ESCUELA POLITECNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO Y DISEÑO DE UNA RED PRIVADA VIRTUAL PARA BRINDAR EL SERVICIO DE VOIP, ADMINISTRADO BAJO EL SISTEMA OPERATIVO LINUX

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN ELECTRONICA Y TELECOMUNICACIONES

CHRISTIAN DAVID LOZA BONILLA
crislozab4@hotmail.com
FRANCISCO JAVIER ORDÓÑEZ SOTO
panchojavicho@hotmail.com

DIRECTOR: Dr. ING. LUIS CORRALES
luis.corrales@epn.edu.ec

Quito, Octubre 2008

DECLARACIÓN

Nosotros, LOZA BONILLA CHRISTIAN DAVID y ORDOÑEZ SOTO FRANCISCO JAVIER, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____ _____

Christian Loza Francisco Ordoñez

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por LOZA BONILLA CHRISTIAN DAVID y ORDOÑEZ SOTO FRANCISCO JAVIER, bajo mi supervisión.

_____

Dr. Luis Corrales

DIRECTOR DE PROYECTO

AGRADECIMIENTOS

Agradezco a Dios por haberme dado la fuerza, paciencia y sabiduría para culminar este trabajo, fruto de los conocimientos vertidos por mis maestros.

A mis padres y hermanos por el gran apoyo que me han brindado siempre. Gracias por el ejemplo y los valores que me han impartido. Gracias por el sacrificio que han hecho al darme el estudio.

A una persona muy especial en mi vida y que por obras del destino apareció en mi vida. Gracias por el apoyo y cariño que me has brindado, gracias amor, gracias Mary.

A mis amigos Juanito, Patty, Vero, Giss, Angy, Jotta, George, Mayra, Diego, Fabian, Pancho, Wilson, Jessica, Nico, Pao, César, David, que siempre me han acompañado y brindado su respaldo incondicional.

Al Dr. Corrales por sus sabios consejos y el apoyo para desarrollar el presente proyecto.

A la UGI por su colaboración en llevar a cabo el presente proyecto y en especial al Ing. Juan Carlos Proaño.

Christian

AGRADECIMIENTOS

No hubiera podido llegar hasta aquí de no ser por el apoyo y ayuda incondicional de mi familia, es muy grato para mi contar con la bendición de mis padres, que son los primeros a quienes debo agradecer, a mi ma Anita y a mi pa Cosme, a mi Abue Rosita; gracias también a mis hermanos, al Negro por tratar siempre de educarme con su ejemplo, pese a la distancia; a la Flaca, que aunque la mate de iras siempre terminamos chismoseando; a la Gordita, que me recuerda lo difícil de crecer y al Enano, que es mi mejor amigo.

A la Escuela Politécnica Nacional, representada en todos sus docentes que tratan de cambiar el horizonte a cada uno de nosotros, esperando que sus esfuerzos prosperen y se reflejen en un futuro prometedor para el bien del país. Gracias a todos los profesores

Fue muy importante para mi poder contar con un buen compañero, no solo durante el desarrollo de la tesis, sino también durante el desarrollo de nuestra carrera, y pese a que nunca fuimos los grandes amigos siempre pude contar con su camarería, gracias Profeshor.

Gracias también al “Doc” Luís Corrales, porque siempre estuvo dispuesto a resolver nuestras inquietudes, y siempre con una grata sonrisa.

A las personas con las que compartí mi vida estudiantil, pero que sobre todo me ayudaron a hacer mi estancia más amena lejos de mi pueblo, gracias por permitirme ser parte de sus vidas y por formar parte de la mía. Gracias a Patty, Nory, Vero, Julio (MRK), David (Bambaro), César (Mono), Morocho (Diego), Juan (Jotta), Fabián (Fabas), Juanito (Diablo). Además a los chamos del SHPE; Kari, Dave, Danny, gracias por las 3 resmas de papel, que no pienso devolver y a los

nunca campeones Kchu Kchu, que me alegro de que hayan cambiado el nombre sino me resultaba difícil agradecerles por escrito.

Una persona que me sorprendió al final de mi camino por la Poli, y que te conocí gracias a la Poli, son muchas cosas que aprendí gracias a ti, y que también gracias a ti reescribía mi tesis cada día, gracias Anita.

Espero haber reconocido el apoyo de todos mis compañeros, me disculpo si olvide a alguien, pero espero recordarlo en la siguiente tesis que realice.

Gracias a todos!

DEDICATORIA

Este trabajo dedico con todo mi amor y cariño…

A toda mi familia y en especial a mi madre querida, que gracias a su ejemplo y amor he seguido siempre adelante.
A mi novia Maria Elena, y a mis queridos amigos quienes siempre me demostraron su amistad en los momentos en los que más los necesite.

Christian

El esfuerzo y dedicación puesto, no solo en éste trabajo sino también a lo largo de mi estancia en la universidad, lo dedico a las mujeres mas importantes de mi vida, mi Ma, mi Abue, mi ñaña la Flaca y mi ñaña la Gordita, por todo lo que significan para mi y por todo lo que han sacrificado por mi.

P@NCHO

CONTENIDO

INDICE DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

INDICE DE TABLAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

RESÚMEN

Este proyecto tiene como objetivo brindar el servicio de voz sobre IP para una empresa típica que cuente con una oficina matriz y una sucursal, utilizando una Red Privada Virtual (VPN) que permita comunicar directamente las oficinas a través de Internet. De esta manera las extensiones telefónicas podrán comunicarse con otras extensiones dentro de la matriz, de la sucursal, o con usuarios remotos.

Para el diseño de la red privada virtual se utilizaron equipos Cisco ASA Serie 5500 como equipos de borde, que se ubican entre la red interna de la empresa y el proveedor de Internet. Se configuraron estos equipos con protocolos IPSec VPN, algoritmos de encripción y herramientas de autenticación, para brindar confidencialidad e integridad a los paquetes que viajan a través del túnel VPN.

Para administrar la red telefónica se seleccionó el sistema operativo Asterisk Now, en donde se configuraron las extensiones de manera que cada usuario cuente con un número de extensión, una identificación y otras características que permiten mantener control y manejo de las llamadas dentro de la central. La red VPN permite que todas las extensiones registradas dentro del servidor Asterisk Now puedan comunicarse entre si, sin importar la localidad en que se encuentren.

Luego del proceso de implementación se realizarón pruebas en un ambiente experimental controlado. Durante este proceso se realizaron llamadas telefónicas dentro de una red LAN y en un ambiente de acceso remoto.

En el periodo de pruebas se pudo apreciar que la calidad de las llamadas telefónicas era buena a pesar que se utilizó una conexión doméstica de Internet de 128 Kbps. Para comprobar la encripción de los paquetes se utilizó una herramienta de monitoreo en un PC en el mismo dominio del usuario remoto, confirmando que los paquetes viajaban encriptados.

PRESENTACIÓN

Las redes de hoy en día están evolucionando y permitiendo el transporte de datos, voz y video, tendiendo de esta forma redes convergentes. Actualmente, con los múltiples servicios sobre Internet y la necesidad de las empresas de bajar sus costos operativos en comunicaciones, considerando que los enlaces de líneas dedicadas son costosos, las empresas han optado por el uso de Internet como un medio de transporte de comunicación con sus oficinas o sucursales remotas. Pero esta alternativa crea la necesidad de diseñar una red privada virtual (VPN) sobre la gran red pública Internet. Una VPN permite brindar la máxima seguridad y confidencialidad en la transmisión de la información (voz), encriptándola para garantizar que la señal no sea interceptada por agentes externos a la red.

El presente proyecto de titulación tiene por objeto el estudio y diseño de una red privada virtual para brindar el servicio de VoIP, y para conseguir este objetivo se ha dividido el trabajo de la forma siguiente:

En el Capítulo 1 se realiza el estudio de las Redes Privadas Virtuales (VPN), sus propiedades, criptografía, algoritmos de encripción y autenticación. Además se realiza un estudio del Protocolo IPSec, sus modos de operación y el conjunto de protocolos que se utilizan en la implementación de un túnel para formar un camino seguro para el transporte de información. Se elabora además una introducción del servicio de VoIP, parámetros de calidad de servicio, tecnologías y protocolos de telefonía IP. Finalmente se realiza un estudio de VoIP frente a tecnologías similares como voz sobre Frame Relay, ATM y sobre VPNs.

En el Capítulo 2 se analizan los escenarios para la implementación del túnel VPN y los requerimientos que se necesitan para establecer llamadas a través de VoIP sobre el túnel. En éste capítulo se realiza el diseño de una red privada virtual, se definen los protocolos que se utilizan en el túnel, además se realiza el diseño para brindar el servicio de VoIP a través del servidor Asterisk.

En el Capitulo 3 se implementa la VPN sobre dos escenarios. El primer escenario es una VPN LAN a LAN, es decir, que se unen a través de un túnel dos redes privadas separadas mediante una nube WAN formada por ruteadores en topologías de red diferentes. El segundo escenario es una VPN de acceso remoto, en el que un host remoto a través de un software cliente, podrá acceder a la red una empresa a través de una red WAN o sobre Internet. En este capítulo se indican todas las configuraciones necesarias tanto para el túnel como para la nube WAN.

Además, en el Capítulo 3, se configura el sistema operativo Asterisk Now, como central telefónica, softphones y un teléfono IP, para establecer llamadas en la LAN y sobre el túnel.

En el Capítulo 4 se realizar pruebas para verificar el establecimiento del túnel en un escenario de acceso remoto sobre una nube WAN y sobre Internet. Además se comprueba el establecimiento de llamadas telefónicas a través del túnel y la comprobación de la calidad de las llamadas sobre Internet. Se comprueba además la encripción de los paquetes que atraviesan el túnel.

En el Capítulo 5 se realiza el estudio de costos de todos los equipos, software, servicio de Internet necesarios para la implementación del presente proyecto.

En el Capítulo 6 se realizan las conclusiones y recomendaciones respectivas de acuerdo al desarrollo del proyecto.

CAPÍTULO 1

1 ESTUDIO DE LAS REDES PRIVADAS VIRTUALES Y EL SERVICO DE VOZ SOBRE IP

Actualmente, la mayoría de empresas utilizan Redes de Telefonía Conmutada para llevar a cabo comunicaciones telefónicas entre sus sucursales y oficinas principales, al mismo tiempo mantienen una conexión con un Proveedor de Servicio de Internet (ISP). Frente a este escenario, se plantea una alternativa para poder llevar a cabo llamadas telefónicas dentro de la misma empresa, pero esta vez utilizando únicamente la conexión existente con el ISP.

La propuesta está encaminada a brindar comunicación entre sucursales y departamentos de una empresa, independientemente de la distancia. De esta manera se facilita el acceso telefónico y se reducen costos en las llamadas de larga distancia.

Para llevar a cabo una comunicación interna, del tipo telefónico, se utilizará telefonía IP con la correspondiente administración que conlleva manejar una cantidad determinada de terminales y extensiones.

El tráfico se transmitirá a través de una red pública, Internet como punto de partida, por lo tanto, se prevé el uso de Redes Privadas Virtuales (VPN de sus siglas en ingles Virtual Private Network).

El uso de redes VPN permiten garantizar una conexión segura de inicio a fin, manteniendo al margen cualquier tipo de escucha o intromisión sobre el canal.

El objetivo del Capitulo 1 es proporcionar un conocimiento claro de las funciones y características de los tecnologías; a saber, redes VPN y servicio VoIP, que

intervienen en el desarrollo del presente proyecto, además de brindar una visión teórica que abarca este trabajo.

El presente capitulo empieza con una descripción de las redes VPN, los requerimientos que satisface y consideraciones de seguridad en los segmentos de red definidos al cruzar trafico sobre Internet. Además se exponen algunas de las herramientas que utilizan, como criptografía, autenticación, y se menciona las consideraciones de seguridad a la par con el enfoque que ofrece el protocolo Internet Protocol Security, IPsec. Se orienta el estudio de las VPN como una base sobre la que se mantendrá una comunicación telefónica IP.

Posteriormente se detallan algunas de las características y ventajas del servicio voz sobre IP, tomando en cuenta parámetros de calidad y estudiando el trato de las llamadas sobre Internet, además se estudia el término Telefonía IP y sus diferencias con respecto al servicio VoIP.

1.1 REDES PRIVADAS VIRTUALES (VPN)

1.1.1 DEFINICIÓN [1] [2]

Inicialmente el término VPN apareció entre las sociedades telefónicas que en un principio pretendían una comunicación segura para empresas que ocupaban redes públicas, a carencia de las suyas propias, con el propósito de emular una PBX[1] local. Actualmente una Red Privada Virtual no difiere en mucho de su origen, la tendencia es la misma, utilizar una red publica con el propósito de mantener una comunicación extremo a extremo pero con la garantía de la integridad y confiabilidad de sus datos.

El RFC[2] 2764 define el término VPN de la siguiente manera:

[1] PBX, Private Branch Exchange
[2] RFC, Request For Coments

“VPN es un termino genérico que abarca el uso de redes publicas o privadas para crear grupos de usuarios que estén separados de otros usuarios de la red y que puedan comunicarse entre ellos como si estuviesen en una red privada”.

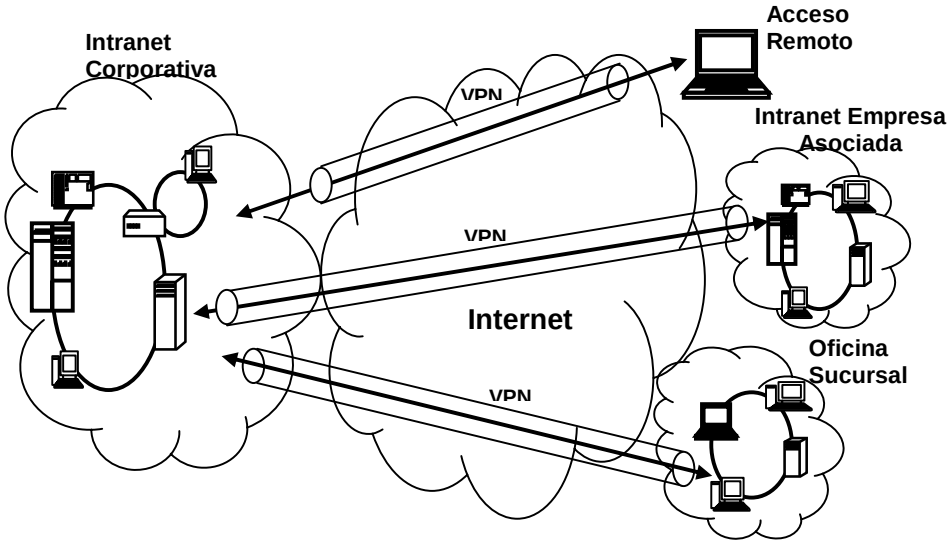


Figura 1-1 Red Privada Virtual

Se entiende entonces que, una VPN es una red que emula las propiedades de una red privada común, como una red LAN[3] o intranet, usando infraestructura de una red pública o privada, con la garantía de integridad y seguridad sobre los datos durante el recorrido de los mismos. Como se ve en la Figura 1-1, una VPN articula un túnel “virtual”, cuyo propósito es comunicar redes afines, simulando una conexión directa entre dichas redes, es decir que ambas redes pertenecerán entonces a un solo dominio.

1.1.2 PROPIEDADES DE UNA VPN [2] [3]

Los paquetes que cruzan una red pública están propensos a cualquier tipo de escucha o interferencia, es por esto que en principio una red VPN se diseña con el propósito de salvaguardar la información a diversos ataques, sean pasivos o activos. Entiéndase por pasivos, aquellos que se limitan a escuchar y/o divulgar la

[3] LAN, Local Area Network.

información, y activos, a aquellas intromisiones más profundas, como la suplantación de entes autorizados, o la modificación de la información, que tiene que ver con la creación o destrucción no autorizada de datos o recursos, y la interrupción, que supone impedir a entes autorizados el acceso a recursos o información a los que tiene derecho.

Dentro de este marco, las redes VPN se caracterizan por cumplir con ciertos procedimientos, que a la larga garantizan un nivel de seguridad, de acuerdo, con la rigidez y eficiencia prescrita sobre los siguientes aspectos:

1.1.2.1 Confidencialidad

Implica que la información que atraviesa por una red pública está dispuesta a cualquier tipo de merodeador. Una VPN protege la información de estas entidades, encriptando los paquetes antes de entrar a la red pública, de esta forma solo el receptor será capaz de desencriptar la información y convertirla en texto claro para sus propósitos.

