



Universidad Austral de Chile

Facultad de Ciencias de la Ingeniería

Escuela de Electricidad y Electrónica

“DISEÑO DE UNA VPN Y VOIP PARA UNA PYME A NIVEL NACIONAL”.

Tesis para optar al título de:
Ingeniero en Electrónica

Profesor Patrocinante:
Sr. Néstor Fierro Morineaud.
Ingeniero Electrónico,
Licenciado en Ciencias de la Ingeniería,
Diplomado en Ciencias de la Ingeniería.

ARIEL HUMBERTO ROMERO VARGAS

VALDIVIA – CHILE

2009

MIEMBROS COMISIÓN DE TITULACIÓN

Profesor Patrocinante Néstor Fierro Morineaud Ingeniero Electrónico
--

Profesor Informante Franklin Castro Ingeniero Electrónico
--

Profesor Informante Pedro Rey Clericus Ingeniero Electrónico

*“A mi familia, especialmente a mis padres y hermanos por su apoyo incondicional,
a todos los que me han ayudado de una u otra forma en este proceso
y en general a quien se alegre por este paso”*

INDICE

RESUMEN_____	X
ABSTRACT_____	X
INTRODUCCION_____	XI
PLANTEAMIENTO DEL PROYECTO_____	XII
OBJETIVOS GENERALES_____	XIV
OBJETIVOS ESPECÍFICOS_____	XIV

CAPÍTULO I. TECNOLOGÍA DE REDES PRIVADAS VIRTUALES

1.1 INTRODUCCIÓN_____	15
1.2 DEFINICIÓN VPN_____	16
1.3 VENTAJAS VPN_____	17
1.4 TIPOS DE ESTRUCTURAS VPN_____	18
1.5 PROCESO DE TÚNELES VPN_____	20

1.5.1 DESCRIPCIÓN TUNNELING	20
1.5.2 TECNOLOGÍAS DE TUNNELING	21
1.5.3 FUNCIONAMIENTO DE LOS TÚNELES	22
1.5.4 PROTOCOLOS DE TÚNELES	23
1.6 RESUMEN	53
 CAPÍTULO II. TECNOLOGÍA DE VOZ SOBRE IP (VOIP)	
2.1 INTRODUCCIÓN	55
2.2 DEFINICIÓN VOIP	56
2.3 PROCESAMIENTO DE LA VOZ	56
2.3.1 CODIFICACIÓN DE LA VOZ	57
2.4 PROTOCOLOS VOIP	60
2.4.1 INTRODUCCIÓN	60
2.4.2 CLASIFICACIÓN DE LOS PROTOCOLOS	60
2.4.3 PROTOCOLOS DE SEÑALIZACIÓN EN VOIP	62
2.5 PROTOCOLOS DE TRANSPORTE DE VOIP	79
2.6 RESUMEN	81

CAPÍTULO III. SEGURIDAD EN REDES VPN

3.1 INTRODUCCIÓN	82
3.2 ANÁLISIS DE RIESGO	83
3.3 OBJETIVOS CLAVE	83
3.4 IDENTIFICACIÓN DE LAS AMENAZAS	84
3.5 PROTOCOLOS DE SEGURIDAD	85
3.5.1 SERVICIOS DE SEGURIDAD TLS	85
3.5.2 SERVICIOS DE SEGURIDAD IPSEC	86
3.6 MÉTODOS DE AUTENTICACIÓN	88
3.6.1 CERTIFICADO DIGITAL	88
3.6.2 FUNCIONES HASH	89
3.6.3 ETOKEN	90
3.7 PROTECCIÓN DE LA INFORMACIÓN POR SOFTWARE	92
3.7.1 CRIPTOGRAFÍA	92
3.7.2 CLAVE PRIVADA (SIMÉTRICA)	93
3.7.3 CLAVE PÚBLICA (ASIMÉTRICA)	96
3.8 FIREWALL	98
3.8.1 FUNCIONES PRINCIPALES DE UN FIREWALL	99

3.9 RESUMEN_____	100
------------------	-----

CAPITULO IV. SEGURIDAD EN VOIP

4.1 INTRODUCCIÓN_____	101
-----------------------	-----

4.2 ANÁLISIS GENERAL_____	101
---------------------------	-----

4.3 CLASIFICACIÓN DE LOS ATAQUES_____	104
---------------------------------------	-----

4.3.1 ACCESOS DESAUTORIZADOS Y FRAUDES_____	105
---	-----

4.3.2 VULNERABILIDADES DE LA RED SUBYACENTE_____	105
--	-----

4.3.3 ATAQUES DE DENEGACIÓN DE SERVICIO (DOS)_____	106
--	-----

4.3.4 ATAQUES A LOS DISPOSITIVOS_____	107
---------------------------------------	-----

4.3.5 DESCUBRIMIENTO Y ENUMERACIÓN_____	108
---	-----

4.3.6 ATAQUES A NIVEL DE APLICACIÓN_____	108
--	-----

4.3.7 ATAQUES DE LA SEÑALIZACIÓN_____	109
---------------------------------------	-----

4.3.8 MANIPULACIÓN DE LA TRANSMISIÓN_____	112
---	-----

4.4 MEDIDAS DE SEGURIDAD PARA LA RED VOIP_____	115
--	-----

CAPITULO V. CALIDAD DE SERVICIO EN VOIP

5.1 INTRODUCCIÓN_____	117
-----------------------	-----

5.2 DEFINICIÓN_____	117
---------------------	-----

5.3 CLASIFICACIÓN DE QOS_____	118
-------------------------------	-----

5.4 CLASIFICACIÓN Y PRIORIZACIÓN DE LA INFORMACIÓN_____	119
---	-----

5.5 PARÁMETROS DE LA QOS	120
5.5.1 RETARDO O LATENCIA	120
5.5.2 JITTER	125
5.5.3 ECO	126
5.5.4 PERDIDAS DE PAQUETES	127
5.6 SUPRESIÓN DE SILENCIO Y RUIDOS	129
5.7 QOS EN VOIP SOBRE VPN	129
5.8 RESUMEN	130

CAPITULO VI. EQUIPAMIENTO REQUERIDO PARA LA IMPLEMENTACIÓN DEL PROYECTO

6.1 INTRODUCCIÓN	131
6.2 SELECCION DEL PROVEEDOR DE TECNOLOGÍA	131
6.3 PARÁMETROS A CONSIDERAR	133
6.4 SEGURIDAD CISCO	133
6.5 QOS EN CISCO	137
6.6 COSTO VS BENEFICIO	139
6.7 SOFTWARE CISCO IOS	139
6.8 DESCRIPCIÓN DEL PROYECTO	141

6.8.1 DIMENSIONES DEL PROYECTO_____	142
6.8.2 EQUIPAMIENTO SELECCIONADO_____	145
6.8.3 DIAGRAMA DE LA RED_____	157
6.9 RESUMEN_____	158
 CAPÍTULO VII. ESTUDIO DE COSTOS	
7.1 INTRODUCCIÓN_____	159
7.2 DESCRIPCIÓN_____	160
7.3 COSTOS DE IMPLEMENTACIÓN_____	162
7.3.1 EQUIPAMIENTO_____	163
7.3.2 GASTOS RECURSO HUMANO_____	164
 CAPÍTULO VIII. CONCLUSIONES_____	 165
REFERENCIAS BIBLIOGRAFICAS_____	167

RESUMEN

Actualmente la red de Internet se ha transformado en una potente herramienta para complementar las funciones de la empresa y PYME¹, brindando ventajas para sus procesos operativos, además de fomentar las opciones de marketing para dar a conocer sus servicios a un mercado global.

Los servicios de comunicación que brinda Internet en la PYME son variados, incluyendo voz, video y datos, sin embargo las amenazas de seguridad opacan en parte dichas ventajas, por lo que en este Trabajo de Titulación se realiza un diseño de una red de voz y datos, teniendo como puntal principal la seguridad de la información que por ella transitan, considerando la mitigación y prevención de los principales ataques que afectan hoy en día la comunicación a través de Internet.

ABSTRACT

Currently the Internet has become a powerful tool to complement the functions of the enterprise and PYMEs, providing benefits to their business processes, and promote options for marketing to publicize its services to a global market.

The communication services offered by the Internet in PYMEs are diverse, including voice, video and data, however, security threats partly obscure these advantages, so this paper of degree is a design of a voice and data network, taking as the main prop up the information that pass by it, considering the mitigation and prevention of major attacks that affect today's communication through the Internet.

¹ PYME: Pequeña Y Mediana Empresa.

INTRODUCCION

Las comunicaciones, actualmente, juegan un papel fundamental dentro de las empresas y microempresas (PYMEs) para mejorar la productividad de sus procesos. En particular, los sistemas telefónicos y de redes de datos son muy utilizados dentro de dicho contexto, sin embargo dicha descripción separada de servicios está evolucionando hacia el concepto de redes convergentes, donde todo el flujo de información transita por redes de datos.

Un punto muy importante y que no se debe menospreciar es la seguridad de la red, ya que en una empresa los datos que se desean transmitir son muchas veces confidenciales y de vital importancia, por lo que en manos de la competencia pueden traer muy malas consecuencias.

Tradicionalmente los servicios de telefonía y de datos han estado soportados por redes distintas, basadas en tecnologías muy diferentes. Para el transporte del tráfico de voz se han utilizado hasta ahora las redes telefónicas clásicas, basadas en las técnicas de conmutación de circuitos, especialmente adaptadas a las características del tráfico de voz, caracterizado por un flujo constante de información. Por el contrario, el tráfico de datos, se caracteriza en general por la falta de continuidad, generalmente denominado “tráfico a ráfagas” y además por su impredecibilidad. Es por ello que las técnicas de conmutación de paquetes, en las cuales la información se divide en unidades de información, denominados “paquetes”, que se transmiten típicamente sin que exista una reserva de recursos a priori, se adaptan mucho mejor a este tipo de tráficos.

Actualmente el desarrollo y maduración de las técnicas de transmisión de voz sobre redes de paquetes ha dado lugar a una fuerte tendencia hacia la integración de los servicios. Esta tendencia recibe el nombre de “convergencia de redes” o “convergencia de voz y datos”, incluyéndose también servicios de video.

PLANTEAMIENTO DEL PROYECTO

La idea de realizar este Proyecto de Titulación surgió por la creciente necesidad que existe actualmente de comunicación en la empresa, esto sumado a la expansión que están experimentando las PYMEs en nuestro país, lo que les da acceso a tecnologías innovadoras y los beneficios que ellas otorgan. Muchas veces estos beneficios se ven opacados por las amenazas de seguridad que afectan a estas tecnologías, sin embargo lo que se busca en este Trabajo de Titulación es prevenir estos ataques, haciéndola segura y confiable para la empresa que desee incursionar en este campo.

Lo primero que debemos tener claro es la clasificación de las PYMEs. Es aquí donde entra el Ministerio de Economía, quien clasifica las empresas de acuerdo al nivel de ventas, considerando como Empresas Pequeñas a las que venden entre UF 2.400 y UF 25.000 al año y como Empresas Medianas las que venden más de UF 25.000 al año pero menos que UF 100.000. Esto implica que en términos de ventas anuales se define como PYMES a las empresas que se encuentran en el rango de UF 2.400 y UF 100.000.

La tecnología mas apta para cumplir con los requerimientos de seguridad del diseño es una Red Privada Virtual o VPN², la cual permite "perforar" una red pública y navegar en ésta como si estuvieran en su propia oficina. Actualmente ya se cuentan con las herramientas necesarias para lograr este propósito y es una llamativa ventaja que tiene esta tecnología para las empresas que requieren de tal servicio, dando movilidad a sus trabajadores a un costo bastante accesible y sin descuidar la seguridad de la información de su red corporativa.

Las aplicaciones VoIP³ ofrecen para la PYME innumerables beneficios tanto económicos como productivos, tales como la posibilidad de colaborar con miembros del equipo, estar conectados con clientes, vendedores y a co-trabajadores en tiempo real, sin importar la ubicación geográfica, esto gracias a que las VPN se implementan usando protocolos especiales que le

² VPN: Virtual Private Network

³ VoIP: Voz sobre IP

permiten a los usuarios comunicarse de manera segura y comprobar que la transmisión se hace desde una fuente confiable, por lo que juntas son una herramienta muy potente para el aumento de la productividad en la empresa.

Este Proyecto Titulación contempla realizar el diseño, con su respectivo estudio técnico y económico, de una Red Privada Virtual con servicios de Voz Sobre IP para una PYME que cuenta con su Casa Matriz en la ciudad de Santiago y además tiene sucursales en ocho capitales regionales de Chile. Para ello se realizará un estudio de los distintos protocolos utilizados actualmente para la implementación de las VPNs, dando énfasis a sus características en cuanto a seguridad de la información que se transmite por la red pública, para poder tomar la mejor decisión en cuanto a él o los protocolos que se utilizarán finalmente para el diseño. Además se estudiarán los distintos protocolos que permiten la comunicación VoIP, codificadores de voz, gestión de calidad de servicio, estudio de las marcas líderes en equipamiento de redes y sus equipamientos compatibles con los requerimientos del diseño y su respectivo estudio de costos para una posible implementación del proyecto..

OBJETIVOS

OBJETIVOS GENERALES

- Diseñar una red privada de datos con altos niveles de seguridad, que sea capaz de comunicar las sucursales de una PYME a nivel nacional.
- Diseñar una red privada de VoIP que comunique las sucursales de una PYME a nivel nacional.

OBJETIVOS ESPECIFICOS

- Diseñar una red privada virtual (VPN), que comunique las sucursales de una PYME con altos estándares de seguridad.
- Buscar las alternativas más factibles para cumplir con los requerimientos de seguridad que se buscan para dicha red, ya sea tanto por software o hardware.
- Proyectar una red de VoIP con altos niveles de seguridad que comunique las sucursales de una PYME a nivel nacional.
- Realizar un estudio de los costos involucrados para la implementación del proyecto.

CAPÍTULO I. TECNOLOGÍA DE REDES PRIVADAS VIRTUALES (VPN)

1.1 INTRODUCCIÓN

Apenas iniciado el siglo XXI nos encontramos con un creciente aumento en la producción de las empresas y microempresas, esto debido principalmente al aumento de la demanda en el mercado, cada vez más exigente y competitivo, y de relacionarse simplemente con asuntos a nivel local, en este momento, están pensando en mercados y negocios a nivel global. Este fenómeno ha ocasionado una creciente expansión, tanto en la empresa como en las PYMEs, por lo que se ha hecho indispensable contar con medios de comunicación que se adecuen a sus requerimientos, tanto en calidad de servicio, seguridad y principalmente la reducción de los costos, ya que las empresa que deseen mantenerse vigentes en este competitivo mercado deberán buscar las opciones más adecuadas para reducir sus costos operativos, sin descuidar algunos aspectos fundamentales que les pueden jugar en contra para mejorar la producción.

Sin embargo esta necesidad de comunicación a acrecentado un problema que actualmente no es un secreto a voces y se ha convertido en una realidad muy temida por las empresas, la inseguridad en las redes de comunicación, por ello surgen las tecnologías en software y hardware que nos proporcionan mayor seguridad de la información que deseamos comunicar. Una tecnología que actualmente lleva la delantera en cuanto a seguridad y conectividad se refiere, son las VPN.

Las redes privadas virtuales deben su creciente popularidad al hecho que las empresas, especialmente las PYMEs, han buscado la posibilidad de utilizar una red pública, ampliamente extendida y de bajo costo como Internet para aumentar la movilidad, mejorar la productividad de los empleados y contribuir a su desarrollo, sin poner en juego la seguridad de la información corporativa.

Desde el punto de vista de un usuario, una VPN es una conexión de punto a punto entre su estación y un servidor corporativo, es decir, desconoce los procesos y mecanismos que hacen que se comuniquen ambos dispositivos, debido a que aparece como si los datos se estuvieran enviando sobre un enlace privado dedicado.

1.2 DEFINICIÓN VPN

Una Red Privada Virtual (VPN), en ingles Virtual Private Network es una red de información privada que hace uso de una infraestructura pública de telecomunicaciones, donde todos los usuarios pertenecientes a una misma VPN parecen estar en el mismo segmento de red, aún cuando estos puedan estar distribuidos por otras redes locales intercomunicadas a través de redes públicas. Esto lo logran al permitir que el cliente haga un túnel (tunneling) a través de Internet u otra red pública de tal forma que permita a los participantes del túnel disfrutar de la misma seguridad y funciones que antes sólo estaban disponibles en las redes privadas.

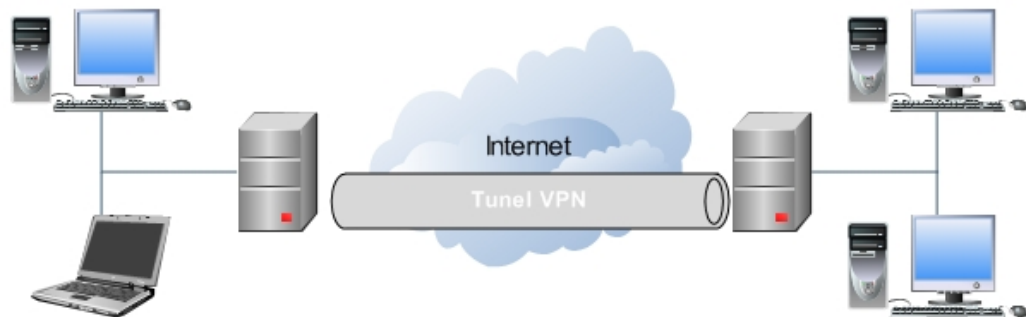


Figura 1. Red Privada Virtual

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación:

Autenticación y autorización. Se refiere a la persona o equipo que solicita autorización para formar parte de la red y el nivel de acceso que se le debe asignar, es decir, a qué contenidos o plataformas se le da autorización para ingresar.

Integridad. Esta se refiere a la garantía de que los datos enviados no han sido alterados, ya sea por efectos de la línea o alteraciones producto de la intromisión maliciosa de un usuario no autorizado, para lo cual se utilizan funciones de Hash⁴, las cuales abordaré posteriormente.

Confidencialidad. En vista de que los datos viajan a través de un medio potencialmente hostil como es Internet, los mismos son susceptibles de interceptación, por lo que es fundamental el proceso de cifrado. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma.

No repudio. Esto se refiere a que todo mensaje enviado por un usuario debe ir firmado, y el que lo firma no puede negar que el mensaje lo envió él. Esto se logra cuando se utiliza Firma Digital⁵ como medio de autenticación.

1.3 VENTAJAS VPN

Dentro de las ventajas de las cuales provee una VPN podemos destacar las siguientes:

Seguridad. Una de las principales ventajas que brinda una VPN es la seguridad, ya que realiza un proceso de encriptación y encapsulación de los datos, de manera que la información viaje codificada y a través de un túnel, dando confidencialidad e integridad de los paquetes que se transmiten. Otra ventaja en cuanto a seguridad es que gracias a la constante competencia que existe entre los protocolos de túneles por dominar el mercado VPN, éstos se siguen perfeccionando y a la vez se van creando nuevos protocolos.

Económica. Se ahorran grandes sumas de dinero en la implementación de costosas líneas dedicadas o enlaces físicos entre las estaciones que se desean comunicar.

⁴ Hash: Función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc.

⁵ Certificado Digital: Método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento.

Mejor administración. Es posible conseguir un mayor control de los usuarios y los niveles de accesos de cada uno de ellos a la red.

Funcionamiento. El control de acceso ayuda a los usuarios de poca experiencia a conectarse a redes corporativas, dándole acceso solo a los recursos que se considere apropiado por el administrador de la red.

1.4 TIPOS DE ESTRUCTURAS VPN

Las redes privadas virtuales se dividen en 3 categorías, de acuerdo con el servicio de conectividad que deseen brindar, de los cuales destacan:

VPN de Acceso Remoto (Remote Access VPNs). Esta categoría de VPNs provee acceso remoto a la intranet o extranet corporativa a través de una infraestructura pública, como lo es Internet, conservando las mismas políticas de seguridad y calidad de servicio.

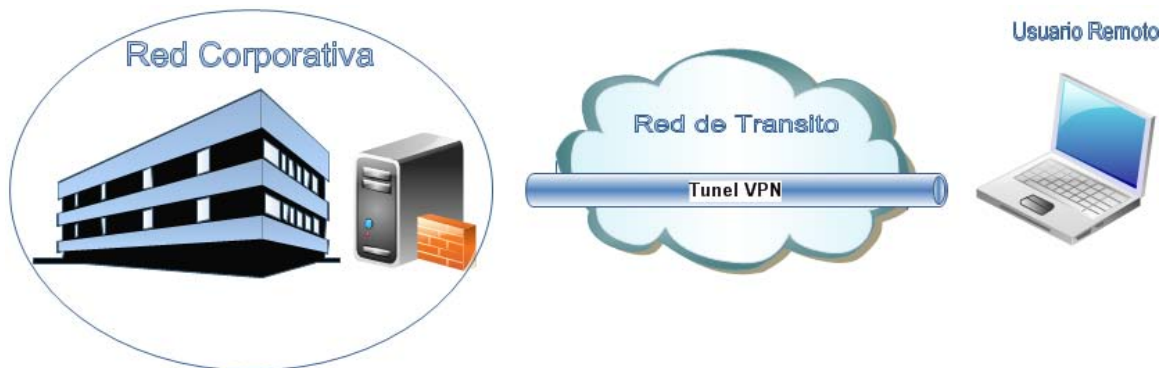


Figura 2. VPN de Acceso Remoto

VPN de Intranet (Site to Site). Esta categoría de VPN's vincula las oficinas remotas o sucursales a la red corporativa central, a través de una red pública, mediante un enlace dedicado al ISP⁶. En este caso la VPN goza de las mismas cualidades que la red privada tales como

⁶ ISP: Internet Service Provider

seguridad, calidad de servicio (QoS⁷) y fiabilidad, entre otras. Además extiende el modelo IP a través de la WAN⁸ compartida.

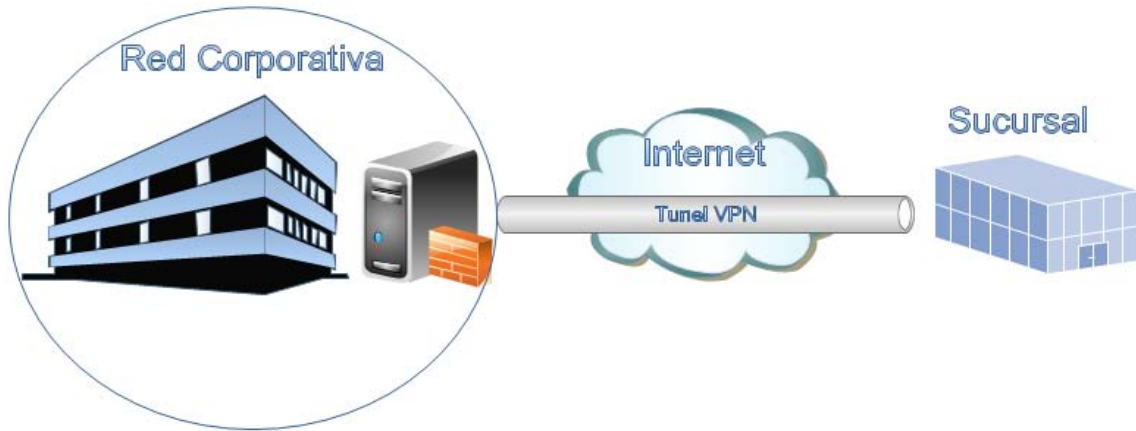


Figura 3. VPN de Intranet

VPN de Extranet. Esta opción permite la conexión de clientes, proveedores, distribuidores o demás comunidades de interés de la empresa a su intranet corporativa a través de una red pública, extendiendo la conectividad a sus usuarios. Además tienen la opción de asignar distintos niveles de acceso según lo determine el administrador.

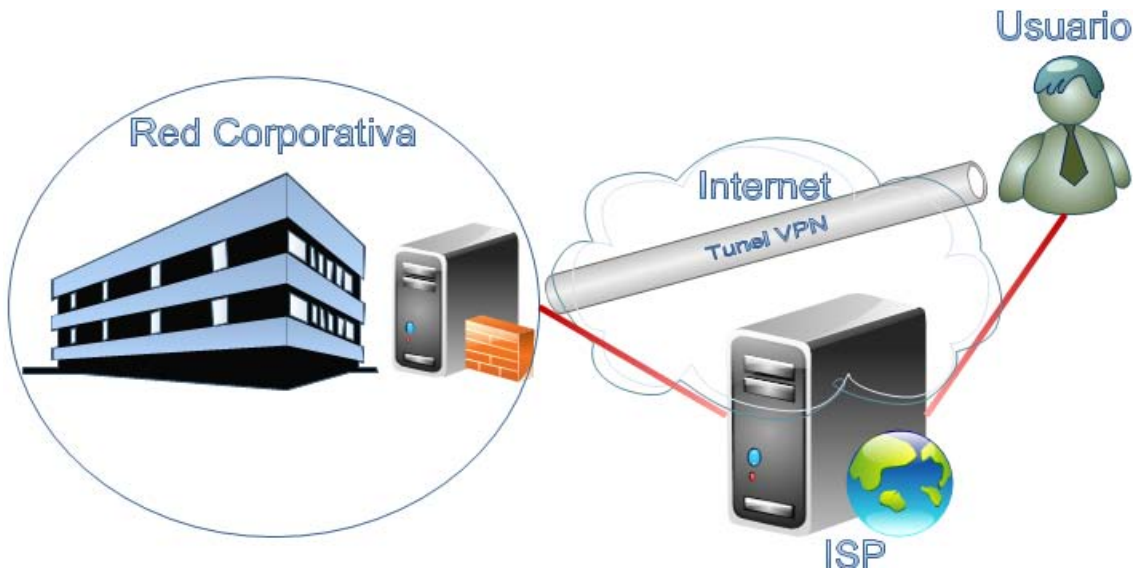


Figura 4. VPN de Extranet

⁷ QoS: Quality of Service

⁸ WAN: Wide Area Network

1.5 PROCESO DE TÚNELES VPN

Como se señaló anteriormente, una Red Privada Virtual se refiere a la creación de un túnel virtual a través de una red pública, donde se transmiten los datos de forma segura, mediante el encapsulado de paquetes, proceso al cual se denomina tunneling.

Esencialmente, tunneling se llama al proceso de encapsular un paquete dentro de otro paquete y enviarlo a través de la red, donde sólo el emisor y receptor conocen el protocolo de encapsulación. El proceso de tunneling comprende la encapsulación, transmisión a través de la red intermedia y desencapsulación del paquete al llegar a su destino para hacerlo legible.

Para que se pueda realizar satisfactoriamente el proceso de tunneling es necesario que tanto el emisor como el receptor utilicen el mismo protocolo de encapsulado, de lo contrario la información contenida en el paquete transportado no podrá ser descifrada por el receptor.

1.5.1 DESCRIPCIÓN TUNNELING

Como se explicó anteriormente, tunneling se llama al método de transporte de información, también denominada “carga útil”, a través de una red pública con un encapsulado adicional mediante un protocolo de tunneling. Para crear el túnel es preciso que un protocolo especial encapsule cada paquete origen en uno nuevo, que incluya los campos de control necesarios para crear, gestionar y deshacer el túnel una vez que la información llegue a su destino.

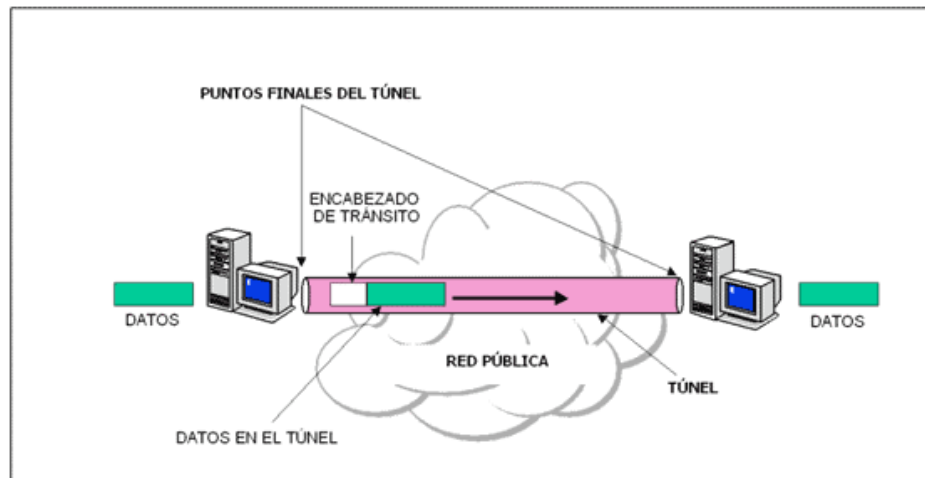


Figura 5. Proceso Tunneling

Existen dos opciones de túneles VPNs y son los siguientes:

Túneles voluntarios. El túnel voluntario se produce cuando una estación de trabajo o un Router utiliza un software de cliente de túnel para crear una conexión VPN con el servidor de túnel de destino. Para ello, debe instalar el protocolo de túnel correspondiente en el equipo cliente. Este tipo de túneles se puede utilizar para la autenticación, autorización y administración de cuentas.

Túneles obligatorios. El túnel obligatorio es la creación de un túnel seguro por parte de otro equipo o dispositivo de red en nombre del equipo cliente. Los túneles obligatorios se configuran y crean automáticamente para los usuarios sin que éstos intervengan ni tengan conocimiento de los mismos, por lo que el equipo del usuario no es un extremo de la conexión.

1.5.2 TECNOLOGÍAS DE TUNNELING

En un túnel VPN los datos que se desean transferir (carga útil) son encapsulados con un encabezado adicional, el cual proporciona la información de enrutamiento, con lo cual se pueden enviar los paquetes a través de la red hacia los puntos finales de la conexión. Una vez que las tramas encapsuladas llegan a su destino sobre la red se desencapsulan y se envían a su destino final.

Las tecnologías de túnel se basan principalmente en niveles 2 y 3 del modelo OSI⁹, existiendo algunas excepciones como lo veremos más adelante. Los protocolos de nivel 2 corresponden al nivel de enlace de datos y utilizan tramas como su unidad de intercambio. Una trama consta de una cabecera (header), datos (payload) y cola (trailer). La cola esta compuesta por un chequeo de errores y la cabecera contiene campos de control de protocolo.

Los protocolos de nivel 3 corresponden al nivel de la red y utilizan paquetes como unidades de intercambio. Estos protocolos encapsulan los paquetes IP en un encabezado adicional antes de enviarlos por la red IP. Un paquete está compuesto de forma muy similar a las tramas. A simple vista una trama y un paquete son iguales, sin embargo la diferencia reside en que los paquetes se crean en el nivel de red y se insertan dentro de una trama, la cual se crea en nivel de enlace.

1.5.3 FUNCIONAMIENTO DE LOS TÚNELES

Para las tecnologías de túnel de nivel 2, un túnel se asemeja a una sesión, es decir los dos puntos finales del túnel deben estar de acuerdo respecto al túnel y deben negociar las variables de la configuración tales como asignación de dirección o los parámetros de encriptación o de compresión. Además se utiliza un protocolo para mantenimiento del túnel como el mecanismo para administrar el mismo.

En las tecnologías de túnel de nivel 3 se supone que se han manejado todos los temas relacionados con la configuración, normalmente por medio de procesos manuales. Sin embargo, puede no haber una fase de mantenimiento del túnel.

Una vez creado el túnel VPN, el cliente envía una carga útil al servidor del túnel con un encabezado de protocolo de transferencia de datos. Los datos viajan encapsulados a través de la red, la cual lo enruta al servidor del túnel. Este acepta los paquetes, quita el encabezado del protocolo de transferencia de datos y envía la carga útil a la red objetivo.

⁹ OSI: Modelo de referencia de interconexión de sistemas abiertos

1.5.4 PROTOCOLOS DE TÚNELES

Es conocido que las tecnologías de túneles se pueden basar en las capas 2 (Capa de Enlace de Datos), 3 (Capa de Red) y 4 (Capa de Transporte) del modelo OSI.

La razón de la diversidad de protocolos es debido a que los usuarios que implementan VPNs tienen requerimientos diferentes, por lo que necesitan un protocolo que se amolde a sus necesidades.

1.5.4.1 PROTOCOLO DE TÚNEL PUNTO A PUNTO (PPTP)

PPTP¹⁰, definido en el RFC 2637, fue desarrollado por Microsoft para permitir la transferencia de datos desde un equipo remoto a un servidor privado, creando una red privada virtual a través de las redes de datos basadas en TCP/IP. Esta tecnología de gestión de redes es una extensión del protocolo PPP¹¹ definido en el RFC 1661.

PPTP es un protocolo de nivel 2, que encapsula paquetes PPP en datagramas IP, para transmitirlos por una red IP, diseñado principalmente para conexión de redes remotas. La comunicación se genera gracias a un túnel del tipo voluntario que trabaja en arquitecturas cliente-servidor.

1.5.4.1.1 PROTOCOLOS UTILIZADOS POR PPTP

Los protocolos utilizados por PPTP son los siguientes:

LCP (Protocolo de Control de Enlace). Éste protocolo se utiliza para la configuración, mantención y finalización de la conexión. Es el encargado de negociar los formatos de encapsulamiento, el

¹⁰ PPTP: Point to Point Tunneling Protocol

¹¹ PPP: Point to Point Protocol

tamaño de los paquetes a transmitir, la calidad del medio de transmisión y negociación de los protocolos a utilizar.

NCP (Protocolo de Configuración de Red). Se utiliza para la configuración de protocolos de red, para que luego los datagramas sean enviados por el medio físico.

GRE (Encapsulación Genérica de Ruteo). Este protocolo encapsula un paquete determinado dentro de un protocolo de transporte. En el caso más normal el sistema tiene un paquete, que debe ser encapsulado y ruteado, el cual se encapsula dentro del paquete GRE que también puede incluir la ruta del mismo, lo que provoca que el protocolo de transporte tome el paquete GRE y lo encapsule para su transmisión.

PPP (Protocolo Punto a Punto). PPP es un protocolo de nivel de enlace, definido en su versión más actualizada en el RFC 1661, que está relacionado a la pila TCP/IP y tiene como función principal, proporcionar un método estándar para el transporte de paquetes multiprotocolo. Este transporte se realiza entre dos pares que están a ambos extremos de la conexión VPN en este caso. Los mismos proveen de operación bidireccional y full-duplex.

PPP consta de las siguientes fases:

a) Establecimiento del enlace PPP. Durante esta fase, utiliza el protocolo de control de enlace (LCP).

b) Autenticación. En esta fase el cliente VPN envía las credenciales del usuario al servidor de acceso remoto. Existen dos protocolos de autenticación, el más básico e inseguro es PAP, aunque no se recomienda, dado que el nombre de usuario y la contraseña se envían en claro. Un método más avanzado es CHAP, en el cual la contraseña se manda cifrada.

c) Configuración de red. En esta tercera fase se negocian parámetros dependientes del protocolo de red que se esté utilizando. PPP puede llevar muchos protocolos de red al mismo

tiempo y es necesario configurar individualmente cada uno de ellos. Para configurar un protocolo de red se usa el protocolo NCP correspondiente.

d) Transmisión. Durante esta fase se envía y recibe la información de red. El protocolo de control de enlace (LCP) se encarga de comprobar que la línea esté activa durante períodos de inactividad.

e) Terminación. El enlace permanece configurado para la comunicación hasta que las tramas LCP o NCP cierran el enlace o hasta que se produzca algún hecho externo tal como el vencimiento de un temporizador de inactividad o la intervención de un usuario.

Protocolo de control de errores en Internet. Este protocolo se complementa con el IP. Se utilizan este tipo de mensajes para el aviso a los host de posibles anomalías en el ruteo de los paquetes.

IGMP (Protocolo de administración del grupo Internet). Este protocolo es parte del ICMP (Protocolo de Mensajes de Control de Internet) y se utiliza para intercambiar información acerca del estado de pertenencia entre routers IP que admiten multidifusión y miembros de grupos de multidifusión. Los hosts miembros individuales informan acerca de la pertenencia de hosts al grupo de multidifusión y los routers de multidifusión, además sondean periódicamente el estado de la pertenencia.

1.5.4.1.2 FUNCIONAMIENTO DE PPTP

La función de este protocolo es crear un túnel dentro de una red IP, para lo cual utiliza el protocolo GRE¹² en la encapsulación de los paquetes PPP.

PPTP nos permite separar las funciones de un servidor de acceso a la red (NAS) utilizando una arquitectura cliente-servidor. Estas funciones se dividen entre el PAC¹³ y el

¹² GRE: Generic Routing Encapsulation

PNS¹⁴, siendo el PAC un dispositivo conectado a una o más líneas PSTN¹⁵ o ISDN¹⁶ con la capacidad de operar con PPP y manejo del protocolo PPTP. El PAC solo necesita implementar TCP/IP para el paso del tráfico hacia una o mas PNS, además también puede trabajar con túneles en protocolos no IP. El PNS es un dispositivo que maneja del lado del servidor el protocolo PPTP. Como el PPTP cuenta con TCP/IP y es independiente de la interfaz de hardware utilizada, el PNS puede utilizar cualquier combinación de interfaces IP incluyendo periféricos de LAN y WAN.

