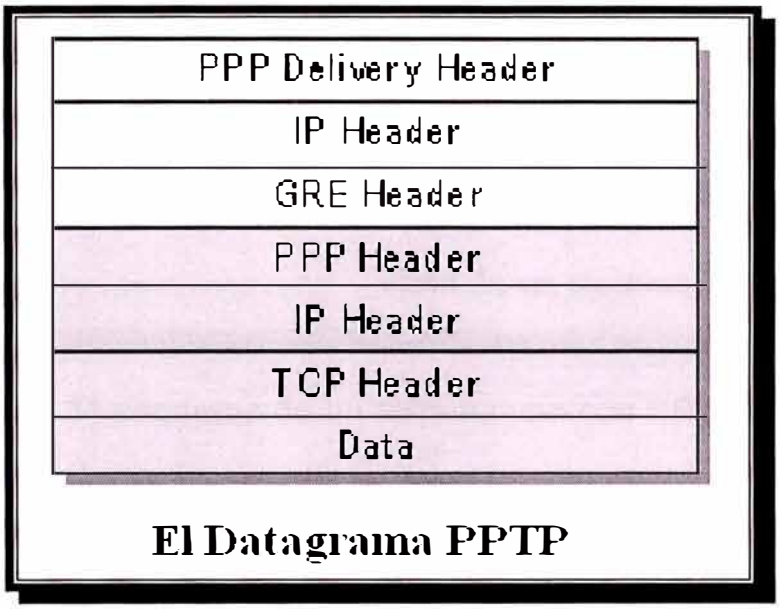


Fig. 30 diagrama del datagrama PPTP

El área sombreada indica la información encriptada. El paquete IP encriptado puede ser también un IPX, NetBEUI, o alguna otra forma de paquete. Teniendo en cuenta que PPTP soporta sólo IP, IPX, NetBIOS y NetBEUI, puesto que son los protocolos de red más comúnmente implementados.

PPTP esta actualmente siendo reemplazado por implementaciones de L2TP.

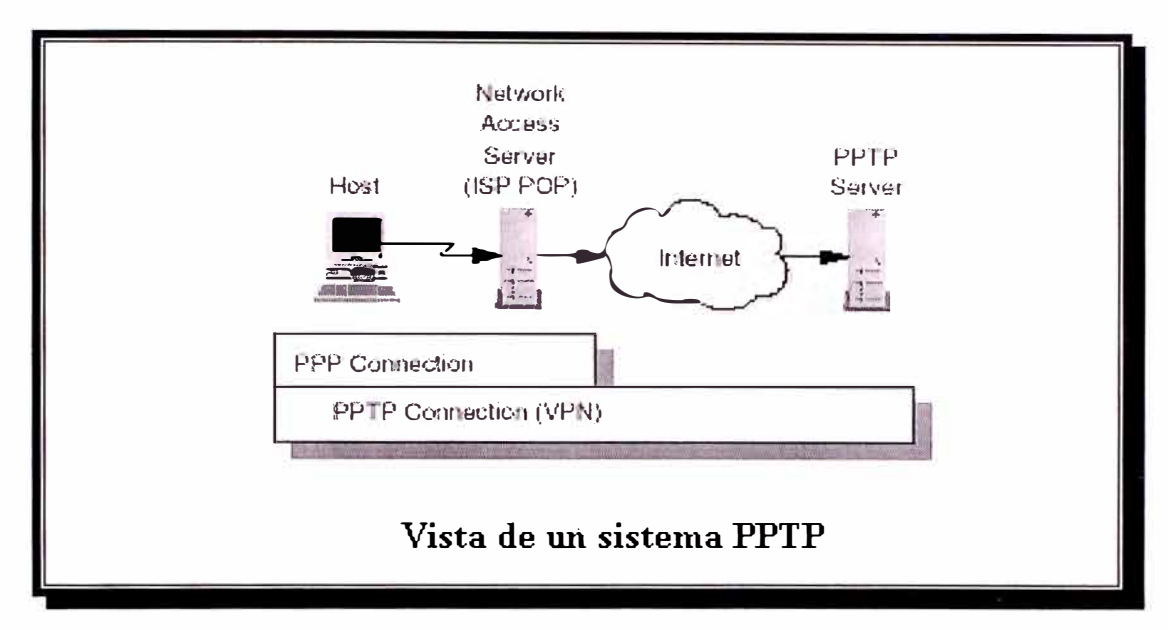


Fig. 31 esquema de un sistema vpn con PPTP

PPTP está definido en el RFC 2637.

- **Layer 2 Tunneling Protocol (L2TP).**

L2TP fue desarrollado para unir los dos primeros protocolos, L2F y PPTP. L2TP es un protocolo de red que encapsula tramas PPP para ser enviado sobre redes IP, X25, Frame Relay o ATM. Cuando se configura para usar IP como transporte de datagramas, L2TP puede ser usado como un protocolo Tunneling sobre Internet. L2TP puede también ser usado directamente sobre diversos medios WAN, tales como Frame Relay, sin un nivel de transporte IP. Por si mismo L2TP no provee una función de

encriptación y L2TP depende de IPSec (o algún otro mecanismo) para encriptación.

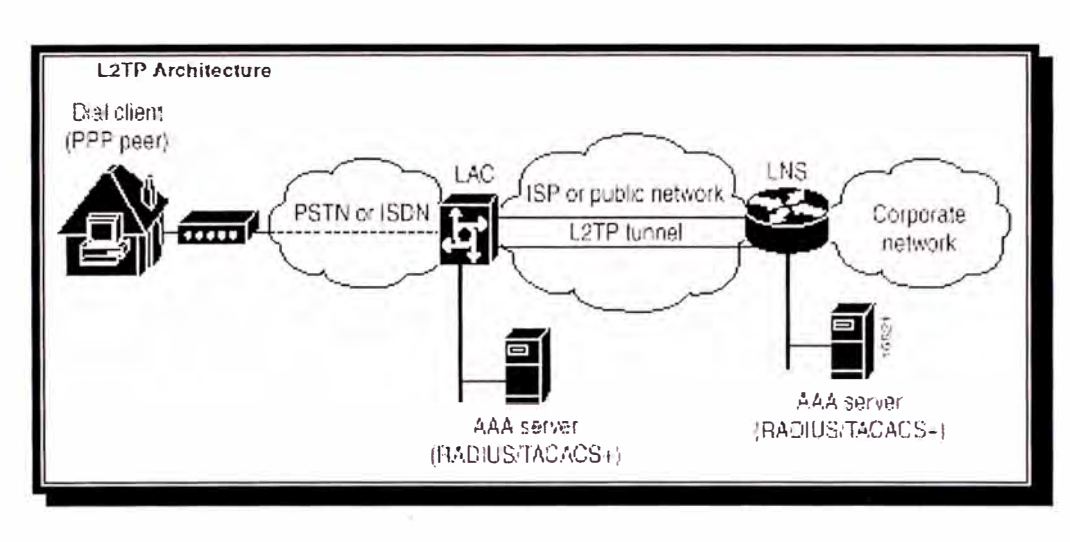


Fig.32 Esquema deuna conexión con arquitectura L2TP

Un túnel L2TP es creado por encapsulación de un frame L2TP dentro de un paquete UDP, quien es nuevamente encapsulado dentro de un paquete IP cuyas direcciones origen y destino definen los extremos del túnel tal como puede ser visto en la figura 33.

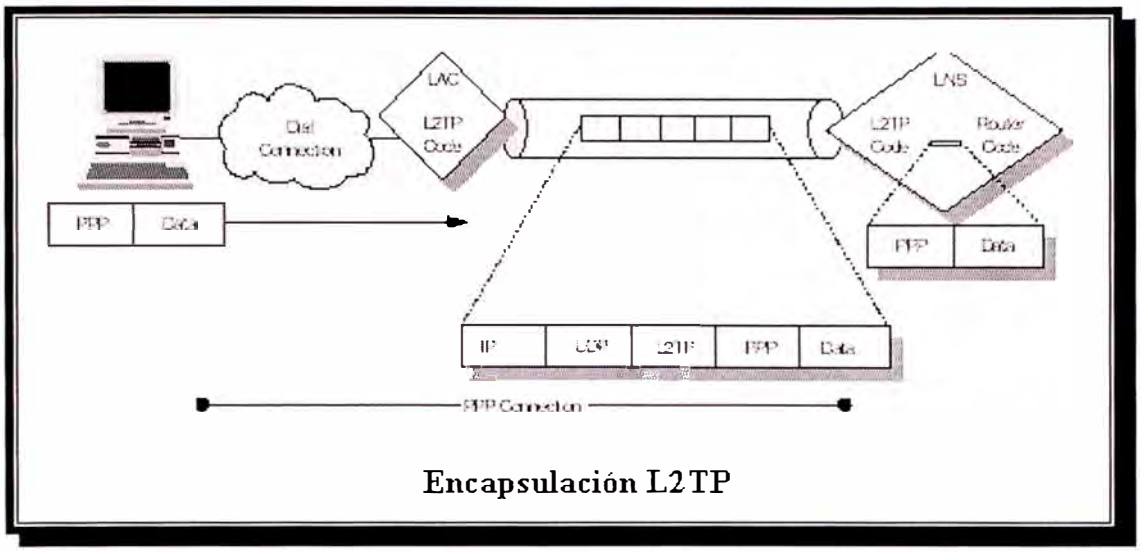


Fig. 33 Encapsulamiento L2TP

Los payloads de las tramas PPP encapsuladas pueden ser encriptadas y /o comprimidas como se observó en la fig 33.

L2TP utiliza una terminología especial para definir los puntos donde inicia y termina la comunicación. Un concentrador de acceso (LAC) L2TP localizado en el POP del ISP se comunica con un servidor de red (LNS) L2TP localizado en la LAN corporativa; tal como se muestra en la figura 34.

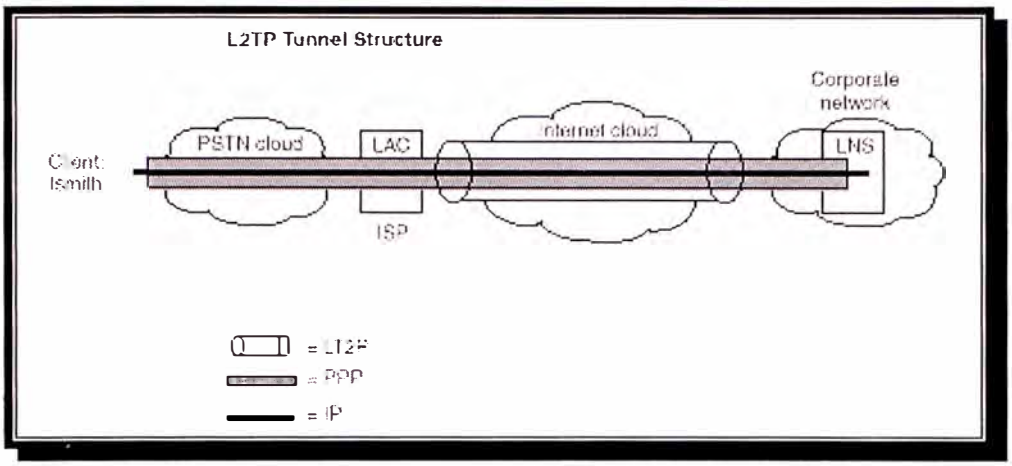


Fig. 34 estructura del tunel L2TP

2.4.13 Internet Protocol Security (IP Sec)

Se hacía pues necesaria la definición de un lenguaje universal en el que los distintos fabricantes pudieran realizar sus desarrollos comerciales. El organismo encargado de realizarlo fue el IETF (Internet Engineering Task Force), y el fruto resultante de sus trabajos es IPSec (Internet Protocol Security), que es hoy en día el estándar en internet para tunneling, encriptación y autenticación.

El IPSec provee seguridad para transmisión de información sobre redes no protegidas como internet, IPSec trabaja en la capa de red (capa 3) protegiendo y autenticando paquetes IP entre dispositivos IPSec ("peers") participantes. Un Túnel de IPSec consiste de un cliente túnel y un servidor túnel, los cuales son configurados para usar IPSec Tunneling y un mecanismo de encriptación negociado.

En el siguiente gráfico se tiene que el datagrama original viene a ser el payload data para el nuevo paquete ESP, y por lo tanto su protección es total si ambos encriptación y autenticación son seleccionados. Como quiera, el nuevo header IP está aún no protegido.

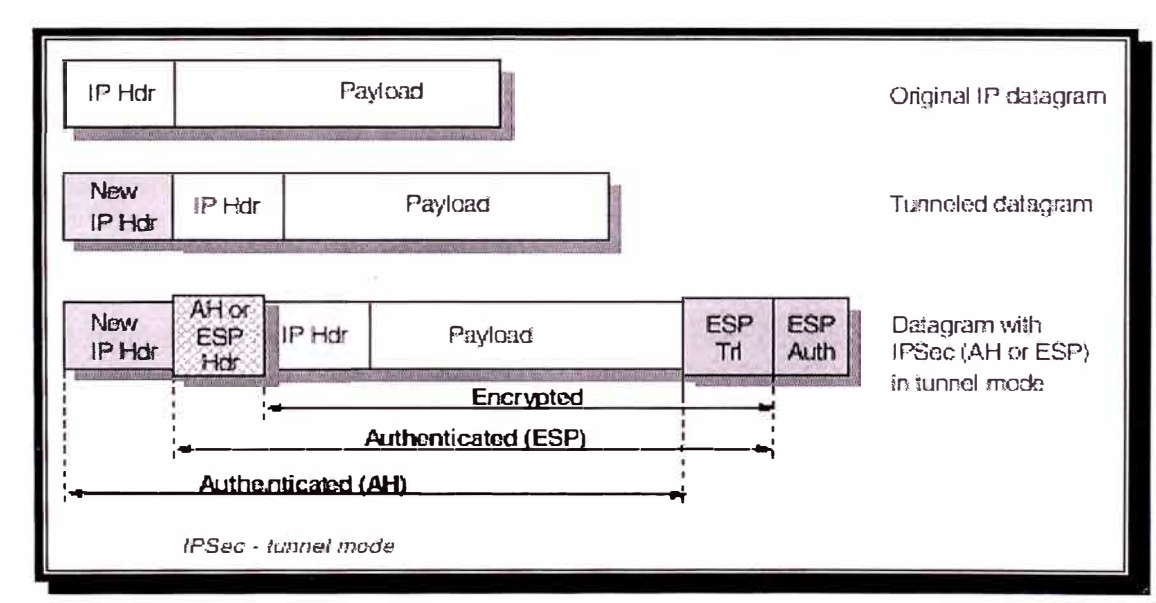


Fig. 35 Encapsulamiento IPSec

En IPSec se tienen dos protocolos de seguridad asociados, como:

IP Authentication Header (AH)

Encapsulating Security Payload (ESP).

Las ventajas del modo túnel son total protección del datagrama IP encapsulado y la posibilidad del uso de direcciones privadas. Sin embargo, allí hay un procesamiento extra de overhead asociado con este modo.

IPSec provee los siguientes servicios de seguridad de red. Estos servicios son opcionales. En general, políticas de seguridad local dedicarán el uso de uno o más de estos servicios:

Confidencialidad de data. El IPSec emisor puede encriptar paquetes antes de transmitir a través de la red.

Integridad de data. El IPSec receptor puede autenticar paquetes enviados por el IPSec emisor para asegurar que la data no ha sido alterada durante la transmisión.

Autenticación del origen de la data. El IPSec receptor puede autenticar el origen de los paquetes IPSec enviados.

No repudio. El IPSec receptor puede detectar y rechazar paquetes devueltos.

El túnel IPSec usa el método de seguridad negociado para encapsular y encriptar paquetes IP enteros para asegurar la transferencia a través de la red IP pública o privada.

El payload encriptado es luego encapsulado con una cabecera IP de texto plano y enviado sobre la red para entregarlo al servidor del túnel. Sobre la recepción de este datagrama, el servidor del túnel procesa y descarta la cabecera IP de texto plano, y luego des encripta su contenido para recuperar el payload del paquete IP original.

Luego, el payload del paquete IP es normalmente procesado y enrutado a su destino sobre la red de tránsito.