1.1.2.2 Integridad

Se refiere a la forma en que un paquete llega a su destino; es decir, si dicho paquete, mientras atravesó la red, no sufrió ninguna alteración. En el caso de que se detectara cualquier tipo de alteración sobre el paquete este sería inmediatamente descartado.

1.1.2.3 No Rechazo

Se refiere a que una conexión no sea denegada por ninguna de las partes durante el transcurso de la comunicación. Previo a iniciar una conexión se realiza un proceso de autenticación entre las partes, mediante identificaciones de usuario, esto con el fin de que la comunicación sea conocida únicamente por los previamente identificados participantes.

Para garantizar que no exista repudio en una comunicación, se usa entre otras, una técnica conocida como firma digital, este proceso garantizada que cada participante en una comunicación es quien dice ser y que esta autorizado a establecer y mantener dicha conexión.

1.1.2.4 Anti-Replay

Ayuda a detectar un paquete inválido y desecharlo. Este paquete inválido en particular ha sido enviado por un agente externo a la red, que es una copia de un paquete original y es retransmitido varias veces hacia el destino. Este proceso no se detecta mediante autenticación ni encripción, debido a que el paquete copiado no es alterado, simplemente es retransmitido varias veces. Para prevenir estos problemas se utiliza una secuencia numérica con la que se chequean paquetes repetidos, comparándolos con los ya recibidos, de esta forma se desechan los paquetes repetidos.

1.1.3 DESCRIPCIÓN DE UN CAMINO DE DATOS [2]

El propósito de describir un camino de datos es identificar las zonas y puntos vulnerables por los que puede atravesar el tráfico en lo que tiene que ver con sitios fuera del alcance y/o monitoreo de los propietarios o emisores. La Figura 1-2 muestra tres segmentos de red, los mismos que se describen a continuación de forma general, enfatizando en los puntos frágiles del trayecto.

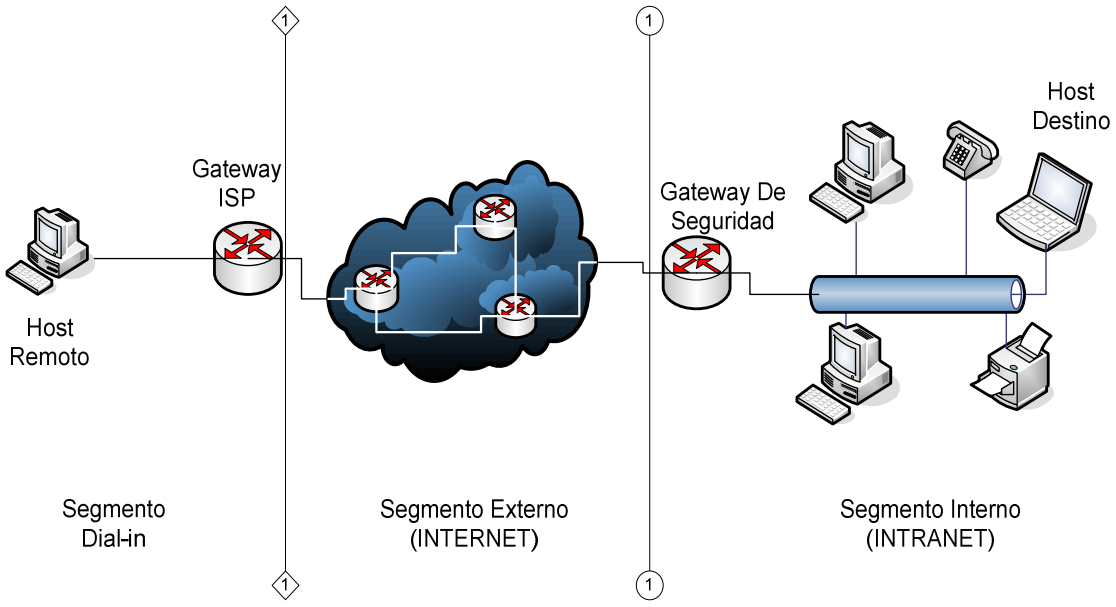


Figura 1-2 Segmentos en un camino típico, sobre Internet, de Inicio a Fin.

1.1.3.1 Segmento Dial-in

Es denominado también tramo de usuario y se caracteriza por permitir el acceso a Internet a través de un ISP. Un segmento Dial-in esta limitado al gateway asignado por el ISP contratado. Este punto puede convertirse en un punto de escucha en que el tráfico, de estar en texto claro, es de fácil acceso para quien administra el ISP. Por lo tanto, si la información que se transmite es de alto nivel de reserva, no se puede permitir ninguna posibilidad de escucha.

En este caso lo más recomendable es implementar encripción y autenticación de las partes que intervienen en el proceso de conexión de inicio a fin. Es decir, desde el host hasta la red corporativa.

1.1.3.2 Segmento Externo (Internet)

Este segmento conocido como Internet, es una gran nube de nodos, que por su magnitud y complejidad se vuelve impredecible. Internet por su naturaleza pública,

permite el acceso a millones de usuarios alrededor de todo el mundo, esto hace que se vuelva una gran nube vulnerable a la disposición de intrusos, ahora comúnmente conocidos como *hackers*.

Durante el trayecto los paquetes tendrán que pasar por algunos nodos empezando por el gateway del ISP, hasta el gateway final de la intranet, lo que significa que un paquete, mientras esta en transito por este segmento externo, esta permanentemente en riesgo y vulnerable a cualquier tipo de ataque.

Para utilizar una red pública como el Internet se plantea la creación de un “túnel”, que de alguna manera simula una conexión directa, y comunica únicamente los extremos participantes en la conexión, aislando de esta manera el tráfico interesante del entorno de Internet. De esta manera se comunica un segmento de la red privada con un usuario remoto, que también puede ser un segmento de otra intranet afín.

1.1.3.3 Segmento Interno (Intranet)

Es el segmento en el que se filtra el tráfico propio de la empresa mediante firewalls aplicados sobre el Gateway de Frontera (denominado así al router que divide la Intranet de la red pública) restringiendo el tráfico entrante.

El buen funcionamiento de la red, en cuanto a su seguridad y a su agilidad al momento de filtrar los paquetes entrantes y salientes, dependerá en mucho de las consideraciones que se hayan previsto. Por ejemplo, autenticación sin criptografía (contraseñas, filtros, cambio de direcciones de red) de paquetes entrantes como salientes brinda protección frente a tráfico no deseado en la red, sin embargo esto facilitaría ataques comunes como address spoofing, ataques que tienen como fin hacerse de direcciones locales.

Las medidas de seguridad que a lo largo de este proyecto están encaminadas a cubrir vulnerabilidades sobre la red, como las ya mencionadas, además de sostener una red privada en un entorno público.

1.1.4 CRIPTOGRAFÍA [2][4][5]

Criptografía es un procedimiento antiguo, utilizado para comunicar información privilegiada con el propósito de mantener la información legible únicamente para quien o quienes esta dirigida; es decir, que nadie durante el trayecto pueda entenderla.

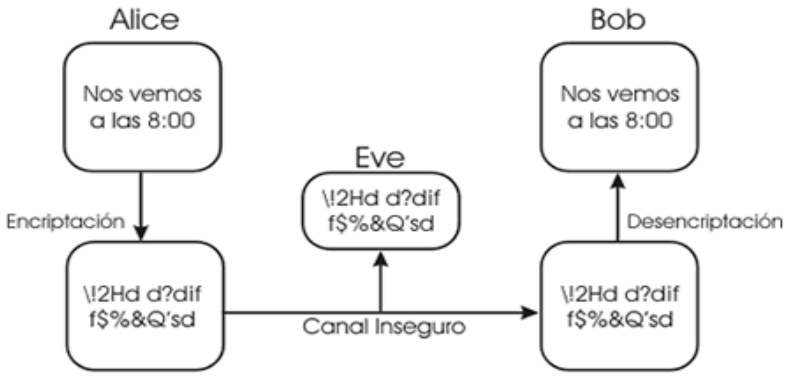


Figura 1-3 Criptografía

La criptografía presenta varios métodos para evitar que si una comunicación es escuchada por terceras personas, éstas puedan descubrir su contenido, como se puede observar en la Figura 1-3. La criptografía involucra un proceso antes de la transmisión y otro en el momento de la recepción.

1.1.4.1 Encriptación y Desencriptación

Encriptar significa transformar un texto claro o texto original en un texto ilegible o texto cifrado, de tal manera que solo será capaz de entenderlo el destinatario de dicho texto. En algunos casos el texto cifrado no podrá ser traducido ni siquiera por el emisario, que es quien lo cifró originalmente. La decripción, por lo tanto, es

el proceso inverso. El proceso de descifrar es volver un texto ilegible en un texto claro.

Para realizar un proceso de encripción y decripción se utilizan funciones matemáticas conocidas como algoritmos criptográficos. Se han desarrollado algunos algoritmos criptográficos, algunos de ellos obsoletos por el avance tecnológico, pero en general se clasifican en algoritmos criptográficos simétricos y asimétricos.

1.1.4.2 Criptografía Simétrica Y Asimétrica

Se distingue un proceso simétrico de un proceso asimétrico por la cantidad de llaves que intervienen previo el intercambio de información. Cuando se intercambia únicamente llaves privadas, es decir, cuando se utiliza una única llave durante el proceso de encripción/decripción, como se observa en la Figura 1-4, a este proceso se conoce como *criptografía simétrica*. Un ejemplo de esto es DES, Data Encryption Standard, que se encuentra detallado más adelante.

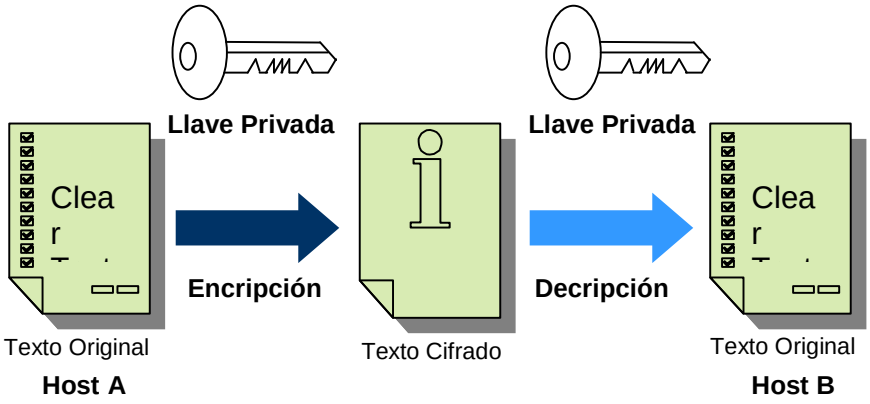


Figura 1-4 Esquema criptográfico simétrico

Un algoritmo criptográfico asimétrico usa 2 llaves diferentes, como se muestra en la Figura 1-5, una llave pública para cifrar la información y otra privada para descifrar. Una de las ventajas, y la más importante, es que el uso de la llave

pública no interviene en el descifrado del mensaje, entonces el riesgo de que se pueda develar el contenido de un mensaje se reduce en el momento en que interviene una segunda llave.

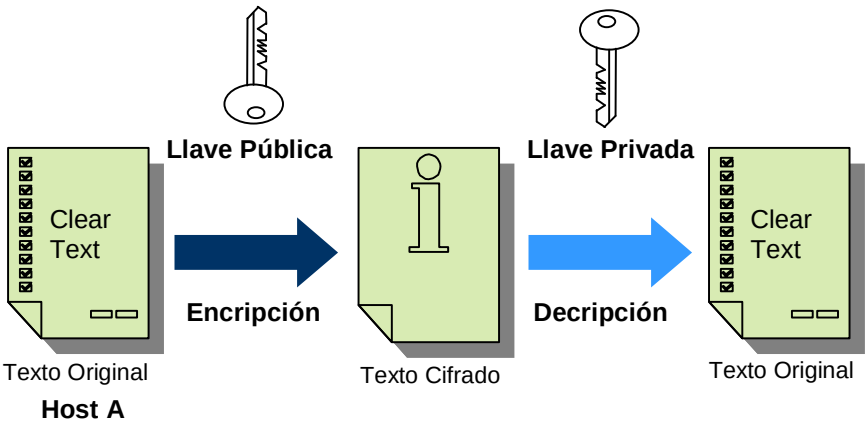


Figura 1-5 Esquema criptográfico asimétrico

Uno de los algoritmos asimétricos más comunes es el RSA (nombrado así por sus inventores, Ron Rivest, Adi Shamir y Leonard Adleman) Esté algoritmo usa una lógica de números primos que para cifrar un texto utiliza una llave *pública,* que es el resultado de una operación matemática, que a su vez es función de dichos números primos, mientras que del otro lado se descifra con otra llave *privada* obtenida de manera similar a la pública, pero que no guardan relación directa entre ellas. Al final de la obtención de las respectivas llaves los números utilizados para esta tarea son desechados.

Los algoritmos criptográficos, independientemente si son simétricos o asimétricos, serán más robustos mientras más complejo sea la función matemática que utilicen, además de cuán grande sea la longitud de la llave generada.

1.1.4.3 Data Encryption Standard (DES) [2][6]

Data Encryption Standard (DES) es un ejemplo de un sistema de cifrado simétrico que utiliza una llave privada. Fue uno de los primeros algoritmos criptográficos que se adopto como estándar, además, es uno de los pilares criptográficos que a dado

paso a nuevos algoritmos. DES apareció con el fin de brindar seguridad sobre redes públicas, siendo su principal fortaleza, en aquel entonces, la longitud de la llave utilizada durante el proceso de encripción.

Se trata de un sistema de cifrado por bloques de 64 bits, de los que 8 bits se utilizan como control de paridad (para la verificación de la integridad de la clave). Cada uno de los bits de la clave de paridad se utiliza para controlar uno de los bytes de la clave por paridad impar; es decir, que cada uno de los bits de paridad se ajusta para que tenga un número impar de "1s" dentro del byte al que pertenece. Por lo tanto, la clave tiene una longitud "útil" de 56 bits, lo que significa que solamente se utilizan 56 bits en el algoritmo, lo que a su vez limita el número de posibilidades a 2^{56} claves diferentes.

El algoritmo se encarga de realizar combinaciones, sustituciones y permutaciones entre el texto a cifrar y la clave, asegurándose al mismo tiempo de que las operaciones puedan realizarse en ambas direcciones (para el descifrado). La combinación entre sustituciones y permutaciones se llama **cifrado del producto**.

La clave es codificada en 64 bits y se compone de 16 bloques de 4 bits generalmente anotadas de k_1 a k_{16}.

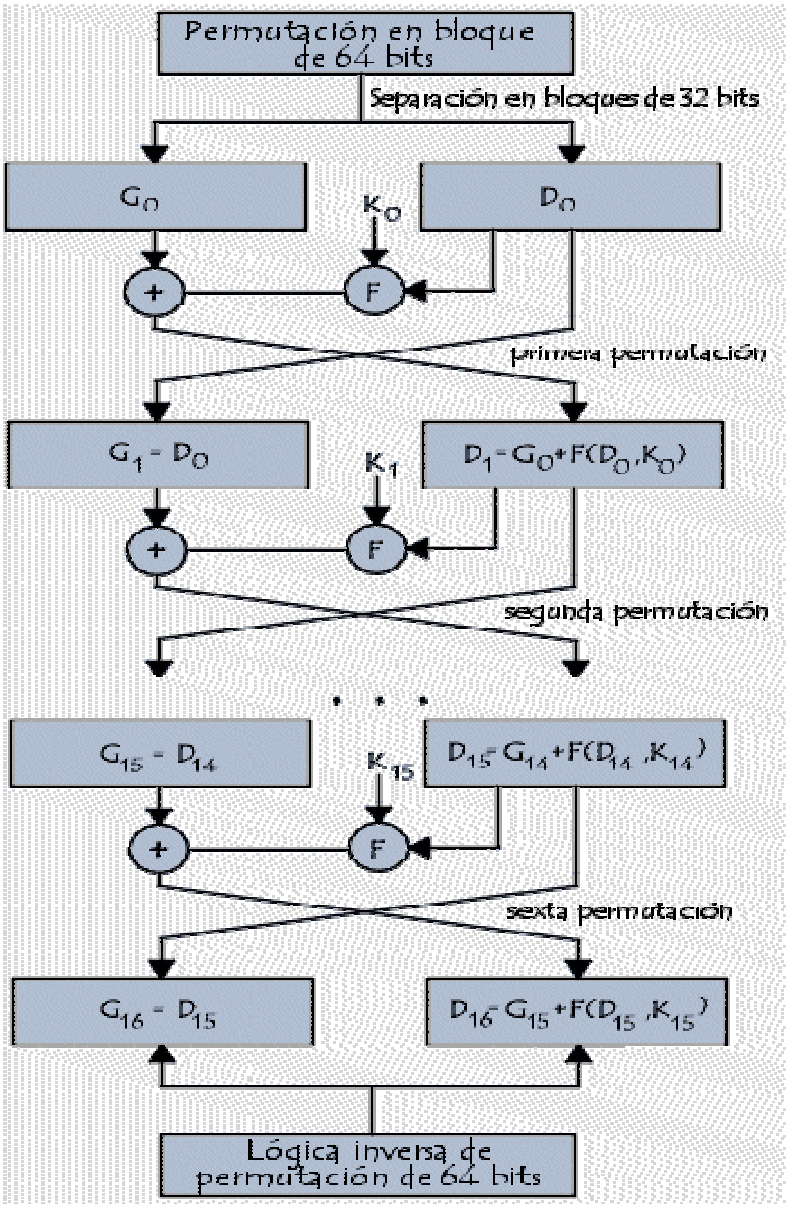


Figura 1-6 Algoritmo DES

Los procesos más importantes del algoritmo de la Figura 1-6, son los siguientes:

a) Fraccionamiento del texto en bloques de 64 bits (8 bytes),
b) Permutación inicial de los bloques, que se entiende como el reordenamiento u ordenamiento aleatorio de los 64 bits entrantes que puede ser como se muestra en la Figura 1-7.