La conexión con el servidor de VPN se puede realizar por medio de un ISP o bien una red con soporte TCP/IP.

1.5.4.1.3 FORMA DE CREACIÓN Y TRABAJO DEL TÚNEL

La conexión puede ser creada por el PNS o por el PAC, si bien no puede el protocolo PPTP distinguir entre el PAC y el PNS, si puede hacerlo entre el emisor y el receptor. El emisor es quien abre la primera conexión TCP.

En una transmisión PPTP, los paquetes no son transportados directamente por el túnel, se encapsulan en paquetes GRE que a su vez son encapsulados en IP. Este último será el que contenga la IP del servidor.

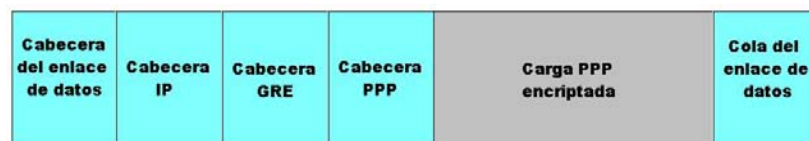


Figura 6. Datos del túnel PPTP

1.5.4.1.3 TRANSMISIÓN DE LOS DATOS PPTP

¹³ PAC: PPTP Access Concentrador

¹⁴ PNS: PPTP Access Server

¹⁵ PSTN: Public Switched Telephone Network

¹⁶ ISDN: Integrated Services Digital Network

Una vez que el túnel ha sido creado, los datos del usuario son transmitidos entre el cliente y el servidor PPTP. Como vimos en la figura anterior el envío se logra con múltiples niveles de encapsulación.

Los datos enviados por el cliente o servidor PPTP son primero, procesados y eliminadas las cabeceras y colas del enlace de datos. Posteriormente se procede a eliminar la cabecera IP, luego las cabeceras GRE y PPP, para poder descryptar, descomprimir o ambas, la carga PPP, si es necesario. Para finalizar se procesa la carga para la recepción o reenvío.

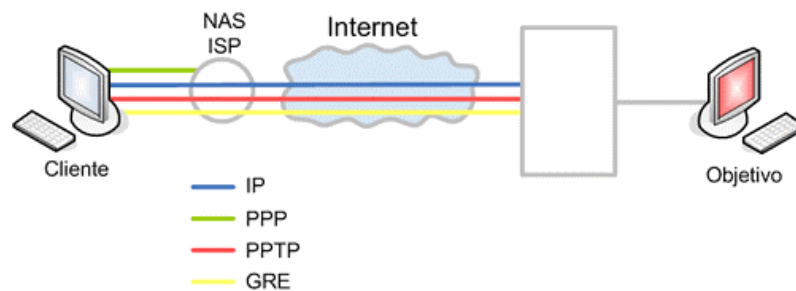


Figura 7. Transmisión de datos PPTP

1.5.4.2 PROTOCOLO L2F

1.5.4.2.1 INTRODUCCIÓN

Este es un protocolo desarrollado por Cisco¹⁷, definido en el RFC 2341 y difiere de PPTP en que permite que los túneles contengan más de una conexión. L2F¹⁸ fue diseñado para establecer túneles de tráfico desde usuarios remotos hasta sus sedes corporativas y es el precursor para el protocolo de túnel L2TP.

¹⁷ CISCO: www.cisco.com

¹⁸ L2F: Layer Two Forwarding

Como L2F es un protocolo de Nivel de enlace de datos según el Modelo de Referencia OSI, ofrece a los usuarios la misma flexibilidad que PPTP para manejar protocolos distintos a IP, como IPX¹⁹ o NetBEUI²⁰.

Además del protocolo PPP, L2F también implementa otros sistemas de autenticación de usuario como TACACS+²¹ y RADIUS²².

Este protocolo trabaja con un servicio de enlace llamado Virtual Dial-Up (VDU), que permite acceder a la utilización de toda la infraestructura de Internet, no solo para conectarse a través de diferentes protocolos al IP sino también cuando las direcciones IP no son reconocidas.

L2F también es capaz de encapsular payloads PPP o payloads SLIP que serán enviados a sus destinos. El protocolo SLIP (Serial Line Internet Protocol) es un estándar de transmisión de datagramas IP para líneas serie, pero que ha quedado bastante obsoleto debido a que fue diseñado para trabajar a través de puerto serie y conexión de módem.

1.5.4.2.2 PROTOCOLOS UTILIZADOS POR L2F

PAP (Protocolo de autenticación de password). Gracias a este protocolo, una vez establecida la conexión entre el servidor y el cliente, este último, envía el par formado por el nombre de usuario y la contraseña, luego se verificará la identidad del usuario y se autentifica o rechaza la petición, con lo cual la conexión será finalizada. Como se mencionó anteriormente este protocolo es muy inseguro debido a que envía el nombre de usuario y contraseña en claro.

CHAP (Protocolo de autenticación periódica del cliente). CHAP es un método de autenticación usado por servidores que utilizan el protocolo PPP. Este verifica periódicamente la identidad del cliente remoto. Esto ocurre cuando se establece el enlace inicial y puede pasar de nuevo en cualquier momento de la comunicación. La verificación se realiza de la siguiente forma:

¹⁹ IPX: Internet Packet Exchange

²⁰ NetBEUI: NetBIOS Extended User Interface, en español Interfaz extendida de usuario de NetBIOS

²¹ TACACS+: Terminal Access Controller Access Control System

²² Radius: Remote Authentication Dial-In User Service

- Después del establecimiento del enlace, el agente autenticador manda un mensaje que "desafía" al usuario.

- El usuario responde con un valor calculado usando una función hash de un sólo sentido.

- El autenticador verifica la respuesta con el resultado de su propio cálculo de la función hash. Si el valor coincide, el autenticador informa de la autenticación, de lo contrario termina la conexión.

A intervalos aleatorios el autenticador manda un nuevo "desafío" con lo que se repite el proceso.

1.5.4.2.3 CREACIÓN Y TRABAJO DEL TÚNEL

Para la creación del túnel L2F, el usuario remoto inicia la conexión PPP por medio de un ISP. Luego el NAS acepta la conexión y el enlace PPP es establecido, para que posteriormente el ISP realice los controles correspondientes de usuario por el protocolo CHAP o PAP según sea el caso.

El campo nombre de usuario es utilizado para determinar si se requiere un servicio de VDU por medio de los protocolos CHAP o PAP, además el ISP debe mantener una base de datos con los usuarios que utilicen el servicio.

Debido a que L2F no tiene un cliente definido y trabaja solo con túneles obligatorios, en caso de ser requerido el servicio designará un punto final del túnel. Si en cambio el servicio no debe ser dado se creará una conexión normal a Internet.

Si no existe un túnel en el extremo indicado, este debe ser inicializado, asignándole un Multiplex ID (MID) y un indicador de conexión al destino de la nueva VDU. En el caso de que el

túnel ya exista un MID no utilizado es asignado a la comunicación. El destino puede aceptar o rechazar este pedido, en este último caso se puede incluir en la respuesta la causa del rechazo.

Una vez creada la conexión se crea el túnel virtual para SLIP o PPP y se empieza a transmitir en ambas direcciones. En forma periódica se verificara que el par en la conexión este activo por medio del protocolo CHAP.

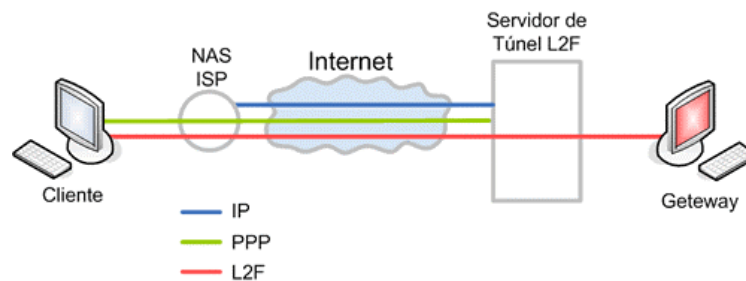


Figura 8. Transmisión de datos L2F

1.5.4.3 PROTOCOLO DE TÚNEL DE CAPA 2 (L2TP)

1.4.4.3.1 INTRODUCCIÓN

El protocolo L2TP²³ como su nombre lo indica trabaja en la capa 2 o capa de enlace de datos del modelo OSI. Fue diseñado por la IETF²⁴ y definido en el RFC 2661, como el heredero de los protocolos PPTP y L2F, creado para corregir las deficiencias de estos protocolos y establecerse como un estándar aprobado por dicha institución.

L2TP facilita el entunelamiento de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para sus aplicaciones.

²³ L2TP: Layer 2 Tunneling Protocol

²⁴ IETF: Internet Engineering Task Force

Este protocolo realiza un proceso de encapsulado, que permite el transporte de diferentes protocolos a través de un enlace punto a punto provisto por un NAS²⁵ con ISDN, ADSL²⁶ ó PSTN en el extremo de la conexión. Combina las mejores características de los protocolos PPTP y L2F.

L2TP Utiliza 2 tipos de Mensajes. Los primeros son los mensajes de Control, que se utilizan para el establecimiento, mantenimiento, y despeje de túneles y llamadas. Los otros son los mensajes de datos, los cuales son utilizados para encapsular las tramas PPP transportadas en el túnel.

Los Mensajes de Control utilizan un "Canal de Control Confiable" dentro de L2TP a fin de garantizar el transporte. Por su parte los Mensajes de Datos no son retransmitidos cuando hay pérdida de Paquetes.

Este protocolo requiere que haya conectividad entre los extremos del túnel, y además puede ser utilizado en una red IP utilizando UDP²⁷.

L2TP permite la creación de múltiples túneles entre dos puntos. Además de la posibilidad de crear distintos túneles para distintas QoS.

Una red que utiliza el protocolo L2TP está compuesta por dos partes, el Concentrador de Acceso (LAC) y el Servidor de Red (LNS). El LAC está ubicado entre un LNS y un sistema remoto y envía paquetes hacia ambos dispositivos. El LNS es el destino del LAC y un punto de finalización lógica de una sesión PPP hacia la cual se esta dirigiendo el túnel desde el sistema remoto por el LAC.

A diferencia de L2F, L2TP soporta dos modos de túneles, obligatorios y voluntarios.

²⁵ NAS: Network Attached Storage

²⁶ ADSL: Asymmetric Digital Subscriber Line

²⁷ UDP: User Datagram Protocol

El estándar permite que se pueda utilizar la seguridad de PPP para asegurar la comunicación sobre el túnel, brindando autenticación PPP, confidencialidad y cifrado PPP.

Una forma de complementar la seguridad de este protocolo es cuando los túneles L2TP aparecen como paquetes IP, ya que pueden aprovechar la seguridad IPsec, a la cual nos referiremos a continuación, gracias al cual pueden lograr una robusta protección de integridad, reproducción, autenticidad y privacidad. L2TP/IPsec, por lo tanto, proporciona túneles bien definidos e ínter operables, con la seguridad de alto nivel que brinda este protocolo.

Los términos más comunes utilizados en L2TP son:

LAC (L2TP Access Concentrador). En una conexión L2TP se añade un dispositivo LAC a los componentes físicos de la red conmutada o se incorpora un sistema de terminación PPP capaz de gestionar el protocolo L2TP. Un LAC solo necesita implementar el medio sobre el cual opera el L2TP para admitir el tráfico de una o mas LNS, además es capaz de tunelizar cualquier protocolo que incluya el PPP. Este dispositivo es el iniciador de las llamadas entrantes y el receptor de las llamadas salientes. En el protocolo L2F es llamado Servidor de Acceso a la Red.

LNS (L2TP Network Server). Un LNS es capaz de operar sobre cualquier plataforma con capacidad de terminación PPP. Este gestiona el lado del servidor del protocolo L2TP. Debido a que el LNS opera sobre el medio final del túnel L2TP, solo debe tener una única interfaz LAN o WAN. Este dispositivo es el encargado de iniciar las llamadas entrantes y además actúa como receptor de las llamadas salientes.

Servidor de Acceso a la red (Network Access Server). Este dispositivo proporciona a los usuarios acceso temporal a la red bajo demanda. Este acceso es punto a punto, de uso típico en las líneas de la red conmutada convencional.

1.5.4.3.2 FUNCIONAMIENTO DEL PROTOCOLO L2TP

Para establecer una conexión L2TP, primero el cliente inicia una conexión sobre una red privada remota a través de una red pública. Este establece una conexión con el punto de acceso de la red pública (LAC ó L2TP Access Concentrador), el cual inicia el establecimiento de un túnel L2TP contra el punto de acceso de la red privada LNS (L2TP Network Server). Una vez establecido el túnel, el cliente establece una sesión PPP contra el LNS, obteniendo acceso a la red privada.

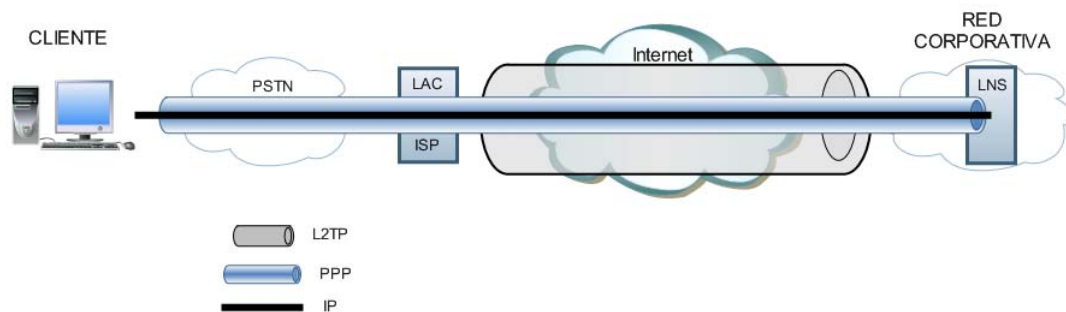


Figura 9. Funcionamiento L2TP

Inicio de sesión PPP en el LAC. En la etapa de inicio de sesión PPP en el LAC, el cliente inicia una conexión, iniciando la fase de negociación con el LAC, donde se realiza el proceso de autenticación. Dicha autenticación se realiza mediante los protocolos CHAP²⁸, PAP²⁹, MsCHAP³⁰, MS-CHAPv2 o EAP³¹.

Una vez que el LAC obtiene la información de la autenticación del usuario, es capaz de identificar la dirección IP del LNS y los parámetros que se negociarán. Dicha configuración debe realizarse de manera local en el LAC, también se puede delegar a un servidor RADIUS.

²⁸ CHAP: Challenge handshake Authentication Protocol

²⁹ PAP: Password Authentication Protocol

³⁰ MsCHAP: Challenge handshake authentication protocol

³¹ EAP: Extensible Authentication Protocol

Creación y autenticación del túnel. El LAC es el encargado de establecer el túnel L2TP contra el LNS utilizando la información recibida en la autenticación del usuario. El LNS y el LAC realizan la autenticación del otro extremo de la conexión, que en el caso de ser aceptada da lugar a la finalización de la negociación, con lo cual se establece el túnel a través del puerto 1701 de UDP.

En el caso de que exista un túnel previo a la negociación de un usuario que haya accedido a la red del mismo LAC, este paso se obvia y se utiliza el túnel existente para la conexión.

Establecimiento de la sesión de usuario. Una vez establecido el túnel se realiza el proceso del establecimiento de la sesión de usuario, para lo cual se debe establecer el protocolo LCP, luego de lo cual se realiza la autenticación y negociación de los parámetros IP. Por lo general este proceso incluye la negociación de una dirección IP y el establecimiento de una ruta en el LNS.

Luego de establecida la conexión, el cliente puede enviar sus paquetes IP, encapsulados sobre PPP. El paquete, originado por el cliente, es enviado al LAC, el cual lo introduce sin modificar el túnel, para luego alcanzar el LNS, donde se desencapsula el protocolo PPP para obtener nuevamente el paquete IP por el usuario.

1.5.4.4 PROTOCOLO DE SEGURIDAD EN IP (IPSEC)

1.5.4.4.1 INTRODUCCIÓN

IPSec corresponde a un conjunto de estándares del IETF para incorporar servicios de seguridad en comunicaciones IP y que responde a la necesidad creciente de garantizar un nivel de seguridad. Su estructura actualmente está definida en RFC 2401.

Su función principal es proporcionar servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP (TCP y UDP, entre otros), autenticando y/o cifrando la información que se desea transmitir. Además posee protocolos para el establecimiento de claves

de cifrado, haciéndolo una herramienta muy robusta en cuanto a seguridad se refiere. Este protocolo opera en la capa de red o capa 3 del modelo OSI y se desarrolló inicialmente para ser utilizado con el estándar IPv6³², adaptándose posteriormente a IPv4.

Este protocolo es considerado como una extensión al protocolo IP, añadiendo dispositivos de seguridad para asegurar el tráfico de los paquetes IP.

Una ventaja fundamental de este protocolo es que no está ligado a ningún algoritmo de encriptación, autenticación, tecnología de claves o algoritmos de seguridad específico, de hecho es un estándar que permite que cualquier algoritmo nuevo se pueda introducir, haciéndolo flexible ante los cambios y avances tecnológicos en la materia.

1.5.4.4.2 DESCRIPCIÓN DEL PROTOCOLO

IPsec se puede definir como un conjunto de estándares que se utilizan para integrar en comunicaciones IP, funciones de seguridad basadas en criptografía. Con ello podemos proporcionar confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública (RSA), algoritmos de cifrado (DES, 3DES, IDEA, Blowfish³³), algoritmos de hash (MD5, SHA-1) y certificados digitales X509v3.

Como una forma de hacerlo un protocolo adaptable, IPSec se diseñó de forma modular, de modo que se pueda seleccionar el conjunto de algoritmos deseados sin afectar a otras partes de la implementación. Se definieron, sin embargo, algunos algoritmos estándar que deberán soportar todas las implementaciones para asegurar la interoperabilidad de la red implementada con Internet. Dichos algoritmos de referencia son DES y 3DES, para cifrado, así como MD5 y SHA-1, como funciones de hash.

Además es posible usar otros algoritmos que se consideren más confiables o más adecuados para un escenario específico: por ejemplo, algoritmo de cifrado de clave simétrica IDEA, Blowfish o AES.

³² IPv6: Nueva versión de IP (Internet Protocol) creada para reemplazar al actual IPv4

³³ Blowfish: Codificador de bloques simétricos

1.5.4.4.3 ESTRUCTURA IPSEC

IPsec cuenta con dos protocolos desarrollados específicamente para proporcionar seguridad a los paquetes IP, así como también con un conjunto de protocolos necesarios para la gestión de claves criptográficas, llamado IKE³⁴, estos son:

- **Cabecera de Autenticación (AH³⁵)**. El protocolo AH es el encargado de garantizar la integridad y autenticación de los datagramas en una red IP. Esto lo logra proporcionando un medio al receptor de los paquetes IP para autenticar el origen de los datos y para verificar que éstos no han sido alterados mientras transitan por la red. Sin embargo una falencia en su funcionamiento es que no proporciona ninguna garantía de confidencialidad, debido a que los datos transmitidos pueden ser vistos por terceros.

En el protocolo AH se inserta una cabecera de autenticación entre la cabecera IP estándar y los datos transportados, que pueden ser un mensaje TCP, UDP, ICMP, o incluso un datagrama IP completo.

Dentro de la cabecera AH se indica la naturaleza de los datos de la capa superior. Cabe destacar que AH asegura la integridad y autenticidad de los datos transportados y de la cabecera IP, excepto los campos variables: TOS, TTL, flags, offset y checksum. La estructura de una cabecera AH se adjunta en la figura 10.

³⁴ IKE: Internet Key Exchange

³⁵ AH: Authentication Header

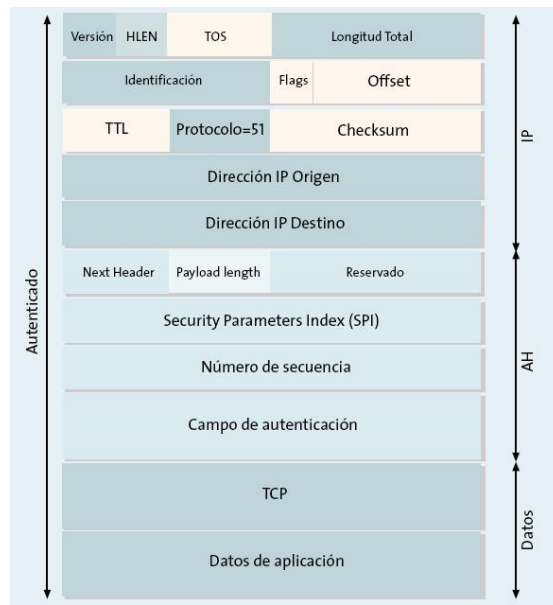


Figura 10. Estructura de un datagrama AH

El numero 51 que se visualiza en el campo Protocolo de la cabecera IP en la figura 10 corresponde al número asignado por el IANA³⁶.

El funcionamiento de AH se basa en un algoritmo HMAC³⁷, que consiste en un código de autenticación de mensajes. Este algoritmo aplica una función hash a la combinación de unos datos de entrada y una clave, obteniendo a la salida una pequeña cadena de caracteres denominada MAC³⁸, la cual corresponde a una “huella personal” asociada a los datos y a la persona que lo ha generado, puesto que es la única que conoce la clave.

³⁶ IANA: Internet Assigned Numbers Authority

³⁷ HMAC: Hash-based Message Authentication Code

³⁸ MAC: Media Access Control address

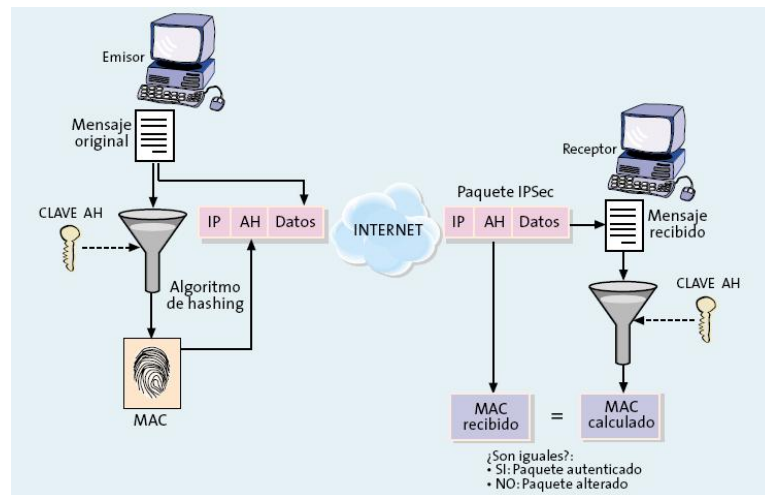


Figura 11. Funcionamiento protocolo AH

El equipo que envía la información calcula la MAC del mensaje original, el cual se copia en uno de los campos de la cabecera AH. El nuevo paquete construido se envía a través de la red, repitiéndose en el extremo receptor el cálculo de la MAC y comparándolo con el recibido en el paquete para realizar la verificación. De ser iguales, el receptor tiene la seguridad de que el paquete IP no ha sido modificado en el trayecto.

- **Encapsulado de Seguridad (ESP³⁹)**. La función principal del protocolo ESP se centra en proporcionar confidencialidad de la información que se está transportando, para ello especifica el modo de cifrar los datos que se desean enviar y cómo este contenido cifrado se incluye en un datagrama IP. Además, puede ofrecer los servicios de integridad y autenticación del origen de los datos incorporando un mecanismo similar al del protocolo AH.

Debido a que ESP proporciona más funciones que AH, el formato de la cabecera es más complejo, el cual consta a grandes rasgos de una cabecera y una cola, que rodean los datos transportados. Dichos datos pueden corresponder a cualquier protocolo IP. En la Figura 12 se muestra la estructura de un datagrama ESP, en la que se observa cómo el contenido o carga útil viaja cifrado. En este caso el IANA ha asignado al protocolo ESP el número decimal 50, por lo

³⁹ ESP: Encapsulating Security Payload

que el campo Protocolo de la cabecera IP contendrá el valor 50, mientras que dentro del mensaje ESP se indica la naturaleza de los datos. Puesto que este campo, al igual que la carga útil, están cifrados, un hipotético atacante que intercepte el paquete no podrá saber si el contenido es TCP⁴⁰ o UDP, lo que dificultará aún más su tarea de descifrar la información.

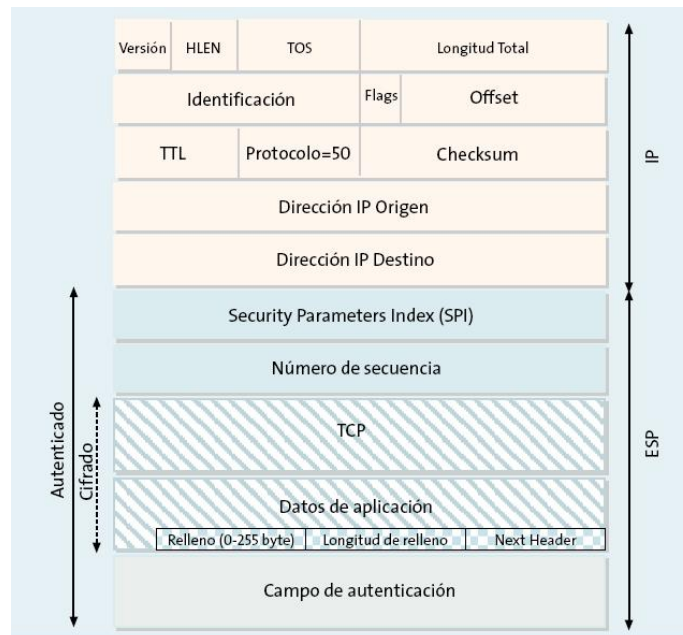


Figura 12. Estructura datagrama ESP

El cifrado de la información es realizado por un algoritmo de cifrado de clave simétrica, generalmente algoritmos de cifrado en bloque, de modo que la longitud de los datos a cifrar tiene que ser un múltiplo del tamaño del bloque, por lo que existe un campo de relleno, gracias al cual es posible ocultar la longitud real y, por tanto, las características del tráfico.

⁴⁰ TCP: Transmission Control Protocol

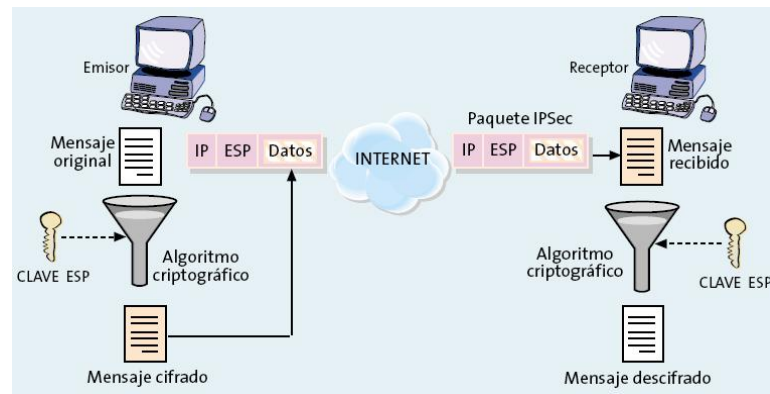


Figura 13. Funcionamiento del protocolo ESP

En la Figura 13 se muestra cómo el protocolo ESP permite el envío de los datos de forma confidencial. Primero el emisor cifra el mensaje original, utilizando una clave determinada, y lo incluye en un paquete IP, a continuación de la cabecera ESP. En el destino, el receptor aplica de nuevo el algoritmo de cifrado con la misma clave, recuperando los datos originales.

Al igual que en el protocolo AH la seguridad reside en la robustez del algoritmo de cifrado, ya que un atacante no puede descifrar los datos sin conocer la clave, por lo que la distribución de claves de forma segura es un requisito fundamental para el funcionamiento de ambos protocolos.

Para establecer el enlace entre el emisor y el receptor es fundamental que ambos estén de acuerdo tanto en el algoritmo de cifrado y el resto de parámetros comunes que utilizan. Esta labor de puesta en contacto y negociación es realizada por un protocolo de control, denominado IKE.

- **Intercambio de claves por Internet (IKE).** Un concepto esencial en IPSec es el de asociación de seguridad (SA⁴¹), que consiste en un canal de comunicación unidireccional que conecta dos nodos, a través del cual fluyen los datagramas protegidos mediante mecanismos criptográficos acordados previamente. Al identificar únicamente un canal unidireccional, una conexión IPSec se compone de dos SAs, una por cada extremo de la comunicación. Hasta el momento se ha supuesto que ambos extremos de una asociación

⁴¹ SA: Security Association

de seguridad deben tener conocimiento de las claves, así como del resto de la información que necesitan para enviar y recibir datagramas AH o ESP. Tal como se ha indicado anteriormente, es necesario que ambos nodos estén de acuerdo tanto en los algoritmos criptográficos a emplear como en los parámetros de control. Esta operación puede realizarse mediante una configuración manual, o mediante algún protocolo de control que se encargue de la negociación automática de los parámetros necesarios; a esta operación se le llama negociación de SAs. El IETF ha definido el protocolo IKE en el RFC 2407 y actualmente actualizado en IKEv2 en el RFC 4306, para realizar tanto ésta función de gestión automática de claves, como el establecimiento de las SAs correspondientes. Además define todos los algoritmos criptográficos soportados en el RFC 4307.

El protocolo IKE es el resultado de la integración de dos protocolos complementarios: ISAKMP⁴², y Oakley, donde ISAKMP establece de forma genérica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan, mientras que Oakley se encarga de especificar la lógica de realizar de forma segura el intercambio de claves entre dos dispositivos.

Las fases necesarias para establecer una asociación de seguridad IPSec son las siguientes:

- a) Aquí ambos nodos establecen un canal seguro y autenticado, el cual se consigue mediante el uso de un algoritmo de cifrado simétrico y un algoritmo HMAC. Las claves necesarias se derivan de una clave maestra que se obtiene mediante un algoritmo de intercambio de claves Diffie-Hellman, sin embargo éste procedimiento no garantiza la identidad de los nodos, por lo que es necesario un paso adicional de autenticación, dentro de los cuales destacan los siguientes:
 - El primero método se basa en el uso de funciones hash, donde ambos equipos manejan un “secreto compartido”, una cadena de caracteres que únicamente conocen los dos extremos que quieren establecer una comunicación IPSec. Para no debilitar la seguridad de este mecanismo de autenticación, debe configurarse un secreto distinto

⁴² ISAKMP: Internet Security Association and Key Management Protocol

para cada par de nodos, por lo que el número de secretos aumenta muy rápidamente cuando aumenta el número de nodos, complicando la gestión de claves.

- Otro de los métodos de autenticación más utilizados corresponde al de certificados digitales X509v3, gracias a los cuales es posible distribuir de forma segura la clave pública de cada nodo, de modo que éste puede probar su identidad mediante la posesión de la clave privada y ciertas operaciones de criptografía pública, sin embargo la utilización de certificados requiere de la aparición de un elemento más en la arquitectura IPsec denominada PKI, a la cual nos referiremos luego.

- b) En la segunda fase el canal seguro IKE es utilizado para negociar los parámetros de seguridad IPsec, donde se negocian las características de la conexión ESP o AH según sea el caso y todos los parámetros necesarios. Luego el equipo emisor ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se hayan configurado, para luego el sistema receptor aceptar la primera que coincida con los parámetros de seguridad que tenga definidos. Asimismo, ambos nodos se informan del tráfico que van a intercambiar.



Figura 14. Funcionamiento protocolo IKE

En la figura 14 se muestra el funcionamiento del protocolo IKE y el modo en que se obtiene una clave de sesión, que es la que se utiliza para proteger las conexiones ESP o AH.

1.5.4.4.4 MODOS DE IPSEC.

Los dos protocolos de seguridad vistos anteriormente (AH y ESP) son capaces de trabajar en dos modos.

- **Modo transporte.** Aquí el contenido del datagrama AH o ESP son datos de la capa de transporte (por ejemplo, datos TCP o UDP), por lo que la cabecera IPsec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación, pero requiere que ambos extremos entiendan el protocolo IPsec.
- **Modo túnel.** En éste modo el contenido del datagrama AH o ESP es un datagrama IP completo, incluyendo la cabecera IP original. Así, se toma un datagrama IP al cual se añade inicialmente una cabecera AH o ESP. Posteriormente se añade una nueva cabecera IP, la cual se utiliza para encaminar los paquetes a través de la red.

Este modo se utiliza normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPsec. Lo utilizan principalmente los gateways IPsec, con objeto de identificar la red que protegen bajo una misma dirección IP y centralizar de este modo el procesamiento del tráfico IPsec en un equipo. Además se utiliza este modo, cuando se utiliza AH junto con ESP, para ocultar la identidad de los nodos que se están comunicando. Otra aplicación del modo túnel, tanto con ESP como con AH, es la aplicación que se desea utilizar en este Trabajo de Titulación, establecer VPNs a través de redes públicas.

IPsec puede ser implementado bien en un host o bien en un equipo dedicado, tal como un router o un firewall, sin embargo cuando cumple estas funciones se denominan gateway IPsec.

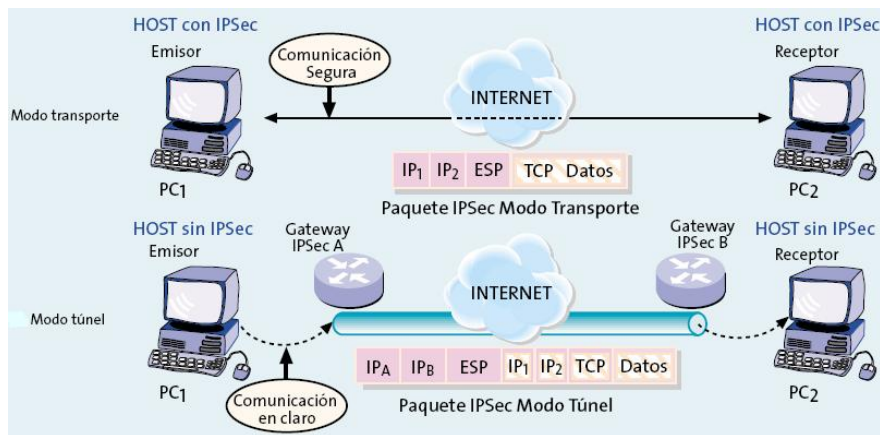


Figura 15. Modos IPsec

La Figura 15 muestra los dos modos del protocolo IPsec, donde en la parte superior de la figura se representan dos hosts que se comunican mediante IPsec. Esta comunicación se realiza en modo transporte, por tanto la información que se protege es únicamente el protocolo TCP o UDP, así como los datos de aplicación. En la parte inferior de la figura se muestran dos redes que utilizan para conectarse dos gateways IPsec, por lo que utilizan una implementación en modo túnel. La comunicación es realizada a través de una red pública, entre un PC situado en una red local con otro PC situado en una red local remota, de modo que entre los gateways IPsec se establece un túnel a través del cual viajan protegidas las comunicaciones entre ambas redes locales. Sin embargo ambos PCs envían y reciben el tráfico en claro, como si estuviesen situados en la misma red local. Este esquema tiene la ventaja de que los nodos situados en redes separadas pueden comunicarse de forma segura y transparente, concentrándose, al mismo tiempo, las funciones de seguridad en un único punto, facilitando así las labores de administración.

1.5.4.4.5 AUTENTICACIÓN MEDIANTE PKI

Como vimos anteriormente cuando se desea autenticar un conjunto muy numeroso de nodos que se desean comunicar por IPsec, es necesaria la utilización de otra técnica menos

engorrosa que la de intercambio de secretos compartidos por medio de funciones hash. La habilitación de una PKI provee de muchas ventajas, ya que se centraliza el alta y baja de los usuarios y posibilita la introducción de tarjetas inteligentes para el intercambio de certificados de forma segura, favoreciendo a los usuarios remotos.

La tecnología PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío, entre otras funciones que nos garantizan que el usuario con el que nos queremos comunicar es quien dice ser.

La función de los certificados es proporcionar un medio fiable para autenticar la identidad de los dispositivos, en este caso los nodos IPsec. Cada uno de los dispositivos dispone de un certificado digital, que corresponde a su clave pública y la información suficiente para identificarlo (Su DNS⁴³, su dirección IP o su número de serie). A este conjunto de asociaciones que incluyen la clave pública y la identidad, esta ligada a la firma de la Autoridad de Certificación (CA), integrada en la PKI, que valida al certificado digital, la cual será válida para todos los dispositivos IPsec, por lo que en cada uno de ellos existe una copia de ella.

A pesar del masivo uso de esta tecnología los protocolos para el diálogo de los dispositivos con una PKI no están estandarizados, sin embargo la mayoría de los fabricantes utilizan los certificados X.509v3 como formato común, así como los estándares de la serie PKCS⁴⁴ para la solicitud y descarga de los certificados.

Los procedimientos básicos que realizan los nodos IPsec con las PKI son: acceder al certificado de la CA, solicitar y descargar un certificado, así como comprobar la validez de un certificado recibido.