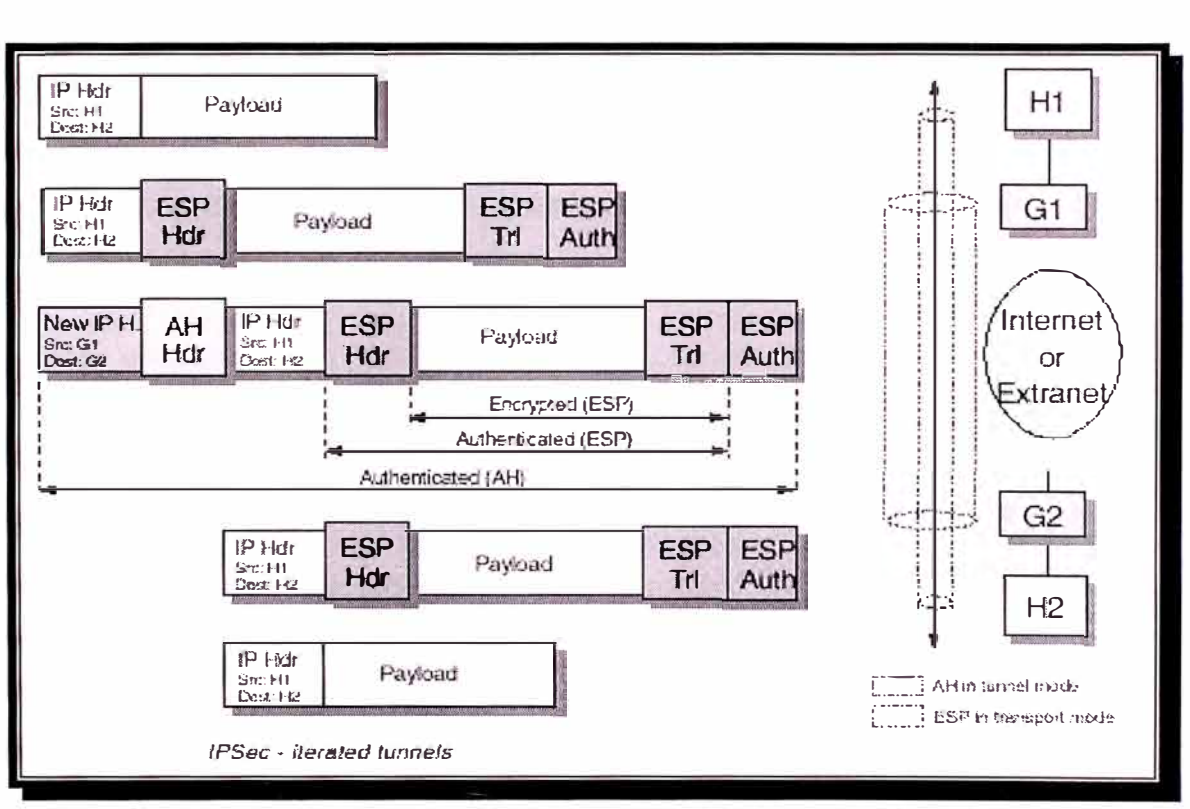


Fig. 35 Iteración de tuneles en IPSec

El modo Túnel IPSec tiene las siguientes características y limitaciones:

- Sólo soporta tráfico IP.

Funciona en la parte inferior del stack IP; por lo tanto las aplicaciones y los protocolos de nivel superior operan sin cambio alguno.

Es controlado por una política de seguridad, conformado por un conjunto de reglas de filtrado. Esta política de seguridad establece el mecanismo de encriptación y tunneling disponible, también el orden de la preferencia. Una vez que el tráfico se presenta, las dos computadoras ejecutan una autenticación mutua, y luego negocia los métodos de encriptación a ser usados. De allí en adelante, todo el tráfico es encriptado usando el mecanismo de encriptación negociado y luego encapsulado con una cabecera del túnel.

Todos los fabricantes de productos de seguridad tienen ya implementaciones usando IPSec (o planes inmediatos para ello), y al existir organismos establecidos para certificar la conformidad con el estándar definido (ICSA) se asegura la interoperabilidad actual y futura.

Puede pues afirmarse, sin temor a equivocarse, que IPSec es el lenguaje común indiscutible de la seguridad, y en un futuro su preponderancia será aún mayor.

- Internet Key Exchange (IKE)

Internet Key Exchange (IKE), definido en el RFC 2409, es el protocolo usado para establecer asociaciones de seguridad que son necesarias para

varios servicios, por ejm. IPSec usa IKE para establecer asociaciones de seguridad necesitadas para generar y actualizar sus claves.

IKE fue originalmente llamado ISAKMP/Oakley. Internet Security Asociation and Key Management Protocol (ISAKMP), provee el framework para establecer asociaciones de seguridad y claves criptográficas.

Los protocolos IPSec AH y ESP requieren que secretos compartidos sean conocidos por todas las partes participantes que requieran entre clave manual o distribución de claves fuera de banda. Un mecanismo de intercambio de claves robusto para IPSec debe reunir los siguientes requerimientos.

Independencia de algoritmos criptográficos específicos.
Independencia de un protocolo de intercambio de claves específico.
Autenticación de entidades administradoras de claves.
Establecer SA (Security Association) sobre transporte no asegurado.
Eficiente uso de recursos.
Adecuar la creación en demanda de host y las basadas en sesión.

El protocolo IKE ha sido diseñado para reunir esos requerimientos. IKE ofrece las siguientes características:

Generación de claves y procedimientos de autenticación de identidad.

Actualización automática de claves.

Solución del problema de la primera clave.

Cada protocolo de seguridad (que es, AH, ESP) tiene su propio espacio de índice de parámetros de seguridad (SPI).

Implementado como aplicación sobre UDP, port 500.

Soporte orientado a certificados orientados a hosts y usuarios.

- **Nociones de la suite IPSec**

IPSec define no un estándar cerrado, sino un paraguas en el que tienen cabida distintas tecnologías actuales y sobre el que se podrán añadir futuros avances tecnológicos, en todos los casos encaminados a proporcionar protección a las comunicaciones sobre el protocolo IP.

IPSec puede trabajar en dos formas básicas: La primera mediante el llamado modo transporte (modo nativo) que establece las comunicaciones host a host, y se usa en dispositivos que incorporan IPSec en la pila TCP/IP. Hasta la fecha para implementar este modo se ha venido usando distintos programas "clientes" para añadir esta capa IPSec sobre la pila original. En un futuro esta capa vendrá incluida en los sistemas operativos (se anuncia en Windows 2000). En este caso el paquete resultante securizado conserva la cabecera IP original.

El segundo modo en el que se puede trabajar con IPSec es el llamado modo túnel. En este caso la encargada de hacer el trabajo de seguridad es una pasarela que captura el tráfico procedente de los ordenadores que no tienen capacidad para mandar a la red tráfico IPSec. La pasarela securiza y encapsula entero el paquete IP que recibe (incluyendo su cabecera original) añadiendo una nueva cabecera IP para que la información pueda viajar por la red pública. En el destino habrá de realizarse la operación inversa. Generalmente estas pasarelas se sitúan en el perímetro en el que se unen las redes públicas con las redes privadas, pero es un error considerar que ese es el único lugar para aplicar IPSec a una comunicación, puesto que al establecerse la seguridad en el nivel IP de la comunicación existe independencia del medio físico usado, ya sea intra-LAN (Ethernet, Token.ring...) o WAN (Frame Relay, RDSI, RTB...); y también de las aplicaciones usadas (correo, navegación web, acceso a bases de datos, trasferencia de ficheros, emulaciones...).

Como se ha expuesto, IPSec no define un estándar cerrado sino una serie de posibilidades. La primera opción de elección la proporcionan sus dos protocolos principales: Authentication Header (AH) que básicamente proporciona autenticación del remitente, integridad de los datos y opcionalmente protección contra el reenvío; y Encapsulating Security Payload (ESP) que proporciona también cifrado de los datos.

Para las labores mencionadas se usan métodos criptográficos entre los cuales puede optarse entre diversas opciones. Generalmente se usan mecanismos de criptografía simétrica o de clave única para el cifrado del campo de datos, destacando DES (Data Encryption Standard) y triple DES por su popularidad. Para la autenticación se usan mecanismos de firma digital mediante funciones resumen (por ejemplo MD5, SHA-1).

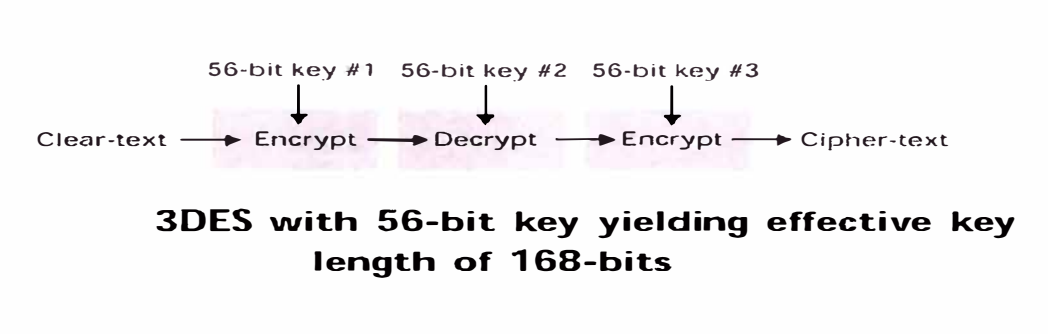


Fig. 36 Modelo de sistema de encriptación 3DES

Para cada sesión en la que se comunican dos redes, se usan una clave de sesión y una de autenticación en cada sentido (cuatro en total). Otro concepto fundamental en IPSec es el de Security Association que es el acuerdo que negocian dos dispositivos que se van a comunicar mediante IPSec en el que se fijan los distintos parámetros que se han ido describiendo (protocolos, algoritmos, claves, duración de las mismas etc.). Las SA son unidireccionales, existiendo dos en cada comunicación entre dos dispositivos. Para establecer y mantener las SA se usan mecanismos de distribución y gestión de claves como IKE (Internet Key Exchange) que hace

uso de distintas técnicas entre las que destacan mecanismos de criptografía asimétrica o de clave pública como Diffie-Hellman y RSA.

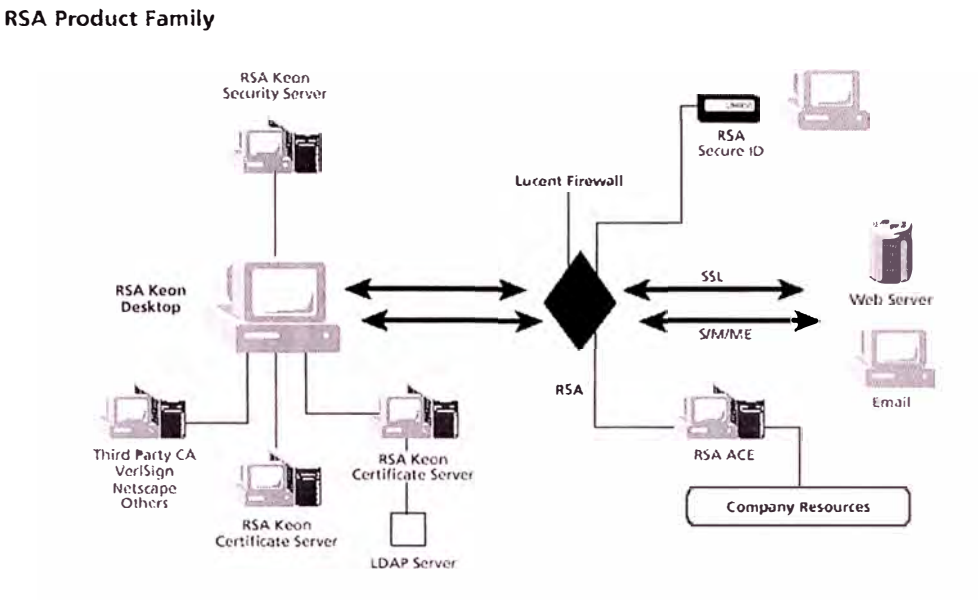
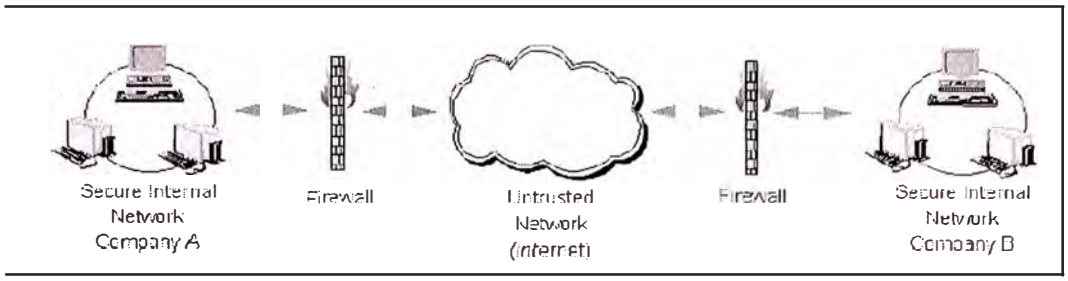


Fig. 37 Esquema VPN con diferentes metodos criptográficos.

Si no tenemos seguridad en algún punto de la VPN, entonces no tendremos seguridad en ningún lado. El Firewall es la base de la seguridad de una VPN.

Los Firewall tienen funciones significativas en la política de seguridad de la organización. Entonces es importante entender estas funciones y aplicarlas a la red apropiadamente.



Firewall Illustration

Fig. 38 Firewall como base de seguridad de la VPN

Un firewall es un sistema o grupo de sistemas que aplica una política de seguridad entre una red interna segura y una red sin seguridad tal como el internet. Los firewalls tienden a ser vistos como una protección de seguridad entre el internet y una red privada. Un firewall puede ser una PC, un router, una estación Unix, o una combinación de estas, el firewall determina que información o servicios pueden ser accesados desde el exterior y quienes son permitidos el acceso. El firewall se instala entre el punto de la red segura y la red externa.

Dependiendo de los requerimientos, un firewall puede consistir de uno o mas de los siguientes componentes:

Packet filtering router

Application level gateway (Proxy)

Circuit Level Gateway (SOCKS)

VPN Gateway

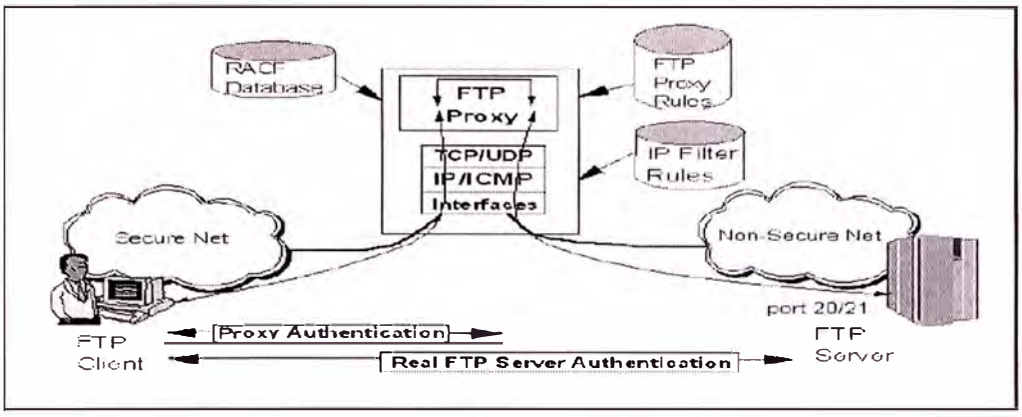


Fig 39 Solución de seguridad con Autenticación por Aplicación

2.4.14 PROTOCOLOS DE AUTENTICACIÓN.

- **Password Authentication Protocol (PAP)**

Protocolo de la suit PPP para autenticación definido en el RFC 1334.

Password Authentication Protocol (PAP) provee un método simple para autenticar un punto de la conexión PPP, Para establecer la identidad se usa un intercambio de contraseña, user y passwords , esto solo se realiza cuando se establece la conexión.

El paquete PAP es encapsulado en el campo de información de la trama PPP donde el campo de protocolo indica el tipo hex c023. La estructura del paquete PAP se muestra en la siguiente ilustración.

Code	Identifier	Length	Data . . .
1 byte	1 byte	2 bytes	

Fig. 40 Estructura del paquete PAP

Code

Indica el tipo de paquete de PAP , es un byte de tamaño y los códigos PAP son asignados de la siguiente manera:

Authenticate-Request

Authenticate-Ack

Authenticate-Nak

Identifier

Identifica la relación entre requests y replies.

Length

Indica la longitud del paquete PAP incluyendo campos de Code, Identifier, Length y Data.