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Posible Resultado Permutación Inicial **PI**

57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

División en 32 Bits, Bits Impares **Lo**

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8

División en 32 Bits, Bits Pares **Ro**

Figura 1-7 Tablas de Permutación

c) Partición de los bloques en dos partes: izquierda y derecha, denominadas *L* y *R* respectivamente, como se muestra en la Figura 1-7.

d) Fases de permutación y de sustitución repetidas 16 veces (denominadas **rondas**). En este punto se cumplen cuatro tareas:

- *Expansión* — la mitad del bloque de 32 bits se expande a 48 bits, mediante la *permutación de expansión*, duplicando algunos de los bits.
- *Mezcla* — el resultado se combina con una *subclave* utilizando una operación XOR. Dieciséis subclaves, una para cada ronda, se derivan de la clave inicial mediante generación de claves.
- *Sustitución* — tras mezclarlo con la subclave, el bloque es dividido en ocho trozos de 6 bits antes de ser procesados por las S-cajas, que se muestran en la Figura 1-8, o *cajas de sustitución*. Cada una de las ocho S-cajas reemplaza sus seis bits de entrada con cuatro bits de salida, de acuerdo con una trasformación no lineal. Las S-cajas constituyen el

núcleo de la seguridad de DES, sin ellas el cifrado sería lineal, y fácil de romper.

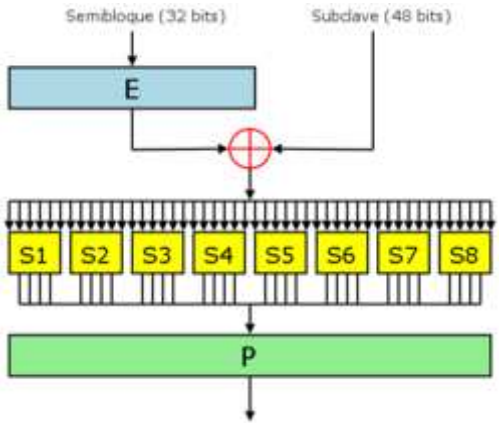


Figura 1-8 Cajas de Sustitución

- *Permutación* — finalmente, las 32 salidas de las S-cajas se reordenan de acuerdo a una permutación fija; la *P-caja*

e) Reconexión de las partes izquierda y derecha, seguida de la permutación inicial inversa.

Actualmente DES no es tan confiable como en sus inicios, debido a que gran parte de los procesos que antes se llevaban a cabo con la ayuda de varios procesadores ahora se pueden realizar con un solo súper procesador. Este hecho se demostró en 1998, cuando en un procedimiento de fuerza bruta se violó la seguridad de DES.

Posteriormente, se planteo Triple DES (3DES) que, en su forma básica, sigue siendo DES, con la diferencia que el proceso se repite 3 veces, pero ahora con 2 diferentes claves o llaves. Reconocido como una solución a corto plazo por que involucra una gran cantidad de recursos, además del hecho de que los procesadores evolucionan a gran velocidad y la posibilidad latente a un nuevo ataque de fuerza bruta.

1.1.4.4 Advanced Encryption Standard [4] [7][8]

Es un algoritmo de encripción diseñado por Joan Daemen y Vincent Rijmen, denominado Rijdael. Rijdael compitió con otros 15 algoritmos criptográficos en una convocatoria realizada por el NIST[4] y luego de un periodo de 3 años de pruebas y discusiones fue anunciado como AES.

Las principales características del algoritmo Rijdael son:

- ✓ Fácil diseño.
- ✓ Fácil de ser implementado en diferentes escenarios.
- ✓ Inmunidad a los ataques conocidos hasta la fecha.
- ✓ Soportar bloques de datos de 128 bits y claves de 128, 192, y 256 bits.

[4] *National Institute of Standars and Technology*

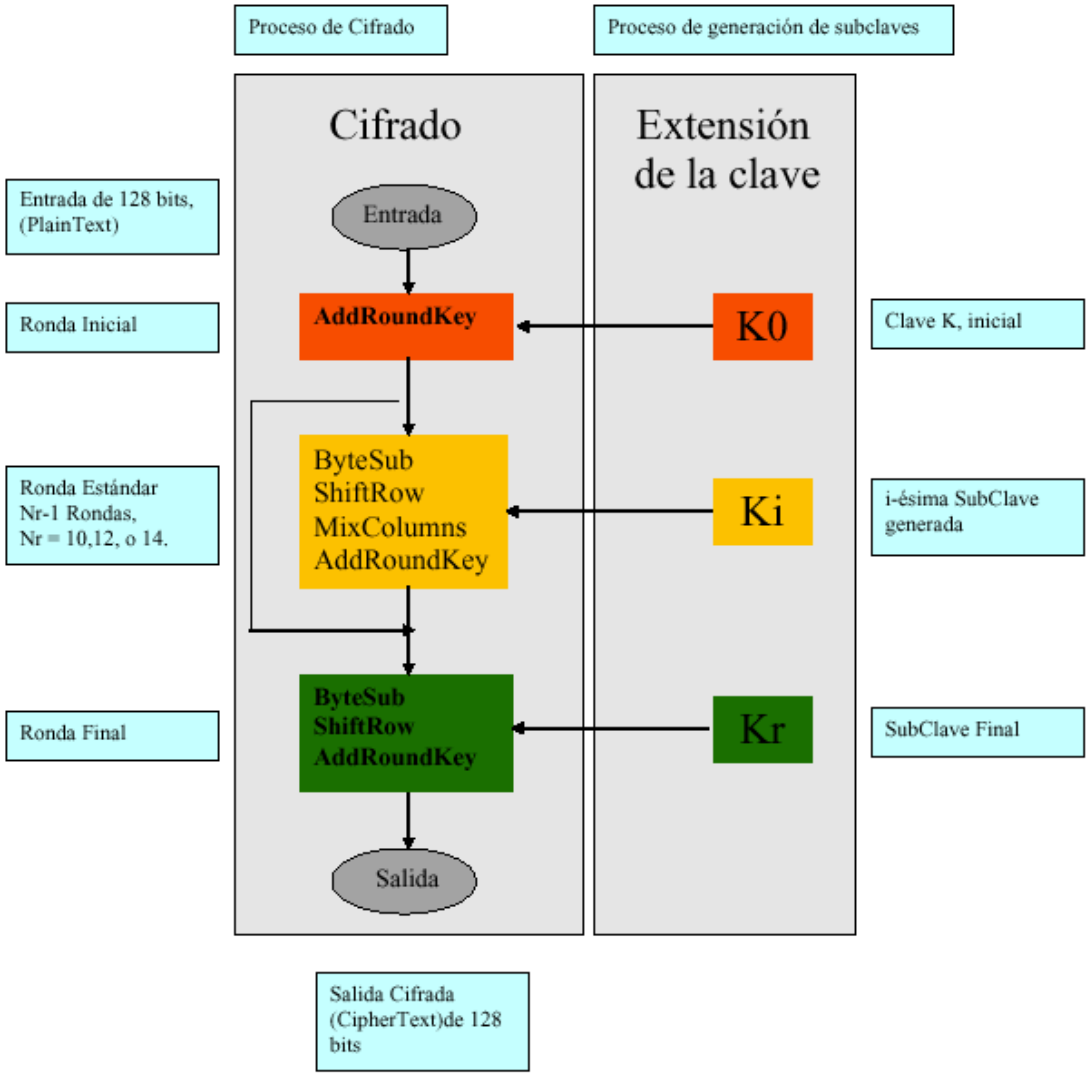


Figura 1-9 Algoritmo AES

Básicamente el proceso AES se explica en dos partes, el proceso de Cifrado y el proceso de Generación de subclaves como se observa en la Figura 1-9. La entrada, de texto plano, es de 128 bits, mientras que la longitud de la clave K puede variar entre 128, 192 y 256 bits, y para cada caso AES admite 10, 12 y 14 vueltas respectivamente. Cada vuelta de AES consiste en la aplicación de una ronda estándar, que consiste de 4 transformaciones básicas:

- ✓ AddRoundKey,
- ✓ SubByte,
- ✓ ShiftRows,

- ✓ MixColumns.

La última ronda es especial, y reemplaza la fase MixColumns por otra instancia de AddRoundKey. AES interpreta al bloque de entrada de 128 bits, como una matriz de 4x4 de entradas de bytes, si el bloque es de 192 bits se agregan 2 columnas más, si lo es de 256 se agregan 4 columnas más.

$$\begin{matrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{matrix}$$

$$a_{ij}$$

Tomando los primeros 4 bytes se forma la primera columna, los segundos 4 bytes son la segunda columna, y así susecivamente.

$a_{00}\ a_{10}\ a_{20}\ a_{30}\ a_{01}\ a_{11}\ a_{21}\ a_{31}\ a_{02}\ a_{12}\ a_{22}\ a_{32}\ a_{03}\ a_{13}\ a_{23}\ a_{33}$

La regla se aplica a los bloques de 192 bits y 256 bits, obteniendo matrices de 6, y 8 columnas respectivamente. La Matriz 1-1 es la entrada del algoritmo AES, y va cambiando en cada una de las rondas, se denota como $[a_{ij}]$ y se conoce como matriz estado.

Transformación AddRoundKey.- La matriz de claves, que se denota $[K_{ij}]$, se genera de forma tal que sea compatible con las dimensiones establecidas; es decir, para 128, 192 y 256 bits. Una vez generada la matriz $[K_{ij}]$, se realiza la operación XOR como se muestra en la Figura 1-10, entre los elementos $[a_{ij}]$ y $[K_{ij}]$.

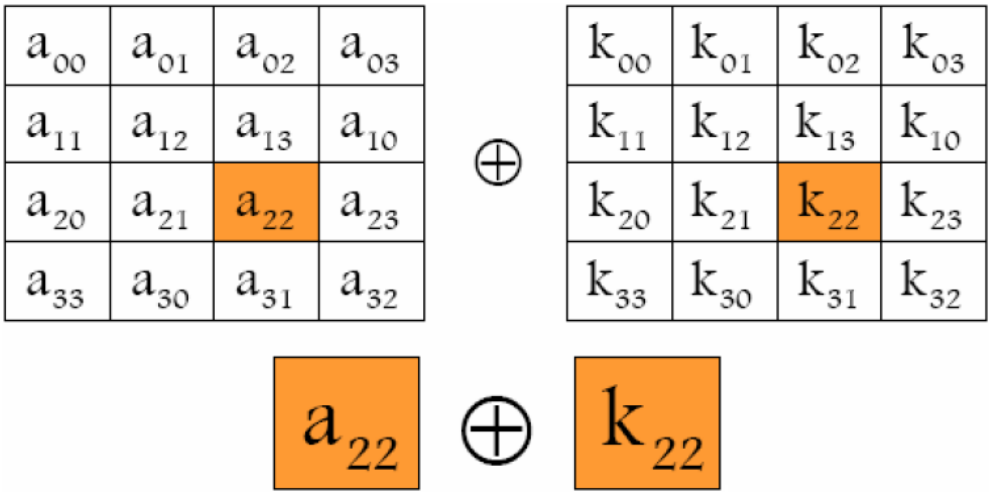


Figura 1-10 Transformación AddRoundKey

Transformación SubByte.- Durante este proceso la matriz $[a_{ij}]$ es sustituida por la matriz $[S_{ij}]$, como se indica en la Figura 1-11, donde S_{ij} es el resultado de aplicar 2 funciones a la matriz a_{ij}. En primera instancia se calcula el inverso multiplicativo a cada a_{ij}, y luego se procede a una transformación lineal.

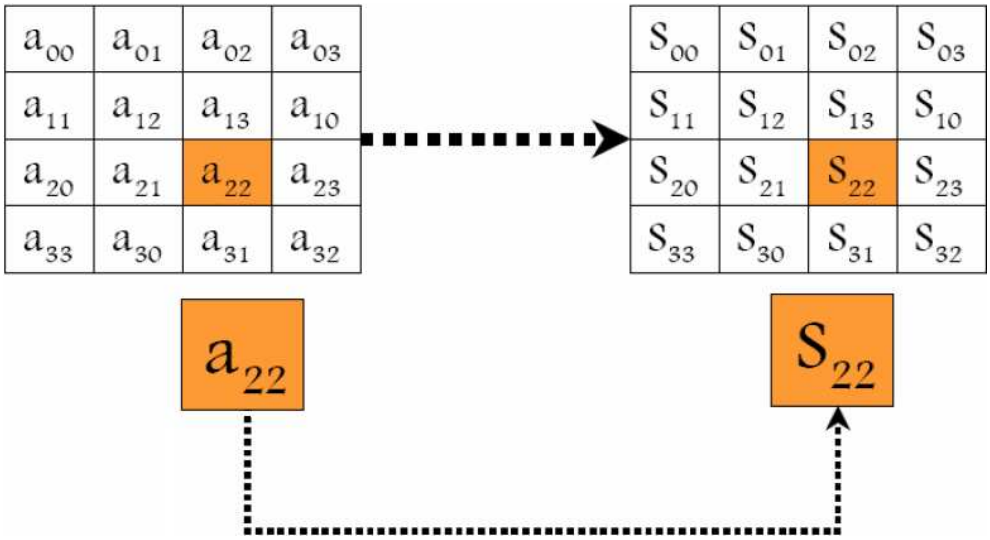


Figura 1-11 Proceso SubByte

Todo byte (8 bits) puede verse como un elemento del campo finito[5] GF(2^8), y todo elemento dentro de este campo tiene un inverso multiplicativo, entonces la primera función de SubByte consiste en asociar el inverso multiplicativo en GF(2^8), es decir, $a_{ij} \rightarrow a_{ij}^{-1} \in GF(2^8)$. En la Tabla 1-1 se muestran los inversos multiplicativos en representación hexadecimal, el cero es el único valor que permanece constante; por ejemplo, el inverso de 7c es a1.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	00	01	8d	f6	cb	52	7b	d1	e8	4f	29	c0	b0	e1	e5	c7
1	74	b4	aa	4b	99	2b	60	5f	58	3f	fd	cc	ff	40	ee	b2
2	3a	6e	5a	f1	55	4d	a8	c9	c1	0a	98	15	30	44	a2	c2
3	2c	45	92	6c	f3	39	66	42	f2	35	20	6f	77	bb	59	19
4	1d	fe	37	67	2d	31	f5	69	a7	64	ab	13	54	25	e9	09
5	ed	5c	05	ca	4c	24	87	bf	18	3e	22	f0	51	ec	61	17
6	16	5e	af	d3	49	a6	36	43	f4	47	91	df	33	93	21	3b
7	79	b7	97	85	10	b5	ba	3c	b6	70	d0	06	a1	fa	81	82
8	83	7e	7f	80	96	73	be	56	9b	9e	95	d9	f7	02	b9	a4
9	de	6a	32	6d	d8	8a	84	72	2a	14	9f	88	f9	dc	89	9a
a	fb	7c	2e	c3	8f	b8	65	48	26	c8	12	4a	ce	e7	d2	62
b	0c	e0	1f	ef	11	75	78	71	a5	8e	76	3d	bd	bc	86	57
c	0b	28	2f	a3	da	d4	e4	0f	a9	27	53	04	1b	fc	ac	e6
d	7a	07	ae	63	c5	db	e2	ea	94	8b	c4	d5	9d	f8	90	6b
e	b1	0d	d6	eb	c6	0e	cf	ad	08	4e	d7	e3	5d	50	1e	b3
f	5b	23	38	34	68	46	03	8c	dd	9c	7d	a0	cd	1a	41	1c