⁴³ DNS: Domain Name Service

⁴⁴ PKCS: Public Key Cryptography Standards

La validación de los certificados la realizan mediante consultas de la Lista de Certificados Revocados (CRL), que se almacena en el directorio de la PKI, para lo cual cada nodo tiene una copia de la CRL, que es actualizada periódicamente.

Para solicitar y descargar los certificados se utiliza el protocolo SCEP. Este protocolo fue desarrollado por Cisco y Verisign⁴⁵, y se basa en el intercambio de mensajes PKCS, mediante el protocolo HTTP⁴⁶, para automatizar los procesos de solicitud y descarga de certificados.

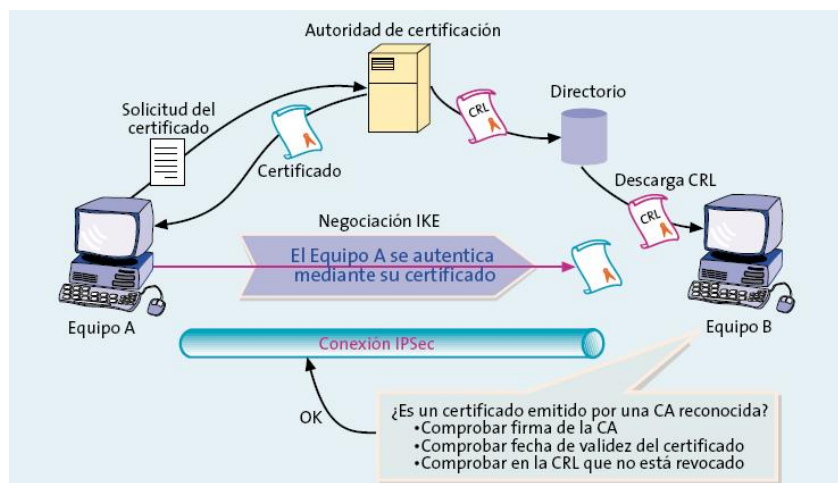


Figura 16. Integración de una PKI en IPsec

En la Figura 16 se observa el diagrama de comunicación entre una PKI y un dispositivo IPsec. Cada nodo genera un par de claves (pública y privada) y envía una petición de certificado a la CA, en ella incluye información de su identidad y su clave pública. Además de esto, descargan el certificado raíz de la CA, la cual genera un certificado para el dispositivo IPsec, el que podrá ser usado por el nodo en una negociación IKE para autenticarse frente a otros dispositivos.

⁴⁵ Verisign: <http://www.verisign.com/>

⁴⁶ HTTP: HyperText Transfer Protocol

1.5.4.5 PROTOCOLOS SSL Y TLS

1.5.4.5.1 INTRODUCCIÓN

El protocolo SSL⁴⁷ fue desarrollado por la compañía Netscape Communications Corporation para incluirlo en su navegador web Netscape Navigator como mecanismo de seguridad. La primera versión de SSL llamada SSL1.0 fue lanzada el año 1994, para luego en el mismo año solucionar algunos problemas de gestión de claves criptográficas con SSL 2.0. En 1995, Microsoft Corporation⁴⁸ consolida el uso de SSL incluyendo soporte para este protocolo en su navegador Internet Explorer.

El objetivo principal buscado por la compañía al desarrollar este protocolo fue crear un canal de comunicaciones seguro entre un cliente y un servidor, que no estuviera limitado por el sistema operativo utilizado por las máquinas y que fuese dinámico y flexible ante los nuevos adelantos en materia de cifrado a medida de que estos estuvieran disponibles, es decir, un protocolo seguro y de propósito general.

A finales de 1995 se incorporó la versión SSL 3.0 al navegador Netscape, para luego ceder el desarrollo de SSL al IETF, el cual lo renombró como TLS⁴⁹, sin embargo este protocolo se basó completamente en su antecesor, existiendo muy pocas diferencias entre ellos, por lo que en algunas figuras de esta sección se hará alusión a SSL o TLS indistintamente.

La primera versión de este protocolo TLS 1.0 fue definida en el RFC 2246 y se publicó en enero de 1.999 y fue actualizado el año 2006 en el RFC 4346, definiéndola como TLS 1.1.

⁴⁷ SSL: Secure Sockets Layer

⁴⁸ Microsoft Corporation : www.microsoft.com

⁴⁹ TLS: Transport Layer Security

1.5.4.5.2 ESTRUCTURA TLS

Como se mencionó anteriormente TLS o SSL es un protocolo de seguridad para Internet, el cual opera entre la capa de transporte del modelo OSI, o entre la capa de transporte y la de aplicación del modelo TCP/IP.

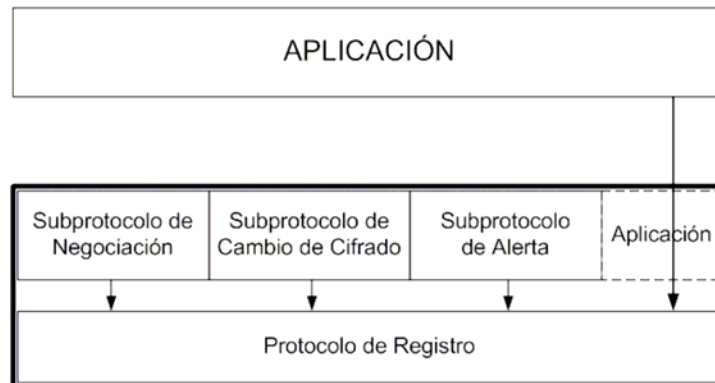


Figura 17. Estructura protocolo TLS.

La función de cada uno de estos subprotocolos es la siguiente:

- **Protocolos de Negociación (*Handshake Protocols*).** Este protocolo es el encargado de negociar los parámetros de seguridad que protegerán la información que se comunicará entre los extremos, donde el protocolo de registro será el encargado de aplicar los parámetros que se negocien con este protocolo. Otra función de este protocolo de negociación será la de autenticar a las entidades que se desean comunicar, negociar los parámetros de seguridad y a la vez notificar las condiciones de error si existieran. Los subprotocolos encargados de realizar cada una de estas funciones son los siguientes:

- **Subprotocolo de Cambio de Cifrado (*Change Cipher Spec Protocol*):** Este subprotocolo se encarga de notificar al otro extremo de la comunicación de un cambio en los parámetros utilizados para la protección de la información.

- **Subprotocolo de Negociación (*Handshake Protocol*):** El subprotocolo de negociación se encarga como su nombre lo indica de negociar los parámetros de seguridad de la comunicación, tal como la versión del protocolo, los algoritmos de cifrado, la firma digital y compresión que se utilizarán, los parámetros de autenticación y las técnicas de clave pública para la negociación de los secretos compartidos. Una vez negociados estos parámetros éste subprotocolo proporciona al protocolo de registro la información que le permita proteger la información.

- **Subprotocolo de Alerta (*Alert Protocol*):** Este subprotocolo se encarga de notificar al resto de protocolos y subprotocolos de una posible condición de error en la comunicación.

- o **Protocolo de Registro (*Record Protocol*).** Este protocolo se encarga de fragmentar en bloques, comprimir, aplicar mecanismos de confidencialidad y autenticidad a los mensajes que las capas superiores de TLS o la capa de aplicación de TCP deseen enviar, para luego transmitirlos a las capas inferiores de la pila de comunicación y a la vez cuando reciba estos mensajes este protocolo debe realizar las operaciones inversas para luego transmitirlo nuevamente a la aplicación o subprotocolo de TLS al cual vaya dirigido.

1.5.4.5.3 FUNCIONAMIENTO SSL

Analizando en forma superficial el funcionamiento de SSL podríamos desglosarlo de la siguiente manera. Primero se procede a intercambiar una clave mediante un algoritmo de cifrado asimétrico, gracias a la cual se establece un canal seguro utilizando para ellos un algoritmo simétrico que ha sido negociado previamente por los agentes de la comunicación. Una vez que se a logrado establecer el canal seguro, se procede a preparar la información que se desea transmitir, fragmentándola en bloques, comprimiéndola, para luego aplicar un algoritmo de hash, el cual da como resultado un resumen (MAC), que es enlazado a cada uno de los bloques comprimidos para asegurar la integridad de los mismos. Luego se realiza el cifrado de la información para luego

enviarla. Todas estas operaciones son supervisadas y controladas mediante una maquina de control de estados.

Antes de comenzar el análisis del funcionamiento en detalle de este protocolo es necesario hacer una diferencia entre dos conceptos que son fundamentales en esta tecnología, los cuales son: sesión y conexión. Una sesión se entiende por una agrupación de parámetros de seguridad y valores utilizados para proteger los datos que se comunican entre dos sistemas que utilizan el protocolo TLS, mientras que una conexión es un flujo de datos que se transmite entre esos dos sistemas conectados, que se protegen utilizando los parámetros y valores de la sesión SSL en la que se basa dicha conexión.

Ahora se procederá a hacer un análisis más exhaustivo del funcionamiento de este protocolo, donde se explicará con más detalle cada uno de los pasos para establecer la conexión SSL.

Como primer paso para establecer la conexión se inicia un proceso de negociación entre el cliente y el servidor. Esta negociación comienza con un mensaje típicamente denominado “*Client hello*” enviado al servidor con el cual se desea establecer la conexión, el cual debe responder con un mensaje de similares características denominado “*Server Hello*”. Estos mensajes son utilizados para conocer ciertas características de ambos, tales como, versión del protocolo utilizada por cada uno de los agentes involucrados en la negociación, algoritmos de cifrado, longitudes máximas de clave que admite, funciones de hash y métodos de compresión a utilizar. Aquí el servidor asigna un identificador a la sesión y se hace constar la fecha y hora de la misma, el cual es enviado al cliente en el mensaje de “*Server Hello*”. En el caso que el servidor no enviara un mensaje de negociación en respuesta al enviado por el cliente, o este fuera invalido o irreconocible, se envía un mensaje de error y se aborta la sesión.

Una vez concluida esta negociación inicial, el servidor tiene la opción de enviar su Certificado (típicamente un X.509v3) de manera que sea autenticado por el cliente y a su vez el mismo reciba su clave pública. De no ser así, el servidor envía al cliente su clave pública mediante un mensaje de *Server Key Exchange*. Uno de estos dos mensajes es válido para

establecer un canal seguro de comunicación. Un último mensaje que puede ser enviado por el servidor es una solicitud de certificado al cliente. De ser exitosa esta fase de negociación, se concluye con un mensaje de “Server Hello Done” desde el servidor, hacia el cliente.

En el caso que el servidor solicite su certificado al cliente, éste debe enviárselo o en el caso de que no lo posea, debe enviar una alerta indicándolo. Luego, por medio de *Client Key Exchange*, el cliente envía al servidor la “clave maestra”, cifrada mediante su clave pública. Dicha clave maestra consiste en un número aleatorio que actuará como clave del algoritmo simétrico acordado para el intercambio de la información.

Por último, si el cliente ha enviado un certificado con capacidades de firma, éste deberá incluir un mensaje de “*Certificate Verify*” con su firma digital, para que el servidor sea capaz de verificar la validez de la firma.

Si se concluyen satisfactoriamente las negociaciones anteriores, el cliente está en condiciones de concluir ésta fase de negociación mediante un mensaje de *Change Cipher Spec*, seguido, inmediatamente, de un mensaje de *Finished*, el cual va cifrado mediante los algoritmos y claves establecidos por ambas máquinas, con lo que se da por finalizada la fase de *Handshake*, luego de lo cual ambos agentes están facultados para transferir sus datos cifrados mediante la conexión TLS establecida.

A continuación se pueden observar en la figura 18 la estructura del proceso de negociación para establecer la sesión TLS o SSL.

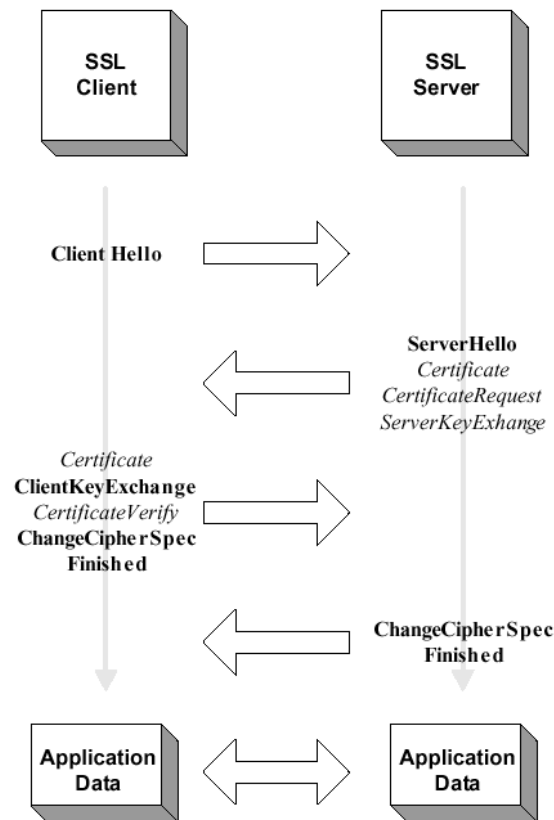


Figura 18. Estructura del proceso de negociación SSL

El protocolo TLS es capaz de establecer múltiples conexiones dentro de una misma sesión o reanudar una sesión previamente interrumpida, lo que es de gran ayuda para lograr iniciar una sesión de forma más rápida y expedita. En estos casos las fases de negociación se reducen considerablemente, logrando una conexión más eficiente.

Para lograr realizar estas conexiones, primero el cliente envía un mensaje de “*Client Hello*” usando el identificador de la sesión anterior. El servidor se encarga de verificarlo y de ser válido devuelve el mensaje “*Server Hello*” usando el mismo identificador de sesión, luego de lo cual envía al cliente un mensaje de *Change Cipher Spec*, seguido por un *Finished*, cifrado con los mismos parámetros negociados anteriormente. Finalmente el cliente responde con sus propios mensajes de *Change Cipher Spec* y *Finished*, para luego reanudar la sesión previamente interrumpida o establecer la nueva conexión sobre la sesión antes iniciada, según sea el caso. En la figura a continuación se puede observar esquemáticamente éste proceso.

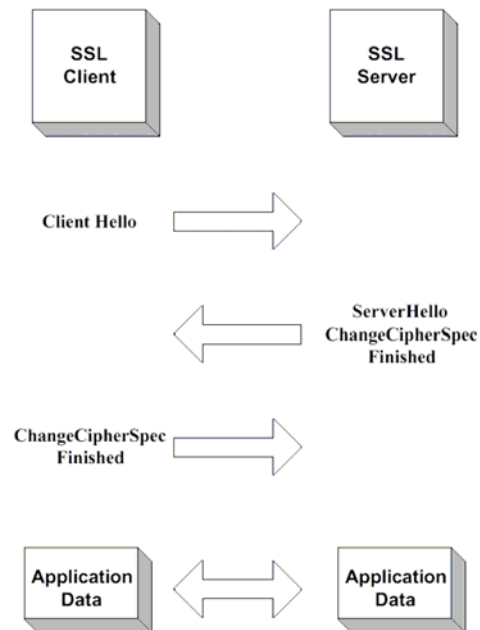


Figura 19. Reconexión o conexión sobre sesión establecida.

1.6 RESUMEN

Una vez estudiados los principales protocolos utilizados para gestionar los túneles VPN y en algunos casos la seguridad de la información que se transporta a través de la red pública, se cuenta con las bases para concluir cuales son las tecnologías que más se ajustan a los requerimientos del diseño.

Como se observó en este capítulo, existen una gran variedad de protocolos capaces de establecer la comunicación que este diseño requiere, sin embargo no todos cuentan con las mismas políticas de seguridad para proteger la información que se desea transmitir.

Dentro de la variedad de protocolos más utilizados para la implementación de redes privadas virtuales, se pueden destacar los protocolos de Capa 2 del modelo OSI (PPTP, L2F y

L2TP). Sin embargo el protocolo más ampliamente utilizado en la actualidad, debido a las estrictas medidas de seguridad que ofrece, además de ser un protocolo adaptable, gracias a su estructura modular que lo hace una herramienta muy potente frente a las amenazas de seguridad a la que están expuestos los datos que se transfieren a través de la red pública de Internet es IPSec, un protocolo de capa 3, que al no estar ligado a ningún protocolo específico puede utilizar cualquier tecnología nueva y adaptarse a los requerimientos que el usuario necesite, brindando encriptación, autenticación, confidencialidad, integridad, protección anti-repetición y protección contra el análisis de flujo de tráfico a la capa de red.

Cabe destacar un protocolo de Capa 4 del Modelo OSI, SSL o también conocido como TLS, el cual encripta las comunicaciones entre los servidores y navegadores web para posteriormente transportar la información a través del túnel VPN sobre Internet en la capa de aplicación, el cual está teniendo un gran auge en las transacciones económicas gracias a su robusta seguridad y a su facilidad de configuración.

Estas dos últimas tecnologías (IPSec y SSL) son las que actualmente lideran el mercado de las VPNs, sin embargo ambas presentan ventajas y desventajas. IPSec se comporta perfectamente frente a conexiones sitio a sitio, pero no así frente a conexiones de usuarios remotos, debido principalmente a lo tedioso y complejo de su configuración. En cambio SSL ofrece todo lo contrario, un muy buen desempeño frente a usuarios remotos, pero no así para conexiones sitio a sitio, siendo superada con creces por IPSec, por lo que un complemento de estas dos tecnologías sería una solución perfecta para una empresa que requiera una robusta seguridad y una gran movilidad.

CAPÍTULO II. TECNOLOGÍA DE VOZ SOBRE IP

2.1 INTRODUCCIÓN

Actualmente la convergencia de las redes de comunicación es un concepto bastante común, que busca la integración entre las tecnologías de voz, datos y video en una única red. La unificación de sistemas de telefonía, el ahorro en llamadas empleando VoIP, soluciones para movilidad de usuarios, y la simplificación e integración de toda la infraestructura de comunicaciones en una única red, son las principales ventajas que hacen que la convergencia esté tomando más y más fuerza en las empresas.

Antes de comenzar es necesario hacer una diferencia entre dos conceptos que serán tratados en éste capítulo: Voz sobre IP y Telefonía IP. VoIP, sigla del inglés Voice Over IP, se refiere a la tecnología que permite la transmisión de voz en tiempo real a través de una red IP en forma de paquetes de datos. Por su parte, telefonía IP se denomina a la aplicación inmediata de dicha tecnología, la cual permite que se puedan realizar todo tipo de llamadas telefónicas sobre redes IP o alguna otra red de paquetes. De esta forma, es posible transportar distintos tipos de servicios de comunicaciones, tales como voz, fax o aplicaciones de mensajes de voz a través las redes IP.

Las tecnologías de Telefonía IP y conmutada cumplen el mismo servicio pero de formas muy distintas. Su diferencia reside principalmente en que ésta última se basa en una técnica denominada conmutación de circuitos, esto es, establece un canal físico único entre los dos puntos que desea comunicar, el cual se mantiene durante toda la comunicación. Una de las principales desventajas de este tipo de tecnologías es que requiere de una excesiva cantidad de ancho de banda para cada llamada y el circuito no es empleado eficientemente. En cambio VoIP está basada en conmutación de paquetes, esto es, la información se discretiza en paquetes, cada uno de los cuales viaja por una ruta no definida hasta llegar al otro extremo de la comunicación.

2.2 DEFINICIÓN VOIP

El servicio de VoIP se refiere al transporte de las conversaciones de voz en tiempo real, en forma de paquetes de datos sobre cualquier red basada en el protocolo IP, de entre las que podemos destacar la red de Internet o una red de área local cualquiera.

Los Protocolos utilizados para realizar el transporte de las señales de voz, sobre la red IP son comúnmente denominados protocolos de Voz sobre IP o protocolos IP. Estos se pueden considerar como implementaciones comerciales de la "Red experimental de Protocolo de Voz", desarrollada por ARPANET⁵⁰ en el año 1973.

Una de las principales ventajas que brinda VoIP a las empresas que la implementan, es la reducción en los costos en servicios telefónicos, ya que al implementar una red de VoIP para comunicar una o varias redes, los costos de las llamadas entre éstas serían totalmente gratuitos, y se disminuirían notoriamente también en llamadas de larga distancia e internacionales si lo que se desea es una interconexión con el sistema de telefonía pública conmutada. Esto es debido a que se utiliza la misma infraestructura de red para la transmisión normal de datos y para la transmisión de voz, invirtiendo una sola vez en la implementación de la red.

2.3 PROCESAMIENTO DE LA VOZ

Cuando se desea transmitir una señal analógica, en este caso, una señal de audio, por la red digital de datos, el primer proceso a realizar consiste en la codificación de la señal de voz, de manera que pueda ser separada en paquetes de datos. Este proceso consta de una serie de etapas, la primera de las cuales consiste en la digitalización de la señal analógica proveniente del transductor del auricular, para lo cual se realiza un muestreo de la información, consistente en la toma de muestras periódicas de la amplitud de una señal a una frecuencia, a lo menos el doble de la máxima frecuencia de la señal de audio, tal como lo estipula el "Teorema del Muestreo" ó también conocido como "Teorema de Nyquist-Shannon". Esto nos asegura que al realizar el

⁵⁰ ARPANET: Advanced Research Projects Agency Network

proceso inverso, es decir, la conversión de digital-análogo obtendremos una señal fiable, evitando un fenómeno denominado “Aliasing”.

Una vez obtenidas las muestras de la señal analógica se procede a realizar un proceso denominado cuantización, que convierte una sucesión de muestras de amplitud continua en una sucesión de valores discretos. Durante este proceso se mide el nivel de tensión de cada una de las muestras, y se les atribuye un valor finito (discreto) de amplitud, seleccionado por aproximación dentro de un margen de niveles previamente fijado.

Para obtener una comunicación más expedita, lo que buscan las nuevas tecnologías es utilizar más eficientemente el ancho de banda disponible, por lo que el proceso siguiente consiste en la compresión de la información obtenida de los pasos anteriores.

Una vez que la información viaja hacia el equipo receptor, el proceso de recuperación se realiza de forma análoga, es decir, se descomprime la señal en caso de que tenga compresión, se decodifican las muestras para obtener la señal en forma de amplitudes (PAM⁵¹) y, finalmente, se realiza un filtrado para remover el ruido que pueda traer la señal.

2.3.1 CODIFICACIÓN DE LA VOZ

Dado que la voz es una señal analógica y la red de datos por la que se desea transportar es digital, es necesario realizar un proceso adicional que consiste en convertir las ondas analógicas en información digital, donde juegan un papel primordial el proceso de codificación y decodificación ó CODEC.

Hay varias formas de realizar esta conversión, las que están regidas por varios estándares, la mayoría de las cuales basadas sobre modulación codificada mediante pulsos (PCM⁵²) o variaciones de ella.

⁵¹ PAM: Pulse Amplitude Modulation

⁵² PCM: Pulse-code modulation

La codificación se puede traducir como el proceso mediante el cual se representa una muestra cuantificada, mediante un número binario y la decodificación como el proceso inverso, para poder recibir el mensaje original.

Para llevar a cabo el proceso de cuantificación de la señal de audio analógica se utilizan 256 intervalos para representar todas las posibles muestras, como ejemplo podemos nombrar al CODEC de audio G.711 tanto en su ley A, utilizada en Europa como en su ley u, utilizada en USA y Japón, por lo que se utilizarán números binarios de 8 bits para representar todos los intervalos posibles. Sin embargo hay otros CODEC que utilizan una variante de la codificación PCM, la ADPCM⁵³ o cuantificación delta adaptiva, que utilizan menos intervalos de cuantificación.

El CODEC es el encargado de la conversión de la señal analógica en datos binarios, para luego comprimir esta secuencia de datos y proporcionar la cancelación del eco que se genera en estos procesos. Esta compresión de los datos se traduce en un significativo ahorro del ancho de banda utilizado para la transmisión de éstos, lo que a su vez permite un mayor número de conexiones VoIP simultáneas.

Otra técnica muy utilizada por los CODEC para aumentar el ahorro de ancho de banda en la transmisión es la supresión de silencios, que se basa en no enviar los paquetes de voz de los silencios entre las conversaciones.

A continuación se adjuntan algunos parámetros por los cuales clasificar los CODEC:

Bit Rate: indica la cantidad de información que se manda por segundo.

Sampling Rate: indica la frecuencia de muestreo de la señal.

Frame size: indica cada cuántos milisegundos se envía un paquete con la información codificada.

MOS: indica la calidad general del CODEC

⁵³ ADPCM: Adaptive Differential Pulse Code Modulation

En la figura 20 se observan algunos de los CODEC mas utilizados actualmente para la codificación y decodificación de las comunicaciones de VoIP y los respectivos retardos en su proceso de codificación

Coder type	Rate (kbit/s)	Frame size (ms)	Look-ahead (ms)	Mean one-way delay introduced by coder-related processing (ms) (see Note 2)		Reference
				Minimum	Maximum	
PCM	64	0.125	0	0.25	0.375	G.711, G.712
ADPCM	40	0.125	0	0.25	0.375	G.726, G.727
ADPCM	32	0.125	0	0.25	0.375	G.721(1988), G.726, G.727
ADPCM	24	0.125	0	0.25	0.375	G.726, G.727
ADPCM	16	0.125	0	0.25	0.375	G.726, G.727
LD-CELP	16	0.625	0	1.25	1.875	G.728
LD-CELP	12.8	0.625	0	1.25	1.875	G.728
CS-ACELP	8	10	5	25	35	G.729
VSELP	7.95	20	0	40	60	IS-54-B, TIA
ACELP	7.4	20	5	45	65	IS-641, TIA
QCELP	8	20	0	40	60	IS-96-A
RCELP	8	20	10	50	70	IS-127
VSELP	6.7	20	5	45	65	Japanese PDC
RPE-LTP	13	20	0	40	60	GSM 06.10, Full-rate
VSELP	5.6	20	0	40	60	GSM 06.20, Half-rate
ACELP	12.2	20	0	40	60	GSM 06.60, Enhanced FR
ACELP	5.3	30	7.5	67.5	97.5	G.723.1
MP-MLQ	6.3	30	7.5	67.5	97.5	G.723.1
NOTE 1 – The PCM codec converts from analogue to digital and vice-versa while all other coders refer to the PCM domain; for PCM in the analogue domain, additional delay is incurred (0.375 ms).						
NOTE 2 – For IP-related applications, the mean one-way delay introduced by codec-related processing: = 2 × frame size + look-ahead (minimum, see A.2.3) = 3 × frame size + look-ahead (maximum, see A.2.3).						

Figura 20. CODECs de compresión de audio más utilizados.

Como se observa en la figura 20, el CODEC G.711 muestrea una señal 64.000 veces por segundo, por lo que puede obtener una señal bastante fiable al oído humano al momento de reconstruirla en el terminal receptor, sin embargo esa alta calidad se traduce en un mayor uso de ancho de banda, lo que puede perjudicar al resto de las comunicaciones.

Por su parte el CODEC G.729A tiene una tasa de muestreo de 8.000 veces por segundo, muy por debajo del G.711, lo que lo hace un CODEC muy eficiente y además cuenta con una calidad aceptable en la transmisión de la voz, posicionándolo dentro de los más utilizados en comunicaciones de voz.

2.4 PROTOCOLOS VOIP

2.4.1 INTRODUCCIÓN

Actualmente existe gran variedad de protocolos destinados a establecer y controlar las comunicaciones de voz sobre redes IP. En esta sección se establecerán las bases de los principales protocolos utilizados, para poder identificarlos y ser capaces de seleccionar el más apropiado para éste diseño.

2.4.2 CLASIFICACIÓN DE LOS PROTOCOLOS

A la hora de establecer una comunicación de voz en una red IP, lo primero que se debe hacer es definir los distintos tipos de negociaciones que deberán intercambiar los usuarios para establecer la comunicación, a este proceso se le llama señalización de llamada (call signalling).

Debido a que la voz es una señal analógica es necesario codificarla en paquetes de datos, para ser transportados por la red IP. Como se explico anteriormente los codificadores más utilizados actualmente son G.729A, G.711, entre otros. Además, debido a que la voz generalmente se transporta sobre segmentos UDP, es necesario realizar la negociación de dichos puertos. Para el intercambio de este tipo de información se definen los Protocolos de control de señalización de llamada (Call Control signaling).

Una vez que se ha establecido la comunicación es necesario enviar la señal de audio codificada en paquetes a través de la red IP, la cual puede presentar variaciones de retardo altos respecto a las redes de telefonía tradicional, esto debido principalmente a que no fueron diseñadas

para tal propósito. Otro fenómeno que podría ocurrir es que al tratarse de una red de datagramas, los datos podrían llegar desordenados. Debido a estas características de las redes IP, es necesario empaquetar los datos sobre algún protocolo que sea capaz de minimizar o por lo menos controlar estos fenómenos. Estos protocolos son llamados Protocolos de transporte de media (*Media Transport Protocols*), los que están asociados con los protocolos de control de transporte de media (*media transport control protocols*), cuya función es enviar información de los parámetros que intervienen en la comunicación, tales como el jitter, paquetes enviados, paquetes recibidos, paquetes perdidos, etc. Los protocolos más utilizados para este fin son RTCP⁵⁴ y RTP⁵⁵.

En este punto se tienen todos los elementos necesarios para establecer y controlar una comunicación de voz a través de dos terminales, sin embargo al aumentar la envergadura y complejidad de la red, comunicándola con la red de telefonía pública tradicional mediante gateways, se hace necesario centralizar cierto tipo de información para que la red sea escalable.

Para lograrlo se incluye en la estructura de la red un dispositivo de control denominado softswitch, que posee capacidades de ruteo, transcoding de señalización y localización de dispositivos entre otras funciones. Al proceso de comunicación entre este dispositivo y los gateways se le denomina protocolos de registro y control. Sin embargo en algunas ocasiones la definición de los protocolos de registro y control esta incluida como parámetros dentro de los protocolos de señalización de llamadas.

Una vez conocidas las etapas de la comunicación y control de VoIP, se puede hablar más específicamente de los dos estándares más utilizados actualmente y las entidades que los definen, tal como se observa a continuación.

⁵⁴ RTCP: Real Time Control Protocol

⁵⁵ RTP: Real time Transport Protocol

	SIP	H.323
	IETF	ITU-T
Señalización de llamada	SIP	H.225/Q.931
Control de Señalización de llamada	SDP	H.245
Registración y control	SIP	H.225/RAS
Tranporte de audio	RTP	RTP
Control de transporte de audio	RTCP	RTCP
SoftSwitch	SIP server	Gatekeeper

Figura 21. Estándares VoIP

Dentro de los protocolos utilizados para establecer una comunicación de voz sobre IP destacan dos grandes grupos, estos son los protocolos de señalización y los de transporte, que a su vez incluyen en su estructura varios protocolos para cumplir las tareas específicas para las cuales fueron diseñados.

2.4.3 PROTOCOLOS DE SEÑALIZACIÓN EN VOIP

Los protocolos de señalización para voz sobre IP nacen con la necesidad de brindar calidad de servicio en este tipo de comunicaciones, es decir, se hace necesaria una gestión de recursos que asegure la optimización de la capacidad de transporte de la voz a través de toda la conexión.

El proceso de señalización corresponde al conjunto de informaciones intercambiadas entre el emisor y el receptor de la comunicación VoIP, que permite que estos realicen operaciones de:

Supervisión: Se refiere a la detección de condición o cambio de estado en la comunicación.

Direccionamiento: Realizar la negociación y el establecimiento de llamada.

Explotación: Esto involucra la gestión y el mantenimiento de la red.

Existen principalmente dos estándares utilizados para este efecto, estos son: H.323 y SIP.

2.4.3.1 H.323

H.323 es una recomendación del ITU-T⁵⁶ desarrollada en 1996, que define los protocolos necesarios para establecer una comunicación de voz, datos y/o video sobre una red no orientada a conexión, y que por lo tanto no garantiza una calidad e servicio.

La red de comunicación de los terminales H.323 puede corresponder a un simple segmento o un anillo, o una red más compleja con múltiples segmentos, como es el caso de Internet, lo se puede traducir en un grado muy variable de rendimiento.

Este estándar de comunicación realiza el control de la llamada, la gestión de la información y el ancho de banda para una comunicación punto a punto o multipunto, dentro de la LAN, así como también define interfaces entre la LAN y otras redes externas.

Además de las funciones anteriormente descritas H.323 establece los estándares para la compresión y descompresión de audio y vídeo, dando compatibilidad a los sistemas que utilicen este estándar.

Como se mencionó anteriormente otra de las funciones que desempeña H.323 es la de gestionar el ancho de banda disponible en la red, para evitar que la comunicación, ya sea de audio o video colapse. Una forma de lograr este propósito es limitando el número de conexiones simultáneas.

2.4.3.1.1 COMPONENTES H.323

Como se ha mencionado el estándar define un amplio conjunto de características y funciones, algunas necesarias y otras opcionales, sin embargo además de eso también define componentes esenciales para la estructura H.323, de los cuales podemos destacar los siguientes.

⁵⁶ ITU-T: International Telecommunication Union

a) Terminal H.323. Se denomina terminal H.323 a un extremo de la red, capaz de proporcionar comunicaciones bidireccionales, en tiempo real con otro terminal H.323, gateway o MCU (Unidad de Control Multipunto). Esta comunicación esta compuesta por señales de control, indicaciones, audio, video y/o datos, considerándose obligatorio el soporte para comunicaciones de voz y opcional para la comunicación de video y datos. Estos terminales se pueden dividir en varios bloques

- **Adquisición de información:** consiste en un conjunto de equipos capaces de recepcionar las señales que se desean transmitir por la red IP, ya sean de audio, video o datos, con sus respectivas interfaces de usuario.

- **CODEC de audio:** Todos los terminales deben incluir un CODEC de audio para poder realizar las operaciones de codificación en el emisor y decodificación en el receptor. Además, opcionalmente, pueden enviar más de un canal de audio simultáneamente.

- **CODEC de video:** En los terminales H.323 es opcional que contengan un CODEC para realizar las operaciones de codificación y decodificación de las señales de video.

- **Canal de datos:** La utilización de uno o más canales de datos es opcional, además éstos tienen la posibilidad de transmitir información unidireccional o bidireccional.

- **Retardo en recepción:** Aquí se incluye el retardo añadido a las tramas, con el fin de mantener la sincronización de la comunicación, esto debido a la oscilación en la llegada de la información al terminal receptor.

- **Unidad de control del sistema:** Proporciona la señalización, que ayuda al correcto funcionamiento del terminal y la conforman tres bloques principales:

- **Función de control H.245:** Es el encargado de transportar los mensajes de control entre ambos terminales involucrados en la comunicación, los cuales establecen el modo de

funcionamiento de la entidad H.323. De entre sus funciones principales destacan la de negociar las capacidades (ancho de banda) intercambiadas entre los dos extremos, de la apertura y cierre de los canales lógicos y de los mensajes de control de flujo.

- **Capa H.225:** Su función es dar formato a las tramas de audio, video, datos y control, transmitidos en mensajes de salida hacia la interfaz de red y de recuperarlos de los mensajes que han sido introducidos desde la interfaz de red. Además se encarga de la alineación de la trama, la numeración secuencial y la detección y/o corrección de errores.

- **Interfaz de red de paquetes:** Esta interfaz es específica para cada implementación, además debe proveer los servicios descritos en la recomendación H.225, que lo obligan a establecer un servicio extremo a extremo fiable para el canal de control H.245, los canales de datos y el canal de señalización. Por otro lado, el servicio de extremo a extremo no fiable ya sea UDP ó IPX, es obligatorio para los canales de audio, los canales de video y el canal de RAS. Estos servicios pueden ser dúplex o simplex y de unicast o multicast, esto sujeto a algunas condiciones tales como la aplicación que se les desee dar, las capacidades de los terminales y la configuración de la red.

b) Gateway. Un gateway o también conocido como pasarela es un elemento opcional en una comunicación H.323, es necesario en el caso que se desee comunicar con un terminal presente en otra red, como es el caso de la comunicación con la red de telefonía conmutada. Su función es proporcionar comunicaciones bidireccionales en tiempo real entre terminales H.323 en la red IP y otros terminales o gateways en una red conmutada. Además brinda servicios de traducción entre formatos de transmisión (por ejemplo H.225.0 a H.221) y entre procedimientos de comunicación (por ejemplo H.245 a H.242).

En general, la función del gateway en una comunicación de VoIP es reflejar transparentemente las características de un extremo en la red IP a otro en una red conmutada y viceversa.

c) Gatekeeper. Los gatekeeper son elementos opcionales en la comunicación entre terminales H.323 y actúan como punto central de todas las llamadas dentro de una zona y proporcionan servicios a los terminales, gateways y MCUs, tales como gestión del ancho de banda y localización de los gateways.

El grupo conformado por los Terminales H.323, Gateways y MCU's gestionados por un gatekeeper se la conoce como Zona H.323.

Las funciones que debe cumplir un gatekeeper de estar presente en la red H.323 son las siguientes:

- Traducción de Direcciones: Traducción de alias a direcciones de transporte, utilizando una tabla, que se modifica con mensajes de registro.
- Control de Admisión: Autoriza el acceso a la red.
- Control de Ancho de Banda.
- Gestión de Zona: Consiste en suministrar todas las funciones anteriores a los elementos de la “Zona H.323”.