Data

Toma el valor de cero o diferente de cero dependiendo del valor del campo Code. El formato del campo de Data para un paquete de Authenticate-Request es mostrado en la siguiente ilustración.

Peer-ID length	Peer-ID	Password length	Password
1 byte	variable	1 byte	variable

Fig. 41 Estructura del paquete de datos para Authenticate-Request

Peer-ID length

Longuitud del campo Peer_ID

Peer-ID

Indicates the name of the peer to be authenticated.

Indica el nombre del puerto a ser autenticado.

Password length

Longuitud del campo de password.

Password

Indica el password a ser usado para autenticación.

El formato del campo de dato para paquetes de Authenticate-Ack y Authenticate-Nak consta de dos campos de mansages una fijo de 1 byte y otro variable de hasta 8 bytes.

Estructura de los paquetes de datos para Authenticate-Ack y Authenticate-Nak

Message Lenght

Longuitud del campo de Mensaje.

Messages

Los contenidos de campo de Message se implementan dependientemente.

- **Protocolo de Autenticación por Intercambio de Reto (CHAP)**

Protocolo de la suit de protocolos PPP para Autenticación y definido en el RFC1334

Challenge Handshake Authentication Protocol (CHAP) es usado para verificar periódicamente la identidad de un punto usando un intercambio de retos de 3 formas, esto se realiza una vez iniciado el establecimiento de la conexión puede repetirse a requerimiento después de establecida la conexión.

Un paquete de CHAP es encapsulado en el campo de información dentro una trame del enlace PPP, donde el campo de protocolo indica el tipo. En el siguiente diagrama se muestra la estructura de un paquete CHAP

Code	Identifier	Length	Data . . .
1 byte	1 byte	2 bytes	variable

Fig. 42 Estructura de un paquete CHAP

Code

Identifica el tipo de paquete CHAP, los códigos CHAP son asignados como siguen:

Challenge

Response

Success

Failure

Identifier

Identifica las correspondencia de retos, requerimientos y respuestas.

Length

Indica la longitud en bytes del paquete CHAP incluyendo los campos de Code, Identifier, Lenght y Data.

Data

Puede ser cero o más bytes, dependerá del campo de código, el formato de la estructura de datos de retos y respuestas es mostrado en la siguiente ilustración.

Fig. 43 Estructura de los datos Challenge y Response CHAP

Value size

Indica la longitud del campo Value.

Value

El valor del Challenge es una cadena de bytes variable la cual debe cambiar cada vez que un reto es enviado.

El valor de Response es calculado a partir de una serie de bytes consistente de valores de Identifier y Challenge secreto.

Name

Identificación del sistema de transmisión de paquetes.

Tanto para Aciertos y Fallas el campo de Data contiene mensajes variables los cuales se implementan dependientemente.

- **Radius**

RADIUS (Remote Authentication Dial – In User Service), es un sistema de seguridad distribuido desarrollado por Livingston Enterprises. RADIUS fue

diseñado basado en una recomendación del Grupo de requerimientos de trabajo de servidores de acceso a red del IETF. RADIUS mantiene el perfil que contiene contraseñas (autenticación), privilegios de acceso (autorización) y otra información necesaria para VPN's tales como información administrativa y contable. El RADIUS emplea una arquitectura Cliente / Servidor con equipos de acceso a la red como clientes y la base de datos RADIUS como el servidor. La capacidad del RADIUS Proxy permite al servidor en el Punto de Presencia (POP) del proveedor de servicio consultar por el servidor "master" de la organización para acceder a los perfiles de los miembros de la VPN. En este camino la organización mantiene completo control sobre el acceso a los recursos de la VPN, mientras permite la provisión de seguridad la cual es reforzada en los POP's del proveedor de servicio. Esta disponibilidad de manejar la administración distribuida con control centralizado hace al RADIUS ideal para las VPN's.

RADIUS consiste de dos partes: Un cliente RADIUS, por ejm. El NAS o algún otro software como un firewall, que envía una petición al servidor RADIUS. En el otro lado, el servidor RADIUS, quien chequea la petición de acuerdo a la data configurada.

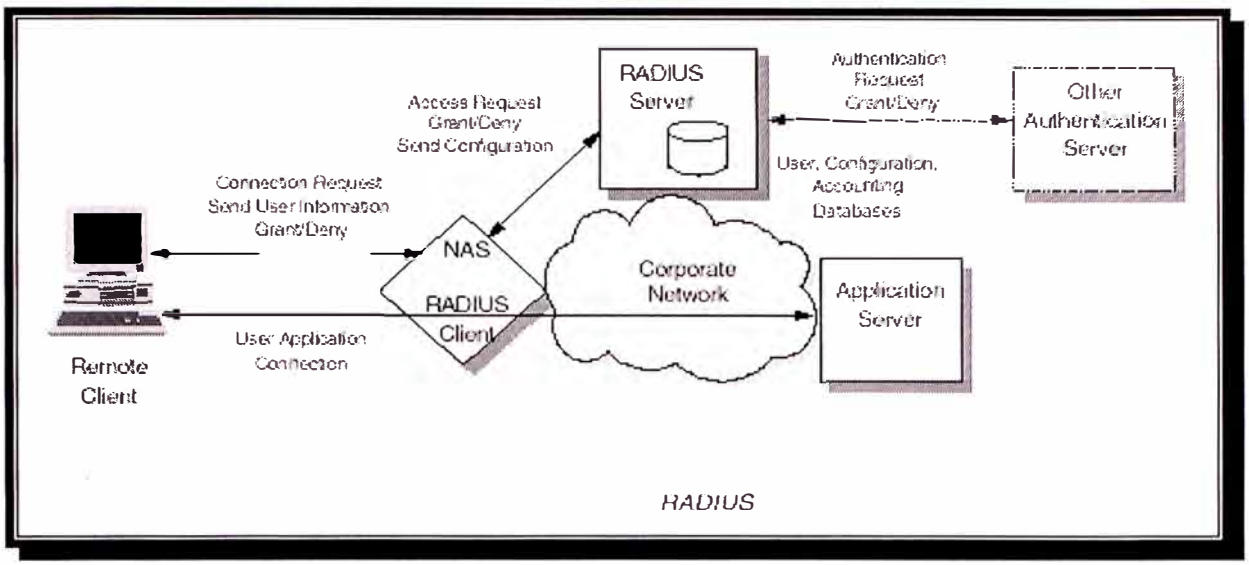


Fig. 44 Esquema de validación por Radius

Protocolo para validación de usuarios remotos definido según los RFCs 1238 y 1239.

Radius es un protocolo el cual maneja un pool de modems para acceso remoto por dial - up para un gran numero de usuarios.

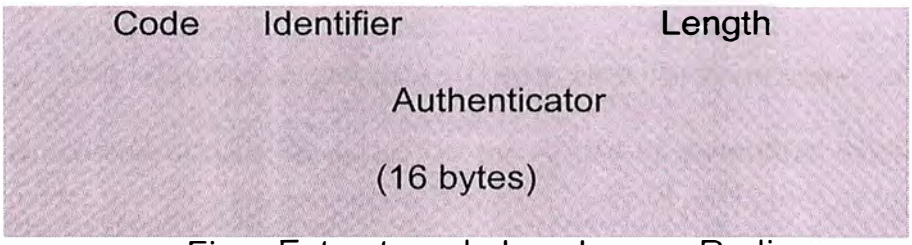


Fig. Estructura de la cabecera Radius

Code

Identifica el tipo de Message

Identifier

Relaciona los Requests y Replies.

Length

Indica la longitud del Message incluyendo el Header.

Authenticator

Un campo usado para autenticar la respuesta del servidor Radius y el password.

Protocolo de configuración dinámica de host (DHCP) y traducción de direcciones de red (NAT) .

Tanto el DHCP y el NAT permiten una distribución de direcciones IP registradas a una gran cantidad de usuarios. El DHCP asigna una dirección de Internet a una PC en forma dinámica. El NAT sustituye una dirección de Internet por una dirección privada. Cada uno proporciona un nivel de seguridad adicional con la finalidad de esconder la dirección interna y evitar sea descubierta desde Internet.

Otras necesidades propias de las LSVPN, los distintos dominios.

Hasta ahora hemos contemplado sobre todo la solución actual a los problemas de las VPN tradicionales. En las LSVPN hay que dar respuesta a necesidades nuevas que surgen básicamente en función de su tamaño y heterogeneidad y que se pueden resumir en una gestión controlada de los recursos a diferentes niveles.

En los grandes sistemas de los que estamos hablando, el control se hace una tarea que ha de ser automatizada de una forma prácticamente imprescindible. El control manual "artesano" es también parte del pasado y de los sistemas más pequeños. Las comunicaciones profesionales necesitan, al igual que las organizaciones que las utilizan, disponer en todo momento de un control eficaz de sus recursos.

Una pieza clave para este control lo forman los llamados directorios, estructuras de datos jerarquizadas en las se ordenan los recursos y los atributos que los caracterizan. Estas estructuras que hasta la fecha eran específicas de productos concretos se transforman ahora en potentes herramientas de Metadirectorio mejoradas que recopilan y consolidan información de diferentes estructuras heredadas controlando la selva de sistemas integrándose con los distintos entornos de las redes LAN / MAN / WAN a interconectar. Desde el manejo de los certificados electrónicos, hasta las opciones de "logon" único y sus permisos asociados controlado una asignación inteligente (y transparente para el usuario) de recursos.

La complejidad de las LSVPN no podrá ser soportada por usuarios más expertos sino por estructuras de control simples de uso y potentes en prestaciones.

Así se puede facilitar tareas como altas, bajas, modificaciones de acceso a algunos recursos etc. que al crecer el tamaño de la red y complicarse la estructura de la misma se vuelven tediosas y expuestas a fallos que son mucho más costosos en las estructuras de mayor tamaño.

La estandarización y automatización de todas las parametrizaciones y, en general, de todas las actividades repetitivas a realizar, tanto en la instalación inicial como en el mantenimiento normal de la LSVPN es algo necesario cuando hablamos de centenares de dispositivos y miles de usuarios. Usar estructuras de datos ya establecidos puede originar gran ahorro de costes; así como tener unas sólidas reglas "por defecto" cuya modificación para los necesarios casos particulares quede claramente registrada.

Otro aspecto diferencial de sistemas grandes y complejos es la gestión a todos los niveles, desde las alarmas de seguridad, hasta las labores de actualización de los dispositivos y monitorización de fallos. La gestión de dispositivos puede realizarse por parte del usurario final, de organizaciones sectoriales que agrupen a las partes involucrada, organismos de administración, etc, o, en muchos casos, el propio operador de datos que

provee el servicio de conectividad puede realizar la gestión de los dispositivos que coloca en las instalaciones de sus clientes.

Varias de estas gestiones pueden ser jerárquicas (la de nivel superior cede ciertas atribuciones a la de nivel inferior) o de igual nivel; y todas han de "convivir armoniosamente".

Es interesante introducir en este punto el concepto de dominio, que se puede aplicar tanto a la gestión como a otros campos de las LSVPN. Un Dominio establece una relación "lógica" entre elementos, que es una forma mucho más adecuada a estas estructuras, en vez de la tradicional agrupación física de elementos. Es un concepto ligado en cierta parte al de directorio.

El tradicional sistema plano en el que todos los usuarios, ubicaciones etc. son iguales respecto al sistema en una sola estrella común van dejando paso a sistemas en los que cada ubicación pertenecerá a distintas VPN lógicas, y por tanto las mismas pasarelas de securización sobre IPSec (o hosts IPSec) soportarán distintos certificados, distintos sistemas de gestión y control etc.

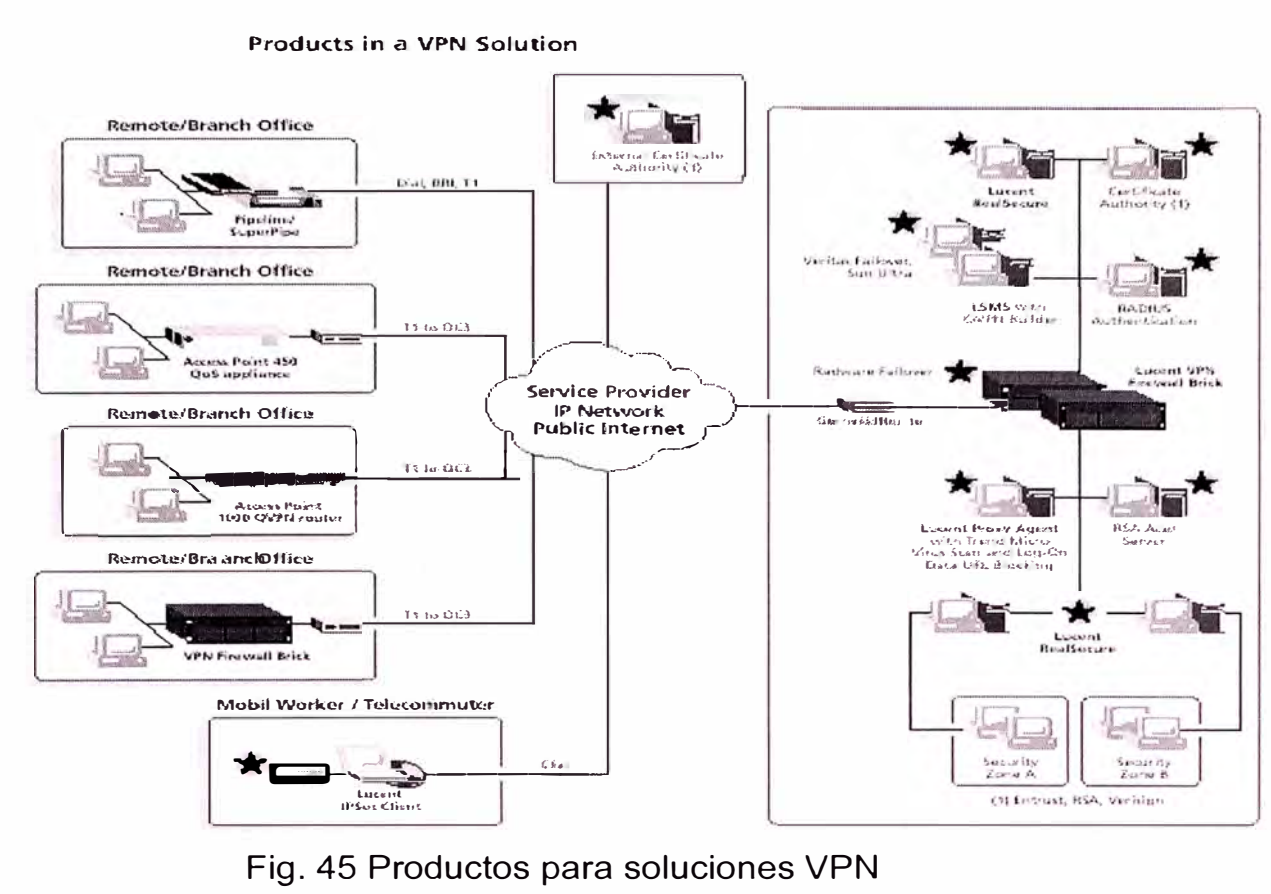


Fig. 45 Productos para soluciones VPN

Otra consideración relevante es la derivada de las distintas regulaciones nacionales de las claves. Las normas no son iguales en este campo en cada país, y cuando se supera el entorno nacional hay que prever la armonización de esta circunstancia para posibilitar la interconexión de los distintos "dominios legales".

2.4.15 Importancia futura de las VPN.

El mercado de la seguridad va a experimentar un tremendo crecimiento en los próximos meses a causa de varios motivos:

Por una parte, tras acabar los efectos (a todos los niveles, desde presupuestarios hasta de acaparación de recursos humanos) referentes al año 2000, las organizaciones tienen previsto grandes proyectos para extender sus comunicaciones creando (y aumentando las existentes) estructuras intra o extranet. La forma de desarrollarlas será, sin duda, mediante redes públicas IP y el lenguaje común de seguridad necesario para ello será IPSec.

Según Infonetics Research el porcentaje mundial de las LAN conectadas mediante VPN pasará de menos de un 3% en 1999 a más de un 20% en el 2001.

Existen diversos factores particulares que potenciarán esta tendencia. En primer lugar la existencia de nuevos operadores de datos que ofrecen diversas posibilidades tanto en el acceso a Internet como a otras redes públicas IP con calidades y costes mejorados. En segundo lugar el marco legal que, tras la reciente promulgación del reglamento de desarrollo de la Lortad y de la ley de firma electrónica, proporciona un "empujón" fundamental para el despliegue de elementos de seguridad en comunicaciones.