Tabla 1-1 Inversos Hexadecimales

[5] Un campo finito es un sistema algebraico que consiste de un conjunto finito F junto con 2 operaciones binarias, + y *

Una vez identificado el inverso multiplicativo para cada elemento de a_{ij} se aplica la transformación lineal bit a bit de acuerdo a la siguiente regla:

$$b_i' = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i$$

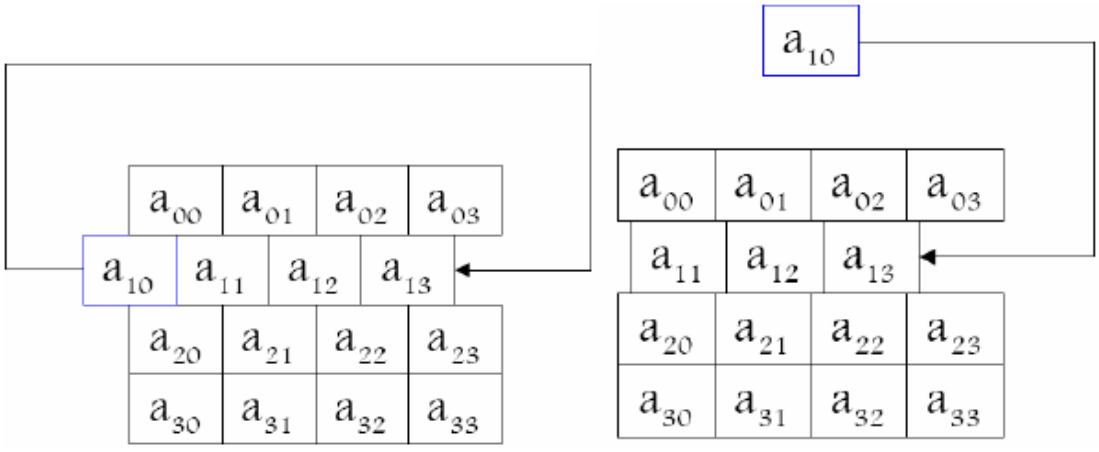
$$0 \le i \le 8$$

La representación matricial a la regla anterior es la que se muestra en la Figura 1-12, se aclara que la el vector *b* es el inverso multiplicativo obtenido en el proceso anterior, y el vector *c* corresponde a un vector aleatorio.

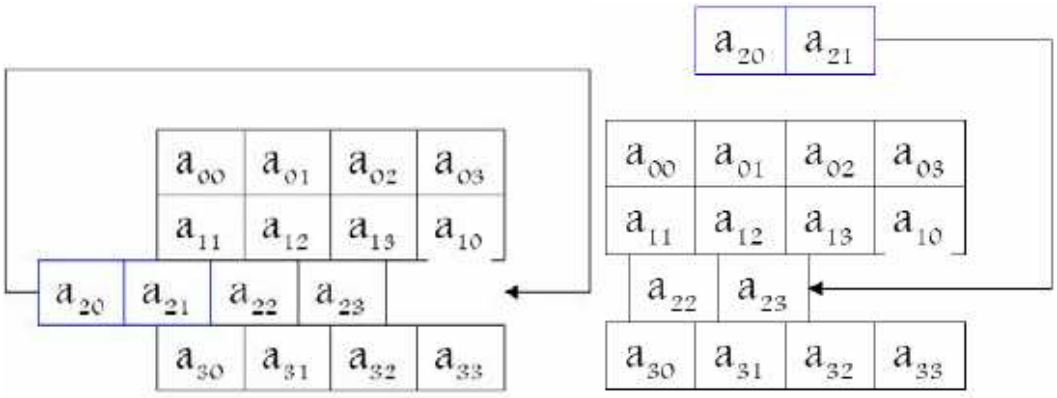
$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix}$$

Figura 1-12 Transformación lineal

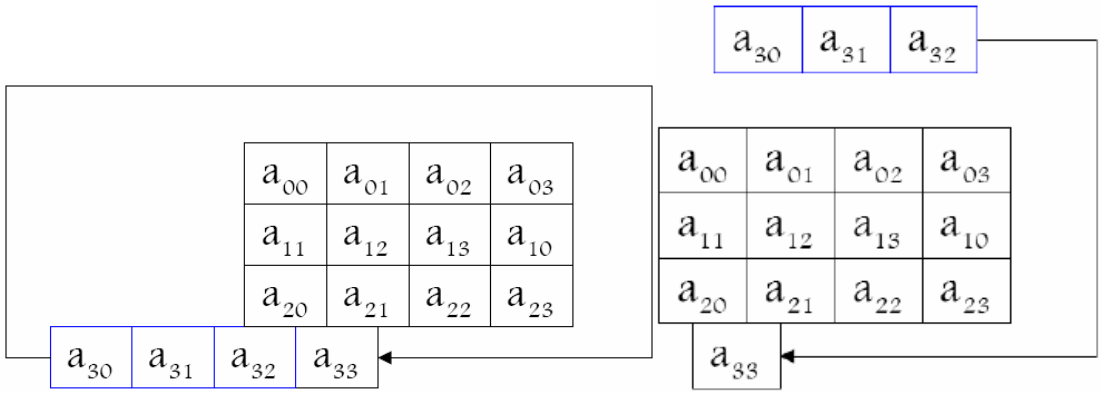
Transformación ShiftRow.- Este paso se realiza sobre la matriz estado aplicando un proceso de corrimiento circular de celdas. Se realiza corrimientos izquierdos circulares de bytes a las renglones de la siguiente manera: se recorre 0 bytes al primer renglón, 1 byte al segundo renglón, 2 bytes al tercer renglón, y 3 bytes recorridos al cuarto renglón, de forma similar a la Figura 1-13. Se puede realizar variaciones sobre los espacios recorridos, pero generalmente se mantiene al primer renglón sin variación.



PRIMERA FILA



SEGUNDA FILA



TERCERA FILA

Figura 1-13 ShiftRow

Transformación MixedColumns.- Se toma cada columna Aj de la matriz de la matriz a_{ij} y se envía a otra columna A'_j, como se aprecia en la Figura 1-14. Cada

colima A'$_j$ se obtiene al multiplicar Aj por un polinomio constante $c(x) \in GF(2^8)[x]/(x^4+1),\ c(x) = 03x^3 + 01x^2 + 01x + 02$, entonces A' = A . c(*x*).

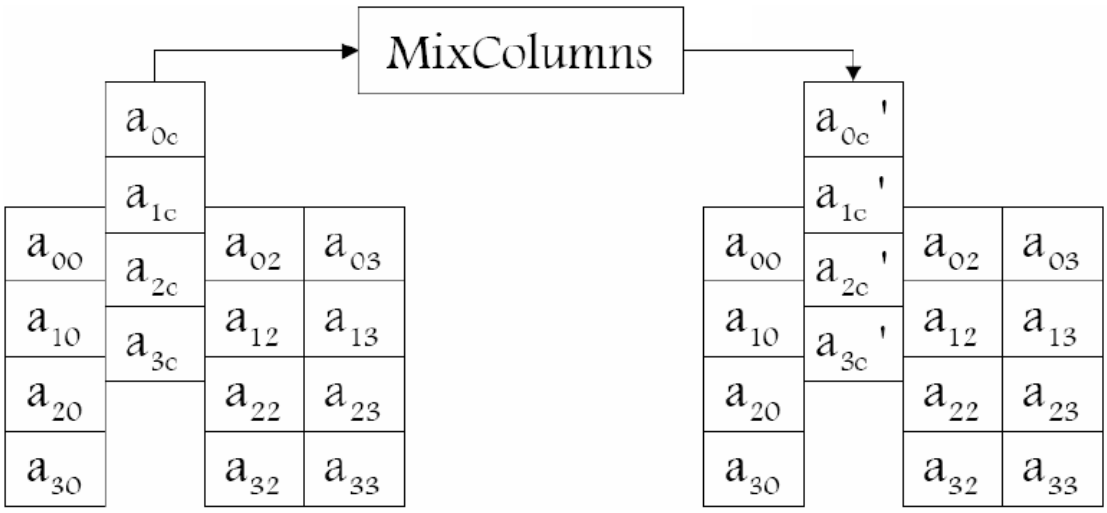


Figura 1-14 MixedColumns

1.1.5 FUNCIÓN HASH

Es una función que hace posible obtener un *resumen de un conjunto de información*, es decir, obtener un número de caracteres finito que representan el texto al cual se le aplica esta función hash. La función hash debe ser tal que asocie únicamente un hash con un texto plano; esto significa que la mínima modificación del documento causará una modificación en el hash. Además, debe ser una función unidireccional para que el mensaje original no pueda ser recuperado a partir del hash.

Como tal, puede decirse que la función hash representa la *huella digital* de un documento, en este sentido se asocia el resultado de la función hash al documento o información recibida, luego de haber sido calculado localmente, de esta manera se comprueba la integridad del documento. 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.

Una función *hash* está definida por su dominio (cadenas de bytes de longitud variable), su imagen (secuencias de bytes de longitud fija) y por la función que relaciona dichos conjuntos (llamada *función H*). Las funciones hash deben caracterizarse básicamente por:

- ✓ Entrada que puede ser de cualquier tamaño.
- ✓ El valor hash (salida) tiene un tamaño fijo.
- ✓ Estar libre de colisiones. Dadas dos cadenas como entrada ``x'' y ``y'', no se obtenga un mismo valor hash tal que H(x)=H(y).
- ✓ Irreversible; es decir, dado un valor hash ``h'', no sea posible encontrar una entrada ``x''
- ✓ Rapidez y facilidad de obtener el resultado.

A continuación se describen 2 de los algoritmos hash mas usados.

1.1.5.1 MD5, Message Digest

El algoritmo de hash más utilizado en estos momentos es el MD5. Este algoritmo fue desarrollado por Ronald Rivest en 1995 y está basado en dos algoritmos anteriores MD2 y MD4. Todos estos protocolos producen un número de 128 bits a partir de un texto de cualquier longitud.

MD4 fue desarrollado para mejorar el rendimiento de MD2, sin embargo, varios problemas fueron detectados y en 1996 fueron publicados elementos que hacen hoy en día inservible el algoritmo. MD5 sustituyó a MD4 y aunque no tiene el rendimiento de su antecesor, hasta el momento no han sido publicados elementos que comprometan su integridad y funcionamiento.

El proceso MD5 comienza rellenando el mensaje a una longitud congruente en módulo, como por ejemplo 448 mod 512 que se puede apreciar en la Figura 1-15; es decir, la longitud del mensaje es 64 bits menos que un entero múltiplo de 512.

El relleno consiste en un bit en 1, seguido por cuantos bits en 0 sean necesarios. La longitud original del mensaje es almacenada en los últimos 64 bits del relleno.

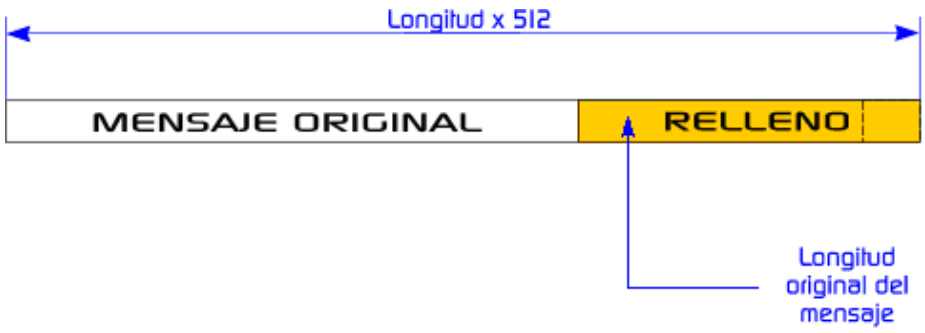


Figura 1-15 Relleno MD5

En un siguiente proceso se inicializa, con un valor fijo, un buffer de 128 bits. Este buffer puede verse como 4 registros de 32 bits (A,B,C,D) y son inicializados con los siguientes valores hexadecimales:

A=67452301; B=EFCDAB89; C=98BADCFE; D=10325476

Luego de varias rondas de procesamiento MD5 toma bloques de 512 bits de la entrada y los mezcla con los 128 bits del buffer. Este proceso es repetido hasta que todos los bloques de entrada han sido consumidos. El valor resultante en el buffer es el hash del mensaje.

1.1.5.2 SHA, Security Hash Association

Es un sistema de funciones *hash* criptográficas relacionadas con la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por NIST. La primera versión de SHA apareció en 1993. Dos años más tarde el primer sucesor de SHA fue publicado con el nombre de SHA-1. Existen cuatro variantes más que se han publicado desde entonces cuyas diferencias se basan en un diseño algo modificado y rangos de salida incrementados: SHA-224, SHA-256, SHA-384, y SHA-512 (llamándose SHA-2 a todos ellos).

SHA produce una huella digital de 160 bits a partir de un mensaje que tiene una longitud máxima de 2^{64} bits y los procesa en bloques de 512 bits y se basa en principios similares a los usados por el profesor Ronald L. Rivest en el diseño de los algoritmos MD4 y MD5.

1.1.6 INTERNET PROTOCOL SECURITY (IPSEC)[9][10]

IPsec fue creado con el propósito de mantener comunicaciones seguras y brindar protección a paquetes que viajan a través de redes IP, paquetes IP. IPsec es por tanto un protocolo que trabaja a nivel de capa 3 de acuerdo con el modelo de referencia ISO/OSI. Además, IPsec brinda seguridad a otros protocolos que pueden ser transportados por IP, incluyendo al mismo protocolo IP.

IPsec crea una barrera que distingue una zona segura de otra insegura, como puede ser una red pública. En la Figura 1-16, el tráfico cruzado a través de la barrera “IPsec” esta sujeto a mecanismos de control de acceso especificados por el administrador de la red, o en su defecto por el responsable de la configuración de IPsec. A la vez que el tráfico que no requiere mecanismos de seguridad simplemente se cursa a través de un “Bypass”. De esta manera IPsec protege conexiones entre un par de hosts, un par de gateways de seguridad, o entre un gateway de seguridad y un host.

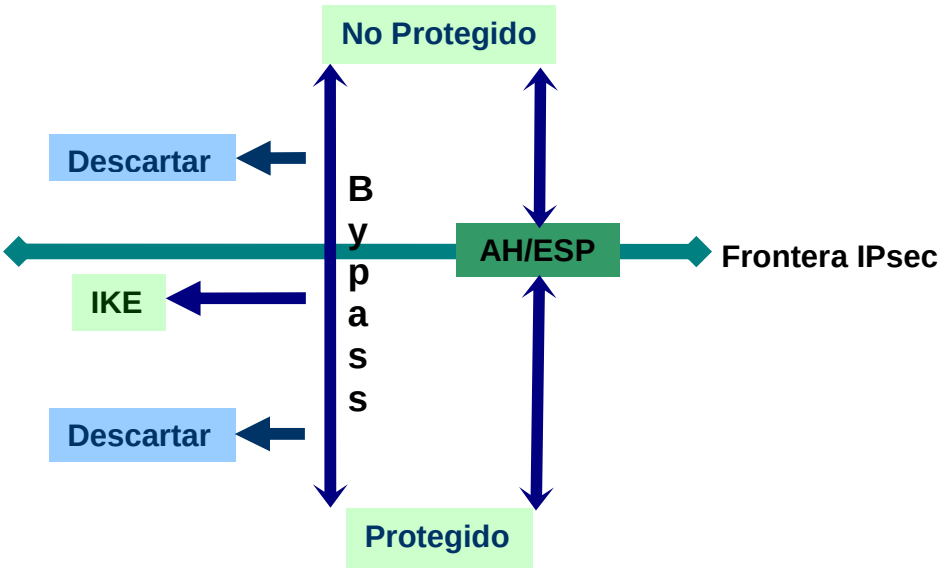


Figura 1-16 Modelo IPsec.