Sin embargo el gatekeeper también tiene funciones opcionales que son principalmente:

- Señalización de control de llamada: como una forma de evitar la gestión de las señales de control H.225.0 el gatekeeper puede elegir completar la señalización de llamada con los extremos y procesar la señalización de llamada el mismo. Alternativamente, puede elegir que los extremos conecten directamente sus señalizaciones de llamada.
- Autorización de llamada: El gatekeeper tiene la capacidad rechazar las llamadas procedentes de un determinado terminal basándose en la especificación Q.931, esto debido principalmente a

ausencia de autorización a terminales o gateways particulares de acceso restringido o acceso habilitado sólo en determinadas franjas horarias.

- **Gestión de llamada:** Para poder gestionar llamadas el gatekeeper tiene la capacidad de mantener una lista de las llamadas en curso.

d) Unidad de Control Multipunto (MCU). MCU está constituida por un controlador multipunto (MC), el cual es obligatorio y uno o más procesadores Multipunto, que son opcionales en la estructura. La MCU está diseñada para transportar la negociación entre tres o más terminales en conferencia, para así determinar las capacidades comunes para el proceso de audio y video y controlar la multidifusión.

- **Controlador Multipunto (MC).** Un MC forma parte de una MCU y es el encargado de gestionar las negociaciones H.245 entre todos los terminales de la conferencia para determinar las capacidades comunes para el procesamiento de audio y video. Además es capaz de controlar recursos de conferencias tales como multicasting.

- **Procesador Multipunto (MP).** Un MP es un componente opcional de los MCU de hardware y software no especializado, encargado de mezclar, conmutar y procesar el audio, video y/o datos transmitidos en la conferencia multipunto, de modo que los procesadores de los terminales no sean sobrecargados.

Las funciones que brindan el MC y MP pueden estar implementadas en un dispositivo dedicado o en su defecto pueden formar parte de otro componente de la red, llámese gatekeeper, gateway, Terminal o MCU.

e) PROXY H.323. Se denomina Proxy H.323 a un servidor, capaz de comunicar de forma segura las redes que forman parte de la comunicación entre dos o más terminales H.323, para así establecer las comunicaciones entre dispositivos ubicados en distintas redes.

2.4.3.1.2 PROTOCOLOS ESPECIFICADOS POR H.323

El estándar H.323 se encarga de especificar los protocolos que van a gestionar la preparación, establecimiento, control de estado, mensajería, CODEC, tanto de audio como de video, transferencia de datos, y el fin de la llamada. Los protocolos utilizados por este estándar de comunicación trabajan sobre la capa de transporte del modelo OSI y están basados en TCP y UDP y/o SCTP.

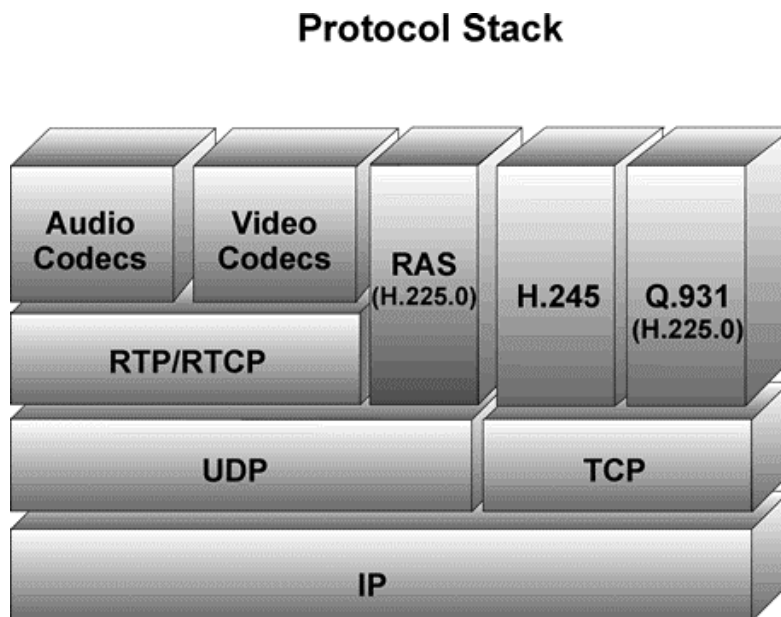


Figura 22. Arquitectura H.323

Como se mencionó anteriormente H.245 es el protocolo de señalización utilizado en el canal de control. Su principal función es gestionar la apertura y cierre de canales lógicos, además del intercambio de información sobre la capacidad de transmisión y recepción de medios de los terminales.

La recomendación H.225 se emplea durante el establecimiento de las conexiones entre puntos finales H.323 (gateways y terminales), es la encargada de definir los mensajes de

señalización de llamadas, con el formato de mensaje definido en el estándar Q.931. Esta señalización define como gestionar datos, video, audio e información de control.

El puerto encargado de establecer el canal de control de llamadas es el TCP 1720, donde se crean los mensajes encargados de realizar, mantener y finalizar una llamada, los que pueden enviarse directamente a los terminales H.323 o bien utilizando un gatekeeper.

H.225.0/RAS es el primer canal que se establece para iniciar la comunicación entre un terminal o gateway y el gatekeeper y se utiliza para descubrir el o los gatekeepers presentes en la red H.323, registrar los gateways o terminales en una zona cubierta por un gatekeeper, localización y control de los puntos finales y notificación de los cambios de estado de la conexión o en el ancho de banda disponible.

RTP y RTCP son dos protocolos definidos en el RFC 3550, utilizados para el transporte de medios y el control de transporte de medios respectivamente, los cuales trabajan con paquetes UDP, debido a la necesidad de transmisión en tiempo real. Sobre estos protocolos se hablará más adelante en el apartado “Protocolos de transporte de VoIP”.

Otro protocolo especificados en el estándar H.323 es RSVP⁵⁷, definido en el RFC 2205, el cual es utilizado en asignar una reserva de recursos para cada flujo de información que se desea transmitir por la red, dando prioridad a los paquetes de audio y video que se deseen transmitir en tiempo real.

Entre los CODEC recomendados por el estándar H.323 para el procesamiento de las señales de audio podemos destacar: G.711, G.722, G.723, G.728 y G.729 principalmente. Para la transmisión de video destacan: H.261 y H.263, H.264 sin embargo no son obligatorios y se puede hacer uso de otro que cumpla con los requerimientos del diseñador.

⁵⁷ RSVP: Resource ReSerVation Protocol

2.4.3.2 SIP

SIP⁵⁸ es un protocolo de control a nivel de aplicación, desarrollado para el establecimiento, mantenimiento y terminación de sesiones interactivas entre usuarios, las cuales pueden tratarse de conferencias multimedia, chat, sesiones de voz o distribución de contenidos multimedia. Sin embargo este trabajo se enfocará en las sesiones de voz, para la aplicación de VoIP. SIP fue creado en 1996 por Mark Handley y Henning Schulzrinne, para luego ser estandarizado por la IETF y definido en RFC 2543. La especificación más reciente de SIP se puede encontrar en el RFC 3261.

La principal aplicación de SIP es la comunicación entre dispositivos multimedia, para lo cual utiliza dos protocolos fundamentales, que son RTP/RTCP y SDP⁵⁹. SDP ó Protocolo de descripción de sesión, es un formato para describir parámetros de inicialización de streaming media, que es un contenido que es visto u oído mientras se envía simultáneamente. Fue publicado por el IETF como RFC 4566.

Al igual que para el estándar H.323, en el transporte de datos de voz en tiempo real se utiliza el protocolo RTP, mientras que para la negociación de las capacidades de los participantes y los tipos de codificación, entre otros, se utiliza el protocolo SDP antes mencionado.

SIP fue diseñado como un protocolo de señalización de extremo a extremo, lo que implica que toda la lógica es almacenada en los dispositivos finales, con excepción del ruteado de los mensajes SIP. Gracias a esta distribución este protocolo cuenta con una gran escalabilidad, sin embargo existe una sobrecarga en la cabecera de los mensajes. Se basa en mensajes de petición y respuesta y reutiliza muchos conceptos de estándares anteriores como HTTP y SMTP⁶⁰.

De entre sus principales ventajas podemos destacar:

⁵⁸ SIP: Session Initiation Protocol

⁵⁹ SDP: Session Description Protocol

⁶⁰ SMTP: Simple Mail Transfer Protocol

Simplicidad. Emplea mensajes de texto plano y con formato HTTP 1.1, lo que ayuda a solucionar los problemas de integración con otras aplicaciones.

Eficiencia. Es muy eficiente en el tiempo de conexión de la llamada, esto debido a que la información necesaria para este propósito se adjunta en el mensaje inicial.

Flexibilidad. Gracias al protocolo SDP, SIP es muy flexible frente a la utilización de CODECs.

Escalabilidad. Debido a que no se mantiene la información del estado de las sesiones UDP en los servidores, es posible manipular un número mucho mayor de clientes por servidor.

Soporte de Movilidad. El protocolo prevé que un mismo usuario pueda estar en diferentes tipos de terminales.

2.4.3.2.1 COMPONENTES SIP

El protocolo SIP define cuatro componentes lógicos en su estructura, los cuales pueden implementarse en distintos dispositivos físicos, tal como teléfonos IP o aplicaciones de software, por lo que cualquiera de estos medios puede incluir uno o más componentes lógicos.

Agente de Usuario. Consiste en una aplicación cliente / servidor utilizado para iniciar y cerrar las sesiones en comunicación SIP. En ella el UAC⁶¹ envía una petición SIP, mientras que un UAS⁶² notifica al usuario cuando recibe dicha petición y responde dependiendo de la acción tomada por el usuario.

Servidor de Redirecciones. Es el encargado de aceptar una petición SIP y enviar al cliente las direcciones de destino o de los servidores con los cuales debe contactarse para establecer la comunicación.

⁶¹ UAC: User Agent Clients

⁶² UAS: User Agent Server

Servidor Proxy. Este realiza funciones de servidor y cliente a la vez, es decir, actúa como un intermediario para realizar peticiones en nombre de otros clientes, para lo cual interpreta la cabecera del mensaje y la reescribe identificando al Proxy como el que inicia la solicitud y además recibe la respuesta del destinatario y se la reenvía al cliente.

Servidor de Registro. Se preocupa de almacenar o actualizar una base de datos con las direcciones SIP (SIP-URI) y sus direcciones IP asociadas, destinada a llevar un registro de la información del usuario que realiza la petición SIP.

2.4.3.2.2 MENSAJES SIP

El protocolo SIP establece y mantiene una comunicación a través de dos tipos de mensajes. Las solicitudes (métodos) y las respuestas (códigos de estado), las cuales utilizan el formato de mensaje genérico establecido en RFC 2822, consistente en una línea inicial, seguida de una o mas cabeceras, una línea en blanco indicando el fin de las cabeceras y por último, el cuerpo del mensaje, el cual es opcional.

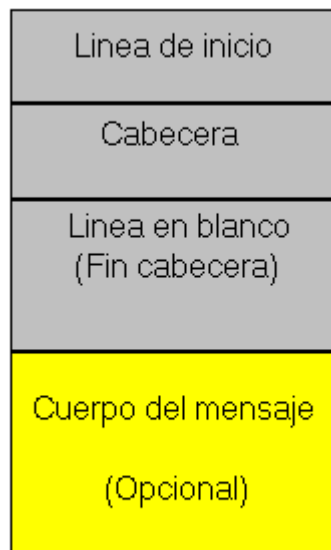


Figura 23.Mensaje SIP

a) Solicitudes (Métodos) SIP

Las peticiones SIP tienen la estructura de la figura 23, donde destacan la línea inicial del mensaje, denominada Request-Line, la cual contiene el nombre del método, el identificador del destinatario de la petición (Request-URI) y la versión del protocolo SIP utilizada. A continuación se describen los métodos básicos utilizados.

INVITE. Solicita el inicio de una llamada o modifica parámetros en una sesión ya existente.

ACK. Confirma el establecimiento de una sesión.

OPTION. Solicita información a un Host acerca de sus capacidades.

BYE. Indica la terminación de una sesión.

CANCEL. Cancela una petición pendiente.

REGISTER. Informa a un servidor de registro sobre la ubicación actual del usuario.

INFO. Transporta la información fuera de banda, como dígitos DTMF⁶³.

MESSAGE. Transporta mensajes de texto entre user agents.

REFER. Solicita generar una sesión desde una tercera parte.

SUSCRIBE. Suscribe al user agent a ser notificado sobre eventos que ocurran en otro user agent.

NOTIFY. Notifica los eventos suscriptos.

⁶³ DTMF: Dual Tone Multi Frequency

UPDATE. Modifica elementos del diálogo activo.

PRACK. Se refiere a una confirmación provisoria.

PUBLISH. Publica la notificación de eventos.

.

b) Respuestas (Códigos de estado).

Esta respuesta es generada por el receptor de la petición SIP. Esta es similar al método SIP, sin embargo difieren en la línea inicial, que en este caso se llama *Status-Line*, la cual contiene la versión de SIP, el código de respuesta (*Status-Code*) y una descripción (*Reason-Phrase*). El código de la respuesta está compuesto por tres dígitos, que sirve para su clasificación.

El primero de estos tres dígitos es el encargado de indicar la clase de la respuesta, esta se clasifica en seis tipos.

Código	Significado
1xx	Mensajes provisionales
2xx	Respuestas de éxito
3xx	Respuestas de redirección
4xx	Respuestas de fallo de método
5xx	Respuestas de fallos de servidor
6xx	Respuestas de fallos globales

La estructura del paquete de respuesta SIP es la siguiente:

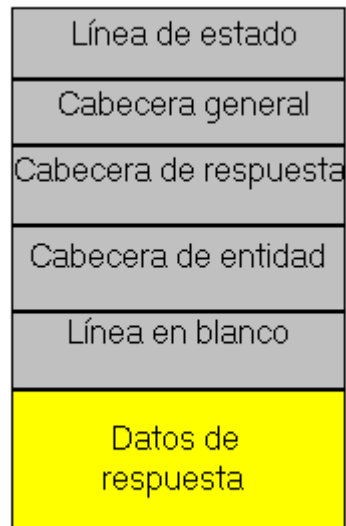


Figura 24. Respuesta SIP

2.4.3.2.3 CABECERA SIP

Las cabeceras son muy similares a las HTTP especificada en el RFC 2616 y se utilizan para transportar información necesaria a las entidades SIP.

Las cabeceras del tipo salto a salto (*Hop-by-Hop*) deben aparecer siempre antes de las cabeceras de extremo a extremo (*end-to-end*), sin embargo las primeras pueden ser modificadas o añadidas por los servidores Proxy, en cambio las segundas deben transmitirse intactas. La clasificación de las cabeceras es la siguiente.

Cabeceras generales (*general headers*). Son utilizadas en los mensajes de solicitud y respuestas. Son las siguientes: Call-ID, Contact, Cseq, Date, Encryption, From, Organization, Retry-After, Subject, Supported, Timestamp, To, User Agent, Via.

Cabeceras de entidad (*entity headers*). De encontrarse presente, son las encargadas de brindar información adicional sobre el cuerpo del mensaje o de lo contrario, referente al recurso

identificado por la solicitud. Son las siguientes: Allow, Content-Encoding, Content-Length, Content-Type, Content-Disposition, Expires, MIME-Version.

Cabeceras de solicitud (*request headers*). Posibilitan la transferencia de información adicional del cliente hacia el servidor y también acerca del propio cliente. Son las siguientes: Accept, Accept-Encoding, Accept-Language, Accept-Contact, Authorization, Hide, In-Reply-To, Max-Forwards, Priority, Proxy-Authorization, Proxy-Require, Record-Route, Reject-Contact, Request-Disposition, Require, Response-Key, Route, Rack, Session-Expire.

Cabeceras de respuesta (*response headers*). Posibilitan al servidor la transferencia adicional de información en relación a la respuesta, la cual no puede situarse en el campo Status-Line. Son las siguientes: Proxy-Authenticate, Server, Unsupported, Warning, WWW-Authenticate, Rseq.

2.4.3.2.4 DIRECCIONAMIENTO

Para establecer una comunicación SIP es necesario realizar el direccionamiento de los usuarios que desean comunicarse, para ello se debe identificar cada uno de ellos mediante un esquema de direccionamiento denominado SIP-URI.

La sintaxis de un SIP-URI se describe a través de la RFC 3986⁶⁴, la cuál especifica que el formato básico de direccionamiento de usuarios para comunicación SIP es el siguiente.

sip:a@b:Puerto

Donde;

“a”= Nombre de usuario;

“b”= equipo (dominio o IP)

“Puerto”= Número de puerto donde se enviará la petición

⁶⁴ RFC 3986: Uniform Resource Identifiers (URI): Generic Syntax

O de otra forma:

sip:usuario@dominio, donde dominio es un nombre de dominio completo.

sip:usuario@dirección_ip, donde dirección_ip es la dirección IP del dispositivo.

sip:número_teléfono@gateway, donde el gateway permite acceder al número de teléfono a través de la red de telefonía pública.

La solución de identificación de SIP, también puede ser basada en el DNS descrito en el RFC 3263, donde se describen los procedimientos DNS utilizados por los clientes para traducir una SIP URI en una dirección IP, puerta y protocolo de transporte utilizado, o por los servidores para retornar una respuesta al cliente en caso de que la petición falle.

2.4.3.2.5 SDP

SDP es un protocolo definido en el RFC 4566 y utilizado para describir las sesiones multimedia en tiempo real, llámese un flujo de audio, video o datos.

Originalmente SDP fue diseñado para anunciar información necesaria para los participantes y las aplicaciones de una sesión MBONE⁶⁵. Sin embargo actualmente su uso se extendió para el anuncio y la negociación de las capacidades de una sesión multimedia, tal como la aplicación VoIP que se está analizando en este Trabajo de Titulación.

Un mensaje SDP está compuesto por una serie de campos, donde los nombres son abreviados por una sola letra, estructurados en un orden específico para simplificar el análisis, por lo que no se considera fácilmente extensible. La única manera de ampliar o de agregar nuevas capacidades al SDP es definir un nuevo atributo. Sin embargo, los atributos desconocidos pueden ser ignorados.

⁶⁵ MBONE: Multicast Backbone

A continuación se detallan los campos utilizados por el protocolo SDP.

- Para descripción de sesión:

Código	Significado
v	Versión del protocolo (obligatorio)
o	Identificador (obligatorio)
s	Nombre de sesión (obligatorio)
l	Información de la sesión (obligatorio)
u	URI de la descripción
e	Dirección de correo
p	Número de teléfono
c	Información de conexión
b	Ancho de banda
z	Tiempo de corrección
k	Clave de encriptación

- Para descripción de tiempo:

Código	Significado
t	Tiempo de sesión (obligatorio)
r	Tiempo de repetición

- Para descripción del medio de comunicación:

Código	Significado
m	Información del protocolo de transporte (obligatorio)
i	Título
b	Líneas de información de ancho de banda
a	Atributos de las líneas

2.5 PROTOCOLOS DE TRANSPORTE DE VOIP

Una vez que se han comentado los protocolos de señalización de VoIP más utilizados actualmente es necesario adentrarse en los protocolos de transporte que se encargan de asegurar que la información llegue intacta desde el origen al destino, cumpliendo con los requerimientos básicos de calidad de servicio.

Como se ha visto anteriormente el protocolo SIP al igual que H.323 utiliza protocolos específicos para desarrollar cada una de las tareas que se requieran para establecer una comunicación multimedia, por lo que trabaja en colaboración con muchos otros protocolos.

El protocolo encargado de la transmisión es RTP, que es un protocolo de transporte de media, encargado de transmitir en tiempo real el contenido de voz, video o datos, encapsulándolo en paquetes UDP. No utiliza TCP debido a que éste es demasiado pesado para las aplicaciones de tiempo real. Debido a que el datagrama UDP no tiene control sobre el orden en el cual los paquetes son recibidos en el receptor, o del tiempo requerido para su transmisión, RTP permite que el receptor ponga los paquetes en el orden correcto y que no espere a los paquetes que se hayan perdido en el camino o tarden mucho en ser recibidos.

RTP está relacionado con otro protocolo denominado RTCP, que es un protocolo de control de transporte de media, encargado de monitorizar la calidad del servicio y de proporcionar información acerca de los participantes en una sesión de intercambio de datos. Ambos protocolos están definidos en el RFC 3550.

RTP se caracteriza por soportar transmisión unicast y multicast, no garantizar la calidad de servicio (QoS), susceptibilidad a pérdida de paquetes, identificación de contenido, secuenciación de paquetes utilizada para que la aplicación pueda reordenar paquetes que no ha recibido en orden, monitorización de la entrega de paquetes, entre otras características.

RTCP es un protocolo de comunicación que monitorea una conexión RTP, para proporcionar información acerca de la calidad de servicio, obteniendo estadísticas acerca de los paquetes enviados y perdidos, el jitter y el retraso de ida y vuelta (RTT^{66}) en la conexión.

Existe una variante llamada SRTP⁶⁷, definida en RFC 3711, la cual define un perfil de RTP, con el fin de proporcionar cifrado, autenticación del mensaje e integridad, y protección contra reenvíos a los datos RTP en aplicaciones unicast y multicast.

RTSP⁶⁸ definido en RFC 2326, es un protocolo a nivel de aplicación, no orientado a conexión, que establece y controla uno o más flujos sincronizados de datos, ya sean de audio o de video. Es similar al protocolo HTTP, en cuanto el cliente y el servidor pueden hacer peticiones, sin embargo, difieren en que debe mantener información de estado. Su similitud con HTTP lo hace un protocolo totalmente adaptable a proxys y firewalls. Además es compatible con el modo de difusión multicast e independiente de la capa de transporte usada: puede utilizar tanto TCP como UDP.

Como principales desventajas se puede mencionar el hecho de que depende de la congestión de red, por lo que la pérdida de paquetes durante la transmisión es imprevisible, además de que si se trabaja en modo unicast, necesita un ancho de banda mayor.

Finalmente me referiré al protocolo RSVP⁶⁹, definido en RFC 2205 el año 1997 y actualizado en el año 2000 en el RFC 2750 (RSVP, *Extensions for Policy Control*). Este protocolo es utilizado para mejorar la calidad de servicio de la comunicación, eliminando las situaciones en que se degrade la calidad de la voz a causa de un tráfico de datos en la red, asignándole prioridad a los paquetes que necesiten ser transmitidos en tiempo real. Para lograr dicho propósito RSVP solicita ancho de banda, divide los paquetes de datos grandes y da prioridad a los paquetes de voz cuando se congestiona un router.

⁶⁶ RTT: Round Trip Time

⁶⁷ SRTP: Secure RTP

⁶⁸ RTSP: Real Time Streaming Protocol

⁶⁹ RSVP: Resource ReSerVation Protocol

A pesar de que RSVP ayuda considerablemente a la mejora de la calidad de los servicios multimedia, éste no garantiza una calidad de servicio como es el caso de redes tales como ATM.

2.6 RESUMEN

En este capítulo se analizaron los distintos procesos que se deben realizar para establecer una comunicación de VoIP, incluyendo los protocolos mas utilizados para la gestión de estas llamadas de entre los cuales podemos destacar las familias de protocolos H.323 y SIP.

H.323 es una recomendación de la ITU que describe los terminales y dispositivos generales para proporcionar servicios de comunicaciones sobre una red paquetizada que no ofrece calidad de servicio. Por otro lado SIP, desarrollado por la IETF que está basado en HTTP.

Una de las diferencias fundamentales entre estos dos protocolos es que H.323 está basado en un bloque monolítico derivado de H.320 para redes conmutadas por circuitos, mientras que SIP está basado en texto, que aprovecha la ventaja de utilizar las características de baja demanda de ancho de banda, que es primordial para comunicaciones que requieran de calidad de servicio, por lo que en este diseño se ha decidido utilizar el protocolo SIP, que además consta de estructura más simple y es mas masivo actualmente.

CAPÍTULO III. SEGURIDAD EN REDES VPN

3.1 INTRODUCCIÓN

Con el amplio desarrollo que han tenido actualmente las redes de comunicación, ha surgido un problema muy común actualmente en la empresa, que las ha llevado a invertir grandes sumas de dinero para poder solucionarlo o cuanto menos estar preparado ante una posible amenaza. Este problema es la seguridad de la información.

La red corporativa muchas veces almacena información de vital importancia, tanto para la empresa como para los clientes. Información confidencial, que en las manos equivocadas puede generar pérdidas incalculables tanto económicas como también de confianza del cliente hacia la empresa, lo que genera un clima de inseguridad.

Para solucionar este problema es que se deben tomar todas las medidas necesarias para proteger la información que se desea transmitir, esto incluye un complemento en soluciones de software y hardware, que brinden las herramientas necesarias para evitar un posible ataque que comprometa la información corporativa.

Los puntos que se deben tener en cuenta para el diseño de la seguridad de la red son los siguientes:

- Servicios ofrecidos vs. Seguridad provista: Aquí se evalúa que cada servicio ofrecido a un usuario tiene, en mayor o menor grado, su propio riesgo de seguridad.
- Facilidad de uso vs. Seguridad: Lamentablemente al establecer más medidas de seguridad para comunicarse por una red, se hace más complejo para el usuario.
- Costo de la seguridad vs. Riesgo de pérdida: Los costos que se manejan por efectos de seguridad en la redes no son solo económicos, sino también de desempeño de ésta y de

facilidad de uso. Sin embargo los riesgos de pérdida pueden ser de privacidad de datos, y servicios, por lo que todos estos factores deben ser balanceados.

3.2 ANÁLISIS DE RIESGO

Para poder resguardar la información que se desea transmitir por éste diseño es necesario realizar un Análisis de Riesgo, que nos permite determinar principalmente qué se necesita proteger, de qué protegerlo, y cómo hacerlo. Para lograr este cometido se deben analizar principalmente dos puntos fundamentales, que son, primero identificar los objetivos clave que se desean proteger, ya sea equipos, terminales, software o simplemente datos en general y el segundo punto es identificar las amenazas a las que está expuesta nuestra red, que pueden ser muy variadas, por lo que la solución debe ser acorde a la situación.

3.3 OBJETIVOS CLAVE

Debido al grado de seguridad solicitado para el diseño, nuestro objetivo de seguridad debe incluir todos los elementos de la red, llámese Hardware, Software o Datos. Desde que los datos salen desde el equipo o terminal de una Sucursal, hasta que transitan a través de la red pública de Internet e ingresan a otra sucursal o a la Casa Central. Es por ésto que se determinó que la solución más apropiada para el diseño sería una Red Privada Virtual, donde gracias a sus funcionalidades podremos proteger tanto el tráfico de datos, como también el tráfico VoIP que circulará a través de los túneles VPN generados por IPSec.

Las medidas consideradas para la protección de la red serán de Hardware y Software, dentro de las cuales se incluyen algoritmos de cifrado, certificados digitales, además de un conjunto de protocolos necesarios para la gestión de claves criptográficas y equipamiento de seguridad para redes de primer nivel.

3.4 IDENTIFICACIÓN DE LAS AMENAZAS

Las amenazas a las que están sujetas las comunicaciones a través de una red pública son muy variadas y muchas veces imperceptibles para el usuario, hasta que han causado un daño, que puede traer nefastas consecuencias para la empresa.

Según se estipula en el RFC 2196⁷⁰, las amenazas de seguridad en las redes de comunicación de datos se pueden clasificar en tres tipos:

- Acceso no autorizado a recursos y/o información
- Exposición no autorizada de información
- Ataques de Rechazo del servicio (DoS⁷¹)

En este diseño se deberán adoptar medidas para prever ataques de estas tres categorías, debido a que los datos no solo transitan a través de una LAN, sino que también lo hacen a través de Internet, por lo que el nivel de riesgo sube considerablemente.

Las amenazas de seguridad a las que se puede ver expuesta ésta red son las siguientes:

Rastreo. Consiste en una aplicación o dispositivo capaz de supervisar y leer los paquetes de la red, capturando todo el tráfico de ésta, por lo que de no estar cifrado, son capaces de obtener una vista completa de los datos del paquete.

Modificación de datos. Un atacante podría ser capaz de modificar y enviar datos falsos, capaces de impedir que el destinatario obtenga la información correcta o que permita al atacante obtener la información protegida.

Contraseñas. Obtener una contraseña y hacer uso de ella fraudulentamente.

⁷⁰ RFC 2196: Site Security Handbook

⁷¹ DoS: Denial of Service

Suplantación de direcciones. Consiste en un ataque mediante softwares que imitan un equipo miembro de una red para poder acceder a ella.

Nivel de aplicación. Este ataque va dirigido a servidores de aplicaciones al explotar las debilidades del sistema operativo y de las aplicaciones del servidor.

Intermediario (MitM⁷²). En este tipo de ataque, alguien entre los dos equipos comunicantes está supervisando activamente, capturando y controlando los datos de forma desapercibida.

Denegación de servicio. El objetivo de este ataque es impedir el uso normal de equipos o recursos de la red. Se logra mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios.

3.5 PROTOCOLOS DE SEGURIDAD

3.5.1 SERVICIOS DE SEGURIDAD SSL

SSL o TLS, proporciona servicios de seguridad de confidencialidad e integridad, y sólo opcionalmente, autenticación, debido a que es capas de soportar autenticación a nivel de usuarios, a nivel de servidor o simplemente carecer de autenticación alguna. Al existir autenticación de al menos una de las partes, el túnel criptográfico es resistente a ataques MitM, que consiste en un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. El túnel IPSec es resistente a este ataque debido a que para autenticarse, cada entidad debe presentar una cadena de certificados, llamados Certificados Digitales, que conduzcan a una Autoridad de Certificación, aceptada por la otra parte, por lo que la seguridad de ésta etapa está basada en estos certificados. Para todo este proceso de negociación se utilizan los servicios de la PKI.

⁷² MitM: Man in the Middle

Dentro de los protocolos que intervienen para establecer una comunicación SSL segura, uno de los protocolos más importantes con respecto a este ámbito de la conexión es el Subprotocolo de Negociación (*Handshake Protocol*), el cual está encargado de la negociación de protocolos de seguridad, tales como la versión del protocolo, la firma digital, compresión, los parámetros de autenticación, las técnicas de clave pública para la negociación de los secretos compartidos y los algoritmos de cifrado para la encriptación de los datos, haciéndolos ilegibles para un posible atacante que los intercepte, ya que estos solo podrán ser descifrados con un código de autenticación o MAC (*Message Authentication Codes*), incluido en el mensaje, el cual permite además detectar modificaciones ilegítimas a la información que transita por el túnel criptográfico.

3.5.2 SERVICIOS DE SEGURIDAD IPSEC

Como se observó en el Capítulo I de este Trabajo de Titulación, IPsec es un protocolo de seguridad para la capa de red IP, dotándola de protección criptográfica, tanto para IPv4 como para IPv6, manteniendo la interoperabilidad entre los dispositivos y equipos que implementen esta solución. En su estructura destacan múltiples protocolos, cada uno de los cuales se encarga de llevar a cabo una tarea determinada dentro de la arquitectura IPsec, ya sea gestión de claves criptográficas, autenticación, confidencialidad, entre otras.

Para asegurar la autenticación, integridad y confidencialidad de la comunicación IPsec hace uso de dos protocolos, específicamente AH y ESP y para la autenticación y el intercambio de claves el protocolo IKE, de los cuales hablaremos a continuación.

De forma breve, el proceso de negociación de claves se lleva a cabo en dos fases:

Fase 1. Aquí se negocian los sistemas que establecerán el túnel seguro, se autentican mutuamente utilizando cualquiera de los métodos previstos para ello en el estándar, y acuerdan los parámetros de seguridad que se utilizarán en la Fase 2 de la negociación.

Fase 2. Esta negociación se lleva a cabo cada vez que es necesario establecer una nueva asociación de seguridad entre dos entidades IPsec. Una vez que se ha protegido el tráfico en la fase 1, se negocian los parámetros de seguridad concretos con los que se protegerá la comunicación de capas superiores. Entre los aspectos que se negocian se encuentran el protocolo a utilizar para proteger la información: ESP o AH, de los cuales me referiré a continuación.

Para la protección de los datos se utilizan dos protocolos específicos, que pueden utilizarse juntos o separados, ya sea en modo túnel o modo transporte. Sin embargo como ya se mencionó en este trabajo se utilizará el modo túnel de IPsec para establecer la VPN.

AH - Cabecera de autenticación (*Authentication Header*). El protocolo AH cuyo soporte en una implementación IPsec es opcional, ofrece servicios de integridad y autenticación del origen de los datos, con la posibilidad a elección del receptor de utilizar técnicas para evitar el reenvío de paquetes. Adicionalmente, proporciona servicios de control de acceso mediante la distribución de claves criptográficas según se defina en las políticas de seguridad que gobiernan IPsec.

ESP - Carga de Seguridad Encapsulada (*Encapsulating Security Payload*). El soporte de este protocolo a diferencia de AH es obligatorio en una implementación IPsec, sin embargo ofrece los mismos servicios que AH, incluyendo confidencialidad, la que se aplica parcialmente también a los datos relativos al tráfico original. Adicionalmente, ESP es capaz de ofrecer resistencia a ataques de reenvío de mensajes, como también, contar con protección frente a posibles ataques de análisis de tráfico si la arquitectura de seguridad IPsec se utiliza para funcionar en modo túnel como este caso, de forma que la información que un posible atacante pueda recuperar se limite a la mínima indispensable para encaminar los mensajes desde el equipo o red de origen hasta el destinatario.

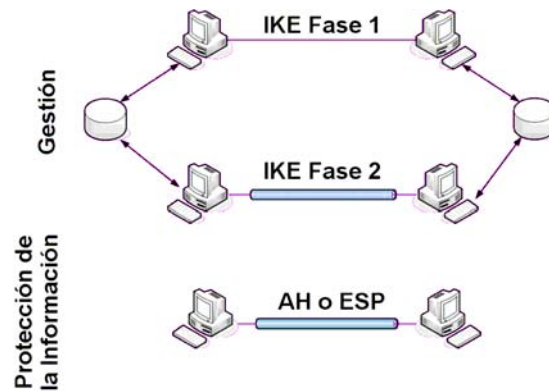


Figura 25. Gestión y protección de datagramas IPSec.

3.6 MÉTODOS DE AUTENTICACIÓN

La autenticación de usuario es uno de los procesos más importantes para proveer de seguridad a una comunicación VPN, gracias a ella un usuario puede ser reconocido como tal y un posible atacante también puede ser reconocido, para denegarle el acceso.

Existen variados métodos para la autenticación de usuarios VPN, sin embargo algunos más seguros que otros y de acuerdo a ello se hará la selección del método que se utilizará para este diseño en particular. Algunos de los métodos más confiables de autenticación son los siguientes.

3.6.1 CERTIFICADO DIGITAL

Un Certificado Digital es un documento digital mediante el cual una Autoridad de Certificación (CA) integrada en la PKI, garantiza que la clave pública pertenece a un usuario o entidad determinada.

Los Certificados digitales más utilizados actualmente para la validación de la clave pública en redes VPN son los regidos por el estándar UIT-T X.509, definidos en el RFC 3280⁷³.

⁷³ RFC 3280: Internet X.509 Public Key Infrastructure Certificate

Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

- Nombre, dirección y domicilio del suscriptor.
- Identificación del suscriptor nombrado en el certificado.
- El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
- La clave pública del usuario.
- La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
- El número de serie del certificado.
- Fecha de emisión y expiración del certificado.

Además de estos campos, para que el certificado sea válido debe estar aprobado por la institución que corresponda en cada país, correspondiendo en el caso a Chile al Ministerio de Economía.

3.6.2 FUNCIONES HASH

Otra herramienta muy importante en cuanto a seguridad de redes privadas virtuales son las funciones de Hash, las cuales se refieren a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. Un hash es el resultado de dicha función o algoritmo.

Una función de Hash es una función para resumir o identificar probabilísticamente un gran conjunto de información, dando como resultado un conjunto imagen finito generalmente menor. Varían en los conjuntos de partida y de llegada y en cómo afectan a la salida similitudes o patrones de la entrada.

Como se ha observado anteriormente las funciones Hash son usadas en múltiples aplicaciones tales como criptografía, procesamiento de datos, firmas digitales, entre otros. Una buena función de hash es una que experimenta pocas colisiones en el conjunto esperado de entrada; es decir que se podrán identificar unívocamente las entradas.

Hay muchos algoritmos de este tipo, sin embargo para esta aplicación los más utilizados son los siguientes:

MD5 (Message-Digest Algorithm 5). El Algoritmo de Resumen del Mensaje 5 es uno de los algoritmos de reducción criptográficos diseñados por el profesor Ronald Rivest del MIT⁷⁴. Fue desarrollado en 1991 y definido en el RFC 1321 como reemplazo del algoritmo MD4 después de que Hans Dobbertin descubriese su debilidad.

Debido al descubrimiento de métodos sencillos para generar colisiones de Hash, debido al tamaño del Hash (128 bit), muchos investigadores recomiendan su sustitución por algoritmos alternativos tales como SHA 1 o RIPEMD-160.

SHA-1 (Secure Hash Algorithm 1). Diseñado por NIST⁷⁵ y definido en el RFC 3174 el año 2001. Produce un valor Hash de 160-bits. Su diseño tiene mucha relación con MD5 pero con ciertas diferencias, la principal es la salida de 160 bit, gracias a lo cual se considera más seguro que MD4 y MD5.