2.5 Tecnología Conmutación de Etiquetas Multiprotocolo MPLS

La formulación del proyecto se basa en la Red IP con transporte MPLS (Multi Protocol Label Switching), tecnología de routing que permite optimizar considerablemente la conmutación de tráfico IP de manera que el traspaso de los paquetes de Nodo a Nodo en Red es conmutado a alta velocidad.

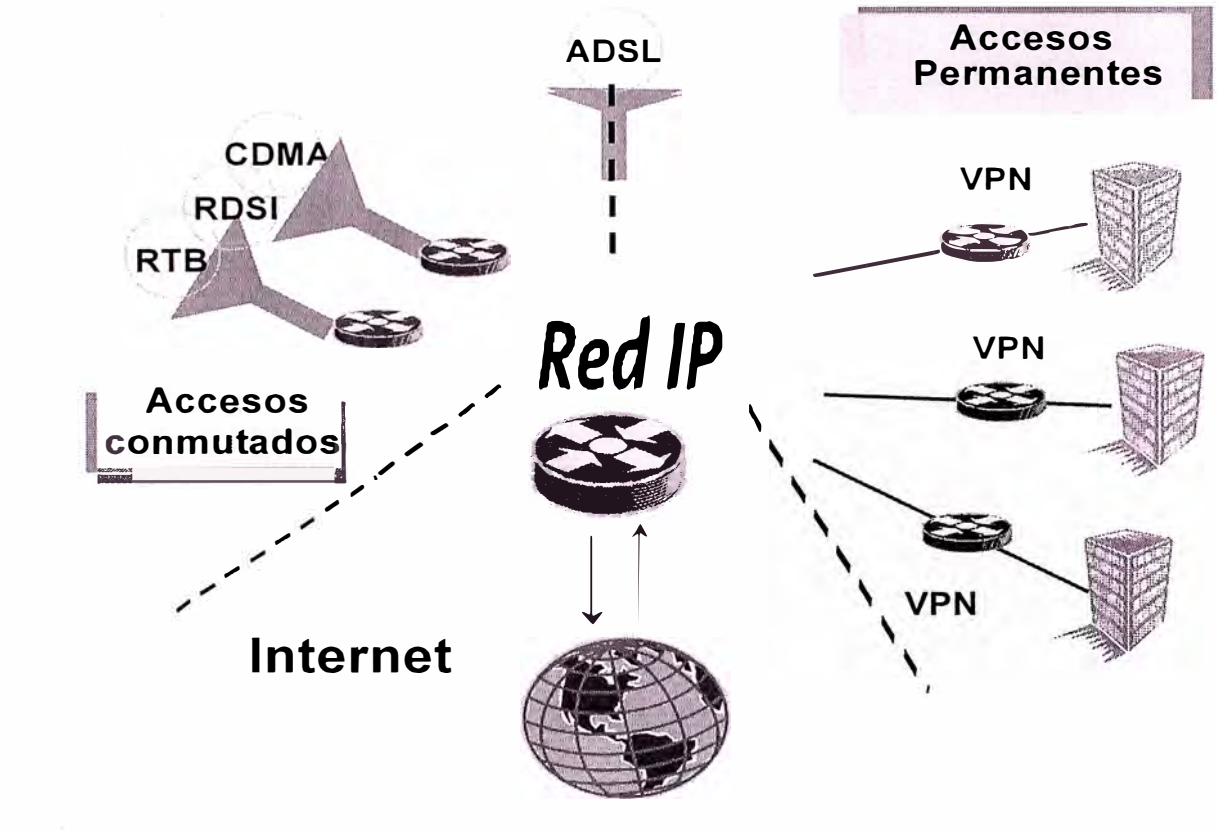


Figura 8. Esquema de accesos sobre la red IP.

La red IP soporta medios de acceso dedicados y conmutados, la figura 8 representa gráficamente los medios posibles de comunicación a través de la red IP.

2.5.1 Virtudes MPLS

El Servicio IP VPN sobre la Red IP pública, es posible gracias a la tecnología MPLS (Multi-protocol Label Switching). Es actualmente la mejor tecnología para el transporte IP en una Red.

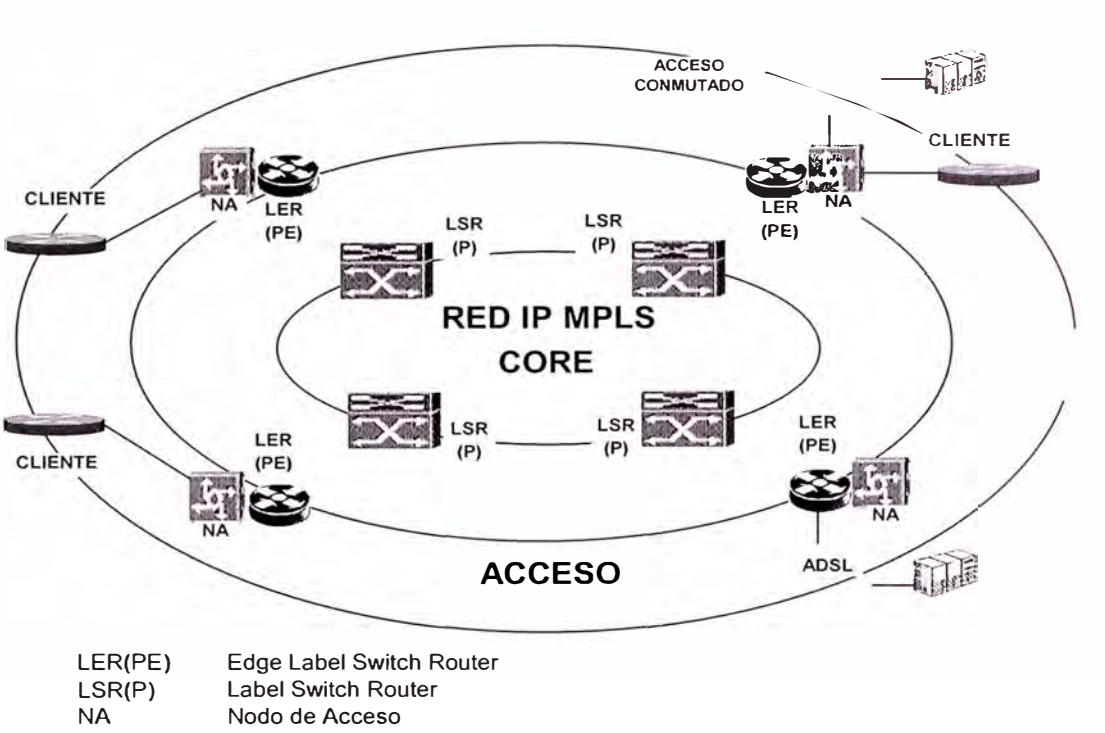


Fig. 46. Core de la red IP MPLS.

MPLS permite optimizar considerablemente la conmutación de tráfico IP de manera que el traspaso de los paquetes nodo a nodo en Red ya no es tradicionalmente enrutado (como se hace hoy en Internet) sino que es conmutado a alta velocidad. Esto reduce los retardos de transporte en Red.

La tecnología MPLS fue diseñada para optimizar y soportar calidad de servicio. Es posible ofrecer reservar ancho de banda en un caudal, para el tráfico de distintas aplicaciones (voz, datos de alta prioridad, video, tráfico transaccional financiero SNA, datos de prioridad media y

baja, etc.) con distintas calidades de servicio asociados a cada aplicación.

El MPLS integra la performance y la capacidad de manejo de tráfico de nivel 2 (Data Link Layer) con la escalabilidad y flexibilidad del nivel 3 (Network Layer Routing) para conmutar dinámicamente paquetes IP de cliente que ingresan a la Red; estableciendo caminos de nivel 2 basándose en la información de nivel 3 (IP) provenientes del acceso.

2.5.2 Descripción del Protocolo MPLS

Antes de iniciar con la explicación del funcionamiento del MPLS, definimos la terminología MPLS:

Edge Label Switch Router (LER o PE): Dispositivo o Nodo de borde que realiza el análisis inicial del encabezado (header) del paquete o datagrama IP que ingresa a la Red, clasifica y aplica la primera etiqueta (label) a dicho paquete.

- Label Switch Router (LSR o P): Dispositivo o Nodo de Transporte o Núcleo que conmuta o reenvía paquetes etiquetados, de acuerdo a su tabla LFIB (Label Forwarding Information Base) y las etiquetas (label) de los paquetes.
- Label: Una etiqueta contenida en el paquete, la cual es utilizada por el LSR para conmutar o reenviar dicho paquete. El label básicamente resume la información esencial sobre el ruteo del paquete, tal como:
  - Destino

- Procedencia
- Membresía VPN
- Clase de Servicio
- La ruta para el paquete, seleccionada de acuerdo a la Ingeniería de Tráfico.

- Label Distribution Protocol (LDP): Es utilizado conjuntamente con los protocolos convencionales de ruteo para distribuir la información de los label entre los nodos de la Red. El LDP asocia los label con los valores de ruteo entre nodos adyacentes; esta operación crea los Label Switched Path
- Label Forwarding Information Base (LFIB): Tabla formada en cada Nodo conjuntamente por los protocolos de ruteo convencionales y el LDP.
- Label Switched Path (LSP): Ruta o camino definido por los label correspondientes asignados en las LFIB, entre dos extremos de la Red.

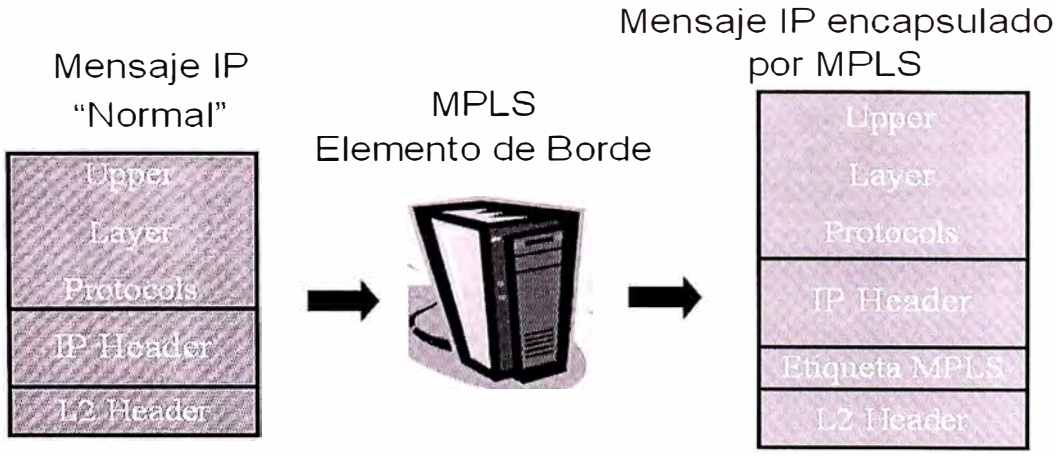


Fig. 47 Esquema del encapsulamiento MPLS

El procedimiento que se sigue para transmitir un datagrama IP de un extremo a otro de la Red IP utilizando el MPLS, es básicamente como se representa en la figura 48.

La Red automáticamente construye las tablas LFIB en cada nodo.

Un datagrama IP ingresa a un LER, el cual realiza el análisis completo del encabezado (header) de nivel 3 de dicho datagrama IP para determinar los beneficios requeridos, tales como clase de servicio, membresía VPN, destino. Basado en el ruteo y en los requerimientos, el LER selecciona y aplica un label al encabezado del paquete y lo reenvía.

En la figura 48, el datagrama IP que ingresa a la red tiene el destino 136.62.52.4; el LER de origen, de acuerdo a la información obtenida del encabezado y a los datos de su LFIB, ha puesto al datagrama IP el label 3 y lo ha reenviado por el interface 1 al nodo adyacente LSR.

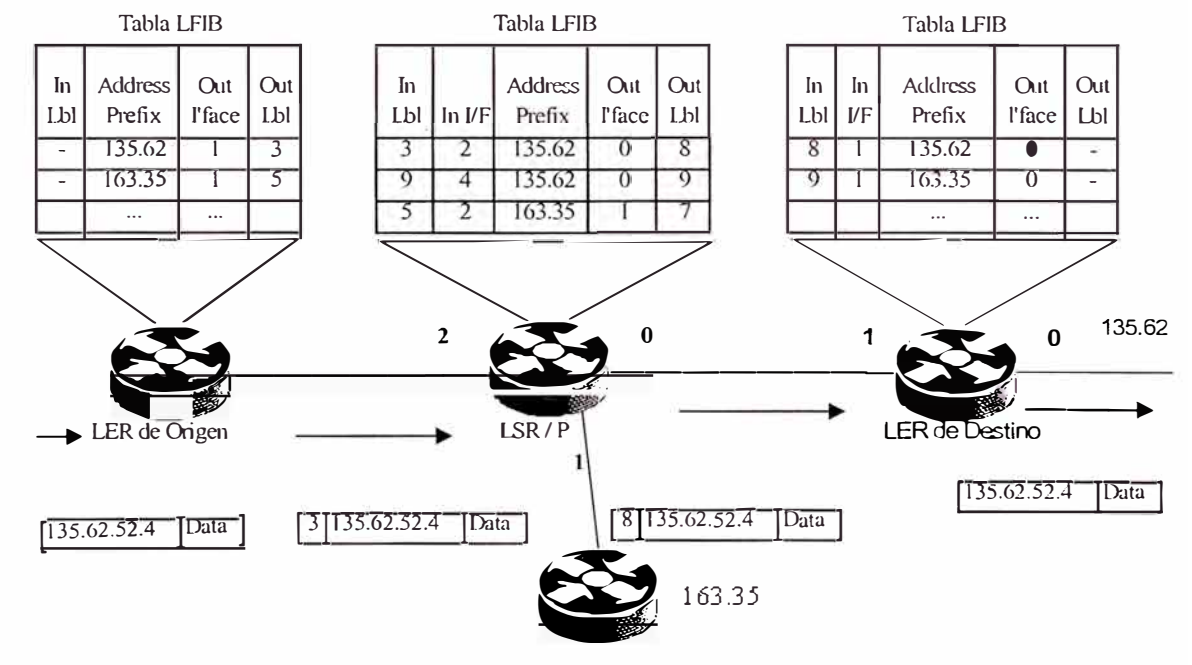


Fig. 48 Envío de paquetes MPLS.

El datagrama IP en cuestión ingresa al LSR, el cual lee el label (label 3 en este caso) y lo utiliza como índice en su LFIB y de acuerdo a los correspondientes datos reemplaza el label de entrada del datagrama IP por el label de salida (label 9 en la figura 10) y lo reenvía al nodo adyacente (LER de destino, interfase 0, en la figura 10)

Cabe resaltar que el LSR ha efectuado el reenvío del datagrama IP en base al label 3, sin necesidad de efectuar el análisis de su encabezado. Este análisis se realiza una sola vez en la Red, en el LER, a diferencia del ruteo tradicional que realiza tal análisis en cada nodo, con el consiguiente retardo e ineficiencia; en consecuencia, gracias al MPLS se logra una gran eficiencia en la transmisión de datos por la Red IP.

Asimismo cabe destacar que los label sólo tienen importancia local entre los nodos adyacentes.

El datagrama IP ingresa al LER de destino, el cual como en el caso anterior lee el Label (8 en este caso) para ser usado como índice en su LFIB y según los datos de la misma, retira el citado label y reenvía el datagrama IP hacia el equipo terminal del cliente (según la figura 10, con dirección IP 135.62.52.4, interfase 0).

Este procedimiento es válido para redes IP con Routers, pero se aplica en forma similar para redes IP con ATM, excepto que el label es llevado en el campo VCI/ VPI (Virtual Channel Identifier/ Virtual Path Identifier) del encabezado de la celda ATM.

CAPÍTULO III

INGENIERÍA DEL PROYECTO

3.1 Elección de la tecnología

Debido a existir una variedad de protocolos para la transmisión de datos probados y satisfactorios para nuestras necesidades (IP, Frame Relay y ATM), situaremos nuestro análisis en escoger el protocolo que más se adecue a nuestras necesidades y realice una satisfactoria entrega de la voz.