IPsec utiliza una gama de protocolos de seguridad de tráfico, algoritmos criptográficos, llaves criptográficas, para brindar los siguientes servicios:

- Control de acceso.
- Integridad.
- Autenticación sobre el origen del tráfico.
- Detección y rechazo de paquetes repetidos.
- Confidencialidad.
- Control de flujo en el tráfico.

1.1.6.1 Asociaciones de Seguridad [2] [9]

Para brindar los servicios anteriormente mencionados IPsec introduce el concepto de Asociaciones de Seguridad (Security Association, SA) con el propósito de establecer un grupo de parámetros de seguridad asociados a una conexión unidireccional.

Una asociación de seguridad se define como una conexión *simplex* que soporta servicios de seguridad para el tráfico cruzado por ése SA. Estos servicios de seguridad se especifican en el Índice de Parámetros de Seguridad (SPI). Un SA se configura para trabajar con un solo protocolo de seguridad de tráfico, ya sea por el protocolo Auntenthication Header (AH) o por el protocolo Encapsulating Security Payload (ESP) pero no por ambos a la vez. De ser necesario se puede establecer dos SAs coordinados, uno operando con AH y otro con ESP.

Según el tipo de tráfico se establecerán diferentes SAs; por ejemplo, para tráfico multicast se define un grupo de SAs acorde con cada uno de los destinos. De manera similar, para una comunicación bidireccional se establece un par de SAs, uno en cada dirección de la transmisión. Así, para cada tráfico definido en una SA, de acuerdo con las necesidades de seguridad y del tipo de tráfico, se establecen diferentes parámetros prescritos en el SPI. De esta forma se mantiene diferenciado al tráfico saliente en niveles de seguridad o en su defecto en tráfico de texto cifrado o de texto claro.

Una asociación de seguridad esta caracterizada por tres parámetros:

- Índice de Parámetros de Seguridad (SPI), es una lista de características específicas para un SA en especial, con los parámetros de seguridad establecidos en ése SA.
- Dirección IP destino, es la dirección unicast del destinatario final, dirección única de capa 3.
- Identificador del Protocolo de Seguridad, específica el tipo de protocolo utilizado en la SA, que comúnmente puede ser AH o ESP.

1.1.6.2 Modos de Operación de IPsec [9]

Existen dos modos de operación de IPsec, modo transporte y modo túnel. La diferencia fundamental en los modos de operación es que en modo transporte se cifra solamente la carga útil del paquete IP, quedando de esta manera la cabecera y las direcciones de ruteo intactas, mientras que en modo túnel todo el paquete IP es cifrado, para lo cual se genera un nuevo paquete IP con una nueva cabecera que pueda facilitar el enrutamiento.
IPsec brinda gran parte de servicios de seguridad a través de dos protocolos de seguridad de tráfico, ESP y AH. Cada uno de estos protocolos puede trabajar tanto en modo túnel como en modo transporte.

1.1.6.3 Auntenthication Header (AH) [9] [11]

El protocolo Cabecera de Autenticación, AH, es un protocolo utilizado para encapsular paquetes IP, protegiendo de esta manera los campos encapsulados, de acuerdo con el modo utilizado.

AH ofrece integridad sobre comunicaciones no orientadas a conexión y autenticación de origen para datagramas IP, además provee protección frente a paquetes repetidos (anti-replay).

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Next header	Payload length	**RESERVED**	
Security parameters index (SPI)			
Sequence number			
Hash Message Authentication Code (variable)			

Figura 1-17 Cabecera AH

Significado de los campos mostrados en la Figura 1-17:

- ✓ *Next header.*-Identifica el tipo de protocolo de los datos transferidos.
- ✓ *Payload length.*- Define el tamaño del paquete AH.
- ✓ *Reserved.*-Reservado para uso futuro (hasta entonces todo ceros).
- ✓ *Security parameters index (SPI).*- Indica los parámetros de seguridad que, en combinación con la dirección IP, identifican la asociación de seguridad implementada con este paquete.
- ✓ *Sequence number.*- Un número siempre creciente, utilizado para evitar ataques de repetición.
- ✓ *Hash Message Authentication Code.*- Valor utilizado para autenticar el paquete, también puede incluir relleno suficiente para garantizar un multiplo de 32-bits.

De acuerdo con el modo, la cabecera AH se puede ubicar de la forma en que se indica en la Figura 1-18. Se utiliza AH en modo transporte cuando se protege un protocolo de nivel superior al de capa tres, mientras que para encapsular IP se utiliza AH en modo túnel.

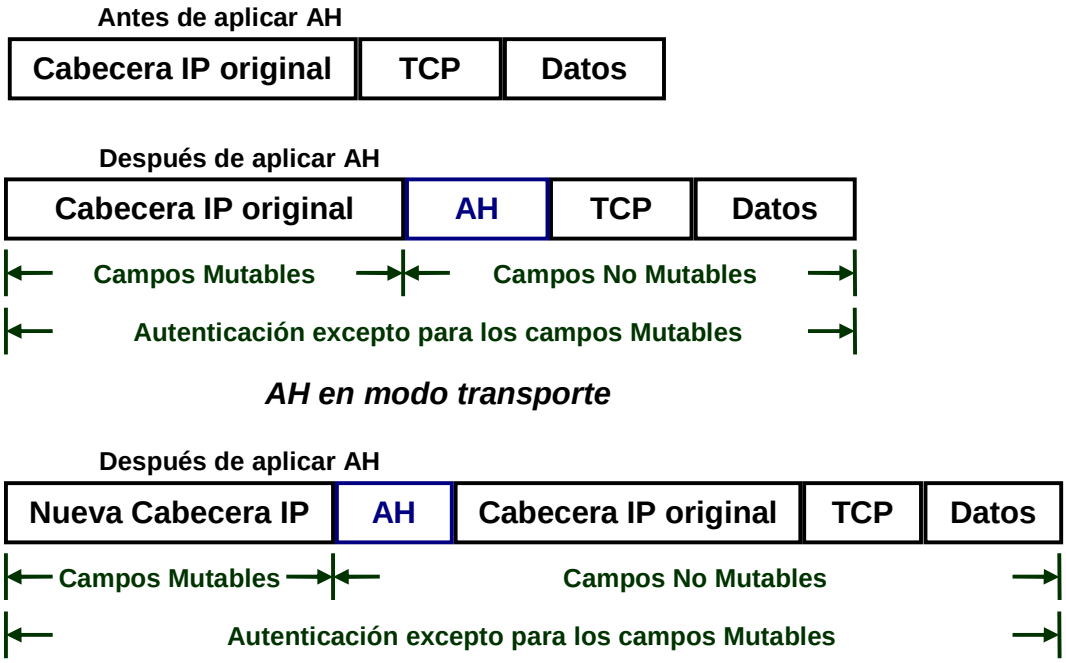


Figura 1-18 Modos AH

1.1.6.4 Encapsulating Security Payload (ESP) [9] [12]

ESP se usa para encapsular paquetes IP o de capa superior. ESP es el protocolo recomendado en el RFC 4301 para ser utilizado como protocolo de encapsulamiento por IPsec para llevar a cabo la transmisión de datos.

ESP ofrece los mismos servicios que AH, con la diferencia que ESP agrega confidencialidad en las comunicaciones y aunque ESP puede brindar integridad sin confidencialidad, no se recomienda el uso de integridad sin confidencialidad. Como se observa en la Tabla 1-1, las diferencias entre AH y ESP, muestran que ESP cumple con todas las necesidades de seguridad requeridas para una VPN.

	AH	ESP (ENCRIP)	ESP (ENCRIP + AUTENT
Control de Acceso	SI	SI	SI
Integridad sin conexión	SI		SI
Autenticación de origen de datos	SI		SI
Rechazo de paquetes repetidos		SI	SI
Confidencialidad		SI	SI
Confidencialidad limitada al flujo de tráfico		SI	SI

Tabla 1-2 ESP y AH

La Figura 1-19 describe el formato de la cabecera ESP.

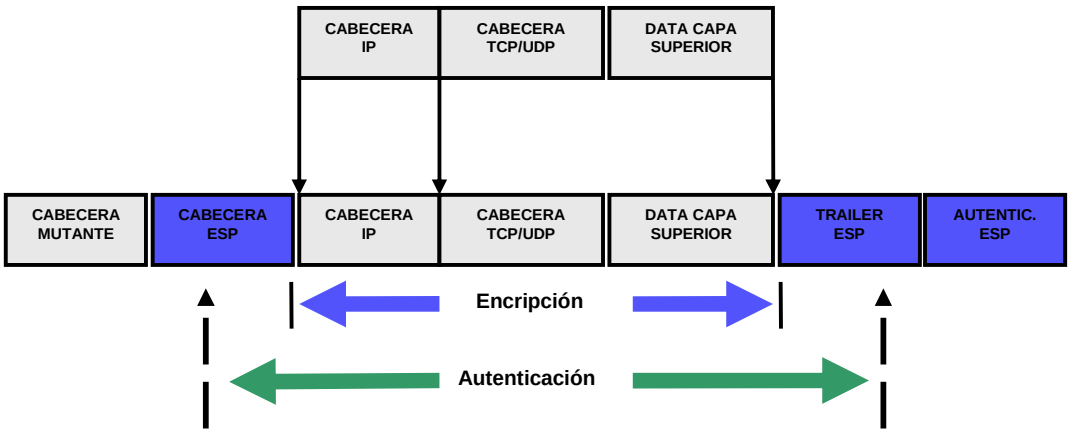
0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Security parameters index (SPI)			
Sequence number			
Payload data (variable)			
Padding (0-255 bytes)			
		Pad Length	Next Header
Authentication Data (variable)			

Figura 1-19 Cabecera ESP

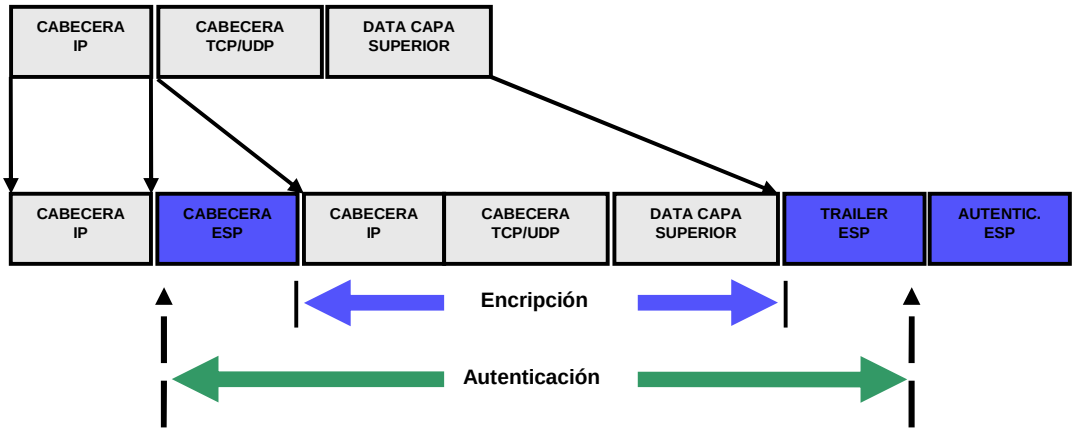
Significado de los campos:

- ✓ *Security parameters index (SPI).-* Identifica los parámetros de seguridad en combinación con la dirección IP.
- ✓ *Sequence number.-* Un número siempre creciente, utilizado para evitar ataques de repetición.
- ✓ *Payload data.-* Los datos a transferir.
- ✓ *Padding.-* Usado por algunos algoritmos criptográficos para rellenar por completo los bloques.
- ✓ *Pad length.-* Tamaño del relleno en bytes.
- ✓ *Next header.-* Identifica el protocolo de los datos transferidos.
- ✓ *Authentication data.-* Contiene los datos utilizados para autenticar el paquete.

ESP puede brindar protección solamente a la carga útil como también a la carga útil más la cabecera, según sea el modo que se utilice. La primera se conoce como ESP en modo transporte. Este modo se usa normalmente para proveer seguridad a una comunicación entre 2 hosts. La segunda se conoce como ESP en modo túnel, utilizado para proveer seguridad en comunicaciones entre redes. ESP en modo túnel se usa para crear redes privadas virtuales. Se puede observar los modos ESP en la Figura 1-20.



ESP en Modo Túnel



ESP en Modo Transporte

Figura 1-20 Modos ESP

1.1.6.5 Internet Key Exchange (IKE) [13]

IKE es un protocolo utilizado por IPsec para establecer, negociar, modificar y/o eliminar asociaciones seguras (SAs), que garanticen la seguridad de los paquetes transmitidos entre dos hosts en una red.

El proceso para llegar a una asociación segura se lleva a cabo en 2 fases. Durante la primera fase IKE autentica a su par brindándole su respectiva acreditación como par autenticado, el propósito de esta primera fase es proteger a una segunda fase,

luego durante una segunda fase IKE negocia políticas de seguridad, algoritmos a utilizar y genera elementos para el manejo y creación de llaves que luego se reflejaran en una autenticación y encripción robusta. El protocolo IKE usa paquetes UDP, normalmente a través del puerto 500, y generalmente requiere entre 4 y 6 paquetes con dos turnos para crear una SA en ambos extremos. Las claves negociadas son entregadas a la pila IPsec.

1.1.6.5.1 Protocolo Diffie-Hellman [4] [14]

IKE utiliza el protocolo criptográfico para intercambio de llaves de Diffie-Hellman, debido a Whitfield Diffie y Martin Hellman. Este protocolo se emplea generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión y permite el intercambio secreto de claves entre dos partes que no han tenido contacto previo, utilizando un canal inseguro, y de manera anónima (no autenticada), sin embargo provee las bases para varios protocolos autenticados. Su seguridad radica en la extrema dificultad (conjeturada, no demostrada) de calcular logaritmos discretos en un campo finito.

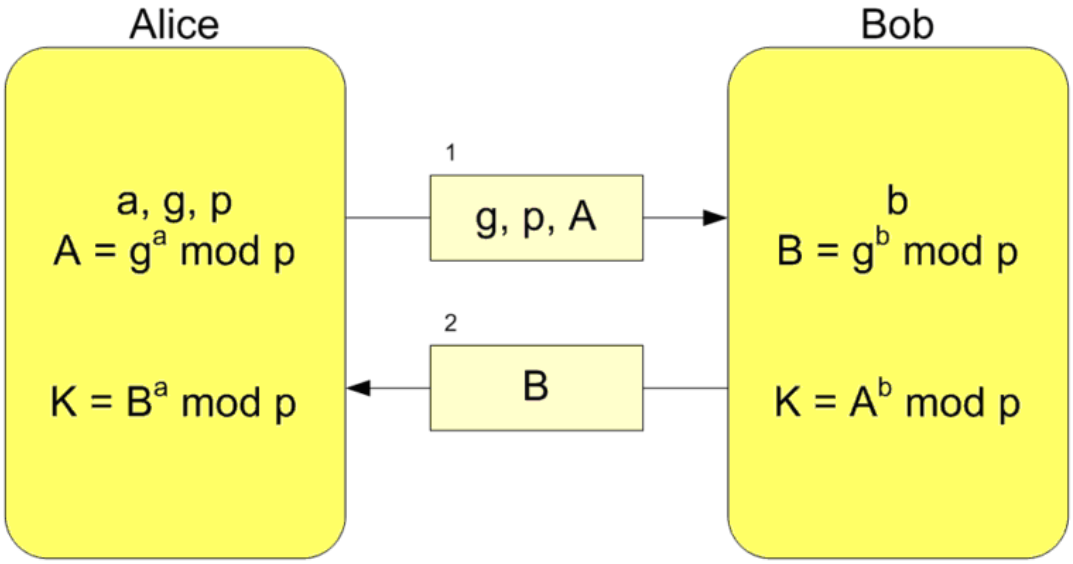


Figura 1-21 Algoritmo Diffie-Hellman

El siguiente ejemplo es una versión básica de cómo funciona el algoritmo Diffie-Hellman, mostrado en la Figura 1-21, en un ambiente entre 2 partes A y B y un adversario E.

Se establecen un primo *p* y un generador $g \in \mathbf{Z}_p^*$, donde $\mathbf{Z}_p^*$ es el conjunto de los enteros menores que *p* que son primos relativos de *p.* Estos son públicos, conocidos no sólo por las partes *A* y *B* sino también por el adversario *E*.