3.6.3 ETOKEN

eToken es el un dispositivos USB de la empresa Aladdin Knowledge Systems Ltd⁷⁶ para procesos de autenticación que proporciona soluciones de administración de contraseñas y autenticación fuerte de usuarios.

⁷⁴ MIT: Massachusetts Institute of Technology

⁷⁵ NIST: National Institute of Standards and Technology

⁷⁶ Aladdin Knowledge Systems Ltd: www.aladdin.com/

Específicamente me enfocaré en la solución etoken para reforzar la seguridad VPN, que garantiza que solo personas autorizadas accedan a la información de la red, lo que permite proteger los datos, reducir los costes en infraestructura de seguridad y aumentar la productividad al dar movilidad a los trabajadores y clientes que quieran acceder a algún recurso de la red de forma segura.

Los avances en seguridad para VPN que brinda este dispositivo se basan principalmente en la autenticación para PKI, que ofrece seguridad y movilidad para claves privadas, esto debido a que para obtener un mayor grado de seguridad, cada usuario debe tener una clave privada única y personal, la cual le permite acceder con seguridad a redes o páginas web protegidas o firmar digitalmente datos y transacciones, con una prueba irrefutable de su autenticidad. Un proceso efectivo de firma digital y autenticación fuerte depende de la seguridad con la que se guarde la clave privada.

Las claves privadas generadas y almacenadas en un entorno informático, como un PC, pueden quedar expuestas y comprometidas, por lo que una firma digital creada con una clave privada basada en software no garantiza que la firma provenga de su propietario legítimo. eToken elimina esta vulnerabilidad generando y almacenando claves y certificados seguros PKI en una tarjeta inteligente, con lo cual se obtiene un elevado nivel de seguridad gracias a la generación de claves PKI y a la ejecución de operaciones criptográficas en el propio dispositivo eToken, sin exponer la clave privada.

Algunas de las ventajas de las tarjetas inteligentes USB eToken para PKI son las siguientes:

Almacenamiento de claves seguro. Las tarjetas inteligentes eToken contienen dispositivos de alta seguridad que permiten la generación de claves cifradas y la ejecución de operaciones criptográficas en el dispositivo. Esto significa que las claves privadas confidenciales no quedarán expuestas en entornos informáticos inseguros y no serán vulnerables a virus, gusanos, troyanos y otras amenazas comunes.

Autenticación fuerte de dos factores. Los usuarios deben conectar su dispositivo eToken y escribir una contraseña/PIN para autenticarse o firmar digitalmente datos y transacciones.

Portabilidad. Ya que las claves se almacenan con seguridad en el dispositivo eToken, puede usarlas donde quiera y cuando quiera, y desde cualquier ordenador con puerto USB.

Fácil de usar. Los usuarios pueden llevar a cabo operaciones PKI de un modo sencillo e intuitivo, de la misma forma en que usan su eToken para otras aplicaciones de seguridad.

Infraestructura más ligera. Las tarjetas inteligentes USB de autenticación eToken proporcionan funciones de administración de contraseñas y autenticación exhaustiva sin necesidad de servidor o lector único.

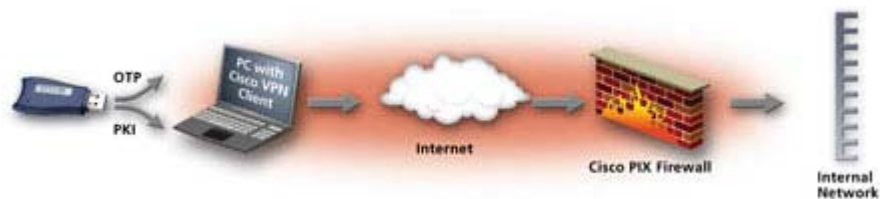


Figura 26. Diagrama dispositivo eToken

3.7 PROTECCIÓN DE LA INFORMACIÓN POR SOFTWARE

3.7.1 CRIPTOGRAFÍA

Para que los datos enviados en una VPN lleguen a su destino de forma segura, lo primero que necesitamos es contar con un canal seguro, esto se logra garantizando que el mensaje que se envía sea legible para el receptor e idéntico al enviado originalmente, además de que la información viaje codificada a través del túnel para evitar que sea interceptada e interpretada por algún usuario no autorizado.

Actualmente existen dos tipos de encriptación para los paquetes que se transmiten a través de los túnele VPN: Simétricas y Asimétricas.

Los modernos algoritmos de encriptación simétricos (Clave privada) mezclan la transposición y la permutación, mientras que los de clave pública se basan más en complejas operaciones matemáticas.

Los sistemas de clave simétrica ofrecen confidencialidad, mientras que los sistemas de clave pública ofrecen autenticidad, integridad, confidencialidad en el envío y no repudio si van asociados a una firma digital.

3.7.2 CLAVE PRIVADA (SIMÉTRICA)

Estos algoritmos de encriptación utilizan una clave para la encriptación y descryptación del mensaje, la cual debe ser intercambiada entre los equipos por medio de un canal seguro debido a que ambos extremos deben tener la misma clave para cumplir con el proceso.

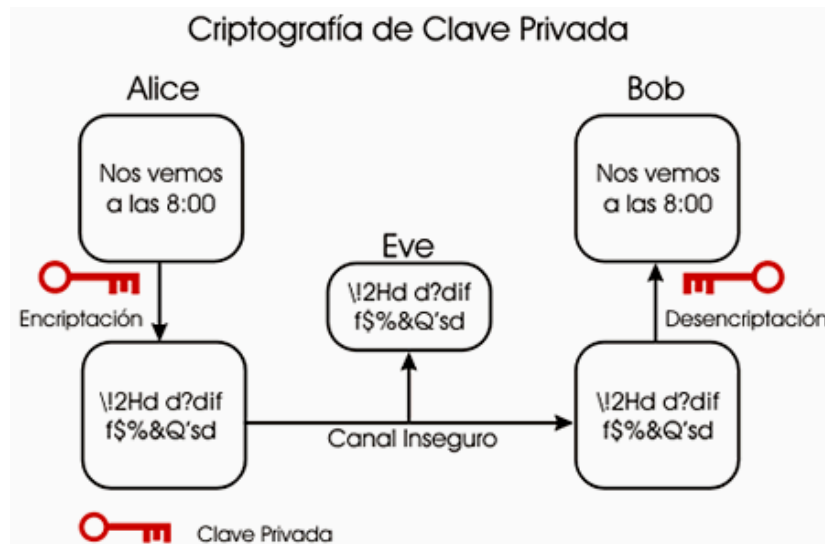


Figura 27. Criptografía de Clave Privada

Para que un algoritmo de este tipo sea considerado fiable debe cumplir algunos requisitos básicos:

- Una vez que se conoce el criptograma (texto cifrado) no se pueden obtener de él ni el texto en claro ni la clave.
- Cuando se conoce el texto en claro y el texto cifrado debe resultar más caro en tiempo o dinero descifrar la clave que el valor posible de la información obtenida por terceros.

Las principales desventajas de los métodos simétricos son la distribución de las claves, el peligro de que muchas personas deban conocer una misma clave y la dificultad de almacenar y proteger muchas claves diferentes. Algunos de los principales algoritmos de encriptación se adjuntan a continuación.

Algoritmo de Encriptación DES⁷⁷. Este Algoritmo de encriptación trabaja con claves simétricas, fue desarrollado en 1977 por la empresa IBM, se basa en un sistema monoalfabético, con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones. Inicialmente el texto a cifrar se somete a una permutación, con bloque de entrada de 64 bits (o múltiplo de 64), para posteriormente ser sometido a la acción de dos funciones principales, una función de permutación con entrada de 8 bits y otra de sustitución con entrada de 5 bits, en un proceso que consta de 16 etapas de cifrado.

En general, DES utiliza una clave simétrica de 64 bits, de los cuales 56 son usados para la encriptación, mientras que los 8 restantes son de paridad, y se usan para la detección de errores en el proceso.

Algoritmo de Encriptación Triple DES. Actualmente se utiliza el Triple DES con una clave de 128 bits y que es compatible con el DES visto anteriormente. Este nuevo algoritmo toma una clave de 128 bits y la divide en dos de 64 bits cada una. Primero se le aplica al documento a cifrar

⁷⁷ DES: Data Encryption Standard

un primer cifrado mediante la primera clave, C1, luego al resultado (denominado ANTIDES) se le aplica un segundo cifrado con la segunda clave, C2 y por último al resultado se le vuelve a aplicar un tercer cifrado con la primera clave, C1.

Algoritmo de Encriptación RC5. RC5 es un algoritmo de cifrado por bloques. Fue diseñada por Ronald Rivest en 1994, RC son las siglas en inglés de "Cifrado de Rivest". RC5 tiene tamaño variable de bloques (32, 64 o 128 bits), con tamaño de clave (entre 0 y 2040 bits) y número de vueltas (entre 0 y 255). La combinación sugerida originalmente era: bloques de 64 bits, claves de 128 bits y 12 vueltas.

Una característica importante de RC5 es el uso de rotaciones dependientes de los datos; uno de los objetivos de RC5 era promover el estudio y evaluación de dichas operaciones como primitivas de criptografía. RC5 también contiene algunas unidades de sumas modulares y de compuertas EXOR. La estructura general del algoritmo es una red tipo Feistel. Las rutinas de cifrado y descifrado pueden ser especificadas en pocas líneas de código, pero la programación de claves es más complicada. La simplicidad del algoritmo junto con la novedad de las rotaciones dependientes de los datos han hecho de RC5 un objeto de estudio atractivo para los criptoanalistas.

Algoritmo de Encriptación IDEA⁷⁸. El Algoritmo Internacional de Cifrado de Datos es un cifrador por bloques diseñado por Xuejia Lai y James L. Massey de la Escuela Politécnica Federal de Zúrich y descrito por primera vez en 1991. Fue un algoritmo propuesto como reemplazo del DES (Data Encryption Standard). Originalmente IDEA había sido llamado IPES (Improved PES, del inglés PES Mejorado).

opera con bloques de 64 bits usando una clave de 128 bits y consiste de ocho transformaciones idénticas (cada una llamada un ronda) y una transformación de salida (llamada media ronda). Gran parte de la seguridad de IDEA deriva del intercalado de operaciones de distintos grupos, adición y multiplicación modular y EXOR bit a bit, que son algebraicamente "incompatibles" en cierta forma.

⁷⁸ IDEA: International Data Encryption Algorithm

El algoritmo de descryptación es muy parecido al de encriptación, por lo que resulta muy fácil y rápido de programar, y hasta ahora no ha sido roto nunca, aportando su longitud de clave una seguridad fuerte ante los ataques por fuerza bruta (prueba y ensayo).

Este algoritmo es de libre difusión y no está sometido a ningún tipo de restricciones o permisos nacionales, por lo que se ha difundido ampliamente, utilizándose en sistemas como UNIX y en programas de cifrado de correo como PGP, además es considerado por muchos como uno de los cifrados en bloque más seguros que existen.

3.7.3 CLAVE PÚBLICA (ASIMÉTRICA)

Este tipo de algoritmos de encriptación se basa en el uso de dos claves diferentes, claves que poseen una propiedad fundamental: una clave puede descryptar lo que la otra ha encriptado.

Una de las claves de la pareja, llamada clave privada, es usada por el propietario para encriptar los mensajes, mientras que la otra, llamada clave pública, es usada para descryptar el mensaje.

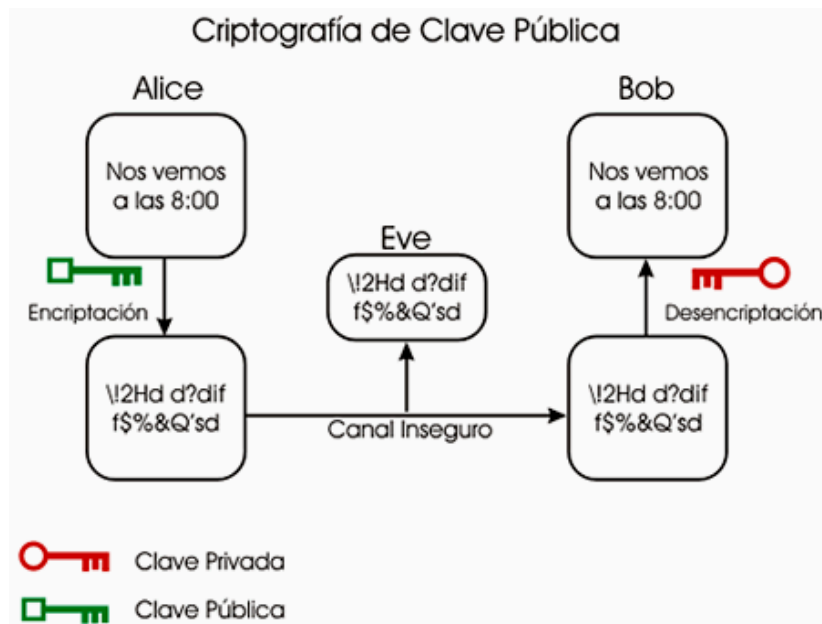


Figura 28. Criptografía de clave pública

Las claves pública y privada tienen características matemáticas especiales, de tal forma que se generan siempre a la vez, por parejas, estando cada una de ellas ligada intrínsecamente a la otra.

Mientras que la clave privada debe mantenerla en secreto su propietario, ya que es la base de la seguridad del sistema, la clave pública es difundida, para que esté al alcance del mayor número posible de personas, existiendo servidores que guardan, administran y difunden dichas claves.

Para que un algoritmo de clave pública sea considerado seguro debe cumplir con los siguientes puntos:

- Conocido el texto cifrado no debe ser posible encontrar el texto en claro ni la clave privada.
- Conocido el texto cifrado (criptograma) y el texto en claro debe resultar más caro en tiempo o dinero descifrar la clave que el valor posible de la información obtenida por terceros.
- Conocida la clave pública y el texto en claro no se puede generar un criptograma correcto encriptado con la clave privada.
- Dado un texto encriptado con una clave privada sólo existe una pública capaz de desencriptarlo, y viceversa.

El primer sistema de clave pública que apareció fue el de Diffie-Hellman, en 1976, y fue la base para el desarrollo de los que después aparecieron, entre los que cabe destacar el RSA como el más utilizado en la actualidad.

Diffie-Hellman. Este algoritmo de encriptación de Whitfield Diffie y Martin Hellman fue el punto de partida para los sistemas asimétricos, basados en claves pública y privada.

Su importancia se debe sobre todo al hecho de ser el inicio de los sistemas asimétricos, ya que en la práctica sólo es válido para el intercambio de claves simétricas, y con esta funcionalidad es muy utilizado en VPNs.

Matemáticamente se basa en las potencias de los números y en la función mod (módulo discreto). Uniendo estos dos conceptos se define la potencia discreta de un número como $Y = X^a \text{ mod } q$. Si bien el cálculo de potencias discretas es fácil, la obtención de su función inversa, el logaritmo discreto, no tiene una solución analítica para números grandes.

RSA. Este es el más conocido y usado de los sistemas de clave pública, y también el más rápido de ellos. Presenta todas las ventajas de los sistemas asimétricos, incluyendo la firma digital, aunque resulta más útil a la hora de implementar la confidencialidad el uso de sistemas simétricos, por ser más rápidos. Se suele usar también en los sistemas mixtos para encriptar y enviar la clave simétrica que se usará posteriormente en la comunicación cifrada.

El sistema RSA se basa en el hecho matemático de la dificultad de factorizar números muy grandes. Para factorizar un número el sistema más lógico consiste en empezar a dividir sucesivamente éste entre 2, entre 3, entre 4,..., y así sucesivamente, buscando que el resultado de la división sea exacto, es decir, de resto 0, con lo que ya tendremos un divisor del número.

El cálculo de estas claves se realiza en secreto en la máquina en la que se va a guardar la clave privada, y una vez generada ésta conviene protegerla mediante un algoritmo criptográfico simétrico.

3.8 FIREWALL

Un firewall o cortafuegos es un dispositivo que combina componentes de software y hardware, además de actividades de administración, que en conjunto administran la seguridad entre la red pública y la red de la cual son parte, por lo que todo el tráfico de entrada y salida debe pasar a través de él.

El enfoque de firewalls está basado en el concepto de permitir a los usuarios locales el uso de todos los servicios de red internos a su red local y otros servicios ofrecidos por la Internet, controlando, además, el acceso de los usuarios externos a los recursos de la red local, su modo de funcionamiento esta estipulado en el RFC 2979⁷⁹, que define las características de comportamiento y requerimientos de interoperabilidad.

3.8.1 FUNCIONES PRINCIPALES DE UN FIREWALL

Un firewall permite proteger una red privada contra cualquier acción hostil, al limitar su exposición a una red no confiable aplicando mecanismos de control para restringir el acceso desde y hacia ella al nivel definido en la política de seguridad.

La tarea de un firewall consiste en inspeccionar y controlar todo el tráfico entre la red local e Internet. De esta forma se intenta detectar y rechazar todo el tráfico potencialmente peligroso antes de que alcance otras partes de la red interna, en algunos casos también se efectúan registros de tales actividades.

La protección que provee un firewall es de diferentes tipos:

- Bloquea tráfico no deseado
- Redirecciona tráfico de entrada a sistemas internos de más confianza
- Oculta sistemas vulnerables, que pueden ser fácilmente asegurados, de Internet
- Puede registrar el tráfico desde y hacia la red privada
- Puede ocultar información como nombres de sistemas, topología de la red, tipos de dispositivos de red, e identificadores de usuarios internos, de Internet
- Puede proveer autenticación más robusta que las aplicaciones estándares

⁷⁹ RFC 2979: Behavior of and Requirements for Internet

Estas son algunas de las protecciones de las que provee un firewall, pero además de protecciones el firewall cumple la función de hacer disponibles a la red pública de forma segura, los servicios y productos de la compañía, ofrecidos por esta red protegida.

3.9 RESUMEN

Según los datos recavados en la investigación en este diseño se utilizará el protocolo IPSec para la conexiones sitio a sitio entre sucursales y la casa central, esto debido principalmente a la robusta seguridad y su estructura modular que agrupa y brinda soporte para la mayoría de protocolos de encriptación y autenticación. También se contempla la incorporación de usuarios remotos mediante la tecnología VPN SSL, que es de fácil configuración y brinda excelentes políticas de seguridad para este tipo de usuarios.

Los protocolos de encriptación y gestión de las comunicaciones VPN IPSec seleccionados para este diseño son los siguientes:

- Triple Digital Encryption Standard (3DES) para encriptar la Internet Key Exchange (IKE) y el tráfico IPSec.
- IP GRE con IPSec en modo túnel.
- Diffie-Hellman Group 2 (1024 bit) para IKE.
- Secure Hash Algorithm (SHA) 160-bit y Keyed Hashing para Message Authentication (HMAC) con Message Digest 5 (MD5)
- Preshared keys

CAPITULO IV. SEGURIDAD EN VOIP

4.1 INTRODUCCIÓN

En este capítulo se analizarán las principales amenazas que afectan a las comunicaciones VoIP, incluyendo las vistas anteriormente de las redes y enfocándose principalmente en las propias de la tecnología VoIP, producto de las falencias en cuanto a seguridad de los protocolos que establecen la comunicación.

Como veremos existen variadas formas de mitigación de las técnicas de intrusión y ataques, sin embargo no existe un modelo que garantice la total seguridad de la comunicación debido al continuo avance que experimentan dichas técnicas y el afán de personas por vulnerar los sistemas y hacer pública o conocer información confidencial que les pudiera prestar un beneficio.

La mejor técnica contra los ataques es la prevención, por lo que este diseño contempla medidas de seguridad primero que nada de prevención y posteriormente mitigación de los posibles ataques que pudieran interferir o interceptar las comunicaciones de la empresa.

4.2 ANÁLISIS GENERAL

Debido a que VoIP se basa necesariamente en muchas otras capas y protocolos de las redes de datos, esta tecnología se beneficia de las ventajas de todos ellos, pero inevitablemente también hereda las desventajas de éstos, incluyendo las falencias de seguridad vistas en el capítulo anterior, que la hacen una tecnología muy susceptible a ataques, a los cuales nos referiremos más adelante, incluyendo también ataques que son propios de ésta tecnología.



Figura 29. Seguridad en VoIP

En la figura 29 se observa que VoIP se construye sobre muchas otras capas de seguridad de la información, sin embargo, cada una de ellas está expuesta a distintas amenazas de seguridad, las cuales se mencionan a continuación.

Capa	Ataques y vulnerabilidades
Políticas y procedimientos	Contraseñas débiles Mala política de privilegios Acceso permisivo a datos comprometidos
Seguridad física	Acceso físico a dispositivos sensibles Un gatekeeper Reinicio de maquinas Denegación de servicios
Seguridad de red	DDoS ICMP Unreachable SYN floods Gran variedad de floods
seguridad en los servicios	SQL Injections Denegación en DHCP DoS

Seguridad en el S.O	Buffer Overflows Gusanos y virus Malas configuraciones
Seguridad en las aplicaciones y protocolos de VoIP	Fraudes SPIT (SPAM) Vishing (Phishing) Fuzzing Floods (INVITE, REGISTER, ETC) Secuestro de sesiones (HIJACKING) Interceptación (Eavesdropping) Redirección de llamadas (Call redirection) Reproducción de llamadas (CALL replay)

Como se puede observar los ataques a los que están propensas las redes de comunicación son muy variados y pueden tener como objetivo desde un robo de información confidencial, hasta degradar la calidad del servicio o simplemente anularla por completo como es el caso de los ataques DoS.

Para el atacante no sólo es importante el contenido de la información sino también los datos de la propia llamada, que utilizados de forma maliciosa permitirán al atacante realizar registros de las llamadas entrantes o salientes, configurar y redirigir llamadas, grabar datos, utilizar información para bombardear con SPAM, interceptar y secuestrar llamadas, reproducir conversaciones, llevar a cabo robo de identidad e incluso realizar llamadas gratuitas a casi cualquier lugar del mundo. Los dispositivos de la red, los servidores, sus sistemas operativos, los protocolos con los que trabajan y prácticamente todo elemento que integre la infraestructura VoIP podrá ser susceptible de sufrir un ataque.

La protección para una red debe estar regida por una política de seguridad, la estandarización más actual de éstas es la ISO27002:2007, formulada para certificarse con la norma UNE 17502:2005.



Figura 30. Modelo de una política de seguridad.

Los objetivos más importantes que buscan las Políticas de seguridad son:

- Comunicar a toda la organización el principio de ver a la información como el activo más valioso para la empresa.
- Sensibilizar al personal en la responsabilidad y obligaciones legales de protegerla.

4.3 CLASIFICACIÓN DE LOS ATAQUES

Como se mencionó anteriormente existen muchas amenazas a las cuales están expuestas las redes de VoIP, sin embargo la mayoría de estas son inherentes de las capas sobre las que se apoya dicha tecnología. Sin embargo hay otras que son propias de ésta tecnología, las cuales se aprovechan de las vulnerabilidades propias de estas redes y sus protocolos, para lo cual se buscarán las soluciones más propicias para éste diseño.

Las amenazas de las redes de VoIP las podemos clasificar en las siguientes categorías:

- Accesos desautorizados y fraudes.
- Vulnerabilidades de la red subyacente.
- Ataques de denegación de servicio
- Ataques a los dispositivos
- Enumeración y descubrimiento.
- Ataques a nivel de aplicación.

4.3.1 ACCESOS DESAUTORIZADOS Y FRAUDES

Una de las mayores amenazas a las cuales se ven expuestas principalmente las redes empresariales de VoIP, son los fraudes consecuencia de un acceso desautorizado a una red, pudiendo obtener datos de registro y/o contraseñas que posteriormente podrían utilizar para suplantar a un usuario legal, además de otros datos de clientes que muchas veces circulan a través de la red corporativa y que en las manos equivocadas pueden ocasionar daños devastadores. Sin embargo este problema se puede contrarrestar adquiriendo una buena política de seguridad, además de realizar un estricto control y registro de las llamadas que se cursan por la red de VoIP.

4.3.2 VULNERABILIDADES DE LA RED SUBYACENTE

Una de las principales ventajas de VoIP actualmente se ha convertido en una de sus peores amenazas, debido a que esta tecnología hace uso de las redes existentes para el tráfico IP, heredando con ella los problemas de seguridad de las redes IP. En el capítulo anterior se mencionaron algunos de los ataques a los cuales estaban expuestas las redes de datos, sin embargo además de estos, a la tecnología de VoIP se le suman algunos propios, por lo que para poder mitigar estos ataques es necesario estructurar la seguridad de tal manera que no queden puntos frágiles que den una puerta de entrada a un posible atacante que ponga en juego la información que transita por la red corporativa.

4.3.3 ATAQUES DE DENEGACIÓN DE SERVICIO

Como se mencionó en el capítulo anterior este tipo de ataques se caracteriza por degradar el rendimiento de los servicios de una red o un sistema, llegando al punto de hacerlo inaccesible para el resto de los usuarios.

Algunas de las técnicas más utilizadas para llevar a cabo este ataque consisten en el envío de paquetes que sean capaces de explotar alguna vulnerabilidad en el software o hardware del sistema, saturar los flujos de datos que se transmiten por la red o generar una sobrecarga de procesos que haga que colapsen los dispositivos.

Una variante de estos ataques es la llamada DDoS o ataques de Denegación de Servicios Distribuidos, que son similares a los anteriores pero mas efectivos, debido a que el ataque es efectuado de múltiples computadoras de forma coordinada, haciendo su objetivo predilecto a las redes de VoIP, debido a principalmente a la dependencia y la necesidad de garantías en QoS, que hacen que estas redes tengan menor tolerancia a problemas de rendimiento. Otra razón que acrecenta la debilidad de las redes VoIP frente a estos ataques es que en ésta arquitectura existen una gran cantidad de dispositivos, encargados cada uno de una tarea específica, por lo que el ataque sobre cualquiera de ellos puede producir un colapso de la comunicación VoIP.

Una forma muy eficaz de contrarrestar este tipo de ataques, como se verá en el próximo capítulo, es priorizando los paquetes que transportan la voz por sobre los paquetes de datos, ya que como se explicó anteriormente el atacante inyectará paquetes de datos en la red para que ésta colapse y se retrasen los paquetes de voz, sin embargo al asignarle una prioridad mayor a la voz se podría evitar este problema.

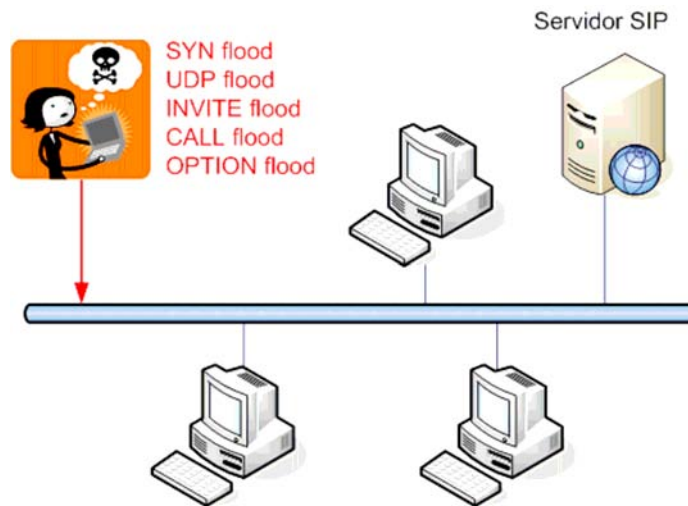


Figura 31. Ataque DoS

4.3.4 ATAQUES A LOS DISPOSITIVOS

Como se mencionó anteriormente algunos ataques DoS se enfocan a los dispositivos que forman la red VoIP, por lo tanto, los gateways, Proxys, teléfonos IP, entre otros, serán potencialmente objetivos a explotar por parte de un intruso. Hay que tener en cuenta que los dispositivos VoIP son tan vulnerables como lo es el sistema operativo o el firmware que ejecutan.

Algunos de los ataques más comunes son los llamados fuzzing, los cuales mediante paquetes mal formados que al ser procesados por el dispositivo de la red VoIP provocan que éste se cuelgue o reinicie. Otros ataques conocidos son los flooders, que tienen como objetivo los servicios y puertos abiertos en los dispositivos, generalmente producto de una mala configuración, lo que incluye dejar los equipos con sus configuraciones por defecto y una gran cantidad de puertos abiertos.

Los teléfonos IP sin un buen diseño que incluya medidas para mitigar las intrusiones son igual de vulnerables que cualquiera del resto de dispositivos de la red VoIP e igual de peligrosas.

4.3.5 DESCUBRIMIENTO Y ENUMERACIÓN

Los ataques de enumeración y descubrimientos consisten en obtener la mayor cantidad de información sobre la red que se desee atacar, esto se puede lograr gracias configuraciones deficientes, que dejen brechas en la seguridad, de las cuales se puede aprovechar un atacante. Actualmente existe una gran cantidad de herramientas que agilizan estos procesos y los hacen accesibles para atacantes no tan hábiles, por lo que el número de intrusos crece día a día.

Una vez que el intruso tenga información suficiente evaluará sus siguientes pasos eligiendo el método de ataque más adecuado para alcanzar su objetivo. De este modo en las primeras etapas el atacante realizará un proceso denominado footprinting u obtención de toda la información pública posible del objetivo.

Después de tener un listado de servicios y direcciones IP consistente, el atacante tratará de buscar agujeros de seguridad, vulnerabilidades y obtener la mayor información sensible de esos servicios mediante un proceso denominado Enumeración, con el fin de encontrar un medio de entrada a la red.

4.3.6 ATAQUES A NIVEL DE APLICACIÓN

El nivel de aplicación de la red IP es quizás uno de los más vulnerables, debido en parte a que VoIP engloba gran cantidad de protocolos y estándares, los que añaden su propio riesgo de seguridad. Un ejemplo claro de ellos es el protocolo SIP, muy discutido desde el punto de vista de la seguridad.

Entre los ataques específicos contra el nivel de aplicación de VoIP encontramos ataques de secuestro de sesión, desconexiones ilegales, inundación de peticiones, generación de paquetes malformados, falsificación de llamadas, entre otros.

4.3.6.1 CRACKEO DE CONTRASEÑAS SIP

El crackeo de contraseñas SIP es un proceso mediante el cual se modifica el proceso de autenticación de usuario, con el fin de obtener el password de un usuario y poder utilizar la identidad de la víctima de forma maliciosa.

4.3.7 ATAQUES DE LA SEÑALIZACIÓN

A continuación se detallan algunos de los ataques que se pueden conseguir capturando y manipulando los mensajes de señalización previos al establecimiento de la llamada.

4.3.7.1 SUPLANTACIÓN DE IDENTIDAD EN EL REGISTRO

Para que una comunicación VoIP que se desea establecer sea entre dos usuarios legítimos, necesariamente la comunicación que se establece entre cada uno de los usuarios y el servidor de registro en su etapa inicial, denominada registro de usuario, debe ser realizada de forma segura, de lo contrario no pueden existir garantías de que el usuario registrado sea quien dice ser durante todo el resto de la sesión.

A través de los mensajes *REGISTER*, los agentes de usuario SIP informan al servidor de su localización actual de manera que el servidor sepa dónde tiene que enviar peticiones posteriores. Si un servidor no autentica las peticiones *REQUEST*, cualquiera puede registrar cualquier contacto para cualquier usuario, y por lo tanto secuestrar su identidad y sus llamadas.

Cuando un Proxy recibe la petición para procesar la llamada (*INVITE*), el servidor realiza una búsqueda para identificar donde puede ser encontrado el destinatario. El mensaje *REGISTER* contiene el campo en la cabecera “*Contact*”, que indica la dirección IP del hardware o software VoIP del usuario destino, por lo que el Proxy redirige la petición *INVITE* hacia esta dirección IP. La forma de realizar este ataque es modificando esta cabecera *Contact* con la dirección del

atacante, y de esta forma el atacante suplanta al usuario legítimo, recibiendo todo el tráfico que iba dirigido hacia él.

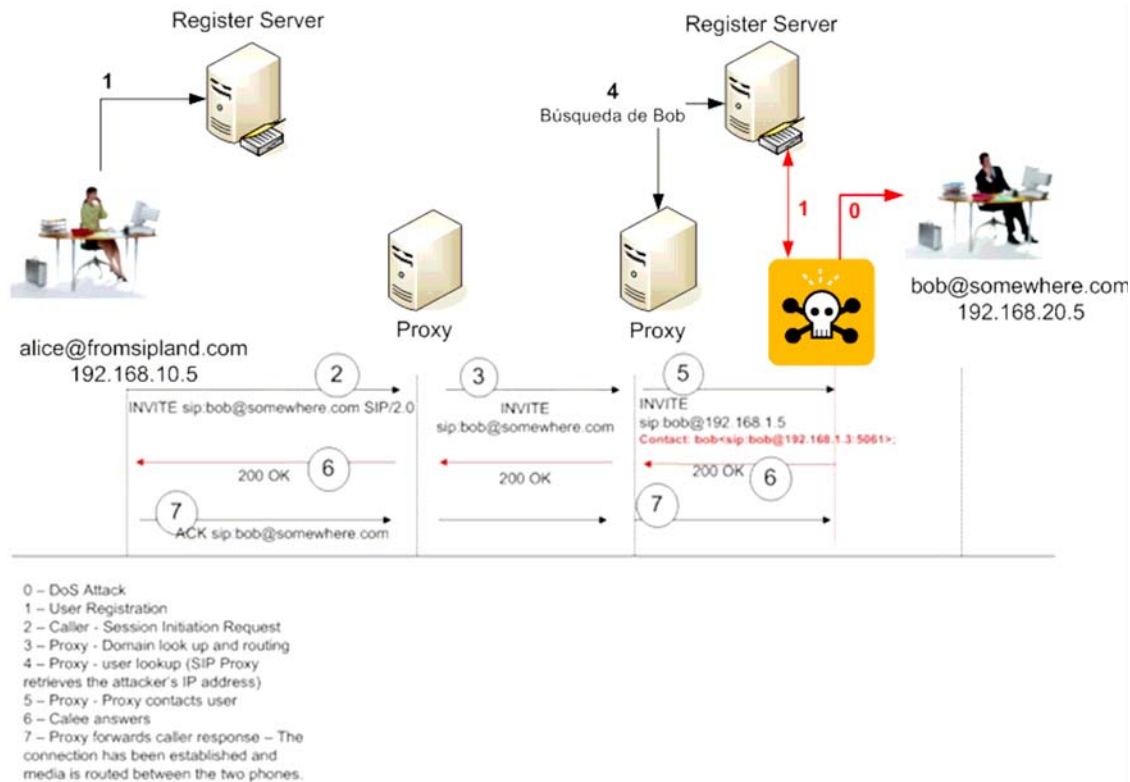


Figura 32. Suplantación de identidad en el registro

4.3.7.2 DESREGISTRAR USUARIOS

Este ataque es primordial para poder lograr la suplantación de los usuarios vista anteriormente. Las formas de llevar a cabo este ataque son principalmente:

- Ataques de denegación de servicios.
- Enviando peticiones *REGISTER* en un corto espacio de tiempo, de modo que se pueda anteceder a la petición del usuario original.
- Desregistrando el usuario con mensajes *REGISTER*.

El intruso puede ser capaz de desregistrar fácilmente un usuario, enviando al servidor de registro una petición REGISTER (simulando ser la víctima) con el siguiente campo “Contact: *” y valor del atributo “Expires” a cero. Esta petición eliminará cualquier otro registro de la dirección del usuario (especificada en el campo “To” de la cabecera). El atacante deberá realizar este envío periódicamente para evitar el re-registro del usuario legítimo o en su defecto provocarle un ataque DoS para evitar que vuelva a registrarse al menos por el tiempo que necesite para realizar el secuestro de la llamada.

4.3.7.3 DESCONEXIÓN DE USUARIOS

Este ataque es posible gracias a la falencia de algunos protocolos, incluido SIP, que envían los textos en claro, es decir, sin ningún tipo de encriptación, donde el atacante, suplantando al usuario legítimo, envía mensajes BYE de finalización de llamada, para lograr la desconexión de éste.

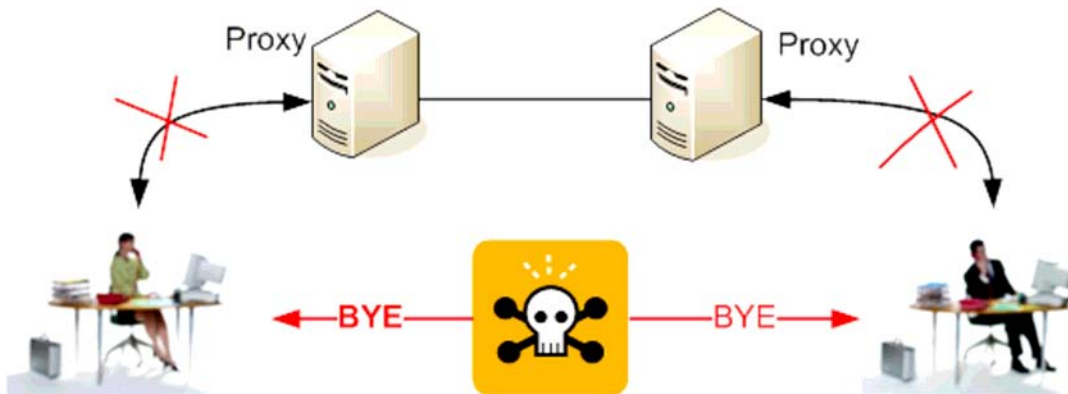


Figura 33. Desconexión de usuarios.