Todos los sistemas de voz por paquetes bajo una misma plataforma WAN, siguen un modelo común, El paquete de voz es transportado a través de la red, la cual puede ser IP, Frame Relay o ATM (Asynchronous Transfer Mode) y se encuentra representada en la figura 49 por una nube. En los extremos de esta red están los dispositivos o componentes que pueden ser llamados "agentes de voz" o gateways. Estos dispositivos tienen por misión encapsular la información de voz de su forma de telefonía tradicional a una forma de un conjunto de paquetes de transmisión. La red entonces envía los

paquetes de datos a un agente de voz, los cuales van a servir al destino o al inicio de la llamada.

Actualmente para integrar redes de voz y datos, observamos 3 tecnologías:

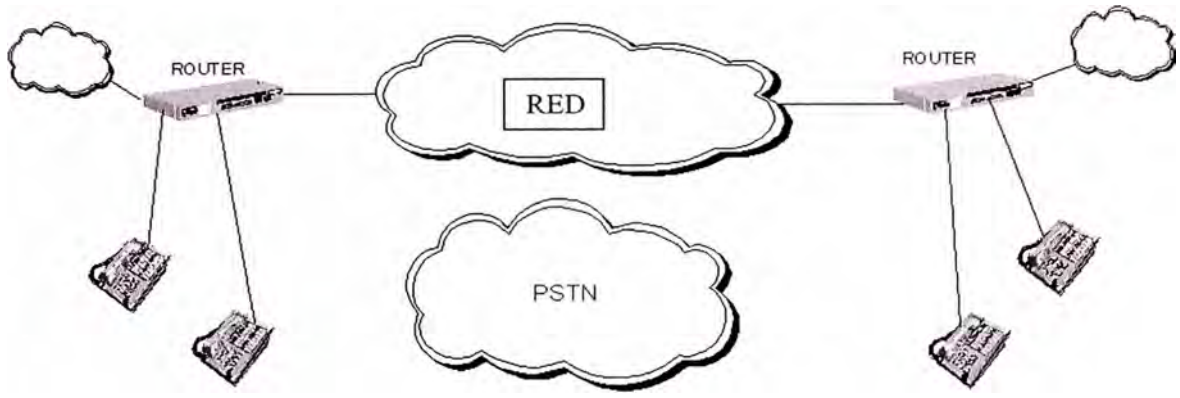


Fig. 49 Modelo de red WAN para datos

1. *Voz sobre ATM (VoATM).*
2. *Voz sobre Frame Relay (VoFR).*
3. *Voz sobre IP (VoIP).*

ATM: Es una comunicación orientada a conexión. Esto fue diseñado para administrar tráficos sensitivos al tiempo, tales como la voz. Su señalización, direccionamiento y enrutamiento permite construir una red que sigue el modelo de traducción.

La función de enrutamiento en particular, es bastante robusta, permitiendo construir conexiones que posean un retraso aceptable y una variación de retraso adecuado.

Frame Relay: Tiene provisión para especificar la voz dentro del campo de tipo. Es también relativamente barato y bastante común en muchas partes en el mundo. Los servicios de Frame Relay deben proveer conmutación de circuitos virtuales (SVC) y soportar calidad de servicio (QoS) en el futuro, pero su falta de señalización sofisticada, direccionamiento y funcionalidad de enrutamiento impedirá que pase de un modelo de transporte a un modelo de traducción.

IP MPLS: No es orientado a la conexión; desarrollo en el área de brindar prioridad al tráfico, reservación de recurso, fragmentación de paquetes son algunas virtudes de MPLS sobre el IP, que al igual que en el ATM tiene una robusta señalización, direccionamiento, y funcionalidad de enrutamiento, que hace que el modelo de traducción sea una posibilidad.

Debemos elegir la red que ofrezca el mas eficiente tratamiento en la transmisión de paquetes IP, y permita implementar eficientemente servicios con Calidad de servicio (QoS). Entonces con esta premisa queda descartada la tecnología frame relay por no ofrecer un adecuado manejo de QoS. El análisis se centrará en las opciones restantes.

Como resultado de lo anteriormente expuesto, la plataforma WAN que integrará voz y datos, contempla el protocolo IP MPLS, el que tiene entre sus

características; tratamiento de los paquetes en forma optima, accesible costos de implantación, tecnología estandarizada y probada.

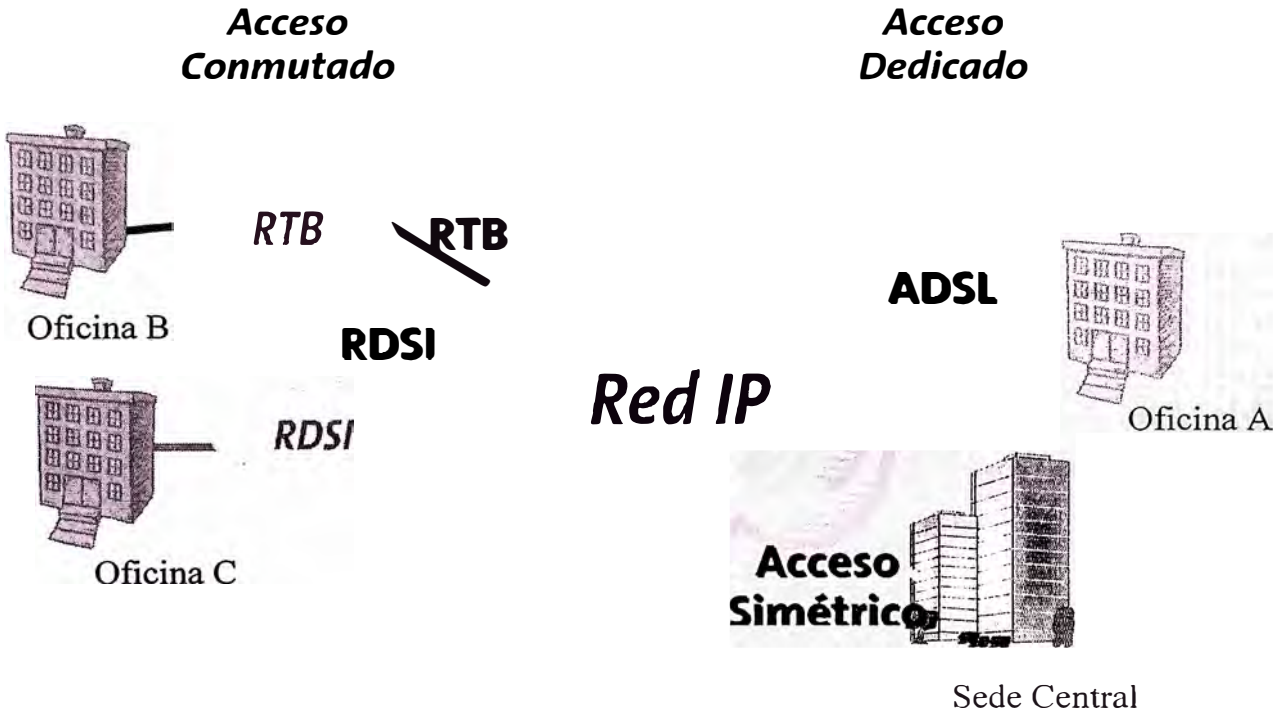


Fig. 50 Tipos de acceso a la Red IP VPN

3.2 Características de la solución

- Permitirá realizar llamadas desde los locales de los clientes empresariales hacia celulares de la empresa de TM (llamadas locales solamente), las soluciones para la interconexión con las centrales privadas de las empresas pueden variar desde 2 a 30 canales de voz.
- Se dispondrá de interfaces analógicas y digitales para la interconexión a las PBX's de los clientes.

- Los costos para el cliente dependerán de la cantidad de canales de voz simultáneos a utilizar (BW), tanto para los servicios de la Red IP como para el equipamiento; además podrán existir casos personalizados de acuerdo a las características de la red del cliente.
- Los equipos de los clientes al ingresar a la VPN de la empresa de TM serán gestionados exclusivamente por empresa proveedora de servicio IP VPN.
- Se utilizará compresión de la voz, reduciendo de esta manera el costo de la transmisión aprox. (12Kbps por canal de voz utilizando vocoders G.723.1 y 16Kbps utilizando vocoders G.729).
- Se deberán reprogramar las PBX's de los clientes para automatizar la redestinación de las llamadas a celulares de la empresa de TM, así como el uso de salidas a celulares por la red de telefonía fija como medida de contingencia.

- Las llamadas solo se realizarán a teléfonos celulares de la empresa en mención Por lo que se deberán generar las tablas respectivas en la PABX del cliente.
- Se soportará exclusivamente por equipos Cisco.

- Para diferenciar el trafico de los clientes proveniente del gateways AS5300 hacia la central de conmutación móvil, las comunicaciones de cada cliente se envían por canales específicos (un grupo troncal por cada Empresa) lo que brindará un nivel adicional de seguridad.

- El ANI se programará en el ruteador del cliente y no en la PABX del mismo. La facturación se realiza sobre la base del grupo troncal de la llamada y al switch que pertenece el mismo, cada empresa tendrá un grupo troncal asignado con la cantidad de canales de voz que haya solicitado.

Características de la Solución

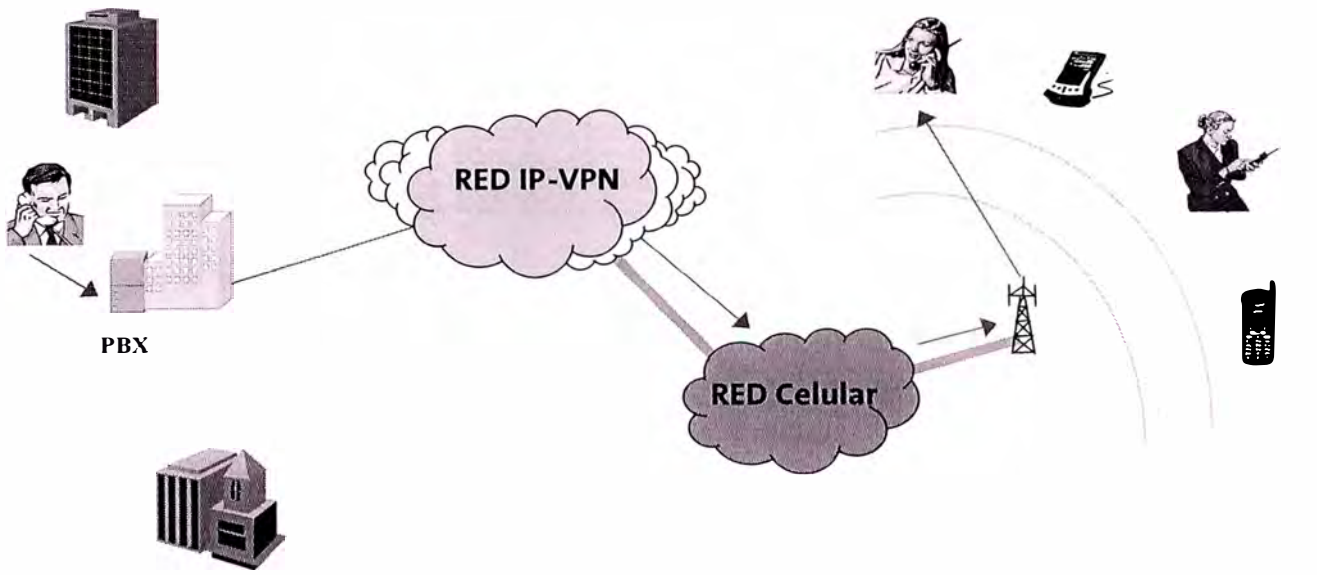


Fig. 51 Esquema de la solución

3.3 Modelos de Solución

Existen, 3 modelos de solución que podrán encajar uno mejor que otros en la red del cliente, beneficiándolos con la reducción de costos u optimización del servicio.

- Modelo 1 : El cliente dispone de acceso a la red IP-VPN con equipos Cisco.
- Modelo 2: El cliente dispone de acceso a la red IP-VPN con equipos no Cisco.
- Modelo 3 : El Cliente no dispone de acceso a la red IP-VPN y sí a otras redes.

3.3.1 Modelo 1 : Red IP-VPN con equipos Cisco

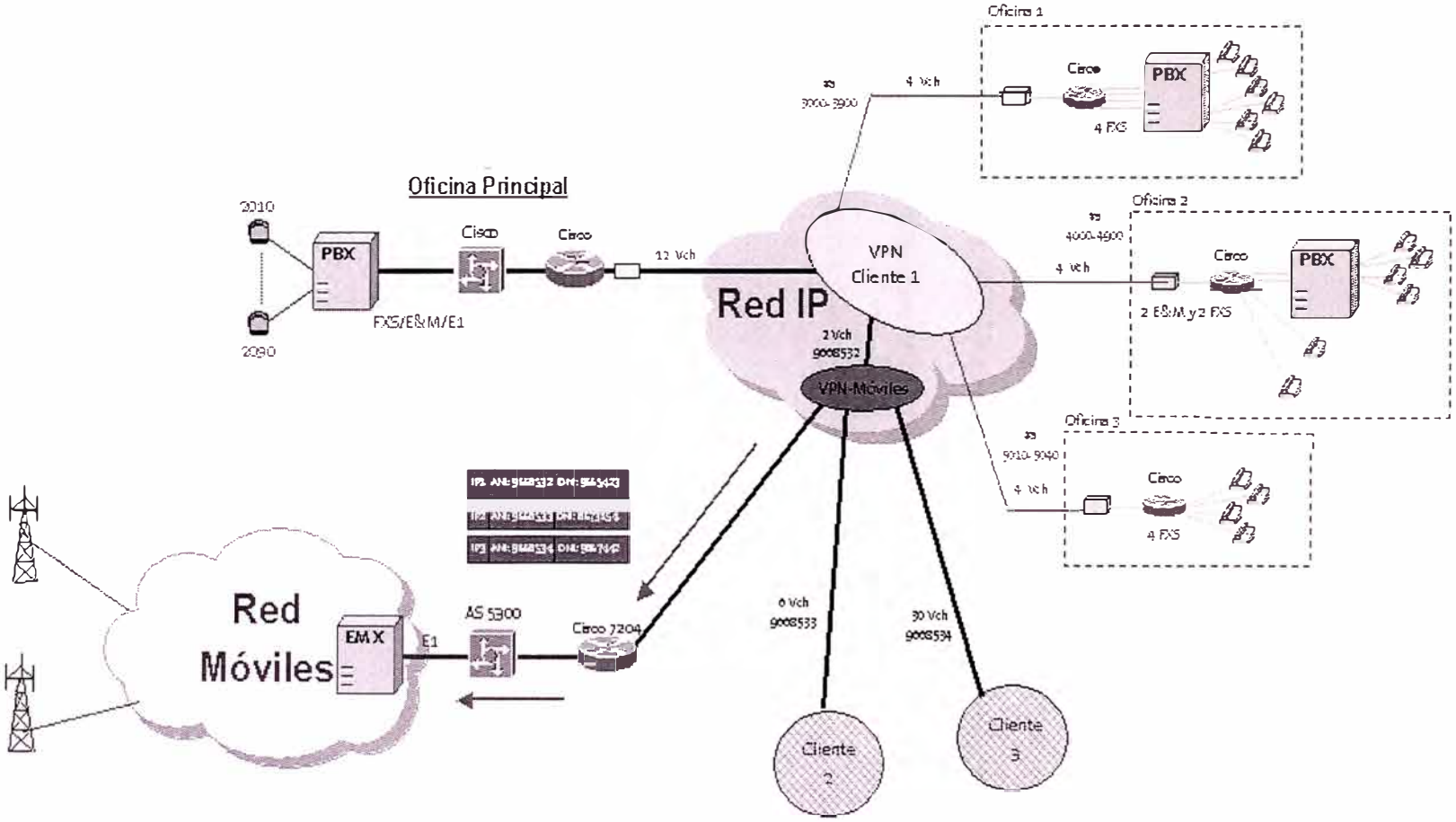
Características

- El cliente está o piensa integrar las comunicaciones de voz de sus oficinas a la red IP-VPN utilizando equipos Cisco.
- La solución consiste en utilizar los equipos Cisco que soporten VoiP con que dispone el cliente, así como todos sus accesos a la red IP.
- Se podrán enrutar las llamadas a Móviles directamente desde cada oficina utilizando el equipamiento disponible.
- Podría requerirse el incremento de número de canales de voz y ancho de banda para algunas oficinas.

- Se deberán reprogramar las PBX's de los clientes para enrutar las llamadas a celulares de la empresa de TM a través de los routers gateways.