A escoge $x \in \mathbf{Z}_{p-1}$ al azar, calcula $X = g^x \bmod p$, y envía *X* a *B*

B escoge $y \in \mathbf{Z}_{p-1}$ al azar, calcula $Y = g^y \bmod p$, y envía *Y* a *A*

Nótese que $X^y = (g^x)^y = g^{xy} = (g^y)^x = Y^x$, con todas las operaciones en el grupo $\mathbb{Z}_p^*$. Llámese *K* a esta cantidad común. El hecho destacable es que *ambas* partes pueden calcularla, y por lo tanto obtener una clave compartida.

Un adversario *E* que poseyera *p*, *g*, *X* e *Y*, podría calcular el secreto compartido si tuviera también uno de los valores privados (*x* o *y*) o lograse invertir la función. Pero calcular *x* dado *X* es el problema del logaritmo discreto en $\mathbf{Z}_p^*$, un problema que se cree intratable computacionalmente. El mismo protocolo, y otros basados en este, pueden llevarse a cabo en cualquier grupo en que a la vez la exponenciación sea simple y el logaritmo discreto difícil.

Dada la explicación anterior, numéricamente se aplica de la siguiente manera:

1. A y B acuerdan usar el número primo p=23 y la base g=5.
2. A elige un número secreto a=6, luego envía a B ($g^a \bmod p$)
   $5^6 \bmod 23 = 8$.
3. B elige un número secreto b=15, luego envía a A ($g^b \bmod p$)
   $5^{15} \bmod 23 = 19$.
4. A calcula $(g^b \bmod p)^a \bmod p$
   $19^6 \bmod 23 = 2$.

5. B calcula $(g^a \bmod p)^b \bmod p$
   $8^{15} \bmod 23 = 2$.

Es claro que el ejercicio anterior es muy sencillo debido a la magnitud de los dígitos elegidos, obviamente en una aplicación real los dígitos deberán ser mucho mayores para prevenir cualquier posibilidad de calculo, debido a que el rango de posibilidades es relativamente pequeño.

1.1.6.5.2 Modos en IKE

La siguiente notación se usa para explicar los modos en que opera IKE:

HDR	HDR es una cabecera ISAKMP cuyo tipo de intercambio es el modo.
*HDR**	La carga útil después de la cabecera ISAKMP está encriptada.
SA	Es un campo de negociación de asociaciones de seguridad con uno o más campos de Propuestas y Transformaciones.
Nonce	Indiferente de la carga útil
KE	Intercambio de llave
IDii	Identidad de la carga útil; Iniciador de la fase uno.
IDci	Identidad de la carga útil; Iniciador de la fase dos.
IDir	Identidad de la carga útil; Iniciador de la fase uno.
IDcr	Identidad de la carga útil; Iniciador de la fase dos.
Auth	Un mecanismo genérico de autenticación.
HASH	Paquete Hash

Existen 2 modos para establecer la primera fase:

- ✓ *Modo Principal*

Este modo se basa en el intercambio protegido de identidad de ISAKMP[6]. ISAKMP define el procedimiento para autenticación y comunicación entre pares, además de la creación y manejo de SA, técnicas de creación de llaves y mitigación de amenazas.

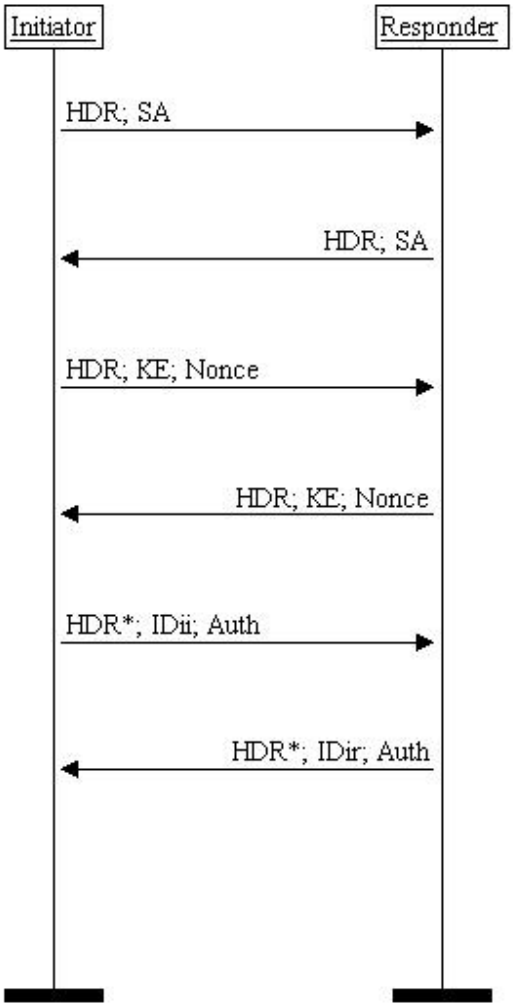


Figura 1-22 Modo Principal

Los dos primeros mensajes que se ven en la Figura 1-22 se usan para negociar políticas de seguridad para el intercambio durante la segunda fase. Los siguientes dos mensajes se usan para el intercambio del material usado por el protocolo Diffie-Hellman. Los dos últimos mensajes de autenticación se encriptan con las

[6] ISAKMP, Internet Security Association and Key Management Protocol

llaves previamente negociadas y las identidades de las partes están protegidas de espías.

- ✓ *Modo Agresivo*

El modo agresivo es un poco más rápido, pero no ofrece protección de identidad a diferencia del modo principal. Es similar al modo principal pero algunos mensajes son embebidos para otros.

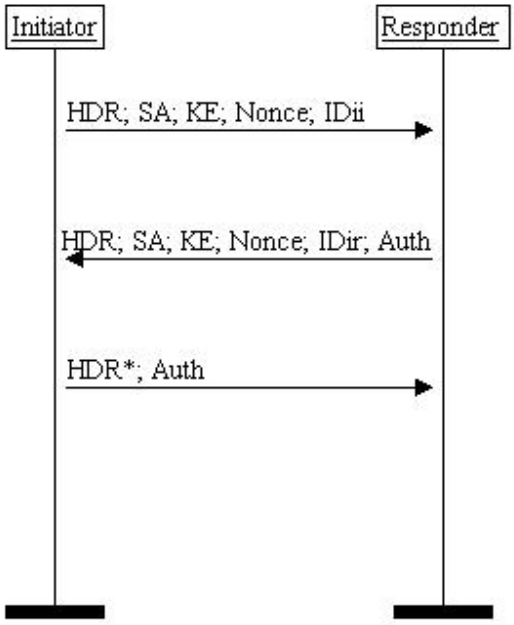


Figura 1-23 Modo Agresivo

De acuerdo con la Figura 1-23, el primer mensaje contiene las políticas y cruza datos para el intercambio de llaves y alguna información para identificación. El segundo mensaje es una respuesta, la misma que autentica la respuesta y concluye las políticas y el intercambio de llaves. El último mensaje se utiliza para autenticar a quien inicio la sesión y provee evidencia de participación durante el intercambio

Para la segunda fase se utilizan también dos modos:

✓ *Modo Rápido*

Este modo se usa para negociar y establecer asociaciones de seguridad por clientes IKE, además se usa para generar nuevo material para generación de llaves.

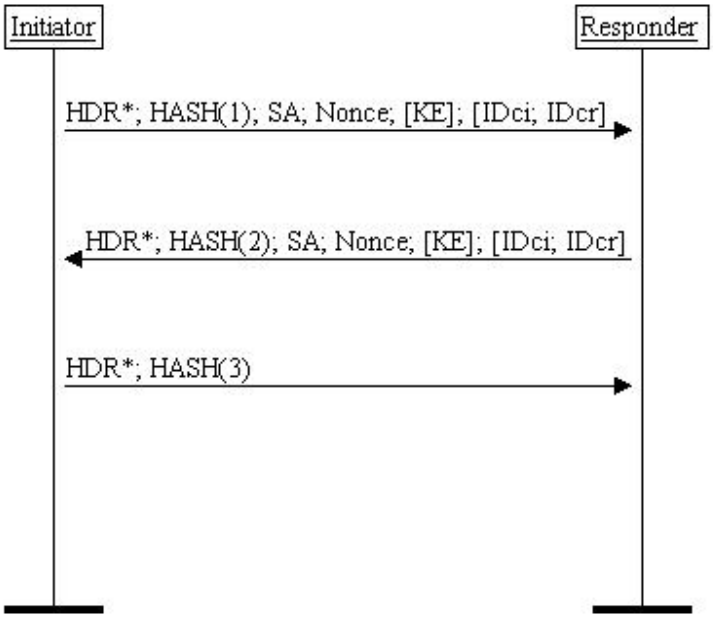


Figura 1-24 Modo Rápido

En la Figura 1-24 se puede ver las siglas HDR* lo que significa que la carga útil, excepto la cabecera ISAKMP, está encriptada. Se puede negociar más de una asociación de seguridad durante el intercambio en un modo rápido.

✓ *Modo New Group*

Se utiliza para negociar un nuevo grupo para llevar a cabo el intercambio Diffie-Hellman. En la Figura 1-25 se puede ver las siglas HDR* lo que significa que la carga útil, excepto la cabecera ISAKMP, está encriptada. Se puede negociar na asociación de seguridad durante el intercambio en un Modo New Group.

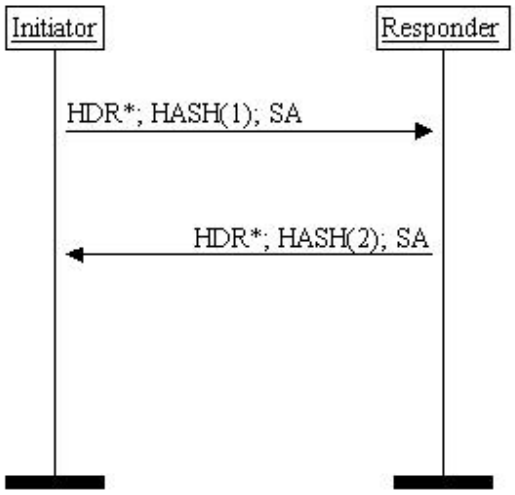


Figura 1-25 Modo New Group

1.2 VOZ SOBRE IP

1.2.1 DEFINICIÓN DE VOIP Y TELEFONÍA IP [15] [16]

Voz sobre IP es una tecnología que permite la transmisión de voz a través de redes IP en forma de paquetes de datos. Esta tecnología a dado paso a la hoy conocida telefonía IP, recalcando la diferencia que existe entre voz sobre IP que telefonía IP. Telefonía IP consiste en agregar y prestar nuevos servicios sobre terminales asociadas a una misma administración, por ejemplo transferencia de llamadas, llamada en espera, entre otros servicios que antes solo se podían encontrar en centrales analógicas.

VoIP se encontró con algunas limitaciones al momento de marcar diferencias respecto a la calidad en las llamadas, puesto que, hasta entonces, las comunicaciones analógicas contaban con algunos parámetros y lineamientos que aseguraban cierta calidad en el servicio. En este sentido se establecieron parámetros mínimos para garantizar una comunicación legible y comparable en calidad a la ya existente comunicación analógica.

1.2.2 CALIDAD DE SERVICIO (QOS) [14] [17]

Calidad de servicio implica tomar en cuenta aspectos como tratamiento diferenciado de los paquetes transmitidos, consideraciones de retardo o variaciones del mismo; calidad de servicio busca establecer y garantizar un nivel de aceptación sobre la información que llega al usuario, que por este precepto es aplicable a redes de datos como analógicas.

Para definir un grado de tolerancia sobre la transmisión de voz se consideran parámetros específicos a continuación detallados:

1.2.2.1 Latencia

En un principio establecer una conexión a un destino implica el intercambio de parámetros o mensajes de control, fundamentales para alcanzar a un destino, y a continuación el intercambio de paquetes de datos; sin embargo, para que el destino y el origen estén comunicados todos los paquetes tienen que atravesar toda una red, esto involucra trasladar un paquete de un nodo a otro y así hasta llegar a su respectivo destino.

Calidad de servicio implica que un paquete tendrá un tiempo máximo para llegar a su destino. A este tiempo se conoce con el nombre de latencia o retardo. El estándar ITU-T G.114 recomienda un retardo no mayor a 150 ms en un sentido de la comunicación, como límite para mantener una comunicación legible y fluida.

1.2.2.2 Jitter

En una red de conmutación de paquetes, los paquetes pueden tomar rutas diferentes para llegar a su destino. Incluso si los paquetes viajan exactamente por

la misma ruta, el tiempo que le lleva a un paquete no será el mismo para los demás. Por lo mismo, la latencia que sufre un paquete difiere de la que sufren los demás. Ésta particularidad puede presentar problemas como tergiversación en el audio, conocido como eco, que se produce por la marcada diferencia en el retardo entre los paquetes.

Para resolver este tipo de variaciones sobre los retardos, se toma una muestra periódica de los retardos que sufren los paquetes, y se trata de corregir la variación en la latencia, simulando una latencia uniforme en la comunicación.

1.2.2.3 Pérdida de Paquetes

Las comunicaciones en tiempo real se basan en el protocolo UDP. UDP es un protocolo no orientado a conexión, esto significa que si un paquete se pierde no es retransmitido; además, la perdida de paquetes también se produce por descartes de paquetes que no llegan a tiempo al receptor.

La perdida de paquetes máxima admitida para que no se degrade la comunicación deber ser inferior al 1%**,** y es bastante dependiente del códec que se utiliza. Cuanto mayor sea la compresión del códec más pernicioso será el efecto de la pérdida de paquetes.

Sin embargo, la voz es bastante predictiva y si se pierden paquetes aislados se puede recomponer la voz de una manera bastante óptima. El problema es mayor cuando se producen pérdidas de paquetes en ráfagas.

1.2.3 PROTOCOLO H.323 [15] [18] [19]

El protocolo H.323 es una recomendación de la ITU-T[7], que describe los protocolos para las comunicaciones en tiempo real sobre redes basadas en

[7] ITU-T International Telecomunication Union, area Telecomunicaciones.

paquetes y que tiene como objetivo proveer a los usuarios con tele-conferencia con capacidad de voz video y datos.

La importancia de este estándar es que permite la integración de voz, vídeo y comunicaciones de datos sobre una red de área local, LAN, como también a través de una red de área amplia compartida, WAN.

El estándar H.323 está diseñado para la compatibilidad de redes y puede ser implementado donde IP sea utilizado como soporte, sin tomar en cuenta la topología física de la red.

Los paquetes IP pueden ser transportados sobre LAN, Ethernet o Token Ring, redes ATM, líneas arrendadas o redes Frame Relay. La recomendación H.323 es un estándar que utiliza el Hardware y el sistema operativo en forma independiente, lo que significa que muchos productos pueden ser fabricados por muchos proveedores y pueden ser utilizados en diferentes ambientes.

H.323 fue diseñado con los siguientes objetivos:

- Basarse en los estándares existentes, incluyendo H.320[8], RTP[9] y Q.931[10].
- Incorporar algunas de las ventajas que las redes de conmutación de paquetes ofrecen para transportar datos en tiempo real.
- Solucionar la problemática que plantea el envío de datos en tiempo real sobre redes de conmutación de paquetes.

1.2.3.1 Pila de protocolos utilizados en H.323

[8] H.320, Estándar desarrollado por la ITU para vídeoconferencia sobre *RDSI*
[9] RTP, Real-Time Transfer Protocol.
[10] Q.931, Señalización de acceso en redes RDSI básico

H.323 fue desarrollado para trabajar con los protocolos contemporáneos más significativos. A continuación se expone un breve resumen de los más importantes.

- ✓ **RTP/RTCP (Real-Time Transport Protocol / Real-Time Transport Control Protocol)** Protocolos de transporte en tiempo real que proporcionan servicios de entrega punto a punto de datos. Éste protocolo fija la secuencia de los paquetes de audio y video a transmitir.

- ✓ **RAS (Registration, Admission and Status):** Diseñado para registro, control de admisión, control del ancho de banda, estado y desconexión de participantes. Utilizado para la comunicación con el componente Gatekeeper y un Terminal IP.

- ✓ **H225:** Protocolo de control de llamada que permite establecer una conexión y una desconexión. Especifica el uso y soporte de mensajes Q.931 y Q.932.