Se puede realizar un ataque similar utilizando mensajes CANCEL, pero solo afectan cuando se está estableciendo la llamada, es decir, antes de que el destinatario descuelgue el teléfono.

Otro tipo de ataques consistirían en utilizar mensajes ICMP-“port unreachable”, mensajes RESET del protocolo SCCP, o HANGUP para AIX.

4.3.7.4 REDIRECCIÓN DE LLAMADAS

Este es otro ataque bastante común en las redes de VoIP. Actualmente existen muchas formas de llevar a cabo este ataque, una de ellas es comprometiendo los servicios de los servidores o el *Call Manager*, con el fin de que éstos redirijan las llamadas donde el atacante se lo indique. Otros métodos de redirección de llamadas son los vistos con anterioridad, suplantación de identidad en el registro, Man in the Middle (MitM), entre otras.

4.3.8 MANIPULACIÓN DE LA TRANSMISIÓN

Algunos de los ataques posibles a través de la manipulación de la transmisión son los siguientes:

- **Eavesdropping.** Este es un ataque que se traduce literalmente como escuchar secretamente, es el término con el que se conoce la escucha de conversaciones VoIP por parte de clientes que no participan en dicha conversación.

Aunque es en principio un ataque completamente pasivo, lo más peligroso del eavesdropping es que es muy difícil de detectar mientras que se produce, de forma que un atacante puede capturar información privilegiada y claves para acceder a más información sin que nadie se de cuenta hasta que dicho atacante utiliza la información capturada, convirtiéndose en un atacante activo.

Para poder llevar a cabo este ataque en VoIP es necesario interceptar la señalización y los streams de audio de la conversación, donde los primeros utilizan protocolos UDP o TCP separadamente, mientras que los streams normalmente se transportan sobre UDP, utilizando el protocolo RTP.

Los procedimientos para llevar a cabo este ataque son los siguientes:

- Primero es necesario capturar y decodificar los paquetes RTP. Esto se logra al esnifar el tráfico de la comunicación, el cual permite además interpretar los paquetes UDP indicándole que son del protocolo RTP.
- Luego se selecciona un flujo de datos y se analiza, ya no como paquetes individuales, sino como un flujo continuo de datos.
- Posteriormente se rescata la información en un fichero de audio para su posterior reproducción.

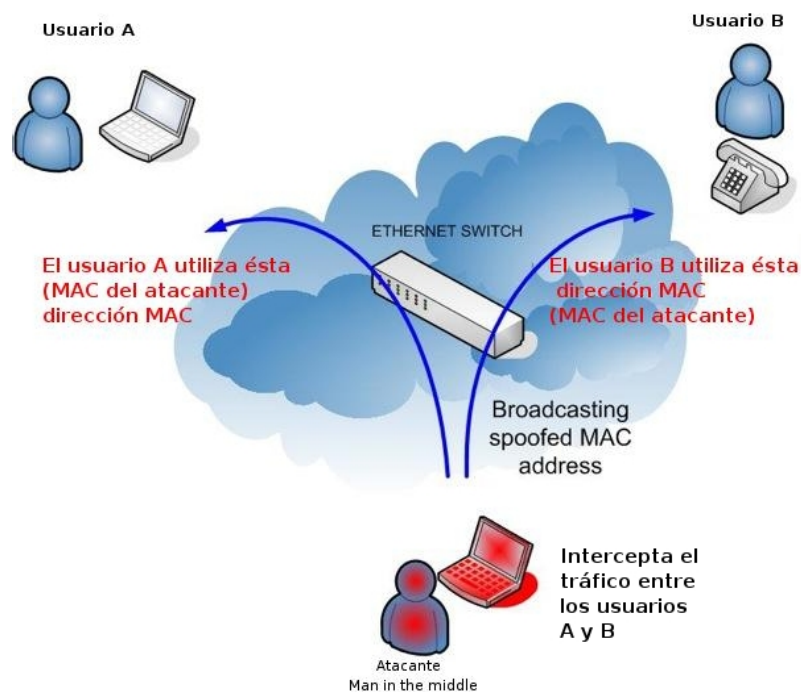


Figura 34. Intercepción de información

- **Insertión de Audio.** Como se ha observado anteriormente la transmisión del flujo de datos de las llamadas es realizada sobre el protocolo UDP, esto debido principalmente a su sencillez y eficiencia. La desventaja de utilizar este protocolo es que no garantiza la entrega de los mensajes y no mantiene información de estado o conexión. Es por éstas

deficiencias que este protocolo es muy susceptible a la inserción de paquetes UDP extraños.

Sumado a estas deficiencias del protocolo UDP, existen las propias del protocolo RTP, encargado del transporte de los paquetes UDP, y que tampoco lleva un control exhaustivo sobre el flujo de datos, relegando estas funciones al protocolo RTCP. El único método de control de tramas perdidas y reordenamiento de tramas es el campo número de secuencia de la cabecera.

Estos son los algunos de los principales protocolos sobre los que se basa el funcionamiento de SIP, por lo que podemos concluir que la inserción de paquetes frente a un atacante en una red insegura es bastante probable.

Estos ataques de inserción de tramas UDP se pueden dar en varios casos, uno de ellos es por ejemplo, que al dispositivo lleguen dos tramas UDP con el mismo número de secuencia y diferentes datos. En este caso dependiendo del dispositivo o de la implementación del software, podría darse el caso que se descarte la última trama por estar repetida, pero si la última fuera la trama legítima, se lograría el propósito del atacante de insertar tramas en el tráfico. Otra opción posible es que se sobrescriban los datos de la segunda a la primera al reordenar y reensamblar, sin embargo en ambos casos se estaría corrompiendo la información original insertando tramas UDP en el flujo RTP, que en el caso de una comunicación VoIP podrían corresponder a mensajes de audio.

- O **Fuzzing.** Este tipo de ataques fue desarrollado en 1990 por Barton Miller en la Universidad de Wisconsin en Madison, sin embargo actualmente se cuentan por decenas los programas de este tipo.

Los ataques Fuzzing también conocidos como testeo funcional del protocolo son muy utilizados para encontrar vulnerabilidades, errores o agujeros de seguridad en un sistema determinado. Esto lo logran enviando paquetes o peticiones especialmente mal estructuradas para comprobar como manejan los dispositivos, las aplicaciones o el mismo sistema operativo que implementa el protocolo. De aquí se llegan a situaciones que no han sido consideradas en el

diseño o implementación, por lo que generalmente terminan en un error, una denegación de servicio o en alguna otra vulnerabilidad, de las cuales se aprovechará el atacante para lograr su propósito.

Esta técnica actualmente se ha desarrollado para encontrar vulnerabilidades en la transmisión de VoIP, gracias a lo cual se han llegado a encontrar gran cantidad de ataques de DoS y buffer overflows en los productos que implementan los protocolos SIP y H.323.

4.4 MEDIDAS DE SEGURIDAD PARA LA RED VOIP

En este capítulo se han estudiado los principales ataques a los que están expuestas las redes de VoIP, además de las falencias de seguridad de los protocolos que hacen a esta tecnología el blanco perfecto para muchos atacantes. Como se pudo observar los ataques son muy variados y es casi imposible realizar un diseño que sea completamente seguro y efectivo frente a todos los ataques existentes y los que con seguridad seguirán desarrollando los intrusos en su afán de obtener información confidencial o simplemente como un desafío personal.

En esta sección me limitaré a señalar qué controles de seguridad deben ser imprescindibles en el entorno VoIP y explicar las medidas necesarias para paliar la mayoría de riesgos y ataques comentados anteriormente.

Uno de los primeros pasos en la protección de la red es mantener las actualizaciones y parches al día, para proteger la red frente a falencias en los softwares o en la configuración de los equipos que se utilizaran para el diseño de la red de VoIP. Además es muy recomendable la existencia en la red de sistemas de antivirus actualizados que la protejan de ataques de virus, gusanos y troyanos.

Como se ha observado los ataques a los cuales esta expuesto este diseño son muy variados, por lo que las medidas de seguridad deben ir enfocadas a cada uno de los servicios que se brindan, llámese transmisión de datos o voz, ambos sobre VPN para aumentar la seguridad de

la comunicación. Uno de los principales elementos de protección son los cortafuegos o Firewalls, los cuales puede repeler muchos de los ataques vistos anteriormente si se encuentran bien administrados.

Una medida muy efectiva contra muchos de los ataques que se realizan a las redes es la utilización de sistemas de detección de intrusos (IDS, *Intrusion detection system*) o de prevención (IPS, *Intrusion Prevention System*) en los lugares estratégicos de la red, algunos de ellos presentes en dispositivos que cumplen muchas funciones a la vez. Gracias a estos dispositivos se podrán detectar y prevenir ataques contra los protocolos que funciona VoIP (fuzzing), ataques contra servicios (exploits y vulnerabilidades), escaneos y ciertos tipos de ataques DoS.

Debido a que la comunicación VoIP transita sin cifrado, la información una vez capturada es interpretada sin mayor problema, por lo que es necesario la autenticación y el cifrado de los canales de señalización de las partes que intervienen en la comunicación cada vez que se envía un mensaje, para ello además los dispositivos deben tener limitado los grupos de elementos con los cuales están autorizados para enviar o recibir tráfico.

IPSec brinda una de las herramientas más importantes que aporta a la seguridad de la comunicación de datos o voz con su función de cifrado como fue visto en el capítulo anterior, con ello se pueden resolver la mayoría de los problemas de eavesdropping, manipulación y reproducción de los mensajes que se intercambian.

De no utilizar una VPN para la transmisión segura de los datos es posible utilizar una alternativa, el protocolo SRTP visto anteriormente, el cual brinda de cifrado a la información de la comunicación VoIP, ofreciendo confidencialidad, autenticación de mensajes y protección, evitando los ataques de interceptación e inserción de audio.

CAPITULO V. CALIDAD DE SERVICIO EN VOIP

5.1 INTRODUCCIÓN

La calidad de servicio en una solución VoIP es uno de los parámetros más importantes de la comunicación de voz sobre Internet, por lo que una buena combinación entre los protocolos de señalización y codificación es primordial para obtener una comunicación de calidad. Actualmente existe una gran variedad de estándares y protocolos para la gestión de comunicaciones de voz en redes IP sin embargo no todas presentan las mismas características, debido a lo cuál en el presente capítulo se realizará un estudio de las principales tecnología utilizadas para este servicio, de modo que la selección sea la más adecuada para el diseño.

5.2 DEFINICIÓN

Una descripción del concepto de “Calidad de Servicio” o QoS, se refiere a la capacidad de una red para sostener un comportamiento adecuado del tráfico que transita por ella, cumpliendo a su vez con los requerimientos de ciertos parámetros relevantes para el usuario final. En el caso de redes VoIP, la calidad de servicio (QoS) se ve perjudicada por una serie de problemas que afectan el tráfico normal de la información a través de la red. Los principales factores a considerar son: Latencia, el Jitter la pérdida de paquetes y el Eco, a los cuales nos referiremos en el desarrollo de este capítulo, además de los métodos de minimizar y hasta eliminar el efecto de dichos éstos en la comunicación.

Alguna de las técnicas mas utilizadas para mejorar la calidad de servicio de un enlace entre dos o más usuarios es la priorización del tráfico sensible al retardo, como es el caso de la voz, frente a información que no lo sea.

5.3 CLASIFICACIÓN DE QOS

Existen muchas clasificaciones posibles en las que se podría analizar la calidad de servicio de una comunicación de datos, sin embargo en esta sección se clasificará según el tipo de tráfico que se desea transmitir, dando mayor prioridad al tráfico más sensible al retardo.

Debido a la variedad de tráfico que transita hoy en día por las redes de datos se hace necesario asignar una prioridad al tráfico más sensible, como es el caso del tráfico multimedia, llámese voz o video, el cual es altamente sensible al retardo. En este caso se ha contemplado la transmisión de voz, por lo que será necesario asignar un mayor ancho de banda y una prioridad mayor a este tipo de tráfico con el fin de evitar retardos en la llegada de los paquetes de voz, lo que ocasiona una denigración del servicio.

Existen otros tráficos que no son tan sensibles al retardo como los anteriores, pero utilizan los mismos mecanismos de asignación de ancho de banda y priorización del tráfico pero en menor grado, con el fin de establecer niveles aceptables de QoS en su comunicación.

Luego siguen tráficos que no son de primera necesidad, por lo que un pequeño retardo no afectará notoriamente en el resultado final de la comunicación. Debido a esto se le asigna la prioridad más baja. Este tipo de QoS utiliza cualquier oportunidad de transmisión restante y asume que la capacidad de los buffers posteriores es suficiente para llevar a cabo la transmisión.

En este Trabajo de Titulación se asignará la mayor prioridad para el tráfico de voz, además de esto aumentando el ancho de banda disponible por su susceptibilidad al retardo, mejorando considerablemente la QoS de este tipo de comunicación, que es primordial para este enlace. El asignar la prioridad más alta a un tipo de tráfico no implica que el resto se fuese a ver perjudicado, esto debido a que el resto de la información que se envía entre las diferentes estaciones de la red son mucho menos susceptibles al retardo que las anteriores.

5.4 CLASIFICACIÓN Y PRIORIZACIÓN DE LA INFORMACIÓN

Como se mencionó anteriormente la QoS es la encargada de asegurar los parámetros de calidad en una comunicación donde se establezca una conexión y se transmita información entre dos o más usuarios a través de una red. Sin embargo no todos las aplicaciones o servicios de una comunicación tienen los mismos requerimientos para poder mantener un estándar de calidad de servicio, por lo que es necesario hacer una clasificación del tráfico que se transmitirá en la red, y con ello establecer una prioridad más alta a aquellos que lo necesiten.

Una de las formas de clasificar los tipos de tráfico que se transmiten a través de la red, es identificándolo mediante el puerto que utilizan para comunicar sus paquetes, sin embargo este método no sirve frente a aplicaciones que utilizan puertos dinámicos, lo que imposibilita el proceso de priorización del tráfico.

Las clasificaciones más comunes del tráfico de una red, generalmente utilizadas, son las siguientes:

- Protocolo
- Número de Puerto
- Cabecera IP
- Cabecera RTP
- Contenido
- Patrón de Velocidad y Flujo
- Serialización RSVP

Una vez clasificado el tráfico es posible asignar prioridad a los datos más susceptibles al retardo, para evitar la pérdida de información o en algunos casos la corrupción de los datos enviados. Este proceso de priorización de la información es posible realizarla mediante software o hardware, tales como equipos administradores de tráfico, de ancho de banda o a través de firewalls.

RSVP o protocolo de reserva de recursos, definido en el RFC 2205, trabaja en la capa de transporte y es el encargado de reservar recursos a los flujos de datos de las aplicaciones específicas a través de una red integrada de servicios de Internet.

A fin de asegurar una mejor QoS en este Trabajo de Titulación se utilizarán las técnicas de clasificación y priorización de la información por hardware, es decir, se buscará un dispositivo que cumpla con los requerimientos de agilidad y eficiencia que se requieren para esta operación tan importante de mejorar la calidad del servicio que se desea brindar.

5.5 PARÁMETROS DE LA QOS

La calidad de servicio (QoS) se puede ver afectada por algunos factores, que pueden afectar la calidad de la comunicación, causando principalmente retraso en la llegada de los paquetes y todos los fenómenos que esto conlleva, por lo que se puede hablar de una pobre QoS.

Como ya se mencionó uno de los principales problemas que afectan la calidad de servicio de una transmisión es el retraso en los paquetes que transitan por la red, este fenómeno es denominado Latencia y afecta directamente a las transmisiones de VoIP.

5.5.1 RETARDO O LATENCIA

El fenómeno denominado Latencia y que afecta la calidad de servicio especialmente en las redes multimedia, en este caso en la red VoIP, se define como el tiempo que tarda un paquete en ser transmitido desde el emisor hasta el receptor, incluyendo todos los procesos intermedios que se realizan para lograr esta comunicación.

En el caso de las redes VoIP la latencia se convierte en un enemigo para la transmisión de voz, debido a que al producirse el retardo en la llegada de los paquetes de datos, se produce la pérdida de calidad de la señal recibida.

Estudios realizados en la especificación de la ITU G.114 indican que el retardo máximo admisible para la voz debe ser menor que 150 mseg, en caso contrario se torna sumamente desagradable, ocasionando que los integrantes de la conversación traten de hablar simultáneamente. Sumado a esto se produce un efecto llamado eco. Los ecos son sumamente molestos a la hora de la comunicación y su amplitud es directamente proporcional al retardo producido en la señal.

Las principales fuentes de retraso en una transmisión VoIP son:

- Codificador de voz
- Formación de los paquetes
- Encolamiento en el router y Buffer
- Señalización
- Transmisión

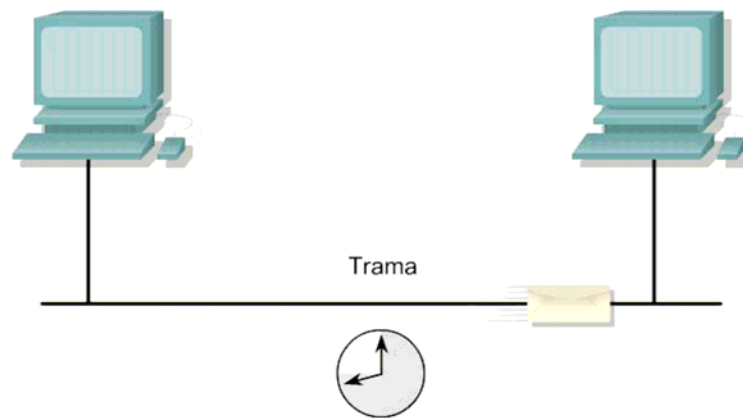


Figura 35. Fenómeno de latencia.

En el caso de este trabajo, a estos factores se suma un retraso producido por el proceso de encriptación de la información, esto proveniente de la tecnología VPN, gracias a la cual tanto la comunicación de datos como la voz viajan encriptados, asegurando la confidencialidad de las conversaciones.

a) Retraso por codificación. Este retardo depende directamente del algoritmo de codificación utilizado, es decir, el CODEC que convierte las señales de voz en una señal digital. Este retardo se puede clasificar en dos partes; el retardo del algoritmo y el retardo por procesamiento. El primero es propio de cada algoritmo de codificación y no puede ser modificado, mientras que el segundo depende directamente de la circuitería con la cual se va a realizar el proceso. En ella se incluyen la velocidad del procesador y la velocidad de acceso a las memorias, entre otros factores que pueden afectar la velocidad de procesamiento de un equipo.

Como se pudo apreciar en el capítulo II, existe una gran cantidad de CODECs, cada uno de los cuales, tiene asociado su propio retardo. A modo de ejemplo podemos mencionar que PCM, ADPCM y EADPCM tienen un retardo de algoritmo de 0,125 mseg (tiempo entre muestras PCM). En el caso de G.729, éste utiliza segmentos de voz de 10 mseg (correspondientes a recolectar 80 muestras PCM) a los cuales les aplica el algoritmo respectivo para lograr la compresión. Adicionalmente, para comprimir esos 10 mseg. de voz, el algoritmo analiza un segmento de voz de 5 mseg, posterior al segmento de 10 mseg de voz que está comprimiendo. De esta manera se tiene que el retardo de algoritmo de G.729 es de 15 mseg. Por otro lado, G.711 opera con segmentos de voz de 0,125 mseg. (Correspondiente a recolectar 1 muestra PCM) y no analiza segmentos de voz posteriores al que está comprimiendo.

En el caso de G.723 utiliza segmentos de voz mucho mayores que G.729, de 30 mseg, correspondientes a 240 muestras PCM. Para la compresión de los segmentos de 30 mseg el algoritmo tiene que analizar un segmento de voz de 7,5 mseg adicionales al segmento de voz que está comprimiendo, con lo cual el retardo del algoritmo resulta en 37,5 mseg.

b) Retardo de empaquetamiento de la información. Como hemos observado anteriormente, la duración de los segmentos de voz depende directamente del CODEC utilizado para la compresión de la información, por ejemplo, si utilizamos G.728, que utiliza segmentos de 0,625 mseg y su velocidad es de 16Kbps, de manera que el segmento de voz queda representado por 10 bits. Si solo estos 10 bits se empaquetan en una trama IP se obtiene una sobrecarga muy grande (overhead), lo que constituye un desperdicio de ancho de banda. Ahora, si agrupamos varios segmentos de voz en un solo paquete de información, reducimos el overhead pero aumentamos el

retardo de empaquetamiento, por lo que se hace necesario evaluar la solución más adecuada para el diseño.

En el caso que la voz viaje en el mismo canal lógico que los datos, es posible agruparlos en un solo paquete, pero en diferentes subpaquetes, para que el receptor pueda identificar cada uno de los tráficos enviados. Gracias a este método es posible optimizar el ancho de banda utilizado. Además de poder integrar voz y datos en un mismo paquete es posible agregar diferentes conversaciones en un paquete, diferenciándolas con un identificador.

c) Retardos por serialización. Este retardo se refiere al tiempo que transcurre cuando el paquete es enviado a través de la red, una vez que éste se encuentra en la cola de transmisión. Este retardo esta relacionado con el tamaño del paquete, mientras mas grande sea éste, mayor será el retardo asociado.

Existe otro factor agravante para este retardo, y es la velocidad de acceso al medio, sin embargo gracias a los avances tecnológicos actualmente podemos contar con grandes velocidades a un menor costo, por lo que éste no sería una limitante para este diseño.

El límite del tamaño de los paquetes que se desea enviar es de vital importancia a la hora de reducir los retardos de serialización como también los retardos de espera en cola, que se analizarán a continuación.

d) Retardo de espera en cola. La espera en cola se refiere a cuando un paquete requiere ser transmitido pero en ese momento la línea se encuentra ocupada en la transmisión de otro paquete, en ese momento se genera una petición para que una vez que la línea se encuentre desocupada se transmita el paquete en cuestión. Ese tiempo de espera entre que se genera la petición y se desocupa la línea para la transmisión del paquete es el denominado retardo de espera en cola.

En el caso de una red de voz y datos, al asignar una prioridad mayor al tráfico de voz, se podría minimizar este problema de retardo, ya que como los paquetes de voz se ven afectados seriamente por un retardo alto se les da prioridad sobre los paquetes de datos que no son tan

susceptibles ante este, transmitiéndose primero que los paquetes de datos que ya se encontraban en cola, sin embargo esta solución no es suficiente, una solución adicional es segmentar los paquetes de datos en paquetes mas pequeños, para que cuando ya se este transmitiendo un paquete de datos, el retardo sea mínimo en la espera del paquete de voz para ser transmitido.

e) Retardos de descompresión. Este retardo se refiere al tiempo que tarde la descompresión de la señal de voz por medio del CODEC, y su duración depende de la complejidad del CODEC utilizado y además del hardware utilizado en la decodificación. Este parámetro es casi imperceptible, debido a que su duración no supera los 4 mseg, considerándose despreciable en comparación a los retardos estudiados anteriormente.

f) Retardo por encriptación. Debido a las conocidas falencias de seguridad que presenta el servicio de VoIP, este proyecto consideró tecnologías adicionales que suplieran este problema, me refiero a una red privada virtual, la cual se encarga de realizar las conexiones entre las distintas sucursales y la casa central de la PYME, para establecer la comunicación de voz entre estas, añadiendo servicios de seguridad. Como ya se explicó en capítulos anteriores esta tecnología de VPN, consta de variadas técnicas de seguridad para proteger la información que por ella se transite a través de la red hostil de Internet, la técnica a la que me referiré en este apartado es a la encriptación.

La encriptación de los paquetes de voz que serán transportados a través de la VPN llevan consigo un retardo que dependerá del protocolo de encriptación utilizado, es decir, la cantidad de bits que utilice para ésta, la complejidad del protocolo, el hardware utilizado, entre otros. Sin embargo este retardo se considera mucho menor que los retardos propios de la transmisión propiamente tal estudiados anteriormente. La figura que se adjunta a continuación muestra la comunicación VoIP a través de un túnel VPN con los retardos aproximados en los procesos de encriptación y desencriptación de la información.

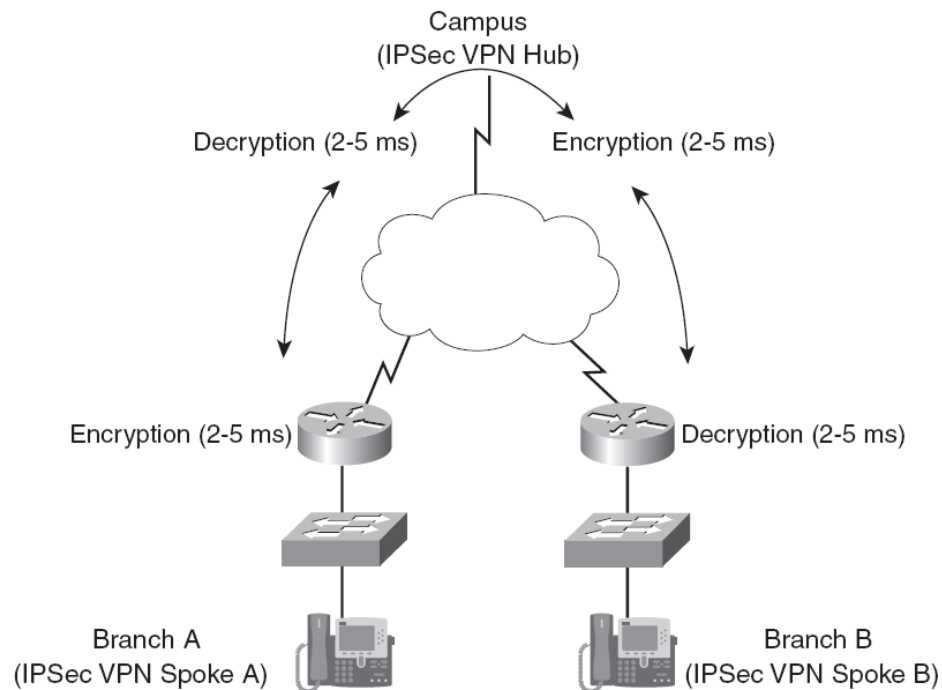


Figura 36. Retardos aproximados por encriptación VPN IPsec

5.5.2 JITTER

Al referirnos a un servicio que funciona sobre una red pública tal como Internet, es posible garantizar que todas las rutas por las que viaje el tráfico entre el usuario llamante y el receptor se encuentren expeditas, además como hemos visto los servicios de VoIP requieren de cierta QoS para que su desempeño cumpla con los requerimientos mínimos. Este es un factor que difícilmente podremos manejar y debido a él podríamos tener congestión que provoque que nuestro servicio sufra de algunos de los fenómenos vistos anteriormente o definitivamente colapse.

El Jitter se define como la variación en el tiempo en la llegada de los paquetes, causada principalmente por congestión de red, pérdida de sincronización o por congestiones presentes en las rutas que sigue la información hasta llegar a su destino.

Como una forma de remediar este fenómeno se pensó en el jitter buffer, que consiste en asignar un espacio para ir almacenando los datos recibidos, para luego procesarlos con un pequeño retardo, que de un tiempo de espera a las tramas que aún no llegan, para así ubicarlas en la secuencia correcta.

En caso de que algún paquete no este en el buffer, luego de un tiempo determinado se descarta. Normalmente en los teléfonos IP (hardware y software) se pueden modificar los buffers, sin embargo un aumento de éste implica menos perdida de paquetes pero más retraso.

5.5.3 ECO

El eco se define como una reflexión retardada de la señal acústica original, es decir, el resultado del acoplamiento entre la señal de transmisión y la de recepción, que ocasiona una molestia al momento de interpretar el mensaje decepcionado.

Este fenómeno tiene directa relación con el retardo, mientras mas alto sea el retardo (Alrededor de los 50 mseg) de los paquetes de voz enviados en la comunicación, mayor va a ser el eco, distorsionando el mensaje original.

El oído humano es capaz de detectar el eco cuando su retardo con la señal original es igual o superior a 10 mseg, sin embargo otro factor a considerar es la intensidad del éste debido a que normalmente la señal de vuelta tiene menor potencia que la original. Es tolerable que llegue a 65 mseg y una atenuación de 25 a 30 dB.

En el caso de no disminuir el retardo mediante los métodos vistos anteriormente y bajo la presencia de eco, actualmente existen dos soluciones para este problema:

- Cancelador de eco. Este sistema esta definido en la recomendación G.168 de la ITU-T y es el encargado como su nombre lo indica, de cancelar el eco presente en una comunicación de VoIP, guardando la información enviada por el emisor al receptor para luego, cuando tenga una

respuesta, ser capaz de compararla con la señal almacenada, de ser igual o parecida, por efectos del ruido, el dispositivo filtra dicha información y cancela esa componente de la voz, dejando solo el nuevo mensaje. El problema que presenta este dispositivo es que requiere de un tiempo de procesamiento.

- Supresor de eco. Este dispositivo definido en la recomendación G.164 de la ITU-T, es capaz de repeler el eco de una comunicación de VoIP, transformando una línea full-duplex en una half-duplex en instantes, de modo que cuando se este enviando un mensaje no pueda ser recibido el mismo mensaje simultáneamente o con un pequeño retardo. El tiempo de conmutación de estos dispositivos es muy pequeño, pero sin embargo convierte la línea bidireccional en una línea de tráfico unidireccional en instantes.

5.5.4 PERDIDAS DE PAQUETES

Como ya se ha mencionado anteriormente, las comunicaciones en tiempo real, tal como VoIP, están basadas en el protocolo UDP, el cual no está orientado a conexión, de tal forma que si se produce una pérdida de paquetes, éstos no se reenvían. El hecho de reenviar los paquetes extraviados implicaría un retardo aún mayor en la comunicación, y como se ha visto a lo largo de este capítulo las comunicaciones de VoIP son muy susceptibles al retardo, por lo que ésta no sería una solución a este problema. No obstante, la voz es bastante predictiva y si se pierden paquetes aislados se puede recomponer la voz de una manera bastante óptima, casi imperceptible para el oído humano. El problema se agudiza cuando la pérdida de paquetes se produce en ráfaga, debido a que se perderían trozos de información muy grandes que no podrían ser reconstruidos.

La pérdida de paquetes se debe principalmente a que la red IP es una red de conmutación de paquetes, donde cada uno de ellos lleva un encabezado que determina hacia donde se dirige y además suministra información para el rearmado cuando éste llegue a destino. Los paquetes se desplazan independientemente y a la vez se mezclan con paquetes de otro tráfico de la red a lo largo del trayecto, por lo que no necesariamente llegarán en el orden ni el tiempo correcto a su destino. Los paquetes pueden perderse en nodos de la red a causa de un desborde en la memoria

intermedia, o porque un router congestionado los descarta para reducir la congestión o también pueden retrasarse en el caso que tomen una ruta más larga o pasen tiempo en la cola de un dispositivo, causando una variabilidad en la hora de llegada al extremo receptor. Una medida de reducir este efecto es la utilización del jitter buffer, el cual se usa para reducir la variabilidad, reteniendo los paquetes para la entrada al decodificador.

Algunos de los principales CODEC utilizados actualmente tienen la capacidad de “predecir” los paquetes perdidos y reemplazarlos, de manera tal que al oído humano la diferencia sea casi inaudible, sin embargo esto se puede lograr satisfactoriamente solo cuando la pérdida sea inferior al 5% de los paquetes totales, ya que hasta ese límite el CODEC es capaz de corregir errores en los mensajes.

Cuando se habla de “predecir”, nos referimos a dos métodos principalmente, que son:

- Intrapolar, cuando falta un paquete el CODEC, toma el paquete anterior y el paquete siguiente y calcula el valor del paquete faltante.
- Sustitución, cuando el CODEC detecta un paquete faltante lo reemplaza por un paquete igual a el paquete anterior.

Para evitar la pérdida de paquetes una técnica muy eficaz en redes con congestión o de baja velocidad es no transmitir los silencios. Gran parte de las conversaciones están llenas de momentos de silencio. Si solo transmitimos cuando haya información audible liberamos bastante los enlaces y evitamos fenómenos de congestión.

5.6 SUPRESIÓN DE SILENCIO Y RUIDOS

Como se mencionó anteriormente las comunicaciones de voz se forman en gran parte de silencios o pausas entre palabras, y como el mensaje que se quiere comunicar no requiere la transmisión estos instantes sin comunicación, lo que se hace es suprimirlos, para ahora enviar solo la información necesaria y contribuir con un importante ahorro de ancho de banda. El resto del tiempo, cuando no existe voz a transmitir, se libera el ancho de banda.

Para una comunicación VoIP típica full-duplex tenemos un tráfico aproximado de 22 Kbps, lo que no se considera un gran ancho de banda, sin embargo, cuando la red utilizada para esta comunicación no es solo para tráfico VoIP se hace necesario transmitir paquetes del menor peso posible para evitar congestión en la red, la cual como ya hemos observado se traduce en degradación de la QoS.

Para la Supresión de Ruidos, se utiliza el VAD (Voice Activity Detection), el cual se encarga de detectar la diferencia entre la existencia de voz y los silencios, de forma tal que no transmitan los paquetes de silencio. Este proceso es posible realizarlo por software y hardware, sin embargo, en términos de funcionamiento se recomienda el hardware, no así en términos económicos.

5.7 QOS EN VOIP SOBRE VPN

El servicio de VoIP sobre VPN presenta un leve retardo adicional por sobre la comunicación VoIP tradicional, esto debido principalmente al proceso de encriptación que presentan las redes virtuales, además del proceso de autenticación de los usuarios que tomarán parte en la comunicación.

Como ya hemos observado este servicio cuenta con numerosas ventajas, incorporando servicios de seguridad de la información y la autenticación de los usuarios por medio de dispositivos de seguridad, tales como certificados digitales, o sistemas de hardware que no estaban contemplados dentro de los estándares más comunes actualmente: SIP y H.323. Este retardo se puede disminuir utilizando equipamiento que realice de forma más expedita la encriptación y clasificación, para poder priorizar los datos que provienen de comunicación de voz.

RESUMEN

Como se observó a lo largo de este capítulo, la QoS en una comunicación multimedia, tal como VoIP es primordial, al igual que conocer los parámetros que la afectan. Por estas razones en este capítulo se analizaron todos los factores que afectan significativamente a una comunicación VoIP, además de los métodos más eficaces para su disminución, de entre los cuales puedo destacar, un dispositivo capaz de encriptar la información de forma rápida y segura, para este caso en particular, en que el tráfico de voz viaja encriptado. Otra forma muy eficaz de evitar los retardos en la comunicación es realizar una clasificación del tráfico más susceptibles al retardo y brindarle una mayor prioridad, para evitar que datos provenientes de voz tengan un retardo innecesario, además de la elección de un CODEC eficiente, que de una buena reproducción del mensaje original, fiable y sin muchas distorsiones, pero con un consumo de ancho de banda aceptable, como es el caso del CODEC seleccionado para esta aplicación, G.729, que además cuenta con supresores de ECO, una herramienta muy utilizada considerando que una comunicación de voz está compuesta en gran parte por silencios que no es necesario enviar como información.

CAPÍTULO VI. EQUIPAMIENTO REQUERIDO PARA LA IMPLEMENTACIÓN DEL PROYECTO

6.1 INTRODUCCIÓN.

En el presente capítulo se realizará una descripción más detallada del diseño de la red, considerando los servicios que debe brindar, por lo que se lleva a cabo un análisis de las marcas y equipos que cumplen con los requerimientos de ésta, considerando los requerimientos de seguridad, integración de servicios, administración de los distintos parámetros que en ella se deben manejar y finalmente la elección de los dispositivos que se utilizarán para lograr la comunicación de todos los usuarios.

6.2 SELECCION DEL PROVEEDOR DE TECNOLOGÍA

El mercado de las Tecnologías de Información (TI), a pesar de las dificultades registradas en los últimos cuatro meses de 2008 debido a la recesión económica, logró cerrar el pasado año con un crecimiento del 8,2 por ciento, alcanzado un volumen de negocio de 806.000 millones de dólares, según un informe presentado por la consultora Gartner⁸⁰. En Chile se observa un leve crecimiento en la inversión de Hardware de Networking entre el 2008 y 2009.

⁸⁰ Gartner: <http://www.gartner.com/>

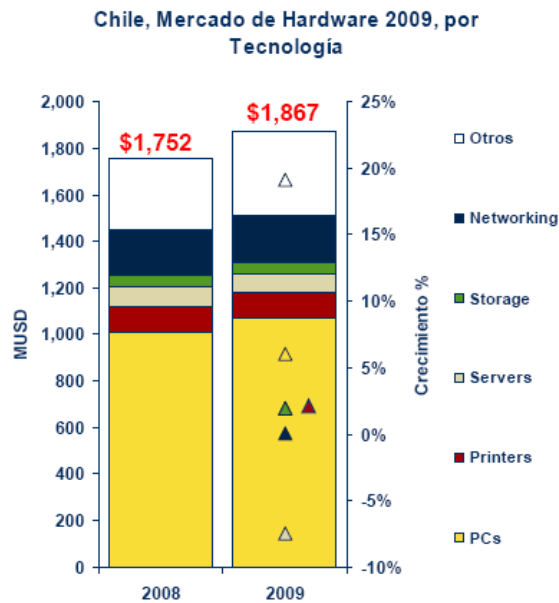


Figura 37. Indicador de la Actividad de TI en Chile⁸¹

Este crecimiento es una muy buena noticia para las empresas proveedoras de tecnología, de las cuales podemos destacar principalmente a ALCATEL-LUCENT⁸², CISCO SYSTEM y su arduo competidor procedente de China, HUAWEI⁸³.