En la figura siguiente se aprecia las bondades de la solución, el cliente no necesita de mucha inversión para adoptar esta solución.

Modelo 1 : Red IP-VPN con equipos Cisco

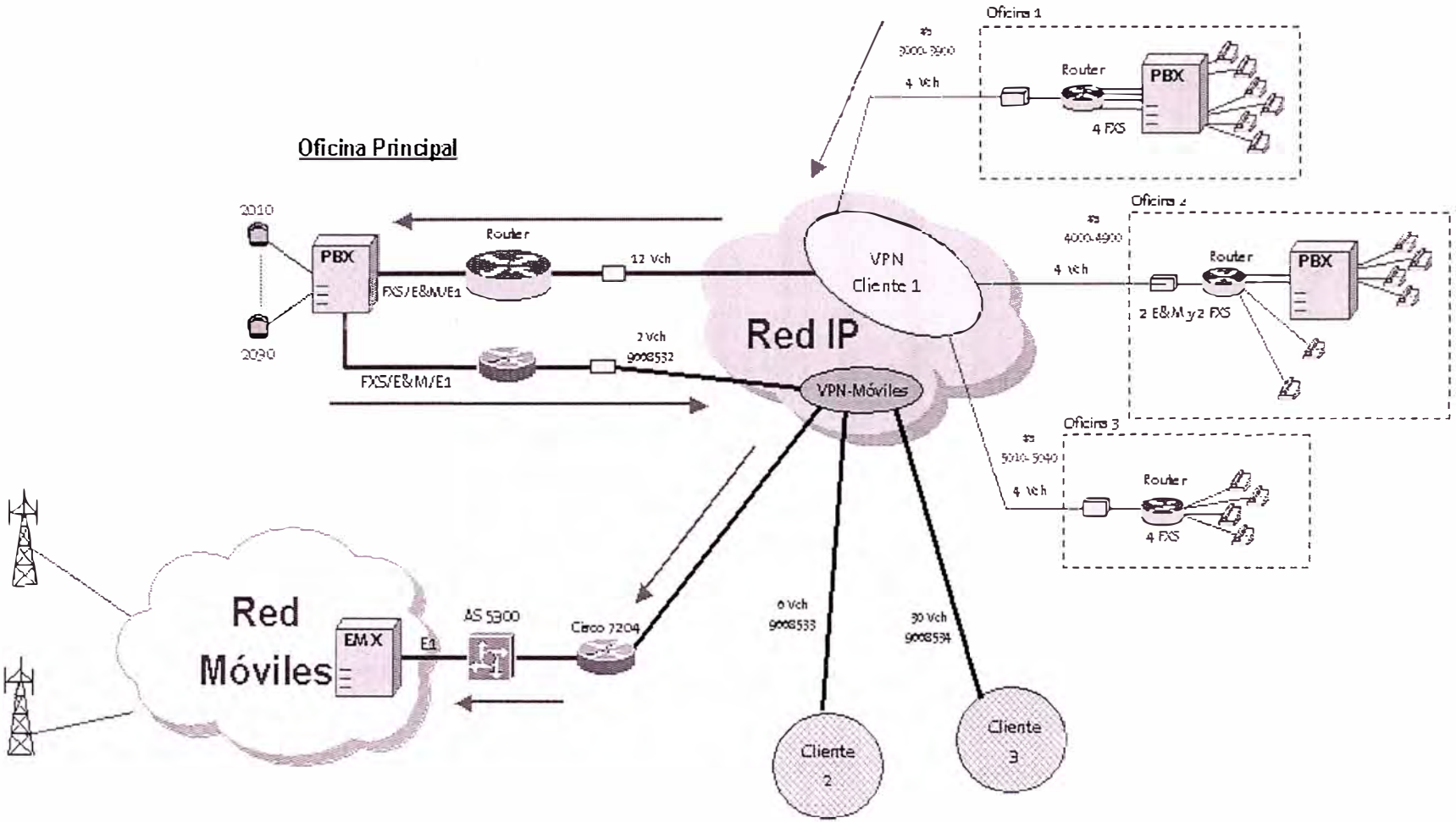


3.3.2 Modelo 2: Red IP-VPN sin equipos Cisco

Características

- El cliente está o piensa integrar las comunicaciones de voz de sus oficinas a la red IP-VPN utilizando equipamiento de un fabricante que no es Cisco.
- Se deberán enrutar las llamadas a Móviles a través de una oficina central la cual deberá disponer de un Router Cisco conectado a la red IP-VPN y a la PBX del cliente.
- Se deberán reprogramar las PBX's de los clientes.

Modelo 2: Red IP-VPN sin equipos Cisco



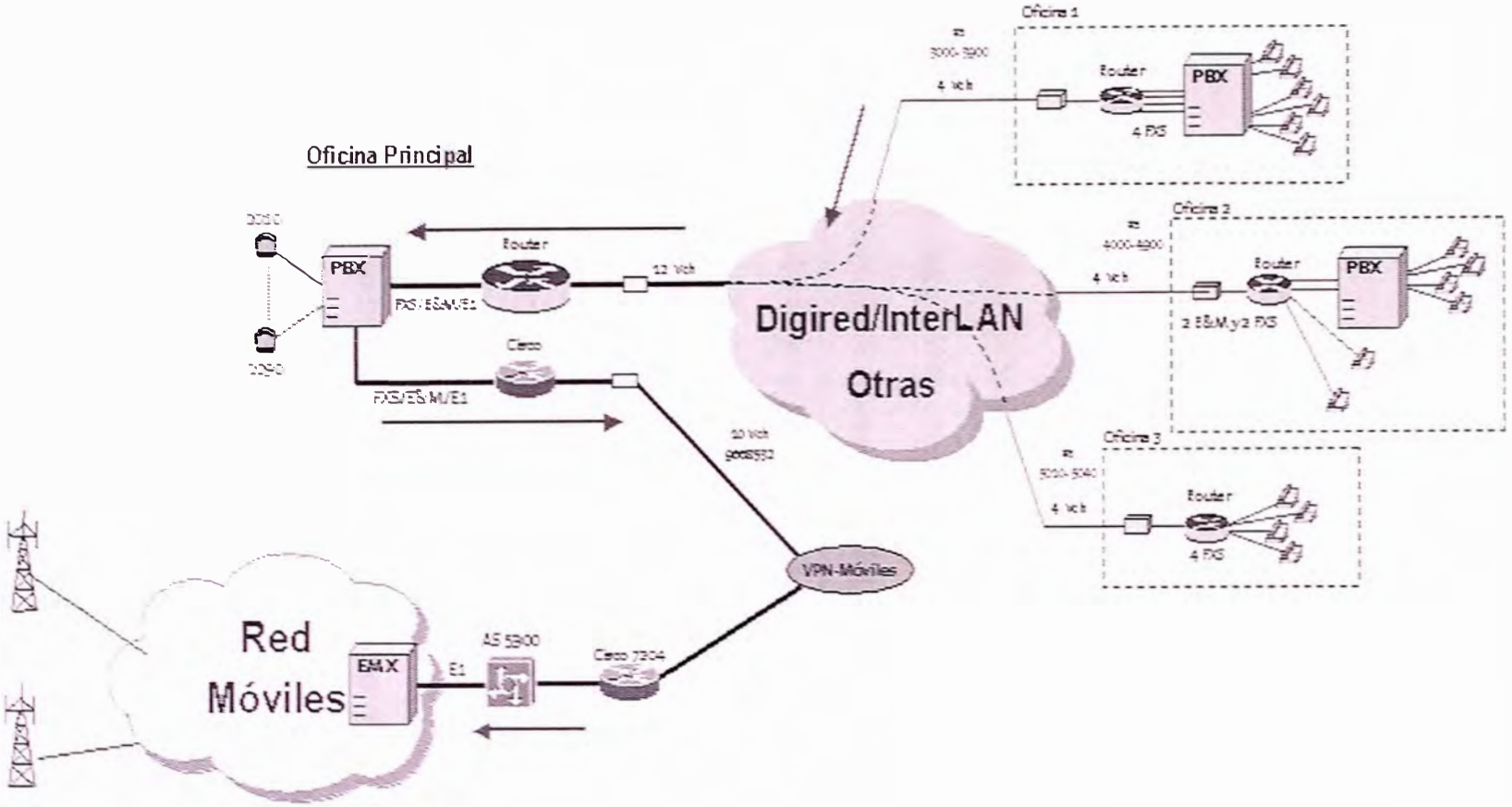
3.3.3 Modelo 3: Otras Redes

Características

- El cliente posee sólo una oficina o sus comunicaciones de voz están soportadas en Digired, InterLAN o redes de la competencia.
- En el caso de disponer de equipamiento Cisco podría no ser necesario un equipo adicional en el lado central.
- Se deberán enrutar las llamadas a Móviles a través de una oficina central vía la PBX o el router.

Se deberán reprogramar las PBX's de los clientes.

3 Modelo 3: Otras Redes



3.4 Configuración de alta disponibilidad y redundancia

Se ha considerado al servicio que se ofrece como crítico y se implementarán sistemas de redundancia a diferentes niveles.

3.4.1 Redundancia a nivel de enlace

Se tiene un enlace a 2MB como principal, con nivel se servicio oro, y existe un segundo enlace a 2MB con nivel de servicio plata como enlace de respaldo, el respaldo es automático. Ambos enlaces provienen de nodos diferentes, rutas diferentes, Nodo San Isidro y nodo Washington por razones de seguridad y fiabilidad, como se muestra en la figura siguiente.

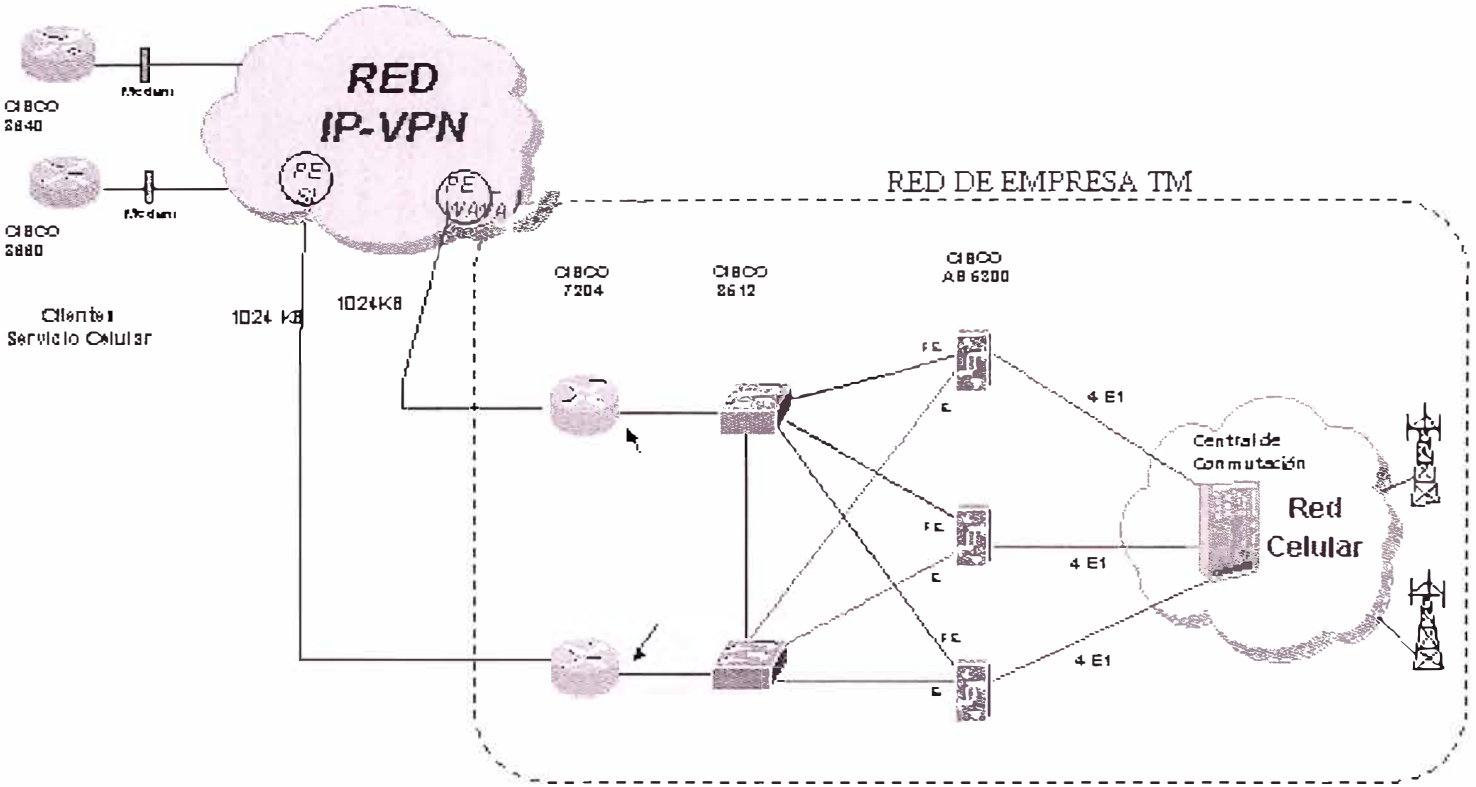
3.4.2 Redundancia a nivel de router de borde

Se ha considerado dos equipos Cisco 7200 , el primero de ellos recibe el enlace activo proveniente del Nodo San Isidro y el segundo recibe el enlace redundante proveniente del Nodo Washington, se define una IP Virtual que la asume el router Cisco 7200 activo, cuando un enlace cae o el equipo activo queda fuera de servicio la IP virtual es trasladada al equipo de respaldo, siendo esta acción totalmente transparente para el usuario del servicio.

3.4.3 Redundancia a nivel de red local

Se utilizan dos equipos Cisco Catalyst 3512 como red LAN, y se definen tres VLANs (Virtual LAN) para manejar la redundancia a nivel de red LAN, la razón de definir tres VLANs es por que la solución proyecta instalar 3 tres gateways AS5300, la Fig. 55 muestra el esquema de redundancia.

Redundancia en la red Local de TM



3.5 Equipamiento

El equipamiento requerido por la empresa de telefónia móvil es basicamente equipos de comunicación de nodo, se requieren 2 routers Cisco 7204 como router de borde, 3 routers AS5300 con software de VOIP y 2 switches 3512 que manejaran la redundancia de la LAN. El equipamiento se detalla a continuación

Tabla 3.5 a

Equipo		Cantidad
Router Cisco 7204 VXR: 4Serial, 1 FE		2
Cisco7204VXR	Cisco7204VXR, 4 slot chassis, 1 AC Supply w/IP Software Cisco 7200 series IOS Enterprise Cisco 7200 Input/Output Controller with Fast Ethernet Port Cisco 7200 I/O PCMCIA Flash Memory, 20 MB 4-port E1 G.703 Serial Port Adapter	
Router Cisco AS5300 : 120 Vch (128 MB DRAM, 16 MB Flash)		3
AS5300	AS5300 Dial Shelf Dual CD Power Supply, AS5300 Cisco AS5300 series IOS IP Voice Plus 120 Voice channels & Quad E1 Card Voice C549 DSP Firmware 128 MB DRAM memory for 5300	
Switch Cisco Catalyst 3512XL		2
WS-C3512-XL-EN	Catalyst 3512XL Enterprise Edition Redundant Power System (RPS 3000) Giga Stack Stacking GBIC	

El equipamiento requerido por el cliente dependerá de la cantidad de tráfico que requiera cursar para sites menores de 24 canales se recomienda cisco 3640 y para sites con mas de 30 canales cisco AS5300.