- ✓ **H.245:** Protocolo de control usado en el establecimiento y control de una llamada. H.245 Presenta las siguientes funciones entre las mas importantes:

    1. Intercambio de capacidades: Cada terminal define los códecs que posee y se lo hace saber a su par correspondiente.
    2. Apertura y cierre de canales lógicos: Los canales de audio y video H.323 son punto a punto y unidireccionales. Por lo tanto, en función de las capacidades negociadas, se tendrán que crear como mínimo dos de estos canales. Esto es responsabilidad de H.245.
    3. Control de flujo cuando ocurre algún tipo de problema.

- ✓ **Q.931:** (Digital Subscriber Signalling) Este protocolo se define para la señalización de accesos RDSI básico.

- ✓ **RSVP** (Resource ReSerVation Protocol): Protocolo de reserva de recursos en la red para cada flujo de información de usuario.

- ✓ **T.120:** La recomendación T.120 define un conjunto de protocolos para conferencia de datos.

La norma H.323 recomienda el uso, principalmente, de los siguientes códecs:

- ✓ **G.711:** De los múltiples códecs de audio que pueden implementar los terminales H.323, este es el único obligatorio. Usa modulación por codificados de pulsos (PCM) para conseguir tasas de bits de 56Kbps y 64Kbps.

- ✓ **H.261y H.263:** Son dos códecs de video que propone la recomendación H.323. Sin embargo, se pueden usar otros.

1.2.3.2 Componentes definidos en H.323

El estándar H.323 define los siguientes componentes principales que interactúan entre si durante una llamada IP:

1.2.3.2.1 Terminal

Un terminal H.323 es un extremo de la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal. Conforme a la especificación, un terminal H.323 puede proporcionar sólo voz, voz y datos, voz y vídeo, o voz, datos y vídeo.
Un terminal H.323 debe soportar la norma H.245, el estándar de señalización Q.931, además los protocolos RAS, RTP/RTCP y RSVP.

1.2.3.2.2 Gateway

En general, el propósito del gateway es reflejar transparentemente las características de un extremo en la red IP a otro en una red conmutada y viceversa. Un equipo gateway cumple con las mismas características de un equipo terminal a la vez que debe soportar los mismos protocolos.

1.2.3.2.3 Gatekeeper

Es una entidad que proporciona la traducción de direcciones y el control de acceso a la red de los terminales, gateways y MCUs[11], puede también ofrecer otros servicios como gestión del ancho de banda y localización de los gateways.

El Gatekeeper realiza dos funciones de control de llamadas que preservan la integridad de la red corporativa de datos. La primera es la traslación de direcciones de los terminales de la LAN a las correspondientes IP o IPX. La segunda es la gestión del ancho de banda, fijando el número de conferencias que pueden estar dándose simultáneamente en la LAN y rechazando las nuevas peticiones por encima del nivel establecido, de manera tal que se garantice ancho de banda suficiente para las aplicaciones de datos sobre la LAN. El Gatekeeper realiza además los siguientes servicios de control:

- ✓ Control de admisiones: Para rechazar aquellas llamadas procedentes de un terminal por ausencia de autorización a terminales o gateways particulares de acceso restringido o en determinadas franjas horarias.
- ✓ Control y gestión de ancho de banda: Para controlar el número de terminales a los que se permite el acceso simultáneo a la red, así como el

[11] MCU, Multipoint Control Unit, en español UCM

rechazo de llamadas tanto entrantes como salientes para las que no se disponga de suficiente ancho de banda.

- ✓ Gestión de la zona: Lleva a cabo el registro y la admisión de los terminales y gateways de su zona. Conoce en cada momento la situación de los gateways existentes en su zona que encaminan las conexiones hacia terminales RCC.

1.2.3.2.4 Unidad de Control Multipunto (MCU)

Su propósito es soportar la conferencia entre tres o más puntos, bajo el estándar H.323, de esta manera lleva a cabo la negociación entre terminales para determinar las capacidades comunes para el proceso de audio y vídeo, y controlar la multidifusión.

1.2.3.2.5 Controlador Multipunto (MC)

Es un equipo que provee capacidad de negociación con todos los terminales para llevar a cabo niveles de comunicaciones, además puede controlar recursos de conferencia tales como multicasting de vídeo.

El Controlador Multipunto no ejecuta mezcla o conmutación de audio, vídeo o datos.

1.2.3.2.6 Procesador Multipunto

Es un elemento tanto de hardware como de software especializado, mezcla, conmuta y procesa audio, vídeo y / o flujo de datos para los participantes de una conferencia multipunto, de tal forma que los procesadores del terminal no sean pesadamente utilizados.

1.2.3.2.7 Proxy H.323

Es un servidor que provee a los usuarios acceso a redes seguras de unas a otras confiando en la información que conforma la recomendación H.323.

H.323 es la primera especificación con características completas sobre el cual los productos pueden ser desarrollados con el más amplio despliegue de protocolo de transmisión IP. Una de las ventajas que se puede observar es de la interoperabilidad entre los equipos, por ejemplo un gateway de un proveedor funcionará consistentemente, cuando este sea conectado a terminales de diferentes proveedores.

1.2.3.3 Procesos en una llamada utilizando H.323

En una llamada H.323 hay varias fases como se indican en la Figura 1-26, en los que intervienen algunos de los protocolos ya mencionados, inmersos en el protocolo H.323.

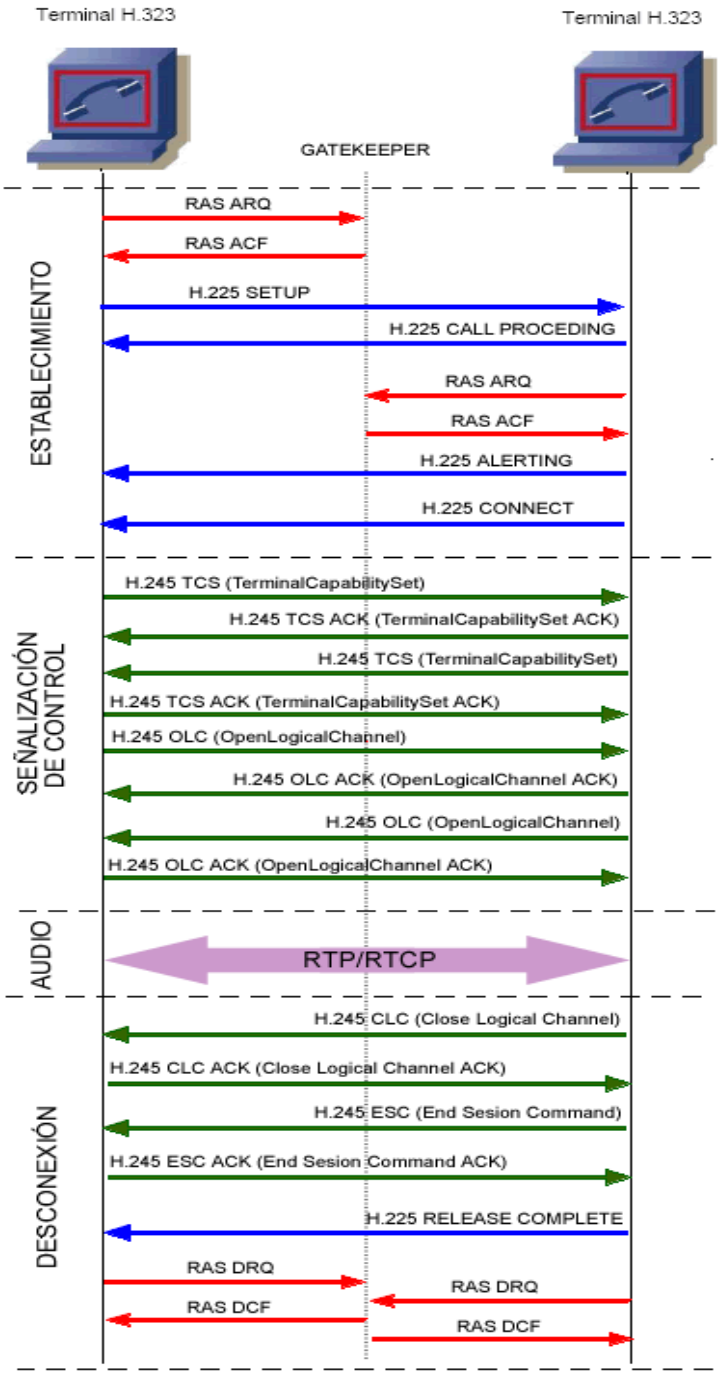


Figura 1-26 Procesos en una llamada H.323

Una llamada H.323 se caracteriza por cumplir con las siguientes fases:

1.2.3.3.1 Establecimiento

En esta fase lo primero que se observa es que uno de los terminales se registra en el gatekeeper utilizando el protocolo RAS (Registro, admisión y estado) con los mensajes ARQ y ACF. Posteriormente, utilizando el protocolo H.225 (que se utiliza para establecimiento y liberación de la llamada) se envía un mensaje de SETUP para iniciar una llamada H.323. Entre la información que contiene el mensaje se encuentra la dirección IP, puerto y alias del llamante o la dirección IP y puerto del llamado.

El terminal llamado contesta con un CALL PROCEEDING advirtiendo del intento de establecer una llamada. En este momento el segundo terminal tiene que registrarse con el gatekeeper utilizando el protocolo RAS de manera similar al primer Terminal.

El mensaje ALERTING indica el inicio de la fase de generación de tono y por último CONNECT indica el comienzo de la conexión.

1.2.3.3.2 Señalización de control

En esta fase se abre una negociación mediante el protocolo H.245 (control de conferencia), el intercambio de los mensajes (petición y respuesta) entre los dos terminales establecen quién será master y quién slave, las capacidades de los participantes y códecs de audio y video a utilizar. Como punto final de esta negociación se abre el canal de comunicación (direcciones IP, puerto).

Los principales mensajes H.245 que se utilizan en esta fase son:

- ✓ Terminal Capability Set (TCS). Mensaje de intercambio de capacidades soportadas por los terminales que intervienen en una llamada.
- ✓ Open Logical Channel (OLC). Mensaje para abrir el canal lógico de información que contiene información para permitir la recepción y

codificación de los datos. Contiene la información del tipo de datos que será transportados.

1.2.3.3.3 Audio

Los terminales inician la comunicación y el intercambio de audio (o video) mediante el protocolo RTP/RTCP.

1.2.3.3.4 Desconexión

En esta fase cualquiera de los participantes activos en la comunicación puede iniciar el proceso de finalización de llamada mediante mensajes Close Logical Channel y End Session Comand de H.245. Posteriormente utilizando H.225 se cierra la conexión con el mensaje RELEASE COMPLETE

Por último se liberan los registros con el gatekeeper utilizando mensajes del protocolo RAS.

1.2.4 Protocolo SIP [15] [20]

El protocolo SIP (Session Initiation Protocol) fue desarrollado por el grupo MMUSIC (Multimedia Session Control) del IETF, definiendo una arquitectura de señalización y control para VoIP. Inicialmente fue publicado en febrero de 1996 en la RFC 2543, ahora obsoleta con la publicación de la nueva versión RFC 3261 que se publicó en junio del 2002.

El propósito de SIP es la comunicación entre dispositivos multimedia. SIP hace posible esta comunicación gracias a dos protocolos que son RTP/RTCP y SDP.

SIP fue diseñado de acuerdo al modelo de Internet. Es un protocolo de señalización extremo a extremo que implica que toda la lógica es almacenada en

los dispositivos finales (salvo el rutado de los mensajes SIP). El estado de la conexión es también almacenado en los dispositivos finales. El precio a pagar por esta capacidad de distribución y su gran escalabilidad es una sobrecarga en la cabecera de los mensajes, producto de tener que mandar toda la información entre los dispositivos finales.

SIP es un protocolo de señalización a nivel de aplicación para establecimiento y gestión de sesiones con múltiples participantes. Se basa en mensajes de petición y respuesta y reutiliza muchos conceptos de estándares anteriores como HTTP y SMTP.

1.2.4.1 Componentes

Existen dos elementos fundamentales, los agentes de usuario (UA) y los servidores.

1.2.4.1.1 User Agent (UA)

Consisten en dos partes distintas, el User Agent Client (UAC) y el User Agent Server (UAS). Un UAC es una entidad lógica que genera peticiones SIP y recibe respuestas a esas peticiones. Un UAS es una entidad lógica que genera respuestas a las peticiones SIP.

Ambos se encuentran en todos los agentes de usuario, así permiten la comunicación entre diferentes agentes de usuario mediante comunicaciones de tipo cliente-servidor.

1.2.4.1.2 Los servidores SIP

Pueden ser de tres tipos:

- ✓ **Proxy Server**: retransmiten solicitudes y deciden a qué otro servidor deben remitir, alterando los campos de la solicitud en caso necesario. Es una entidad intermedia que actúa como cliente y servidor con el propósito de establecer llamadas entre los usuarios. Este servidor tiene una funcionalidad semejante a la de un Proxy HTTP que tiene una tarea de encaminar las peticiones que recibe de otras entidades más próximas al destinatario. Existen dos tipos de Proxy Servers: Statefull Proxy y Stateless Proxy.

    - ➢ Statefull Proxy: mantienen el estado de las transacciones durante el procesamiento de las peticiones. Permite división de una petición en varias (forking), con la finalidad de la localización en paralelo de la llamada y obtener la mejor respuesta para enviarla al usuario que realizó la llamada.
    - ➢ Stateless Proxy: no mantienen el estado de las transacciones durante el procesamiento de las peticiones, únicamente reenvían mensajes.

- ✓ **Registrar Server**: es un servidor que acepta peticiones de registro de los usuarios y guarda la información de estas peticiones para suministrar un servicio de localización y traducción de direcciones en el dominio que controla.

- ✓ **Redirect Server**: es un servidor que genera respuestas de redirección a las peticiones que recibe. Este servidor reencamina las peticiones hacia el próximo servidor.

La división de estos servidores es conceptual, cualquiera de ellos puede estar físicamente en una única máquina. La división de éstos puede ser por motivos de escalabilidad y/o rendimiento.

1.2.4.2 Procesos en una llamada utilizando SIP

En una llamada SIP hay varias transacciones SIP, como se ven en la Figura 1-27. Una transacción SIP se realiza mediante un intercambio de mensajes entre un cliente y un servidor. Consta de varias peticiones y respuestas y para agruparlas en la misma transacción está el parámetro CSeq.

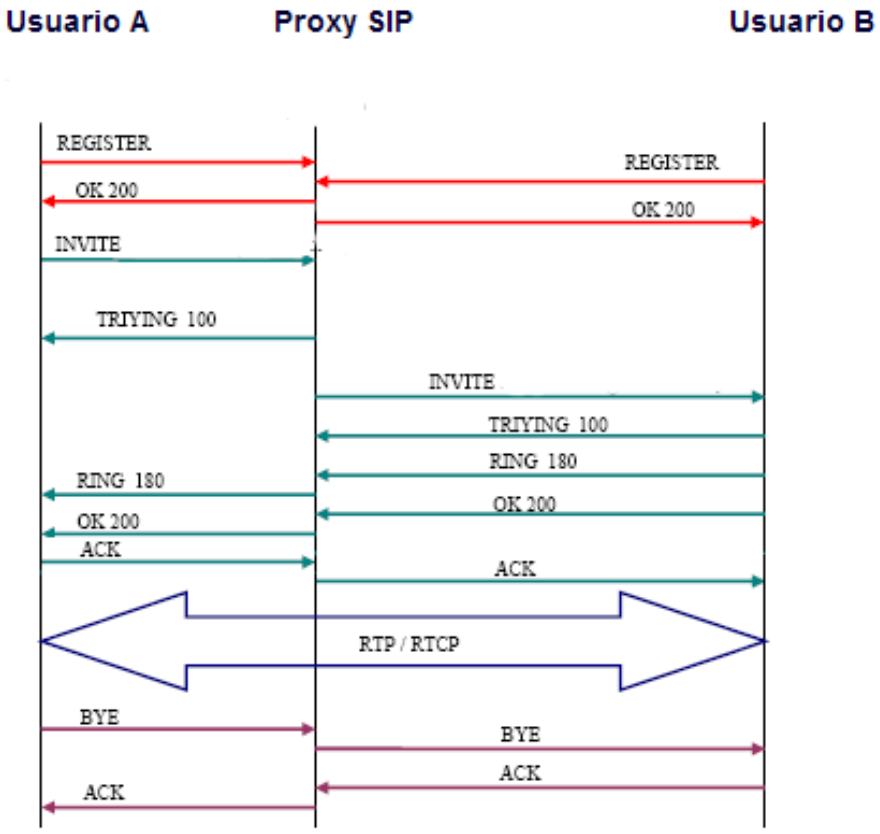


Figura 1-27 Procesos en una llamada SIP

1. Las dos primeras transacciones corresponden al registro de los usuarios. Los usuarios deben registrarse para poder ser encontrados por otros usuarios. En este caso, los terminales envían una petición REGISTER, donde los campos from y to corresponden al usuario registrado. El servidor Proxy, que actúa como Register, consulta si el usuario puede ser autenticado y envía un mensaje de OK en caso positivo.