Todas estas empresas mencionadas brindan tecnología capaz de implementar los servicios solicitados para este proyecto, sin embargo para la selección realicé una investigación primero que nada sobre la reputación de cada una de ellas, donde me encontré que CISCO se encontraba mejor catalogada que las otras empresas mencionadas anteriormente⁸⁴, lo que brinda un respaldo extra al proyecto.

Otro punto considerado para la selección fue el registro de patentes en los últimos 5 años (<http://www.thomsonscientific.com/>) de cada una de las empresas, donde nuevamente arrojó que CISCO superaba ampliamente a sus competidores, sin embargo indica que HUAWEI tiene un

⁸¹ www.idclatin.com

⁸² ALCATEL-LUCENT: www.alcatel-lucent.com

⁸³ HUAWEI: www.huawei.com

⁸⁴ http://www.forbes.com/2009/04/28/america-reputable-companies-leadership-reputation_table.html

gran futuro como proveedor de los operadores de telecomunicaciones principalmente por los costos que involucra la implementación de un proyecto con esta tecnología.

Con estos antecedentes se resolvió que la tecnología más apropiada para la implementación de este proyecto es CISCO SYSTEM, gracias al respaldo que brinda una implementación utilizando estos dispositivos, además de presentar una gran variedad de soluciones en cuanto a seguridad, integración de servicios y gestión de calidad de servicio.

6.3 PARÁMETROS A CONSIDERAR

Debido a que la red privada virtual propuesta en el diseño es la columna vertebral de este proyecto, se ha decidido utilizar equipamiento de calidad comprobada, como es el caso de la Compañía Cisco System, líder mundial en la fabricación de componentes de networking, además de ofrecer la más amplia variedad de hardware para redes. Este liderazgo se ve reflejado en sus ventas, las cuales el primer trimestre del año fiscal que finalizó el 25 de octubre de 2008 alcanzó ventas netas por \$ 10.300 millones de dólares⁸⁵.

6.4 SEGURIDAD CISCO

Un punto muy importante que se evalúa a la hora de tomar ésta decisión son los avances en cuanto a seguridad, en el cual la Compañía Cisco System lleva la delantera sobre sus competidores, gracias a sus avances en la llamada red de autodefensa Cisco, donde con el objetivo de satisfacer las necesidades crecientes en la gestión de riesgos relacionados con la seguridad y el cumplimiento con las normativas vigentes, ha anunciado una serie de mejoras en su catálogo de soluciones para Redes de Autodefensa que incluye elementos concretos para la seguridad de la red, las aplicaciones y los contenidos. Las mejoras en seguridad de Cisco incrementan la capacidad de las empresas para proteger sus infraestructuras tecnológicas frente al malware y les ayuda a cumplir los requisitos de seguridad necesarios, como la prevención de

⁸⁵ http://www.ciscoredaccionvirtual.com/redaccion/comunicados/ver_comunicados.asp?Id=1524

fugas de datos, la conformidad con las políticas corporativas y la aplicación de las normativas vigentes en materia de seguridad.

Conforme las redes se convierten en plataformas para un número cada vez mayor de dispositivos, aplicaciones y contenidos, la protección es una cuestión fundamental. La nueva Red de Autodefensa de Cisco aporta mejoras en la protección de los puntos terminales, en la prevención de intrusiones, en los cortafuegos de red y de aplicaciones y en el control y análisis de la seguridad, así como gestión centralizada de las políticas de seguridad. Los sistemas de defensa con que cuentan estas redes son:

- **Sistemas de prevención de intrusiones.** Cisco cuenta con soluciones IPS para empresas de todos los tamaños simplificando su gestión. La solución IPS incorpora Cisco IPS Manager Express, una nueva aplicación integral para aprovisionamiento, supervisión y generación de informes. Además de las ampliaciones de software, Cisco ofrece un nuevo módulo IPS para dispositivos de seguridad ASA que proporciona un rendimiento de hasta 650 MBps y servicios que ayudan a proteger las Comunicaciones Unificadas y que mejoran la detección de amenazas de punto a punto ampliando la protección ante vulnerabilidades de aplicación.

- **Cisco Firewall Service Module 4.0 (para Routers):** Cisco FWSM 4.0 acelera la entrega segura de información en entornos para grandes volúmenes de tráfico, como pueden ser copias de seguridad de datos de gran tamaño o transferencias de datos de gran volumen. Incorpora una aplicación de aceleración del flujo seguro que permite que los hosts seguros intercambien información a una velocidad de entre 20 y 50 Gigabits por segundo.

- **Redes Privadas Virtuales:** Cisco ha incorporado una serie de tecnologías para la gestión de las conexiones VPN, entre ellas destaca Group Encrypted Transport Virtual Private Network (GET VPN, Red Privada Virtual de Transporte Encriptado de Grupo), que aporta mejoras de hasta el 300% en el rendimiento. GET VPN representa una nueva categoría de VPNs diseñadas para encriptar datos transmitidos en redes de área extendida WAN. Su desventaja es que solo opera con dispositivos router Cisco.

Otra de las opciones que brinda VPN para poder configurar estas redes privadas virtuales es Cisco Easy VPN, que opera con dispositivos Cisco ASA 5500 Series, Cisco VPN 3000 Series y Cisco PIX Firewall, brindándole interoperabilidad y un gran desempeño. Otras tecnologías utilizadas son principalmente Dynamic Multipoint VPN (DMVPN) y Routed Generic Routing Encapsulation (GRE).

- **Cisco Security Agent 6.0:** Cisco Security Agent es un agente de software diseñado para proteger los puntos terminales (servidores u ordenadores portátiles). El Agente ayuda a identificar las amenazas y controla el acceso a la información confidencial. La versión 6.0 representa la primera oferta en seguridad de punto terminal del sector que integra en un solo agente la gestión de los dispositivos de defensa de ataques desde el día cero, la prevención de pérdida de datos y la detección de antivirus basada en firmas. Cisco Security 6.0 incorpora actualizaciones automáticas de antivirus sin ningún coste adicional de licencia. La combinación única de estas funciones ayuda a las empresas a protegerse contra amenazas persistentes y emergentes y refuerza las políticas de red y facilita la conformidad con las normativas vigentes.

- **Filtrado de contenidos:** Cisco ha mejorado los servicios de seguridad ofrecidos a través de sus routers de servicios integrados (ISR), añadiendo el filtrado de contenidos de la compañía Trend Micro. La incorporación de esta tecnología ayuda a las empresas a proteger a los usuarios del acceso a sitios Web que sean fuentes conocidas de malware, les ayuda a restringir el acceso a contenidos inapropiados y asegura el cumplimiento de las políticas de uso de Internet aceptadas por la compañía.

- **Protección SIP para comunicaciones unificadas seguras:** un aporte de utilidad para las soluciones de seguridad es la protección para el Protocolo de Iniciación de Sesión SIP, que enriquece la función de IOS⁸⁶ Firewall de Cisco establecida con seguridad de voz. Esta protección ayuda a las empresas a adaptarse a entornos distribuidos mejorando la productividad al mismo tiempo que se reduce el riesgo en las comunicaciones de voz.

⁸⁶ IOS: Internetworking Operating System

- **Cisco Security Monitoring Analysis Response System 6.0:** Cisco Security MARS 6.0 proporciona visibilidad en tiempo real de las operaciones de seguridad e identifica las amenazas agregando información de seguridad desde cualquier dispositivo y determinando las acciones apropiadas para mitigar los ataques. Cisco Security MARS también proporciona la creación de informes con el fin de cumplir con la normativa vigente. La versión 6.0 añade un nuevo marco de desarrollo de soporte de dispositivos que permite a los usuarios, o a terceros, incorporar dispositivos que no sean de Cisco dentro de un desarrollo basado en tecnología Cisco Security MARS, acelerando la posibilidad de gestionar la inteligencia en seguridad en la red corporativa.

- **Cisco Security Manager 3.2:** Cisco Security Manager gestiona la seguridad en toda la empresa de forma eficaz centralizando las tareas de configuración de políticas y controles para implantaciones de seguridad de Cisco. La versión 3.2 ayuda a mejorar la eficacia operativa, reduce significativamente los tiempos de resolución de problemas y simplifica la gestión de firmas IPS. Esto se logra mediante la integración y colaboración estrechas con los datos provenientes de eventos de seguridad de Cisco Security MARS.

Estas son algunas de las herramientas de seguridad disponibles en entornos CISCO, gracias a los cuales podremos gestionar una excelente política de seguridad, para contar con una red confiable.

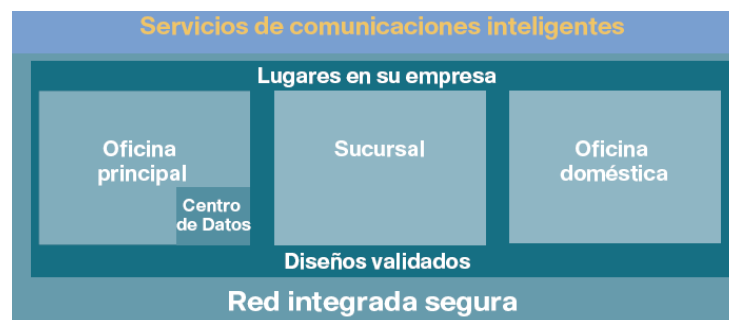


Figura 38. Arquitectura de Comunicaciones Empresariales Inteligentes de Cisco.

6.5 QOS EN CISCO

En VoIP, los principales parámetros que se tomaron en cuenta fueron la QoS y la seguridad del tráfico, por lo que la solución que brinda Cisco System es ideal para implementar este diseño, brindando herramientas para administrar ambos parámetros y una serie de protecciones contra los ataques más comunes que afectan actualmente a las redes de voz, haciendo de ella una comunicación segura, parámetro que no está considerado efectivamente en los protocolos de VoIP.

Para obtener QoS es necesario manejar los parámetros que producen retardo en la comunicación, tales como el jitter, la distribución del ancho de banda en los distintos servicios, y los parámetros de pérdida de paquetes, por lo tanto, QoS es el conjunto de técnicas para la gestión de los recursos de la red, con el propósito de lograr una comunicación fluida de extremo a extremo.

En este diseño se requiere brindar comunicación VoIP de calidad, por lo que se dará prioridad a los datos de voz, evitando que estos paquetes queden en espera ante tráfico que no es tan susceptible al retardo.

Para gestionar la QoS en este diseño se hará uso del asistente para calidad de servicio (QoS), el cual permite a un administrador de la red activarla en los túneles VPN IPSec. Los servicios que suministra esta herramienta son los siguientes:

- Tráfico de voz. El valor por defecto es el 33 por ciento del ancho de banda.
- Señalización de llamadas: Esta es la señalización necesaria para controlar el tráfico de voz. El valor por defecto es el 5 por ciento del ancho de banda.
- Enrutamiento: El tráfico generado por éste y otros routers para administrar el enrutamiento de paquetes. El valor por defecto es el 5 por ciento del ancho de banda.

- Administración: Telnet, SSH y otros tráficos generados para administrar el router. El valor por defecto es el 5 por ciento del ancho de banda.
- Transaccional: por ejemplo, el tráfico generado para aplicaciones comerciales o actualizaciones de base de datos. El valor por defecto es el 5 por ciento del ancho de banda.
- Mejor esfuerzo: ancho de banda restante para otro tráfico, como el tráfico de correo electrónico. El valor por defecto es el 47 por ciento del ancho de banda. El valor de Mejor esfuerzo se actualiza dinámicamente según el porcentaje total para los otros tipos de tráfico.

En este diseño se priorizará el tráfico de voz (VoIP), por lo que en este caso asignaremos un 40% del ancho de banda a los paquetes provenientes de esta aplicación, el 7% se lo restaré al tráfico de el “Mejor esfuerzo”, por lo que para el tráfico de correos electrónicos y otros tipos de tráfico quedará con un 40% del ancho de banda en las peores condiciones, ya que en el caso que no se estén cursando llamadas el ancho de banda quedaría disponible para el resto de aplicaciones.

A continuación se adjunta la arquitectura de un paquete de voz que viaja a través de una VPN IPSec en modo túnel con encriptación GRE, codificado con el CODEC G.729 que será utilizado para las comunicaciones de VoIP en este diseño.

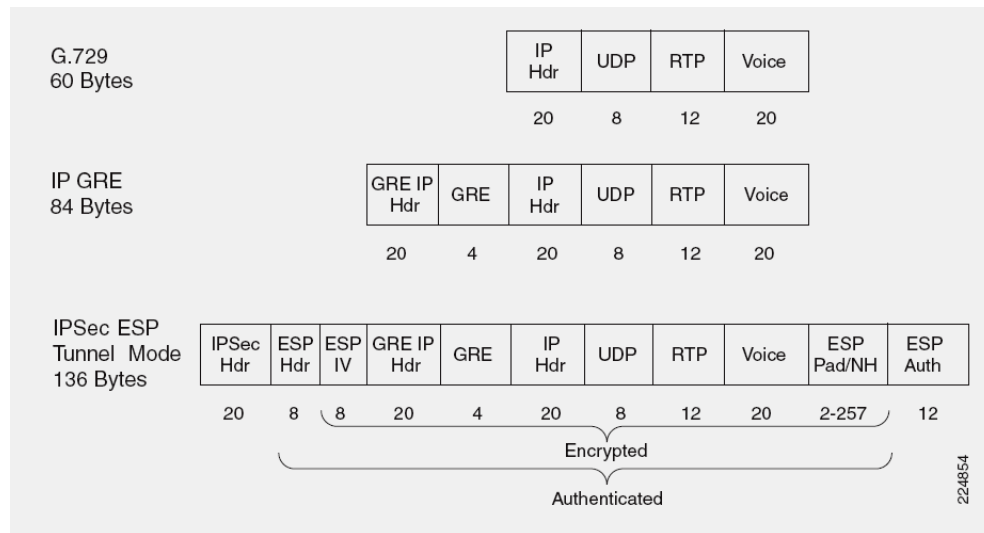


Figura 39. Arquitectura paquete de voz con codificación G.729

6.6 BENEFICIO VS COSTO

Un punto en contra de los equipamientos Cisco System frente a sus competidores es el costo un tanto más elevado, esto producto de sus licencias de softwares que facilitan de gran manera la configuración y protección de la red, proporcionando en este caso servicios de configuración para redes VoIP, QoS, configuración de protocolos de seguridad VPN, encriptación, Firewall, entre otros.

Para tomar esta decisión se consideran las prestaciones, confiabilidad y respaldo que brindan para un proyecto de esta envergadura tanto en las tecnologías de VoIP como en VPN los equipamientos de la marca CISCO y se considera que es posible asumir los costos agregados, los cuales serán evaluados en el siguiente capítulo

6.7 SOFTWARE CISCO IOS (INTERNETWORKING OPERATING SYSTEM)

Cisco IOS es el software encargado de proporcionar la integración de innovación tecnológica, servicios críticos para el negocio, y soporte de hardware en equipamientos Cisco

System, manejando áreas tales como: Seguridad, Enrutamiento IP, servicios de datos, voz y video, administración de parámetros tales como QoS, entre muchos otros, según sean los requerimientos del usuario o la red de la cual forman parte. Estos se agrupan en bloques, cada uno de los cuales cumple tareas específicas, partiendo desde un IOS básico (IP BASE), hasta llegar al Full Cisco IOS Software, que engloba todas las aplicaciones que brindan actualmente los IOS Cisco.

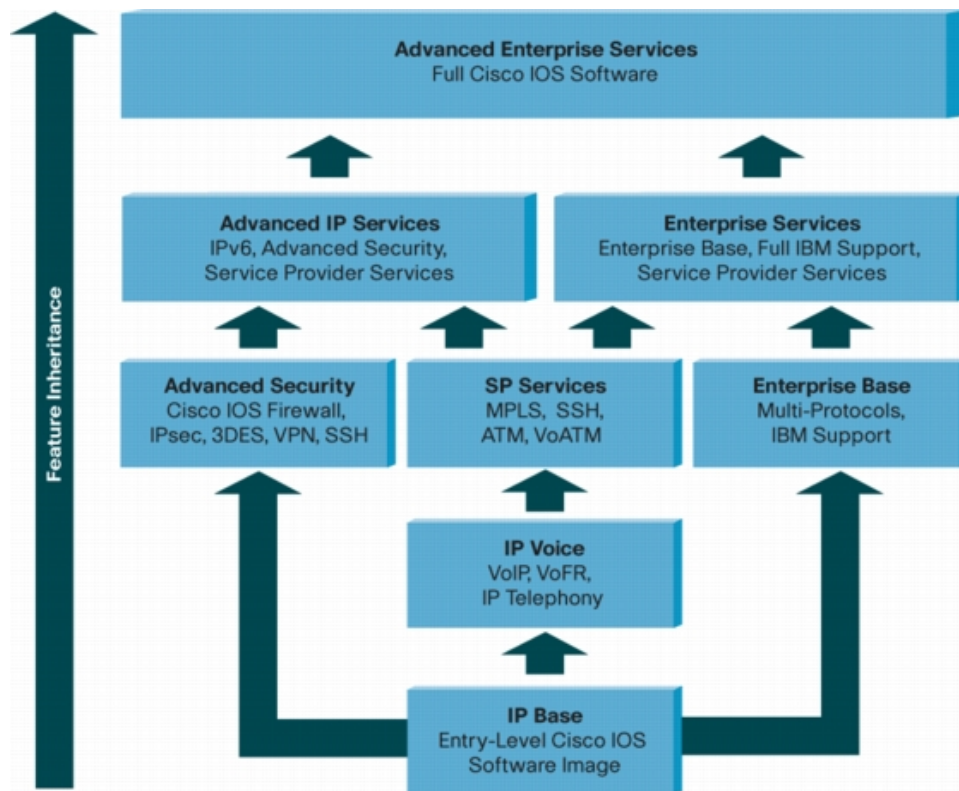


Figura 40. Estructura Softwares Cisco IOS

En este diseño en particular se harán uso de las herramientas presentes en los IOS IP Voice, para administrar las comunicaciones de VoIP y además de un software más avanzado denominado Advanced Security, encargado de establecer las comunicaciones VPN, entre otras funciones de seguridad, de las cuales haremos uso en este proyecto para prevenir posibles intrusiones que pongan en juego la seguridad de las comunicaciones de la PYME. En la figura 40 podemos observar que el IOS que engloba las capacidades de ambos softwares es el Advanced IP Services, por lo que se deberá adquirir la licencia de dicho IOS.

6.8 DESCRIPCIÓN DEL PROYECTO

El proceso de diseño de una red de multimedia, comienza definiendo las necesidades que se desean satisfacer para los usuarios finales, teniendo en cuenta los recursos disponibles para implementar el proyecto, de manera de conseguir la mejor relación costo/beneficio. Una vez que se define a grandes rasgos las directrices del proyecto se procede a estudiar en detalle los aspectos tecnológicos involucrados, tales como, tipo de red a utilizar, tecnología involucrada, marca de fabricantes, entre otros. Sin embargo el punto más importante dentro del diseño corresponde a la selección del tipo de tecnología y más específicamente el protocolo a utilizar, el cual forma el pilar fundamental de todo diseño, ya que esta decisión afectará directamente sobre el rendimiento de la red y los servicios que se brindarán a los usuarios finales.

Este proyecto en particular consta principalmente de dos partes. La primera de ellas es la comunicación de la Casa Central de la PYME en cuestión con sus sucursales, además de la comunicación entre sus ocho sucursales entre sí, ubicadas a lo largo del territorio nacional. Esta comunicación consta de servicios de transferencia de datos mediante una VPN de sitio a sitio, que encriptará la información que se transmita a través de la red pública de Internet. El proceso de establecer las conexiones virtuales se realizará a través del protocolo IPSec, el cual se encargará de establecer los túneles VPN, autenticación de usuarios y posterior encriptación de la información.

La segunda parte de este diseño consiste en la comunicación de VoIP de las sucursales entre sí, además de comunicarlas con la Casa Central. Esta comunicación debe estar provista de servicios de autenticación y encriptación, por lo que la transmisión de los datos de voz se realizará a través de la red privada virtual antes implementada y quedará provista de los mismos servicios de seguridad. El protocolo seleccionado para establecer la comunicación VoIP será SIP, esto debido principalmente a su ventaja con respecto a H.323 en cuanto a simplicidad de codificación y decodificación de los paquetes de voz. Otro factor que influyó en la decisión fue una comparación en la modularidad de los paquetes de ambos protocolos. Debido a que H.323 utiliza el estándar “paraguas” que se apoya sobre varios protocolos, al momento de realizar una

modificación es muy complicado desligar la interacción con los otros subprotocolos, no así para SIP, que puede interactuar con cualquier protocolo que lleve a cabo calidad de servicio, acceso de directorio, etc, sin tener q llevar a cambios en el protocolo SIP.

Una de las claves del ahorro de tiempo de transmisión y retraso de codificación es la selección apropiada del CODEC a utilizar. Debido a su ahorro de ancho de banda y sus características he decidido utilizar el G.729, estandarizado por la ITU.

6.8.1 DIMENSIONES DEL PROYECTO

Este proyecto está contemplado para una PYME que consta de una Casa Central con un número definido de sucursales, sin embargo se contempla una posible expansión de éstas para hacerlo un diseño flexible a los posibles cambios en la organización corporativa.

Las instalaciones que se desean comunicar son las siguientes.

NUMERO	REGION	SUCURSAL
I	Tarapacá	Sucursal Iquique
II	Antofagasta	Sucursal Antofagasta
IV	Coquimbo	Sucursal La Serena
RM	Metropolitana de Santiago	Casa Central Santiago
VIII	Biobío	Sucursal Concepción
IX	La Araucanía	Sucursal Temuco
XIV	Los Ríos	Sucursal Valdivia
X	Los Lagos	Sucursal Puerto Montt
XII	Magallanes y de la Antártica Chilena	Sucursal Punta Arenas



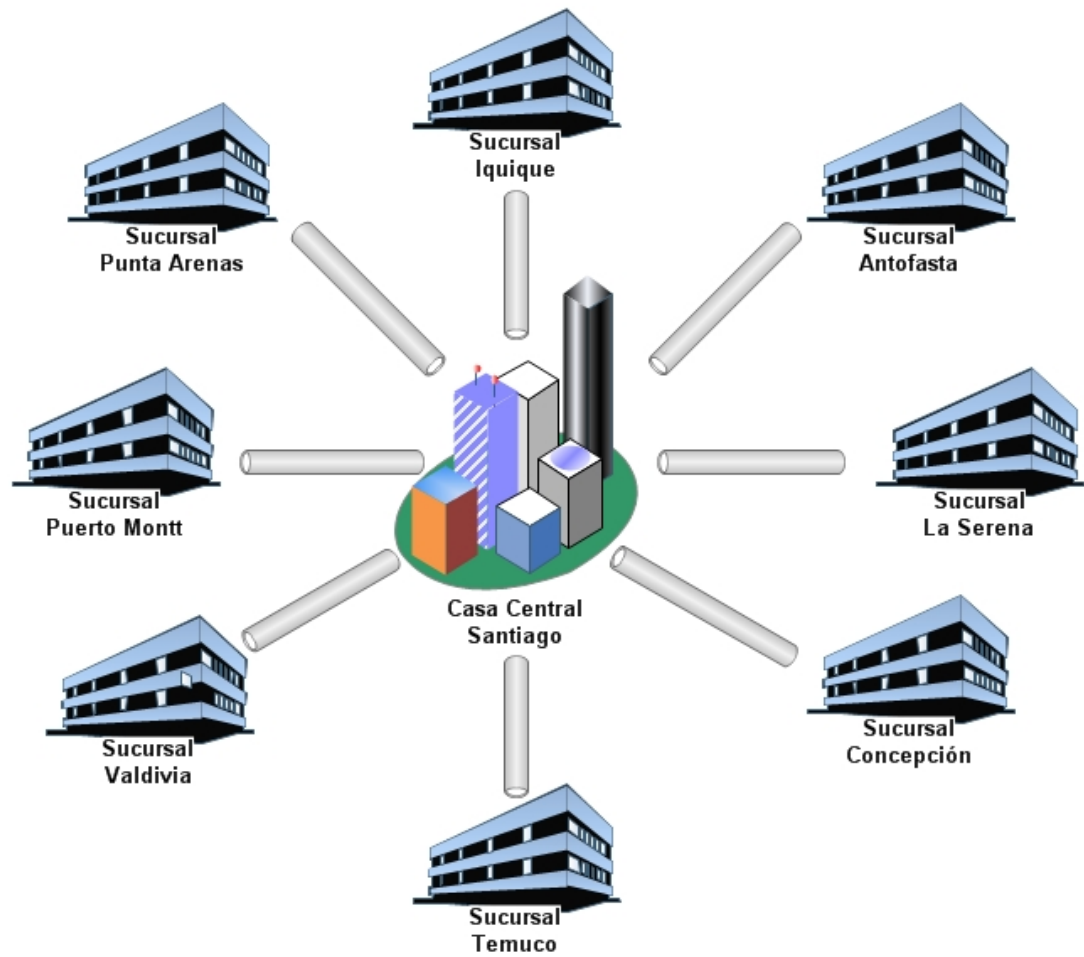


Figura 41. Diagrama general del diseño

El número total de usuarios será de 42, concentrándose la mayor cantidad en la Casa Central ubicada en Santiago. El detalle es el siguiente:

	Nº Usuarios	Nº Total
Sucursal	4	32
Casa Central	10	10
Total		42

6.8.2 EQUIPAMIENTO SELECCIONADO

Como se mencionó en el apartado anterior, el diseño de la red privada virtual, haciendo una analogía, corresponde a la columna vertebral de este proyecto, por lo que cuando se trata de elegir el equipamiento para establecer las conexiones de las redes virtuales, se hace necesario utilizar la mejor tecnología disponible, que se encuentre al alcance de la PYME, en cuanto a costos se refiere. Los costos de estos equipos están un tanto sobre el resto de los equipos, sin embargo, gracias a las funcionalidades y ventajas que brindan en los distintos campos frente a su competencia, es un costo que se puede asumir en este proyecto. Además estas funcionalidades pueden economizar en tareas que requerían de financiamiento y que hoy en día se realizan a través de la red. El ahorro más importante que proporciona esta tecnología es al proporcionar los medios para gestionar las comunicaciones VoIP, ya que éstas se realizarían sin costo para la empresa entre sucursales o casa central.

El diseño cuenta con 8 sucursales, que se desean comunicar con la casa central y además que tengan comunicación entre ellas. Esta comunicación consta de un servicio de VPN, por el cual transitan voz y datos, sin embargo este diseño estructuralmente también sería capaz de soportar tráfico de video (V3PN), pero esto no se encuentra dentro de los objetivos del proyecto, por lo que se dejaría como un trabajo adicional. A continuación se analizarán algunas de las alternativas disponibles en el mercado Cisco System para lograr los objetivos propuestos en el proyecto. Los puntos más importantes que se evalúa son su soporte para encriptar el tráfico VoIP y enviarlo a través de una VPN, el número máximo de usuarios de VoIP, el número de túneles VPN que son capaces de manejar, la velocidad de encriptación, y manejo de QoS de las comunicaciones, entre otros.

6.8.2.1 ROUTER CISCO SERIE 2800 DE SERVICIOS INTEGRADOS

Equipado con Cisco IOS, la familia Cisco 2800 soporta la llamada "Cisco Self-Defending Network", o Red de Auto Defensa de Cisco, que es un sistemas estratégicos para la seguridad de la información que incluye funciones de gestión de comunicaciones de voz, video y datos,

servicios avanzados de seguridad como el acelerador de encriptación por hardware, VPN IPSec (AES, 3DES, DES), cortafuegos, prevención de intrusos (IPS), control de acceso a la red (NAC) y funciones de filtraje por URL. La gestión basada en web del router está preinstalada en todos los productos de la serie Cisco 2800 para ayudar a simplificar la gestión y configuración. Esta serie de equipos de servicios integrados incluyen los modelos Cisco 2801, Cisco 2811, Cisco 2821 y Cisco 2851 y están pensados para optimizar las comunicaciones de la pequeña y mediana empresa, comunicando sus sucursales con fuertes niveles de seguridad.

Esta serie de equipos se encuentra dentro de las posibilidades para implementar el diseño, gracias a la amplia gama de dispositivos y aplicaciones de seguridad y administración de información, luego se procedió a la selección del modelo requerido, la cual se realizó de acuerdo número de teléfonos IP que es capaz de comunicar, para obtener la solución más apta para el proyecto en cuestión.

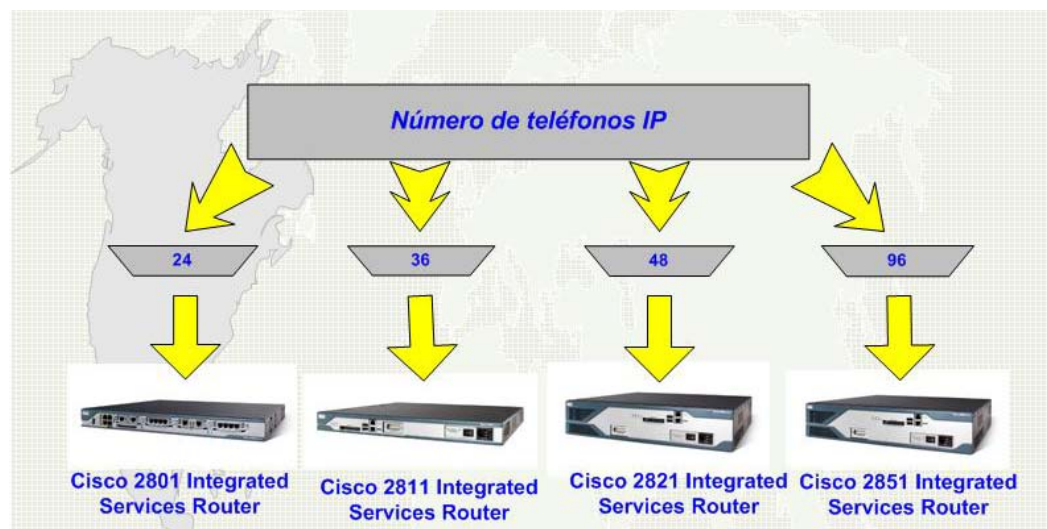


Figura 42. Descripción de routers serie 2800

ROUTER CISCO MODELO 2821 DE SERVICIOS INTEGRADOS

Como se mencionó anteriormente la serie 2800 de routers Cisco está diseñada para brindar comunicación de datos, voz y video con seguridad para las redes de pequeñas y medianas

empresas. Algunas de las características principales y sus beneficios se adjuntan en la siguiente tabla resumen.

Características	Beneficios
Arquitectura modular	Amplia gama de opciones WAN y LAN Interfaces expandibles Soporte para más de 90 módulos, incluidos WIC ⁸⁷ , VIC ⁸⁸ , módulos de red, PVDM ⁸⁹ y AIM ⁹⁰
Hardware acelerador de seguridad	Incluyen un acelerador de encriptación por hardware para VPN
Incluyen Dual Fast Ethernet y Gigabit Ethernet	Proporcionar dos puertos 10/100 en los modelos 2801 y 2811 y dos puertos 10/100/1000 en los modelos 2821 y 2851
Soporte para Cisco IOS Software	Proporcionan soporte para el software Cisco IOS para gestión de QoS, seguridad y administración de datos

Específicamente en el área seguridad, algunas características con que cuenta este equipo se puede apreciar en el siguiente cuadro resumen.

Características	Beneficios
Cisco IOS Software Firewall	Proporciona filtrado de contenidos, alertas de tiempo real, firewall para IPV6
Secure Sockets Layer (SSL)	SSL provee seguridad para transacciones web de autenticación, encriptación y firmas digitales
Acelerador de encriptación VPN	Soporta encriptación IPSec DES, 3DES, AES 128, AES 192, y AES 256
Network Admissions Control (NAC)	La red de autodefensa de Cisco provee capacidades para prevenir, identificar y adaptarse a las amenazas de red, mediante la herramienta de NAC
Soporte para USB eToken	Este dispositivo permite almacenar las credenciales para la autenticación de usuarios VPN

⁸⁷ WIC: WAN Interface Card

⁸⁸ VIC: Voice Interface Card

⁸⁹ PVDM: Packet Voice Data Modules

⁹⁰ AIM: Advanced Integration Module

Intrusion Prevention System (IPS)	Sistema provisto por el Cisco IOS de alto rendimiento en la detección de intrusos (IDS)
Cisco Easy VPN y soporte para servidores	Facilita la gestión de VPNs punto a punto y su configuración de forma remota
Group Encrypted Transport (GET) VPN	GET VPN IOS Software es una solución que simplifica la seguridad de capa 2 o redes MPLS transmitiendo la información mediante túneles VPN
Filtros URL	Puede incluirse mediante un modulo adicional o a través de una maquina externa al dispositivo que ejecute el software de filtrado de URL

Específicamente el Router Cisco 2821 de Servicios Integrados dispone de las siguientes características.

- Alto rendimiento en servicios de voz sobre IP y telefonía IP, ya que cuenta con soporte para enlaces T1/E1/xDSL y WAN
- Soporta hasta 90 módulos para distintos servicios y aplicaciones.
- Dos puertos 10/100/100 Ethernet
- Seguridad
 - Acelerador de encriptación
 - Soporte para 1500 túneles VPN con el modulo AIM-EPII-PLUS
 - Network Admission Control (NAC)
 - Intrusion Prevention (IPS) presente en el IOS Firewall
- Voz
 - Soporta entradas de voz análoga y digital
 - Incluye un modulo exclusivamente dedicado a servicios de voz
 - Opcionalmente soporta mensajes de voz
 - Soporta el software Cisco CallManager Express (Cisco CME) que administra hasta 48 teléfonos IP

El equipo seleccionado para ser el punto central de éste diseño será el **2821 VSEC Bundle with PVDM2-32, FL-CCME-48, Adv IP Serv, 128F/256D (C2821-VSEC-CCME/K9)**, que viene con el software Cisco CallManager Express con licencia para 48 usuarios y además incorpora el software Cisco IOS Advanced IP Services, que incorpora las funciones de los IOS IP VOICE y Advanced Security para proveer de comunicaciones VoIP y VPN respectivamente. A este equipo se agrega un módulo EthernetSwitch con 16 puertos Ethernet 10Base-T, Ethernet 100Base-TX.

Modelo	Descripción	Código de orden	Cantidad
2821	2821 VSEC Bundle with PVDM2-32, FL-CCME-48, Adv IP Serv, 128F/256D	C2821-VSEC-CCME/K9	1
Modulo EthernetSwitch	Cisco EtherSwitch Service Module - switch - 16 ports	NME-16ES-1G-P-RF	1

6.8.2.2 ROUTER CISCO SERIE 800 DE SERVICIOS INTEGRADOS

Esta serie de equipamientos está diseñado para pequeñas empresas, sucursales y teletrabajadores, que deseen interconectarse a una red corporativa con servicios de voz, video y/o datos con altos estándares de seguridad.

Características principales

Junto con una fácil implementación y capacidades de gestión centralizada, estos routers ofrecen características tales como:

- Filtros de contenido
- La herramienta Cisco Configuration Professional para simplificar la gestión de la red.
- Cuatro 10/100 Mbps Fast Ethernet con puertos de switch administrado PoE opcional de dos puertos de switch
- Soportan hasta 20 túneles VPN

- Access point incorporado, basado en IEEE 802.11n en algunas versiones con compatibilidad para redes wireless

Más específicamente la serie 800 de routers de Servicios Integrados vienen por defecto con:

- 4 puertos 10/100 Mbps
- Elementos de seguridad, incluyendo Cisco IOS Firewall

Además los modelos 871, 876, 877, 878, 881, y 888 incluyen:

- Prevención de intrusos con advanced IP services
- Cisco Dynamic Multipoint VPN, Cisco GETVPN, y SSL VPN

Los modelos Cisco 881 y 888 también incluyen:

- Filtrado de Contenidos Cisco

CISCO 871 INTEGRATED SERVICES ROUTER



Figura 43. Imagen Cisco 871

El modelo de Routers Cisco 871 Integrated Services for Small Offices es un equipo de fácil configuración destinado a proveer conectividad a pequeñas sucursales con soporte para tráfico de voz, video y/o datos con altos estándares de seguridad y rapidez en la encriptación de la información si así se requiere. Además brinda opcionalmente conexión inalámbrica.