Tabla 3.5 b

Router Cisco 3640 2 slot , 32 MB RAM		
Cisco 3640	Cisco 3640 2 slot chassis Cisco 3600 IOs Software w/IP Voice Plus 32 MB RAM	
Router Cisco AS5300 : 120 Vch (128 MB DRAM, 16 MB Flash)		
AS5300	AS5300 Dial Shelf Dual CD Power Supply, AS5300 Cisco AS5300 series IOS IP Voice Plus 120 Voice channels & Quad E1 Card Voice C549 DSP Firmware 128 MB DRAM memory for 5300	

3.6 Costo de Equipamiento

El costo de instalación del equipamiento en el nodo de la empresa de telefonía móvil es el siguiente:

Tabla 3.6

Equipo		Cant.	Costo/unid	Costo
Router Cisco 7204 VXR: 4Serial, 1 FE		2	32000	64000
Cisco7204VXR	Cisco7204VXR, 4 slot chas, 1 AC Supply w/IP Software Cisco 7200 series IOS Enterprise Cisco 7200 Input/Output Controller w/ Fast Eth. Port Cisco 7200 I/O PCMCIA Flash Memory, 20 MB 4-port E1 G.703 Serial Port Adapter			
Router Cisco AS5300 : 120 Vch (128 MB DRAM, 16 MB Flash)		3	48000	144000
AS5300	AS5300 Dial Shelf Dual CD Power Supply, AS5300 Cisco AS5300 series IOS IP Voice Plus 120 Voice channels & Quad E1 Card Voice C549 DSP Firmware 128 MB DRAM memory for 5300			
Switch Cisco Catalyst 3512XL		2	3600	7200
WS-C3512-XL	Catalyst 3512XL Enterprise Edition Redundant Power System (RPS 3000) Giga Stack Stacking GBIC			
Circuito de datos a la red IP - VPN		2	850	1700
	instalación de 2 enlace Plata Plus a 2048 KB			
			Total	216900

Adicionalmente el costo mensual de los dos enlaces de 2048 KB es de $ 2940.

ANEXO A

CONFIGURACIÓN ROUTER CISCO 7200

Las VPNs reducen sustancialmente los costos y son fáciles de usar, pero es necesario indicar que las redes privadas virtuales implican costos, requisitos organizacionales y cargas de trabajo al personal de sistemas adicionales para una organización, pero que son sopesados al obtener ahorros en el costo, al utilizar una red pública en vez de una instalación de línea rentada y la facilidad de utilizar dicha red con el fin de hacer negocios.

MPLS es actualmente la mejor tecnología y el protocolo mas adecuado para transporte IP , el cual permite además aplicar QoS con relativa prioridad.

En todo diseño de red se deben establecer sistemas de respaldo, que nos asegure la disponibilidad del servicio, para este proyecto se consideraron principios de alta disponibilidad, enlaces de respaldo, equipos de respaldo, respaldo de energía, no se escatimaron costos en el tema de redundancia, por tratarse de un servicio que esta dirigido a los clientes corporativos mas importantes de la compañía.

CONCLUSIONES Y RECOMENDACIONES

Las solución presentada en este informe es viable gracias al desarrollo de la tecnología VoiP que ha permitido mejorar las técnicas de compresión de voz y abaratar los costos de equipamiento.

Todos los estudios al respecto dan como imparable el desarrollo de la telefonía IP, y ya esta muy cercano el momento que el número de minutos de comunicaciones vocales cursadas por redes IP superará a los cursados por las redes tradicionales

La telefonía sobre IP abre un espacio muy importante dentro del universo que es Internet. Es la posibilidad de estar comunicados a costos más bajos dentro de las empresas y fuera de ellas, es la puerta de entrada de nuevos servicios apenas imaginados. Lentamente, la telefonía sobre IP está ganando terreno y todos querrán tenerla.

```
TM-RED-IP-7200-1#sh run
Building configuration...
 Current configuration:
!
! Last configuration change at 15:16:41 UTC Sun Sep 29 2002 by netsecurity
! NVRAM config last updated at 15:16:42 UTC Sun Sep 29 2002 by netsecurity
!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname TM-RED-IP-7200-1
!
logging buffered 125000 debugging
aaa new-model
aaa authentication login default local
aaa authorization exec default local
enable secret 5 $1$74F5$cnfMYgmKxvigBboEeUVne.
enable password 7 0822455D0A16
!
username cisco password 7 055A020A205E410718454E
!
!
```

```
!
!
ip subnet-zero
no ip domain-lookup
ip host central1 10.144.6.2
!
lane client flush
cns event-service server
!
!
!
!
!
controller E1 3/0
!
controller E1 3/1
!
!
process-max-time 20
!
interface Loopback0
 no ip address
!
interface FastEthernet0/0
```

```
 ip address 192.162.40.2 255.255.255.0
 no ip redirects
 ip nat inside
 half-duplex
 standby 1 priority 100 preempt
 standby 1 ip 192.162.40.1
 standby 1 track Serial2/0
!
interface FastEthernet1/0
 no ip address
 shutdown
 full-duplex
!
interface Serial2/0
 bandwidth 2048
 ip address 10.144.6.2 255.255.255.252
 ip nat outside
 encapsulation ppp
 timeslot 1-31
 ts16
!
interface Serial2/1
 bandwidth 2048
 ip address 10.104.6.50 255.255.255.252
```

```
 ip nat outside
 encapsulation ppp
 timeslot 1-31
 ts16
!
interface Serial2/2
 no ip address
 shutdown
!
interface Serial2/3
 no ip address
 shutdown
!
router rip
 version 2
 redistribute static
 network 10.0.0.0
 network 192.162..40.0
 network 192.162..160.0
 no auto-summary
!
ip nat pool VPN 192.162.40.200 192.162.40.200 prefix-length 24
ip nat inside source list 10 pool VPN overload
ip nat inside source static 192.162..100.91 192.162.40.91
```

ip nat inside source static 192.162.197.53 192.162.40.53

ip nat inside source static 192.162.197.151 192.162.40.151

ip nat inside source static 192.162.120.144 192.162.40.144

ip nat inside source static 192.162.120.143 192.162.40.143

ip nat inside source static 192.162.120.147 192.162.40.147

ip nat inside source static 200.4.196.99 192.162.40.99

ip nat inside source static 200.4.196.98 192.162.40.98

ip nat inside source static 200.4.196.100 192.162.40.100

ip nat inside source static 192.162.120.202 192.162.40.202

ip nat inside source static 192.162.120.201 192.162.40.201

ip classless

ip route 0.0.0.0 0.0.0.0 Serial2/0

ip route 10.1.104.0 255.255.248.0 Serial2/0

ip route 10.1.124.0 255.255.255.0 Serial2/0

ip route 10.1.220.0 255.255.255.0 Serial2/0

ip route 10.125.25.0 255.255.255.0 10.144.6.1

ip route 10.226.104.0 255.255.248.0 192.162.40.33

ip route 172.19.0.0 255.255.0.0 Serial2/0

ip route 172.24.0.0 255.255.0.0 192.162.40.33

ip route 172.24.104.0 255.255.255.0 192.162.40.33

ip route 172.24.106.0 255.255.255.0 192.162.40.33

ip route 172.24.107.0 255.255.255.0 192.162.40.33

ip route 172.26.105.0 255.255.255.0 Serial2/0

ip route 172.26.106.0 255.255.255.0 Serial2/0

```
ip route 172.26.107.0 255.255.255.0 Serial2/0
ip route 172.31.1.0 255.255.255.0 10.144.6.1
ip route 192.162.0.0 255.255.0.0 192.162.40.33
ip route 192.162.100.0 255.255.255.0 192.162.40.33
ip route 192.162.120.0 255.255.255.0 192.162.40.33
ip route 192.162.160.10 255.255.255.255 192.162.40.10
ip route 192.162.160.62 255.255.255.255 192.162.40.10
ip route 192.162.193.0 255.255.255.0 192.162.40.33
ip route 192.162.197.0 255.255.255.0 192.162.40.33
ip route 200.4.196.98 255.255.255.255 192.162.40.33
ip route 200.4.196.99 255.255.255.255 192.162.40.33
ip route 200.4.196.100 255.255.255.255 192.162.40.33
no ip http server

access-list 10 permit 192.162.193.0 0.0.0.255
access-list 177 permit ip any host 192.162.100.91
access-list 177 permit ip host 192.162.100.91 any
snmp-server engineID local 0000000902000000428576C00
snmp-server community mplschimu view v1default RO
snmp-server community MOVILES RO
snmp-server packetsize 2048
snmp-server location MOVILES CD
snmp-server contact CGRC-IP-VPN
snmp-server enable traps snmp
```

```
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps syslog
snmp-server enable traps voice poor-qov
snmp-server host 10.10.25.2 mplschimu
!
!
!
line con 0
 password 7 082C4358000A1116001F
 transport input none
line aux 0
line vty 0 4
 exec-timeout 30 0
 password 7 105A0C1500111D0505072B
!


end
```

ANEXO B

CONFIGURACIÓN GATEWAY CISCO AS5300

```
AS5300-2#sh run
Building configuration...
 Current configuration:
!
! Last configuration change at 10:39:49 GMT-05: Fri Sep 20 2002 by cisco
! NVRAM config last updated at 09:54:29 GMT-05: Fri Sep 20 2002 by cisco
!
version 12.1
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname AS5300-2
!
logging buffered 16000 debugging
aaa new-model
aaa authentication login default local
aaa authorization exec default local
enable secret 5 $1$HBKM$BshGYK5ONwEoOia2bZKPv/
enable password 7 030752180500
!
username secure password 7 12140005111E1E0D7A6B37
username cisco password 7 05080F1C22431C594954
!
```

```
resource-pool disable
!
!
!
!
!
clock timezone GMT-05:00 -5
ip subnet-zero
no ip finger
no ip domain-lookup
!
mgcp package-capability trunk-package
mgcp default-package trunk-package
mta receive maximum-recipients 0
!
!
controller E1 0
 framing NO-CRC4
 clock source line primary
 ds0-group 2 timeslots 26-31 type r2-digital r2-compelled ani
 ds0-group 4 timeslots 3-6 type r2-digital r2-compelled ani
 ds0-group 5 timeslots 7-10 type r2-digital r2-compelled ani
 ds0-group 6 timeslots 11 type r2-digital r2-compelled ani
 ds0-group 7 timeslots 12 type r2-digital r2-compelled ani
```

```
 cas-custom 2
  country venezuela use-defaults
 cas-custom 4
  country venezuela use-defaults
 cas-custom 5
  country venezuela use-defaults
 cas-custom 6
  country venezuela use-defaults
 cas-custom 7
  country venezuela use-defaults
!
controller E1 1
 framing NO-CRC4
 clock source line secondary 1
 ds0-group 8 timeslots 1-12 type r2-digital r2-compelled ani
 ds0-group 9 timeslots 13-15,17-29 type r2-digital r2-compelled ani
 cas-custom 8
  country venezuela use-defaults
 cas-custom 9
  country venezuela use-defaults
!
controller E1 2
 clock source line secondary 2
!
```

```
controller E1 3
 clock source line secondary 3
!
!
voice-port 0:2
 cptone PE
!
voice-port 0:4
 cptone PE
!
voice-port 0:5
 cptone PE
!
voice-port 0:6
 cptone PE
!
voice-port 0:7
 cptone PE
!
voice-port 1:8
 cptone PE
!
voice-port 1:9
 cptone PE
```

```
!
!
dial-peer voice 210 voip
 destination-pattern 18443129
 session target ipv4:192.162.40.12
 ip precedence 5
!
dial-peer voice 211 pots
 max-conn 6
 answer-address 180.....
 destination-pattern #2003080.....
 port 0:2
 prefix 80
!
dial-peer voice 212 pots
 max-conn 6
 answer-address 184.....
 destination-pattern #2003084.....
 port 0:2
 prefix 84
!
dial-peer voice 213 pots
 max-conn 6
 answer-address 186.....
```

```
 destination-pattern #2003086.....
 port 0:2
 prefix 86
!
dial-peer voice 214 pots
 max-conn 6
 answer-address 187.....
 destination-pattern #2003087.....
 port 0:2
 prefix 87
!
dial-peer voice 215 pots
 max-conn 6
 answer-address 188.....
 destination-pattern #2003088.....
 port 0:2
 prefix 88
!
dial-peer voice 216 pots
 max-conn 6
 answer-address 189.....
 destination-pattern #2003089.....
 port 0:2
 prefix 89
```

```
!
dial-peer voice 217 pots
 max-conn 6
 answer-address 190.....
 destination-pattern #2003090.....
 port 0:2
 prefix 90
!
dial-peer voice 218 pots
 max-conn 6
 answer-address 196.....
 destination-pattern #2003096.....
 port 0:2
 prefix 96
!
dial-peer voice 219 pots
 max-conn 6
 answer-address 197.....
 destination-pattern #2003097.....
 port 0:2
 prefix 97
!
dial-peer voice 220 pots
 max-conn 6
```

```
 answer-address 198.....
 destination-pattern #2003098.....
 port 0:2
 prefix 98
!
dial-peer voice 221 pots
 max-conn 6
 answer-address 199.....
 destination-pattern #2003099.....
 port 0:2
 prefix 99
!
dial-peer voice 222 pots
 max-conn 16
 answer-address 180.....
 destination-pattern #2002080.....
 port 1:9
 prefix 80
!
dial-peer voice 223 pots
 max-conn 16
 answer-address 184.....
 destination-pattern #2002084.....
 port 1:9
```

```
 prefix 84
!
dial-peer voice 224 pots
 max-conn 16
 answer-address 186.....
 destination-pattern #2002086.....
 port 1:9
 prefix 86
!
dial-peer voice 225 pots
 max-conn 16
 answer-address 187.....
 destination-pattern #2002087.....
 port 1:9
 prefix 87
!
dial-peer voice 226 pots
 max-conn 16
 answer-address 188.....
 destination-pattern #2002088.....
 port 1:9
 prefix 88
!
dial-peer voice 227 pots
```

```
 max-conn 16
 answer-address 189.....
 destination-pattern #2002089.....
 port 1:9
 prefix 89
!
dial-peer voice 228 pots
 max-conn 16
 answer-address 190.....
 destination-pattern #2002090.....
 port 1:9
 prefix 90
!
dial-peer voice 229 pots
 max-conn 16
 answer-address 196.....
 destination-pattern #2002096.....
 port 1:9
 prefix 96
!
dial-peer voice 231 pots
 max-conn 16
 answer-address 198.....
 destination-pattern #2002098.....
```

```
 port 1:9
 prefix 98
!
dial-peer voice 232 pots
 max-conn 16
 answer-address 199.....
 destination-pattern #2002099.....
 port 1:9
 prefix 99
!
dial-peer voice 230 pots
 max-conn 16
 answer-address 197.....
 destination-pattern #2002097.....
 port 1:9
 prefix 97
!
dial-peer voice 244 pots
 max-conn 4
 answer-address 180.....
 destination-pattern #2005080.....
 port 0:4
 prefix 80
!
```

```
dial-peer voice 245 pots
 max-conn 4
 answer-address 184.....
 destination-pattern #2005084.....
 port 0:4
 prefix 84
!
dial-peer voice 246 pots
 max-conn 4
 answer-address 186.....
 destination-pattern #2005086.....
 port 0:4
 prefix 86
!
dial-peer voice 247 pots
 max-conn 4
 answer-address 187.....
 destination-pattern #2005087.....
 port 0:4
 prefix 87
!
dial-peer voice 248 pots
 max-conn 4
 answer-address 188.....
```

```
 destination-pattern #2005088.....
 port 0:4
 prefix 88
!
dial-peer voice 249 pots
 max-conn 4
 answer-address 189.....
 destination-pattern #2005089.....
 port 0:4
 prefix 89
!
dial-peer voice 250 pots
 max-conn 4
 answer-address 190.....
 destination-pattern #2005090.....
 port 0:4
 prefix 90
!
dial-peer voice 251 pots
 max-conn 4
 answer-address 196.....
 destination-pattern #2005096.....
 port 0:4
 prefix 96
```

```
!
dial-peer voice 252 pots
 max-conn 4
 answer-address 197.....
 destination-pattern #2005097.....
 port 0:4
 prefix 97
!
dial-peer voice 253 pots
 max-conn 4
 answer-address 198.....
 destination-pattern #2005098.....
 port 0:4
 prefix 98
!
dial-peer voice 254 pots
 max-conn 4
 answer-address 199.....
 destination-pattern #2005099.....
 port 0:4
 prefix 99
!
dial-peer voice 255 pots
 max-conn 4
```

```
 answer-address 180.....
 destination-pattern #2006080.....
 port 0:5
 prefix 80
!
dial-peer voice 256 pots
 max-conn 4
 answer-address 184.....
 destination-pattern #2006084.....
 port 0:5
 prefix 84
!
dial-peer voice 257 pots
 max-conn 4
 answer-address 186.....
 destination-pattern #2006086.....
 port 0:5
 prefix 86
!
dial-peer voice 258 pots
 max-conn 4
 answer-address 187.....
 destination-pattern #2006087.....
 port 0:5
```

```
 prefix 87
!
dial-peer voice 259 pots
 max-conn 4
 answer-address 188.....
 destination-pattern #2006088.....
 port 0:5
 prefix 88
!
dial-peer voice 260 pots
 max-conn 4
 answer-address 189.....
 destination-pattern #2006089.....
 port 0:5
 prefix 89
!
dial-peer voice 261 pots
 max-conn 4
 answer-address 190.....
 destination-pattern #2006090.....
 port 0:5
 prefix 90
!
dial-peer voice 262 pots
```

```
 max-conn 4
 answer-address 196.....
 destination-pattern #2006096.....
 port 0:5
 prefix 96
!
dial-peer voice 263 pots
 max-conn 4
 answer-address 197.....
 destination-pattern #2006097.....
 port 0:5
 prefix 97
!
dial-peer voice 264 pots
 max-conn 4
 answer-address 198.....
 destination-pattern #2006098.....
 port 0:5
 prefix 98
!
dial-peer voice 265 pots
 max-conn 4
 answer-address 199.....
 destination-pattern #2006099.....
```

```
 port 0:5
 prefix 99
!
dial-peer voice 500 pots
 max-conn 1
 answer-address 19.....
 destination-pattern #200409.....
 port 0:7
 prefix 9
!
dial-peer voice 501 pots
 max-conn 1
 answer-address 18.....
 destination-pattern #200408.....
 port 0:7
 prefix 8
!
dial-peer voice 502 pots
 max-conn 1
 incoming called-number 18443129
 destination-pattern 18.....
 direct-inward-dial
 port 0:6
 prefix 1
```

```
!
dial-peer voice 503 pots
 max-conn 1
 incoming called-number 18443129
 destination-pattern 19.....
 direct-inward-dial
 port 0:6
 prefix 1
!
dial-peer voice 266 pots
 max-conn 12
 answer-address 180.....
 destination-pattern #2007080.....
 port 1:8
 prefix 80
!
dial-peer voice 267 pots
 max-conn 12
 answer-address 184.....
 destination-pattern #2007084.....
 port 1:8
 prefix 84
!
dial-peer voice 268 pots
```

```
 max-conn 12
 answer-address 186.....
 destination-pattern #2007086.....
 port 1:8
 prefix 86
!
dial-peer voice 269 pots
 max-conn 12
 answer-address 187.....
 destination-pattern #2007087.....
 port 1:8
 prefix 87
!
dial-peer voice 270 pots
 max-conn 12
 answer-address 188.....
 destination-pattern #2007088.....
 port 1:8
 prefix 88
!
dial-peer voice 271 pots
 max-conn 12
 answer-address 189.....
 destination-pattern #2007089.....
```

```
 port 1:8
 prefix 89
!
dial-peer voice 272 pots
 max-conn 12
 answer-address 190.....
 destination-pattern #2007090.....
 port 1:8
 prefix 90
!
dial-peer voice 273 pots
 max-conn 12
 answer-address 196.....
 destination-pattern #2007096.....
 port 1:8
 prefix 96
!
dial-peer voice 274 pots
 max-conn 12
 answer-address 197.....
 destination-pattern #2007097.....
 port 1:8
 prefix 97
!
```

```
dial-peer voice 275 pots
 max-conn 12
 answer-address 198.....
 destination-pattern #2007098.....
 port 1:8
 prefix 98
!
dial-peer voice 276 pots
 max-conn 12
 answer-address 199.....
 destination-pattern #2007099.....
 port 1:8
 prefix 99
!
dial-peer voice 277 pots
 max-conn 4
 answer-address 163.....
 destination-pattern #2006063.....
 port 0:5
 prefix 63
!
dial-peer voice 278 pots
 max-conn 4
 answer-address 164.....
```

```
 destination-pattern #2006064.....
 port 0:5
 prefix 64
!
dial-peer voice 279 pots
 max-conn 6
 answer-address 163.....
 destination-pattern #2003063.....
 port 0:2
 prefix 63
!
dial-peer voice 280 pots
 max-conn 6
 answer-address 164.....
 destination-pattern #2003064.....
 port 0:2
 prefix 64
!
dial-peer voice 281 pots
 max-conn 16
 answer-address 163.....
 destination-pattern #2002063.....
 port 1:9
 prefix 63
```

```
!
dial-peer voice 282 pots
 max-conn 16
 answer-address 164.....
 destination-pattern #2002064.....
 port 1:9
 prefix 64
!
dial-peer voice 283 pots
 max-conn 4
 answer-address 163.....
 destination-pattern #2005063.....
 port 0:4
 prefix 63
!
dial-peer voice 284 pots
 max-conn 4
 answer-address 164.....
 destination-pattern #2005064.....
 port 0:4
 prefix 64
!
dial-peer voice 285 pots
 max-conn 12
```

```
 answer-address 163.....
 destination-pattern #2007063.....
 port 1:8
 prefix 63
!
dial-peer voice 286 pots
 max-conn 12
 answer-address 164.....
 destination-pattern #2007064.....
 port 1:8
 prefix 64
!
dial-peer voice 287 pots
 max-conn 4
 answer-address 163.....
 destination-pattern #2006063.....
 port 0:5
 prefix 63
!
dial-peer voice 288 pots
 max-conn 4
 answer-address 164.....
 destination-pattern #2006064.....
 port 0:5
```

```
 prefix 64
!
!
!
interface Loopback0
 ip address 192.162.62.62 255.255.255.255
!
interface Loopback1
 ip address 192.162.60.11 255.255.255.255
!
interface Ethernet0
 ip address 192.162.61.62 255.255.255.0
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
 clockrate 2015232
!
interface Serial1
 no ip address
 shutdown
 no fair-queue
 clockrate 2015232
```

```
!
interface Serial2
 no ip address
 shutdown
 no fair-queue
 clockrate 2015232
!
interface Serial3
 no ip address
 shutdown
 no fair-queue
 clockrate 2015232
!
interface FastEthernet0
 ip address 192.162.160.62 255.255.255.0
 duplex full
 speed 100
!
router rip
 version 2
 network 10.0.0.0
 network 192.162.0.0
!
 ip classless
```

ip route 0.0.0.0 0.0.0.0 192.162.40.2

ip route 10.226.104.0 255.255.248.0 192.162.40.33

ip route 192.162.40.0 255.255.255.0 192.162.40.10

ip route 192.162.40.0 255.255.255.0 192.162.160.10

ip route 192.162.100.0 255.255.255.0 192.162.40.33

ip route 192.162.110.0 255.255.255.0 192.162.40.33

ip route 192.162.120.0 255.255.255.0 192.162.40.33

ip route 192.162.130.0 255.255.255.0 192.162.40.33

ip route 192.162.140.0 255.255.255.0 192.162.40.33

ip route 192.162.150.0 255.255.255.0 192.162.40.33

ip route 192.162.190.8 255.255.255.252 192.162.40.33

ip route 192.162.191.0 255.255.255.0 192.162.40.33

ip route 192.162.192.0 255.255.255.0 192.162.40.33

ip route 192.162.193.0 255.255.255.0 192.162.40.33

ip route 192.162.194.0 255.255.255.0 192.162.40.33

ip route 192.162.197.0 255.255.255.0 192.162.40.33

no ip http server

access-list 1 permit 10.10.108.108

access-list 1 permit 10.10.107.79

access-list 1 permit 192.162.110.2

access-list 2 permit 10.10.108.108

snmp-server engineID local 0000000902000030943 3E074

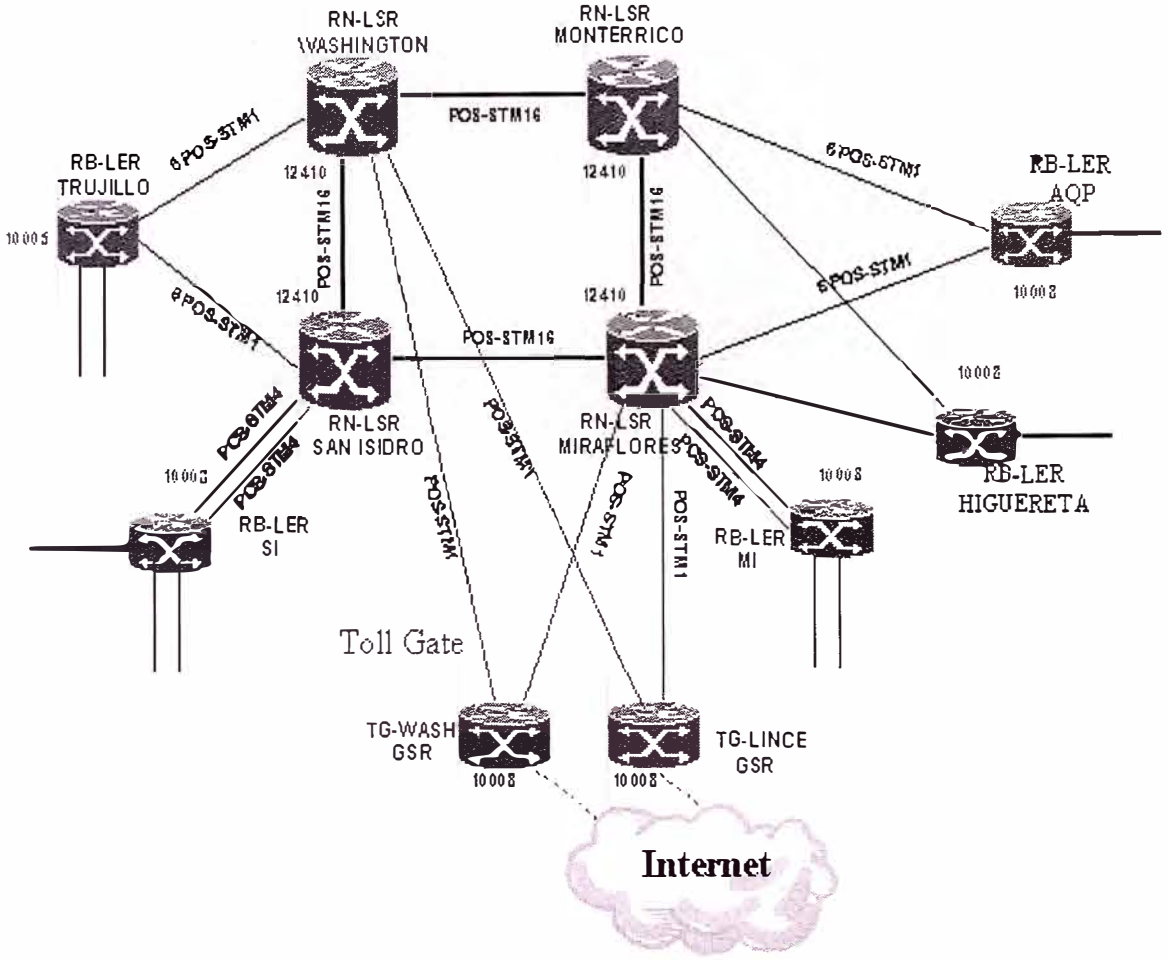
```
snmp-server community mplschimu view v1default RO
snmp-server community moviles RO
snmp-server community ComMovCorp
snmp-server community public RO
snmp-server community private RW
snmp-server community Nebula view v1default RO
snmp-server trap-source FastEthernet0
snmp-server contact CGRC-IP-VPN
snmp-server system-shutdown
snmp-server enable traps snmp
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps config
snmp-server enable traps envmon
snmp-server enable traps frame-relay
snmp-server enable traps syslog
snmp-server enable traps voice poor-qov
snmp-server host 10.10.65.142 Nebula
snmp-server host 10.12.25.2 mplschimu
snmp-server host 192.162.150.59 public
!
banner exec ^C


!
```

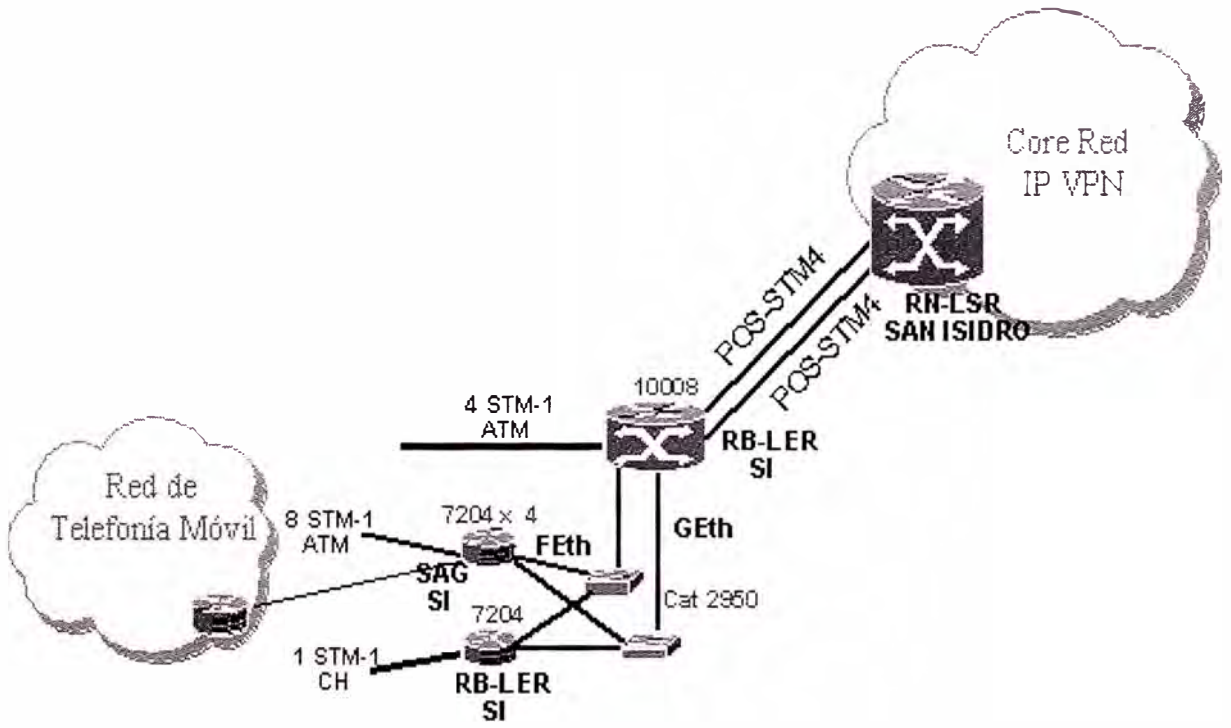
```
line con 0
 password 7 14141B180F0B
 transport input none
line aux 0
line vty 0 4
 exec-timeout 10 30
 password 7 111D1C09121404020D292A
!
ntp clock-period 17180527


end
```

ANEXO C

DIAGRAMAS DEL NUCLEO DE LA RED IP VPN MPLS

Core RED IP VPN




Core Red
IP VPN
RN-LSR
SAN ISIDRO
POS-STM4
POS-STM4
10008
RB-LER
SI
4 STM-1
ATM
Red de
Telefonía Móvil
8 STM-1
ATM
7204 x 4
FEth
SAG
SI
GEth
Cat 2950
7204
1 STM-1
CH
RB-LER
SI

BIBLIOGRAFÍA

[1] BLACK, U.. Voice over IP. New Jersey: Prentice Hall PTR. (1999)

[2] Andew S. Tanenbaum, “Redes de Computadoras”, Prentice Hall, México. (1997).

[3] DOUSKALIS, B. IP telephony: the integration of robust VoIP services. New Jersey: Prentice Hall PTR. (2000).

[4] Huitema, C. “IPv6 The New Internet Protocol”, Prentice Hall, Inglaterra. (1996).

[5] HAMDI, M., VERSCHEURE, O., HUBAUX, J-P., DALGIC, I. y WANG, P.Voice Service Interworking for PSTN and IP Networks. IEEE Communication Magazine, Mayo 1999,

[6] HERSENT,O., GURLE, D. y PETIT, J.P. IP telephony: packet – based multimedia communication systems. Great Britain: Addison – Wesley. (2000).

[7] ITU-T Study Group 16. Recommendation H.323v4 (draft). Noviembre 2000.

[8] Lackerbauer, I., “Internet”, Marcombo S.A., España, 2001.

[9] Piscitello,D.M., and Chapin, A.L., “Open System Networking”, Addison Weslwy, 1998.

[10] . MINOLI, D. y MINOLI, EDelivering Voice over IP Networks. New York: John Wiley & Sons, Inc. . (1998).

[11] Guichard Jim, “MPLS and VPN Architecture: A prectical guide to understanding, designing and deploying MPLS and MPLS-Enabled VPNs”, Cisco Press, 2001

[12] Osborne Eric., “Traffic Engineering with MPLS ”, Cisco Press, 2000