Este modelo incluye:

- Firewall y encriptación para VPNs
- Intrusion prevention system (IPS)
- Opcionalmente 802.11g/n para incrementar la movilidad de los usuarios
- Quality of service (QoS) para múltiples aplicaciones

Algunos de los servicios disponibles en este modelo son:

- Conectividad segura mediante Firewalls e IPSec VPN con encriptación (Triple Data Encryption Standard [3DES] ó Advanced Encryption Standard [AES]) para conexiones de sitio a sitio si lo que se desea es conectar una pequeña oficina con una oficina central como es éste caso.
- Conectividad inalámbrica (802.11g/n) segura
- Fácil configuración con herramientas de administración remota

La siguiente tabla resume las ventajas y beneficios de cada uno de las características disponibles por esta serie de equipos.

Características	Beneficios
Soporte para Firewall y VPNs	Provee conectividad segura para accesos a Internet u otro sitio de la red administrativa
4 Puertos 10/100 Fast Ethernet 2 pueros USB 2.0	Provee conectividad entre distintos equipos en la red que administra y conectividad para USB eToken
Access Point 802.11g/n (opcional)	Provee conectividad inalámbrica segura
Puerto AUX/CONS	Puerto de doble propósito para conectar a una consola o Modem externo para configuración
Cisco Configuration Professional (CCP) y Cisco IOS Software para administración remota	Simplifica la configuración del equipo, además de proveer servicios para configuración remota

Algunas de las características presentes en el Cisco IOS incorporado en el Router Cisco 871 son las siguientes:

Características	Beneficios
IP y Servicios IP	<ul style="list-style-type: none"> • Routing Information Protocol (RIPv1 and RIPv2) • Layer 2 Tunneling Protocol (L2TP) • Cisco Express Forwarding (CEF) Port Address Translation (PAT) • Point-to-Point Protocol over ATM (PPoA) (DSL models only) • PPP over Ethernet (PPPoE) • Dynamic Host Control Protocol (DHCP) server/relay/client • Access control lists (ACLs) • Generic routing encapsulation (GRE) • Dynamic DNS Support para Cisco IOS
Seguridad	<ul style="list-style-type: none"> • Intrusion detection system/intrusion prevention system (IDS/IPS) • Tunnel-less Group Encrypted Transport (GET VPN) • Certificados digitales (PKI) • Firewall • NAT transparency • Hardware acelerador 3DES para IPSec • Hardware acelerador AES para IPSec • Cisco Easy VPN Client and Server • Point-to-Point Tunneling Protocol (PPTP) • L2TP • Secure HTTP (HTTPS), FTP, and Telnet authentication proxies • 10 túneles VPN • Advanced Application Inspection and Control
QoS	<ul style="list-style-type: none"> • Weighted Fair Queuing (WFQ) • Class-Based WFQ (CBWFQ) • Low-Latency Queuing (LLQ) • Class-Based Traffic Shaping (CBTS) • Class-Based QoS MIB • Policy-based routing (PBR)

El equipo seleccionado para cada una de las sucursales será el **Cisco 871 Ethernet Security Router (CISCO861-K9)**, el cual no cuenta con Access Point para conexiones inalámbricas, esto para evitar posibles ataques a la red corporativa por este medio.

Modelo	Descripción	Código de orden	Cantidad
871	Cisco 871 Security Bundle with Plus Feature Set	CISCO871-SEC-K9	8
IOS	Cisco IOS Advanced IP Services - (v. 12.4(22)T)	S870AISK9-12422T	8

6.8.2.3 DISPOSITIVO USB ETOKEN

Para poder autenticar a cada usuario de una PKI es fundamental que cada persona posea su propia clave privada. Esta clave privada actúa como un identificador único para cada individuo y les permite tener acceso a las redes protegidas o sitios web, o firmar digitalmente datos y las transacciones, con una verdadera prueba de su autenticidad. Una autenticación de la firma digital segura depende de la seguridad con la que se maneja la clave privada del usuario.

Claves privadas generadas y almacenadas en un ambiente de software, como en un PC, pueden estar expuestas a potenciales atacantes, por lo que una firma digital creada con un software basado en clave privada no garantiza que la firma fue creada por el usuario legítimo. El dispositivo eToken de la empresa Aladdin, elimina esta vulnerabilidad mediante la generación y almacenamiento de claves de seguridad PKI y certificados a bordo de un dispositivo de tarjetas inteligentes basadas en eToken.

Con este dispositivo USB portable, soportado por los router CISCO 2821, es posible obtener el máximo nivel de seguridad mediante la generación de claves PKI y la realización de operaciones criptográficas en el dispositivo eToken, sin la exposición de la clave privada, por lo que se ha pensado incluirlo en este diseño para algunos usuarios remotos que deseen acceder a la red corporativa de forma segura, brindando movilidad a los usuarios sin comprometer la información confidencial ante posibles atacantes que intenten suplantar la identidad de un usuario legítimo.

6.8.2.3.1 VENTAJAS DE ETOKEN USB

Encriptación de clave publica en el dispositivo

El dispositivo eToken USB contienen un microprocesador de alta seguridad que permite la generación de claves de cifrado y las operaciones criptográficas a bordo del dispositivo, esto implica que las claves privadas de autenticación de usuarios VPN en este caso nunca están expuestas a la inseguridad y el entorno del PC, por lo que no son vulnerables a los virus, gusanos, troyanos y otras amenazas comunes.

Dos métodos de autenticación

Si un usuario desea acceder a una red corporativa está obligado a conectar su dispositivo eToken e introducir una contraseña (PIN) para autenticarse o firmar digitalmente datos y transacciones, por lo que no se restringe sólo a un método de verificación de su identidad.

Alta Portabilidad

Dado que las claves están almacenadas en el dispositivo portátil eToken, se pueden utilizar dondequiera que estén, siempre que sea necesario desde cualquier ordenador con un puerto USB estándar.

Facilidad de uso

Los usuarios pueden realizar operaciones de PKI fácilmente y de manera intuitiva, de la misma manera que utilizan sus eToken para otras aplicaciones de seguridad.

Infraestructura ligera

El dispositivo eToken USB de autenticación proporciona la contraseña de autenticación y la capacidad de gestión sin necesidad de instalación de servidores, haciendo más simple y compacta la infraestructura de la red, sin descuidar las políticas de seguridad.

ETOKEN PRO



Figura 44. Dispositivo USB de autenticación de usuario eToken PRO

Este dispositivo está diseñado para una fuerte autenticación de usuarios remotos, administración de contraseñas y firmas digitales. Es compatible con los sistemas operativos más utilizados actualmente tales como Windows 2000/XP/2003/Vista, Mac OS X y Linux, soporta los estándares y protocolos PKCS#11 v2.01, Microsoft CAPI, PC/SC, certificados digitales X.509 v3, SSL v3, IPSec/IKE.

Además incorpora en su estructura un microprocesador para encriptación RSA 1024-bit / 2048-bit, DES, 3DES y SHA1. Sus dimensiones de 52 x 16 x 8 mm lo hacen un dispositivo portable para utilizarlo en cualquier lugar que se disponga de un equipo con conexión USB. Cumple con la normativa ISO 7816, que es un estándar internacional relacionado con las tarjetas de identificación electrónicas, en especial las tarjetas inteligentes, gestionado conjuntamente por la Organización Internacional De Normalización (ISO) y Comisión Electrotécnica Internacional (IEC).

A continuación se adjunta la descripción de los dispositivos solicitados:

Modelo	Descripción	Cantidad
eToken PRO	Dispositivo USB	10

6.9.2.4 TELÉFONOS IP DE COMUNICACIONES UNIFICADAS DE CISCO SERIE 500

Esta serie de teléfonos IP de la empresa Cisco están diseñados para optimizar y simplificar las comunicaciones en las pequeñas empresas, incrementando la productividad de los empleados, mediante el acceso a comunicaciones de voz y datos, a la par que se reducen los costos.

Los teléfonos IP de Comunicaciones Unificadas de Cisco serie 500 ofrecen:






Voz y datos: las comunicaciones integradas en el teléfono permiten a los empleados realizar llamadas de voz y acceder a los datos de la empresa, como los directorios, de manera rápida y sencilla, independientemente del lugar en el que estén trabajando.

Funciones telefónicas tradicionales: los empleados pueden aprovechar el acceso a varias líneas y otras funciones, como por ejemplo, altavoz, rellamada, transferencia de llamadas, localización, intercomunicación, control de volumen, indicadores de mensajes en espera y correo de voz, tecla de silenciamiento y auriculares.

Los teléfonos IP de Comunicaciones Unificadas de Cisco serie 500 ofrecen una amplia gama de funciones y características, entre las cuales cabe destacar:

- Modelos básicos y de bajo coste para distintos entornos
- Tecla de menú para acceder al historial de llamadas, preferencias del usuario y directorio
- Modelos con función de dos u ocho líneas
- Pantallas monocromáticas con luz de fondo
- Modelos que son fáciles de configurar y reubicar
- Timbres que los usuarios pueden cambiar con facilidad

Los modelos y sus principales ventajas de esta serie disponibles en el mercado son los siguientes:

	Modelos y sus principales ventajas
<p>521G</p> 	<ul style="list-style-type: none"> * Teléfono de una sola línea con acceso a dos líneas * Utiliza Power over Ethernet o un adaptador de energía opcional
<p>521SG</p> 	<ul style="list-style-type: none"> * Teléfono de una sola línea con acceso a dos líneas * Utiliza Power over Ethernet o un adaptador de energía opcional * Incluye un switch 10/100 para la conexión de LAN a una PC ubicada en el mismo lugar * Permite designar redes LAN virtuales (VLAN) (802.1q) separadas para la PC y el teléfono para que pueda contar con una transmisión más segura y confiable del tráfico de voz y datos por igual
<p>524G</p> 	<ul style="list-style-type: none"> * Teléfono de cuatro líneas con acceso a ocho visualizaciones de líneas de llamada * Utiliza Power over Ethernet o un adaptador de energía opcional
<p>524SG</p> 	<ul style="list-style-type: none"> * Teléfono de cuatro líneas con acceso a ocho visualizaciones de líneas de llamada * Utiliza Power over Ethernet o un adaptador de energía opcional * Incluye un switch 10/100 para la conexión de LAN a una PC ubicada en el mismo lugar * Permite designar redes LAN virtuales (VLAN) (802.1q) separadas para la PC y el teléfono para que pueda contar con una transmisión más segura y confiable del tráfico de voz y datos por igual
<p>SPA525G</p> 	<ul style="list-style-type: none"> * Teléfono IP de cinco líneas con funciones completas, hasta 10 visualizaciones de línea de llamada y compatibilidad con hasta dos consolas de operadora SPA932 * Es compatible con los protocolos SIP o SPCP * Conectividad a la red a través de Power over Ethernet o modo de cliente inalámbrico 802.11g * Es compatible con Bluetooth o auriculares de 2,5 mm * Pantalla a color QVGA 320 x 240 de 3,2 pulgadas y alta resolución * Altavoz dúplex completo integrado

De acuerdo a estas especificaciones los teléfonos seleccionados para este diseño son los siguientes:

Modelo	Descripción	Código de orden	Cantidad
521SG	Teléfono IP	CP-521SG=	33
524SG	Teléfono IP	CP-524SG=	9

6.8.3 DIAGRAMA DE LA RED

Como se mencionó anteriormente el número total de usuarios que componen este diseño son 42, todos con sus respectivos teléfonos IP, estos distribuidos en 8 sucursales, más la casa central, de los cuales uno se considera como recepcionista, por lo que su teléfono será el modelo CISCO 524SG, que dispone de 4 líneas para recibir las llamadas. A continuación se adjunta el diseño final con los respectivos equipos que se utilizarán en el diseño de cada Sucursal y la Casa Central.

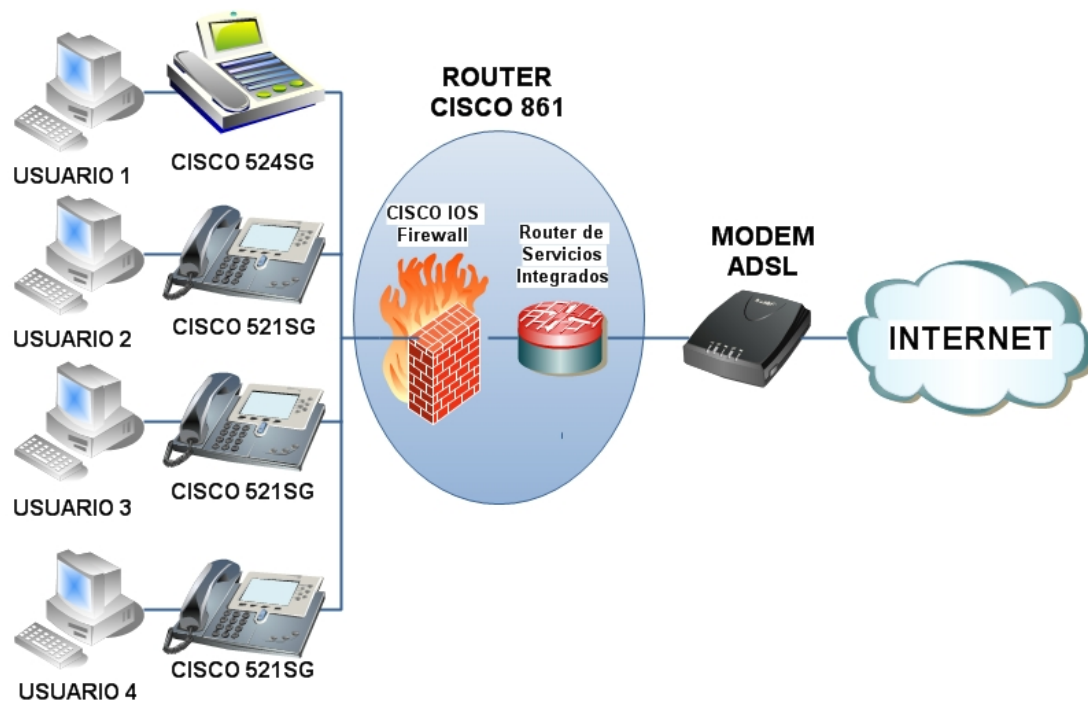


Figura 45. Diagrama sucursales

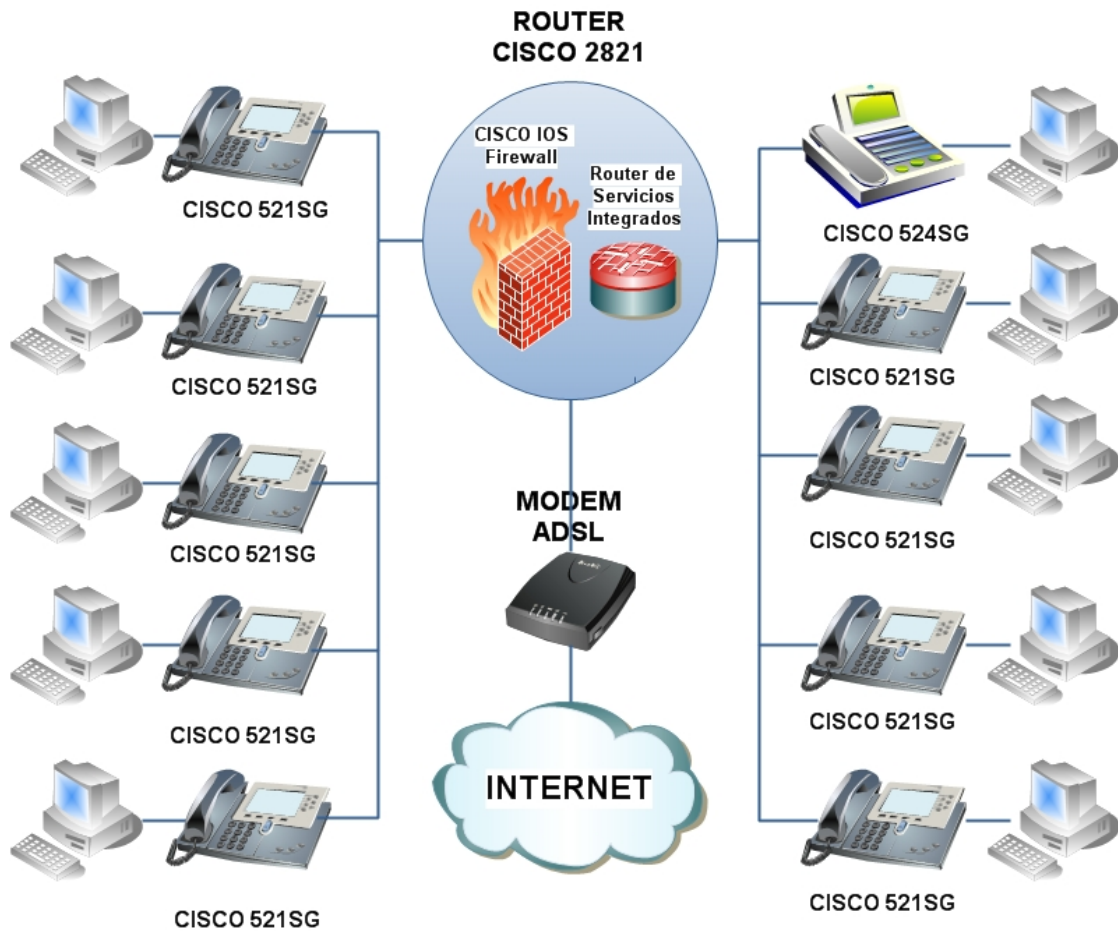


Figura 46. Diagrama Casa Central

6.9 RESUMEN

En este capítulo se especificó acerca de los detalles del proyecto, tales como número de los usuarios, ubicación y número de oficinas, con el respectivo detalle de la cantidad de usuarios y equipamientos necesarios en cada una de ellas, esto con el propósito de realizar una búsqueda y análisis exhaustivo de los equipamientos compatibles con los requerimientos del diseño. Para ello se analizan las series de equipos CISCO de servicios integrados y sus software de aplicaciones para la administración de las comunicaciones tales como **GET VPN** incluido en el software **CISCO IOS ADVANCED IP SERVICE** para gestionar las conexiones VPN,

además de la configuración de los parámetros de QoS del tráfico y **CISCO CallManager Express** para gestionar las comunicaciones VoIP entre los distintos usuarios, que se incluye en el paquete del router 2821.

Para la selección de los equipos y softwares se procedió a analizar cada una de las series compatibles con los servicios de VoIP, VPN y seguridad, sin embargo la selección final de todos los equipos que cumplieran con estos requerimientos fue acorde al número de usuarios para no sobredimensionar el diseño y aumentar excesiva e innecesariamente los costos del proyecto. El número total de equipos (Teléfonos IP) soportados por el diseño es de 48, sin embargo el número total de usuarios VoIP que se pueden conectar por otros medios es 250.

CAPÍTULO VII. ESTUDIO DE COSTOS

7.1 INTRODUCCIÓN

En el diseño de un proyecto para una PYME es muy importante tener siempre presente los costos que involucra dicho trabajo, debido a que éstas muchas veces cuentan con recursos económicos limitados, por lo que se busca encontrar la alternativa que brinde las mejores prestaciones a un costo aceptable, sin descuidar los requerimientos que en el diseño original se plantearon.

En este capítulo se realizará el análisis de los costos involucrados en la instalación, administración y puesta en marcha del proyecto de comunicación, considerando tanto los equipamientos para brindar las comunicaciones entre las sucursales y la casa central, como también la mano de obra necesaria para realizar la instalación y configuración del diseño.

7.2 DESCRIPCIÓN

Este proyecto, como se ha mencionado anteriormente, consiste en el diseño de una red de VoIP que comunica 8 sucursales ubicadas en 8 capitales regionales del país con una casa central ubicada en Santiago de Chile mediante VPN IPSec con equipamiento y softwares CISCO que ayudarán a la administración de la red. El proceso de implementación del proyecto se contempla en dos etapas, para lo cuál se necesitará recurso humano que se encargará de la instalación y configuración de los equipos. Las etapas son las siguientes:

Primera etapa: En esta etapa se contempla la instalación de los dispositivos físicos que formarán parte de cada una de las redes LAN en las sucursales y casa central. Además de la configuración de los equipos para que funcionen de forma local y pueda acceder el profesional encargado de administrar la red de forma remota.

- Instalación del cableado de la red local en cada sucursal
- Montaje de los routers en cada sucursal
- Montaje de los teléfonos IP en cada sucursal
- Conexionado de los routers, PCs y teléfonos IP en cada sucursal
- Configuración de la red local en cada sucursal
- Configuración de routers y teléfonos IP en cada sucursal
- Instalación del Software GET VPN para la administración de las conexiones VPN y certificados digitales.

- Instalación de los software de administración remota CISCO Router and Security Device Manager (SDM) en cada sucursal
- Instalación del Software Cisco CallManager Express para la administración de las comunicaciones VoIP en cada sucursal
- Habilitar los equipos con acceso a Internet en cada sucursal

Segunda etapa: En esta segunda etapa se procederá a realizar la instalación y configuración de los equipos en la casa central, además de la integración de todas las redes locales a la red corporativa mediante administración remota, por lo que se llevará a cabo en la Oficina central.

- Instalación del cableado de la red local en la casa central
- Montaje de los routers en la casa central
- Montaje de los teléfonos IP en la casa central
- Conexionado de los routers, PCs y teléfonos IP en la casa central
- Configuración de la red local en la casa central
- Configuración de routers y teléfonos IP en la sucursal
- Instalación del Software GET VPN para la administración de las conexiones VPN y los certificados digitales.
- Instalación de los software de administración remota CISCO Router and Security Device Manager (SDM) en la casa central

- Instalación del Software Cisco CallManager Express para la administración de las comunicaciones VoIP en la sucursal
- Habilitar los equipos con acceso a Internet en la sucursal
- Instalar las licencias y certificados digitales en cada equipo de la casa central
- Configurar el acceso de las sucursales a la casa central mediante el software GET VPN y el software Cisco Router and Security Device Manager (SDM) para administración remota.

7.3 COSTOS DE IMPLEMENTACIÓN

Los costos de los equipos que se presentan en el siguiente apartado son expresados en dólares americanos (USD) debido a que los equipos son cotizados en EEUU en un Partner CISCO INSIGHT⁹¹ y convertidos a la moneda nacional (CLP).

7.3.1 EQUIPAMIENTO

MODELO	DESCRIPCIÓN	CODIGO DE ORDEN	CANTIDAD	VALOR (USD)
ROUTER CISCO 2821	2821 VOICE VSEC Bundle with PVDM2-32, FL-CCME-48, Adv IP Serv, 128F/256D	C2821-VSEC-CCME/K9	1	\$ 4309.99
MODULO ETHERNETSWITCH PARA ROUTER 2821	Cisco EtherSwitch Service Module - switch - 16 ports	NME-16ES-1G-P-RF	1	\$ 1101.65
ROUTER CISCO 871	Cisco 871 Security Bundle with Plus Feature Set	CISCO871-SEC-K9	8	\$ 4431.92
IOS ROUTER 871	Cisco IOS Advanced IP Services - (v. 12.4(22)T)	S870AISK9-12422T	8	959.92

⁹¹ Insight: <https://www.insight.com/>

eToken PRO	DISPOSITIVO DE AUTENTICACIÓN USB	ETOKEN PRO-SMARTCARD-72K (1-100 USERS)	10	\$ 199.9
TELEFONO IP CISCO 521SG	Cisco Unified IP Phone 521SG - VoIP phone - SPCP - silver, dark gray	CP-521SG=	33	\$ 5510.67
TELEFONO IP CISCO 524SG	Cisco Unified IP Phone 524SG - VoIP phone - SPCP - silver, dark gray	CP-524SG=	9	\$ 1889.91
TOTAL				\$ 18403.96

Actualmente un dólar esta avaluado a aproximadamente \$ 566.- pesos chilenos, por lo que en equipamiento se invierte un total aproximado de **\$10.416.641.-(Diez millones cuatrocientos diez y seis mil seiscientos cuarenta y uno) Pesos (CLP).**

Además se agrega un ítem de extras, en el cual se incluyen gastos de cableado, herramientas, soportes, entre otros elementos que sean de utilidad para instalar el equipamiento.

ITEM	DESCRIPCION	Valor (Pesos)
EXTRAS	CABLES, HERRAMIENTAS, ETC.	\$ 1.000.000
PASAJES	PASAJES TERRESTRES	\$ 500.000
TOTAL		\$1.500.000

7.3.2 GASTOS RECURSO HUMANO

Para realizar estas labores se considera la incorporación de 2 profesionales, un **Técnico Informático** y un **Ingeniero Electrónico**, los cuales se encargarán de la instalación, configuración y puesta en marcha del proyecto. El tiempo estimado para la implementación del diseño es de **2 meses**.

Profesional	Salario mensual (Pesos)
Técnico Informático	\$ 500.000
Ingeniero Electrónico	\$ 800.000
Total	\$ 2.600.000

La suma de los gastos de insumos, mano de obra, y extras es la siguiente:

ITEM	Valor (Pesos)
Equipamiento	\$10.416.641.-
Extras	\$1.500.000.-
Mano de obra	\$ 2.600.000.-
Total	\$14.516.641.-

CAPÍTULO VIII. CONCLUSIONES

Una vez finalizado el Trabajo de Titulación se puede concluir que un diseño para una PYME no es tarea fácil, esto debido principalmente a los recursos limitados con que generalmente cuentan, de ésta manera se busca encontrar las mejores prestaciones en cuanto a seguridad, calidad de servicio, interoperabilidad y ahorro en contratación de servicios de telefonía, que a un mediano plazo, dependiendo de la frecuencia con que se comuniquen con sus sucursales van a hacer recuperar la inversión del proyecto.

En relación al proyecto, concluyo que la mejor forma de comunicar las sucursales de la PYME con la casa central es mediante conexiones VPN sitio a sitio con la ayuda del protocolo de seguridad IPSec. Una herramienta que simplifica de gran manera la gestión y administración de éstos túneles es la herramienta de software provista por el SOFTWARE CISCO IOS ADVANCED IP SERVICES denominada GET VPN. Refiriéndome a las conexiones de usuarios remotos el diseño contempla la gestión de conexiones VPN SSL, que simplifican los procesos de configuración y conexión de usuarios que no se encuentran conectados físicamente a la red corporativa, sin menoscabar las políticas de seguridad que son imprescindibles para la comunicación de la PYME. La autenticación de estos usuarios se ha reforzado gracias a un sofisticado dispositivo USB denominado eToken que almacena las credenciales de los usuarios remotos, poniendo una barrera ante posibles atacantes que quieran suplantar la identidad de un usuario legítimo ingresando a los contenidos de la red corporativa.

Una de las ventajas principales con que cuentan la serie de routers CISCO seleccionados para esta aplicación es el acelerador de encriptación por hardware, que posibilita el procesamiento de la información a transmitir por los túneles VPN en un lapso de tiempo mucho menor que encriptándola por software, disminuyendo notablemente los retardos para la transmisión de la información que pueden degradar la calidad de los servicios de voz y datos principalmente.

Para la gestión de los servicios de VoIP se utilizó la herramienta de software CISCO CallManager Express que simplifica la configuración de las comunicaciones de voz, además de gestionar la QoS de esta aplicación priorizando su tráfico sobre el resto con la ayuda del software CISCO IOS presente en los routers con integración de servicios seleccionados. El CODEC utilizado para esta aplicación fue el G.729 con supresión de silencios, que en conjunto con el protocolo SIP da muy buenos resultados en cuanto a calidad de voz y ancho de banda utilizado en la transmisión.

Para concluir cabe destacar la amplia gama de soluciones provistas por CISCO en el campo tecnológico, las cuales son de primera calidad, por lo que los costos extras que se pudieran generar si se buscan buenos resultados y una solución confiable, se pueden asumir en este proyecto.

Como trabajo adicional se consideró la interconexión del servicio de VoIP con la telefonía conmutada brindando servicios de telefonía IP, que abriría un campo bastante amplio de aplicaciones a la red corporativa. Los equipos seleccionados para este diseño proporcionan soporte para este servicio, lo que facilita la migración de la red. Otro punto que se contempla como trabajo adicional que también puede ser implementado sobre la base de los equipos y protocolos seleccionados para este diseño es la transmisión de video sobre IP, que pueden ayudar a la PYME a obtener servicios de gran nivel a un costo bastante accesible.

Finalmente, puedo concluir que este Trabajo de Titulación fue de gran ayuda en mi desarrollo tanto profesional como personal, debido a que se convirtió en un verdadero reto el realizar un proyecto de esta envergadura, con lo que me considero en condiciones de afrontar una responsabilidad laboral y responder de la mejor manera ante las exigencias.

REFERENCIAS BIBLIOGRAFICAS

- [1] A. RAMIREZ, ESTUDIO DE TECNOLOGIAS EN CONECTIVIDAD SEGURA Y SIMULACION DE LA TECNOLOGIA IPSEC PARA REDES DE COMUNICACIONES, ESCUELA DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA, UNIVERSIDAD DEL VALLE, SANTIAGO DE CALI, 2005.
- [2] M. GUTIÉRREZ G., A SANCHO B., A. CASAS C., ESTUDIO SOBRE LAS VPN, INFORMÁTICA. 4º INGENIERÍA INFORMÁTICA, UNIVERSIDAD DE VALLADOLID, ESPAÑA.
- [3] DANIEL E. FONTAGNOL, VIRTUAL PRIVATE NETWORKS, IV CONGRESO DE BIBLIOTECARIOS DEL INTA, ARGENTINA, 2005
- [4] JESÚS FERNÁNDEZ H., JOSÉ LUIS ALONSO B., CARLOS G.-FIGUEROLA P., ÁNGEL F. ZAZO R., REDES PRIVADAS VIRTUALES, DEPARTAMENTO DE INFORMÁTICA Y AUTOMÁTICA, UNIVERSIDAD DE SALAMANCA, 2006
- [5] RAMIRO J. CAIRE, INTRODUCCION A LAS REDES PRIVADAS VIRTUALES (VPN) BAJO GNU/LINUX.
- [6] ALEX FLORES A., RODRIGO HENRÍQUEZ J., CONEXIONES IPSEC EN MULTIPLES PLATAFORMAS, FACULTAD DE CIENCIAS, UNIVERSIDAD CATOLICA DE TEMUCO, TEMUCO, 2004.
- [7] SANTIAGO PÉREZ I., ANÁLISIS DEL PROTOCOLO IPSEC: EL ESTÁNDAR DE SEGURIDAD EN IP, TELEFÓNICA INVESTIGACIÓN Y DESARROLLO, 2001.
- [8] JUAN SEPULVEDA H., CONVERGENCIA DE REDES A TRAVES DE IMS, FACULTAD DE INGENIERIA, UNIVERSIDAD MAYOR, SANTIAGO, 2007.

- [9] SERGIO ÁVILA M., F. DE JESÚS, OMAR OCAMPO O., SERGIO VALLEJO E., SEGURIDAD EN REDES, DEPARTAMENTO DE SISTEMAS Y COMPUTACIÓN, INSTITUTO TECNOLÓGICO DE VERACRUZ.
- [10] JOSÉ MARÍA MORALES V., SSL, SECURE SOCKETS LAYER Y OTROS PROTOCOLOS SEGUROS PARA EL COMERCIO ELECTRÓNICO, UNIVERSIDAD POLITÉCNICA DE MADRID, CURSO 2001/2002.
- [11] ENRIQUE SORIANO S., ARQUITECTURAS DE SEGURIDAD PARA SISTEMAS DISTRIBUIDOS FRACCIONABLES, DINÁMICOS Y HETEROGÉNEOS CON APLICACIÓN A LA COMPUTACIÓN UBICUA, DEPARTAMENTO DE INGENIERÍA TELEMÁTICA Y TECNOLOGÍA ELECTRÓNICA TESIS DOCTORAL, UNIVERSIDAD REY JUAN CARLOS DE MADRID, MADRID, 2006.
- [12] ANTONIO IZQUIERDO M., METODOLOGÍA PARA LA VALIDACIÓN Y EVALUACIÓN REMOTA DE IMPLEMENTACIONES DE PROTOCOLOS DE SEGURIDAD. APLICACIÓN A LA ARQUITECTURA IPSEC, UNIVERSIDAD CARLOS III DE MADRID, LEGANÉS, 2006.
- [13] ALFREDO ÁLVAREZ B., ESTUDIO TÉCNICO-ECONÓMICO DE REDES DE AGREGACIÓN DE NUEVA GENERACIÓN, ESCUELA TÉCNICA SUPERIOR DE INGENIEROS DE TELECOMUNICACIÓN, UNIVERSIDAD POLITÉCNICA DE MADRID, MADRID, 2008.
- [14] ADRIANA FERRERIRA, MARCELO PEPE, FERNANDO LOPEZ, JULIO GUANI, VOIP EN REDES CORPORATIVAS, ANTELDATA.
- [15] JOSÉ MORENO, IGNACIO SOTO, DAVID LARRABEITI, PROTOCOLOS DE SEÑALIZACIÓN PARA EL TRANSPORTE DE VOZ SOBRE REDES IP, DEPARTAMENTO DE INGENIERÍA TELEMÁTICA, UNIVERSIDAD CARLOS III DE MADRID, MADRID.

[16] RODOLFO CASTAÑEDA SEGURA, PROTOCOLOS PARA VOZ IP, DIRECCIÓN DE TELEMÁTICA, CICESE, 2005.

[17] PABLO CATALINA, SEGURIDAD EN VOIP, AUDITOR SEGURIDAD TELEMÁTICA, S21SEC, 2008.

[18] SERGIO LILLO M., EVALUACIÓN TÉCNICO – ECONÓMICA DE IMPLEMENTACIÓN DE TELEFONÍA IP EN EMPRESA QUINTEC, FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS DEPARTAMENTO DE INGENIERÍA ELÉCTRICA, UNIVERSIDAD DE CHILE, SANTIAGO, 2006.

[19] ALEXIS IGA J., METODOLOGÍAS, HERRAMIENTAS Y CRITERIOS PARA LA PLANIFICACIÓN GENERAL DE PLATAFORMAS DE TELECOMUNICACIONES, FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS, UNIVERSIDAD DE CHILE, SANTIAGO, 2007.

[20] SERGIO MAURICIO BRAVO CID, ESTUDIO Y PUESTA EN SERVICIO DE UNA CENTRAL TELEFÓNICA – IP HÍBRIDA PARA LA CENTRAL HIDROELÉCTRICA PULLINQUE – SUBSIDIARIA DE ENEL, FACULTAD DE CIENCIAS DE LA INGENIERÍA, ESCUELA DE ELECTRICIDAD Y ELECTRÓNICA, UNIVERSIDAD AUSTRAL DE CHILE, VALDIVIA, 2006.

[21] CRISTIAN BORGHELLO, SEGURIDAD INFORMÁTICA: IMPLICANCIAS E IMPLEMENTACIÓN, ARGENTINA, 2001.

[22] CARLOS EDUARDO CONTRERAS OYARZÚN, DISEÑO, OPERACIÓN Y GESTIÓN DE REDES DE VIDEO IP, FACULTAD DE CIENCIAS DE LA INGENIERÍA, ESCUELA DE ELECTRICIDAD Y ELECTRÓNICA, UNIVERSIDAD AUSTRAL DE CHILE, VALDIVIA, 2006.

[23] CRISTINA RIVAS, INDICADOR DE LA ACTIVIDAD DE TI EN CHILE, RESEARCH MANAGER, IDC CONO SUR, 2008.

DIRECCIONES ELECTRÓNICAS

[23] [HTTP://WWW.IETF.ORG/RFC](http://www.ietf.org/rfc)

[24] [HTTP://WWW.CISCO.COM/](http://www.cisco.com/)

[25] [HTTP://WWW.ITU.INT/NET/HOME/INDEX.ASPX](http://www.itu.int/net/home/index.aspx)

[26] [HTTPS://WWW.INSIGHT.COM/](https://www.insight.com/)

[27] [HTTP://WWW.MICROSOFT.COM/](http://www.microsoft.com/)

[28] [HTTP://WWW.TEXTOSCIENTIFICOS.COM](http://www.textoscientificos.com)

[29] [HTTP://WWW.DELITOSINFORMATICOS.COM/](http://www.delitosinformaticos.com/)

[30] [HTTP://WWW.TRESTECH.COM.AR/](http://www.trestech.com.ar/)

[31] [HTTP://WWW.ALADDIN.COM/](http://www.aladdin.com/)

[32] [HTTP://WWW.ALFREDCERTAIN.COM/?P=9](http://www.alfredcertain.com/?P=9)

[33] [HTTP://WWW.VOIPFORO.COM](http://www.voipforo.com)

[34] [HTTP://WWW.SII.CL](http://www.sii.cl)

[35] [HTTP://WWW.GARTNER.COM/](http://www.gartner.com/)

[36] [HTTP://WWW.ALCATEL-LUCENT.COM](http://www.alcatel-lucnet.com)

[37] [HTTP://WWW.IDCLATIN.COM](http://www.idclatin.com)

[38] [HTTP://WWW.HUAWEI.COM](http://www.huawei.com)

[39] [HTTP://WWW.FORBES.COM/2009/04/28/AMERICA-REPUTABLE-COMPANIES-LEADERSHIP-REPUTATION_TABLE.HTML](http://www.forbes.com/2009/04/28/AMERICA-REPUTABLE-COMPANIES-LEADERSHIP-REPUTATION_TABLE.HTML)