2. La siguiente transacción corresponde a un establecimiento de sesión. Esta sesión consiste en una petición INVITE del usuario al proxy. Inmediatamente, el proxy envía un TRYING 100 para parar las retransmisiones y reenvía la petición al usuario B. El usuario B envía un Ringing 180 cuando el teléfono empieza a sonar y también es reenviado por el proxy hacia el usuario A. Por ultimo, el OK 200 corresponde a aceptar la llamada (el usuario B descuelga).

3. En este momento la llamada está establecida, pasa a funcionar el protocolo de transporte RTP con los parámetros (puertos, direcciones, codecs, etc.) establecidos en la negociación mediante el protocolo SDP.

4. La última transacción corresponde a una finalización de sesión. Esta finalización se lleva a cabo con una única petición BYE enviada al Proxy, y posteriormente reenviada al usuario B. Este usuario contesta con un OK 200 para confirmar que se ha recibido el mensaje final correctamente.

1.2.5 Protocolo SIP frente a H.323

SIP es un protocolo mucho más flexible que H.323, pese a ser un protocolo poco detallado en relación a H.323, que es a su vez un protocolo que abarca y prevé la interoperabilidad entre equipos de diferentes marcas, además de la integración con versiones mejoradas del mismo protocolo.

La Tabla 2 es una comparación de los aspectos más relevantes tanto de H.323 como de SIP.

	H.323	SIP
Arquitectura	H.323 cubre casi todos los servicios como capacidad de intercambio, control de conferencia, señalización básica, calidad de servicio, registro, servicio de descubrimiento y más.	**SIP es modular y cubre la señalización básica, la localización de usuarios y el registro. Otras características se implementan en protocolos**

	H.323	SIP
		separados.
Componentes	Terminal/Gateway	**UA**
	Gatekeeper	**Servidores**
Funcionalidades de control de llamada		
Transferencia de llamada (Call Transfer)	**Si**	**Si**
Expedición de llamada (Call Forwarding)	**Si**	**Si**
Tenencia de llamada (Call Holding)	**Si**	**Si**
Llamada estacionada/recogida (Call Parking/Pickup)	**Si**	**Si**
LLamada en espera (Call Waiting)	**Si**	**Si**
Indicación de mensaje en espera (Message Waiting Indication)	**Si**	**No**
Identificación de nombre (Name Identification)	**Si**	**No**
Terminación de llamada con subscriptor ocupado (Call Completion on Busy Subscriber)	**Si**	**Si**
Ofrecimiento de llamada (Call Offer)	**Si**	**No**
Intrusión de llamada (Call Intrusion)	**Si**	**No**

Tabla 1-3 H.323 y SIP

1.2.6 VOZ SOBRE IP FRENTE A OTRAS TECNOLOGÍAS SIMILARES

1.2.6.1 Voz Sobre Frame Relay (VFR) [21] [22]

Frame Relay es una tecnología versátil al momento de transmitir voz, su fortaleza radica en que opera a nivel de capa 2, lo que libera a los equipos intermedios del procesamiento y/o rectificación de errores durante la transmisión, dejando esta tarea a los equipos terminales.
Para una transmisión, sin importar su naturaleza, Frame Relay establece circuitos virtuales. En el caso en particular de tramas de voz, se asigna una prioridad, de esta manera los circuitos virtuales destinados a transportar voz son menos propensos a grandes retardos durante la transmisión.

Una conexión FR se compone básicamente de 4 elementos:

- ✓ Un equipo multiplexor instalado en el domicilio del cliente, es un equipo tipo FRAD (Frame Relay Access Device), con capacidad para tratamiento de voz.
- ✓ Una línea de acceso a la red de datos.
- ✓ Facilidades de transporte sobre la red Frame Relay.
- ✓ Servicio de gestión.

El mayor uso de esta tecnología se puede observar en redes privadas o en interconexión de redes locales. En estas redes el cliente accede mediante un FRAD, que cumple con la tarea entramar los datos y conducirlos hacia la red FR.

Por el principio de que Frame Relay es una tecnología no adaptable a la mayoría de las redes, FR no es una solución valida para transmitir voz fuera de una red corporativa.

1.2.6.2 Voz Sobre ATM [21] [23]

ATM es una tecnología muy particular por la uniformidad de sus celdas, denominadas así porque cada una es de tamaño constante e igual a 53 bytes. Este es uno de los principales inconvenientes al momento de cruzar un paquete IP por una red ATM, pues la diferencia de tamaños entre una celda y un paquete introduce un nuevo proceso de segmentación, lo que se refleja en un tiempo mayor de procesamiento.

ATM puede transmitir voz en dos maneras diferentes. La primera utilizando CBR (Constant Bit Rate) y la segunda mediante VBR (Variable Bit Rate). Como la estructura de ATM, que se indica en la Figura 1-28, tiene su propio modelo en capas tanto CBR como VBR trabaja en distintas capas AAL (ATM Adaptation Layer). CBR funciona sobre la capa AAL 1 y VBR sobre la capa AAL 2.

La ventaja al utilizar CBR es que se garantiza ancho de banda constante durante toda la comunicación, pero por otra parte se desperdicia ancho de banda durante los silencios. En tanto VBR optimiza los periodos de silencio para permitir otros servicios de menor prioridad.

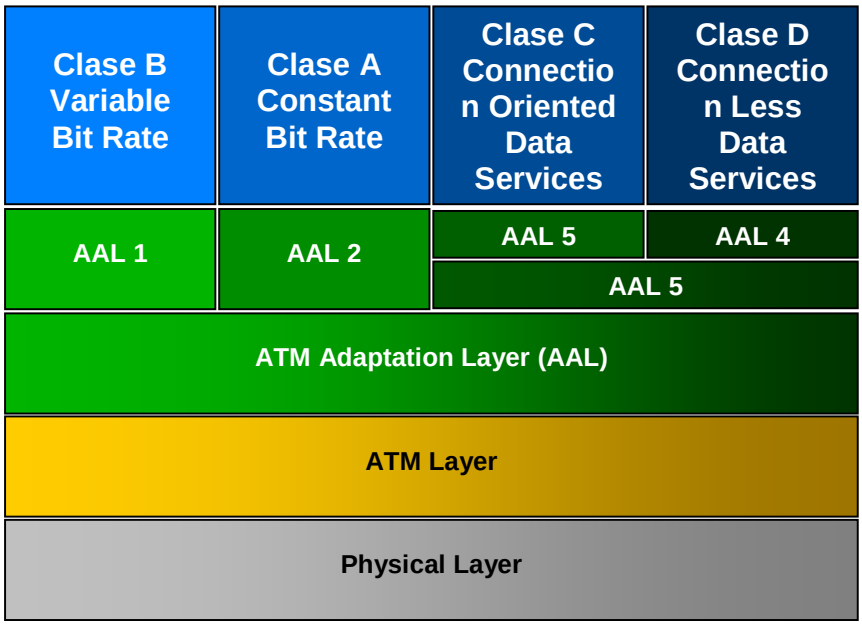


Figura 1-28 Clases y Tipos de Servicios AAL

La ventaja de usar VoIP a diferencia de usar voz sobre ATM o voz sobre FR, es básicamente que VoIP no tiene límites en cuanto a red se refiere. Un paquete IP es fácilmente transmitido por todas las redes que soportan IP. Esto se debe principalmente a que la gran mayoría de las redes utilizan el Protocolo de Internet (IP), como Internet, mientras que para acceder a una transmisión de VFR se deben tener en cuenta ciertos requisitos de compatibilidad, además de otros aspectos relacionados con la forma en que se conectan a la red los terminales.

ATM es por otra parte una buena solución corporativa, pero cuando se trata de llamadas fuera de la red se presentan problemas por el tamaño estándar de sus celdas, se introducen retardos debido a la fragmentación y reensamblaje de un paquete.

1.3 VOZ SOBRE IP EN VPNs

Una plataforma VPN permitirá montar una comunicación VoIP sobre una red pública, como se puede ver en la Figura 1-29. Un túnel VPN transparentaría el tráfico transmitido sobre éste sin interferir con el acceso normal a la Internet por

parte de los usuarios que requieren de ese servicio. Este proceso se lleva a cabo en los gateway que diferencian el acceso a Internet del túnel VPN. El proceso permitirá diferenciar entre varios servicios, recalcando la competencia del presente proyecto a la administración, seguridad y continuidad del servicio VoIP. En este sentido se provee el uso de herramientas administrativas para manejar el desempeño de la comunicación.

En la presente sección se presentan algunas de las características de VoIP, los componentes necesarios que permiten este servicio, al igual que algunos de los protocolos orientados a normar y estandarizar el mismo.

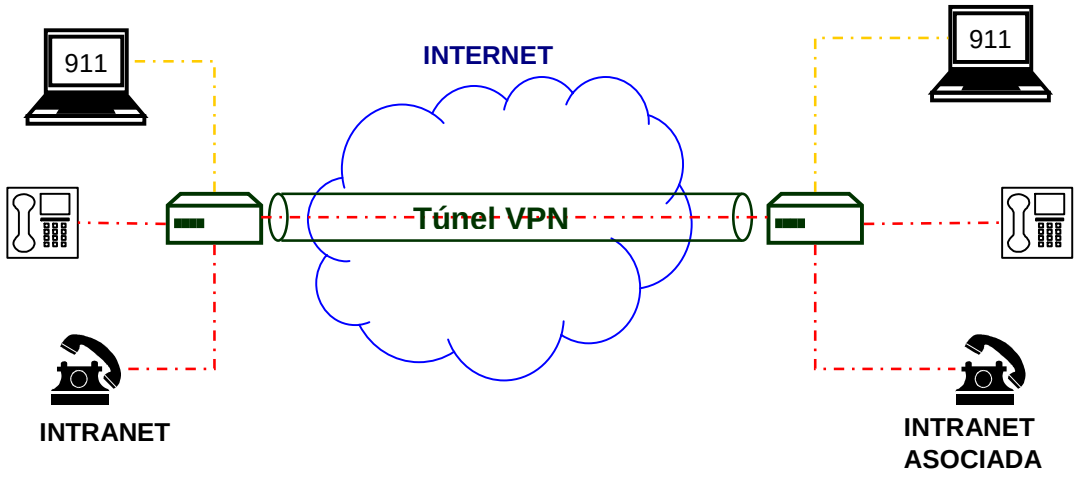


Figura 1-29 Voz sobre IP Sobre un Túnel VPN

Una de las ventajas que supone el utilizar una red VPN es el considerable ahorro tanto en equipos como en llamadas de larga distancia, pero mas allá del costo beneficio que implica el uso de una red de estas características, se ha tomado en cuenta que una aplicación de VoIP sobre una red VPN conlleva un beneficio mayor para entidades cuya restricción sobre sus datos, en este caso conversaciones, se llevaría a cabo utilizando un ambiente seguro, con protocolos que proveen integridad, confiabilidad, autenticación entre sus principales características.

La carga tomada en cuenta para la transmisión es ahora más pesada de lo común; es decir, un paquete de voz encriptado lleva ahora doble cabecera aunque se puede aligerar la carga utilizando los campos estrictamente necesarios, reduciendo así la latencia al mínimo. Además, el sistema de prioridades que brindan los protocolos utilizados por las VPNs permiten asignar prioridades sobre ciertos paquetes designados por el administrador.

Las ventajas que se obtienen al utilizar una VPN para el servicio de VoIP son:

- Comunicación segura desde el momento que se pretende establecer una comunicación hasta el momento del cierre de la misma.
- Ahorro en el cargo de llamadas dentro de la compañía, independientemente del lugar geográfico que se encuentren los terminales comunicados.
- La conectividad esta limitada a una conexión de Internet independientemente si se usa o no un ISP en cuyo caso seria una conexión de acceso remoto.

Así mismo, la comunicación de voz utilizando una VPN introduce ciertos retardos. En si este sería la única desventaja de utilizar una VPN para estos propósitos, debido a que la carga se volvería un tanto más pesada. El presente proyecto esta encaminado a suplir esta deficiencia, optimizando la configuración tanto de los equipos como del software a utilizar.

BIBLIOGRAFIA - CAPITULO 1

[1] RFC 2764, A framework for IP Based Virtual Private Networks, B. Gleeson A. Lin, J. Heinanen, Telia Finland, G. Armitage, A. Malis; Febrero 2000

[2] MURHAMMER Martin W, “A guide to virtual Private Networks”, Editorial Prentice Hall PTR, 1998.

[3] OLIVIER Victor, Different Flavours of VPN: Technology and Applications, http://www.ja.net/documents/services/mcas/different-flavours-of-vpn-web.pdf

[4] URL: http://www.textoscientificos.com/criptografia/privada

[5] URL: http://www.kriptopolis.org/

[6] URL: http://es.wikipedia.org/wiki/Data_Encryption_Standard

[7] ANGEL José de Jesús, Advanced Encription Standard, http://computacion.cs.cinvestav.mx/~jjangel/aes/AES_v2005_jjaa.pdf

[8] URL: http://tools.ietf.org/html/rfc4309 Using Advanced Encryption Standard (AES) CCM

[9] RFC 4301, Security Architecture for the Internet Protocol, S. Kent, K. Seo; Diciembre 2005

[10] URL: http://seguridad.internet2.ulsa.mx/congresos/2001/cudi2/tutorial_ipsec.pdf

[11] RFC 4302, IP Authentication Header**,** S. Kent, Diciembre 2005

[12] RFC 4303, IP Encapsulating Security Payload (ESP)**,** S. Kent, December 2005

[13] RFC 4306, **Internet Key Exchange (IKEv2) Protocol,** C. Kaufman, Diciembre 2005

[14] URL: http://es.wikipedia.org/wiki/Diffie-Hellman

[15] URL: www.voipforo.com

[16] VoIP no es Telefonía IP (iptel), http://www.uberbin.net/archivos/rants/voip-no-es-telefonia-ip.php

[17] FLANNAGAN Michael, CCNA, CCDA, CISCO QoS Administering IP networks, Syngpress Publishing, 2001.

[18] ITU T H.323, Sistemas de comunicación multimedios basados en paquetes, Febrero 1998.

[19] Huidobro José Manuel, H.323 Multimedia sobre redes IP, http://www.coit.es/publicac/publbit/bit109/quees.htm

[20] RFC 3261, *Session Initiation Protocol (SIP)*, J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler; Junio 2002

[21] Nuevas Tecnologías De Conmutación De Voz Sobre Datos, Valero Dario, Universidad Bicentenaria de Aragua, Diciembre 1998, Maracay – Venezuela

[22] Voz sobre Frame Relay, Gustavo Salvuci, http://www.monografias.com/trabajos12/framerelay/framerelay.shtml

[23] URL: http://isis.faces.ula.ve/COMPUTACION/Internet/VoIP/atm.htm

CAPÍTULO 2

2 DISEÑO DE RED PRIVADA VIRTUAL

Las redes privadas virtuales ofrecen una alternativa segura para la interconexión de redes a través de Internet utilizando lo que se conoce como un túnel VPN. Este permite que la información viaje de manera segura por un medio abierto de forma encriptada, ilegible para todos excepto para el destinatario.

Esta característica abre una alternativa para empresas que requieren transportar su información con seguridad, mientras permiten a usuarios de otras localidades, geográficamente separadas, acceder de forma segura a la red LAN de la empresa. Cualquier tipo de aplicación que se tenga en una Intranet podrá ser accedida por medio de esta alternativa. Por ejemplo, acceder remotamente a los recursos de la red, a un servidor de bases de datos, compartir documentos, impresoras y, en el presente caso, brindar el servicio de VoIP.

Para el desarrollo del Capítulo 2 se considera un ambiente empresarial típico conformado por una oficina matriz y una oficina sucursal, en Quito y Guayaquil respectivamente, como se aprecia en la Figura 2-1, considerado además el acceso por parte de usuarios remotos.

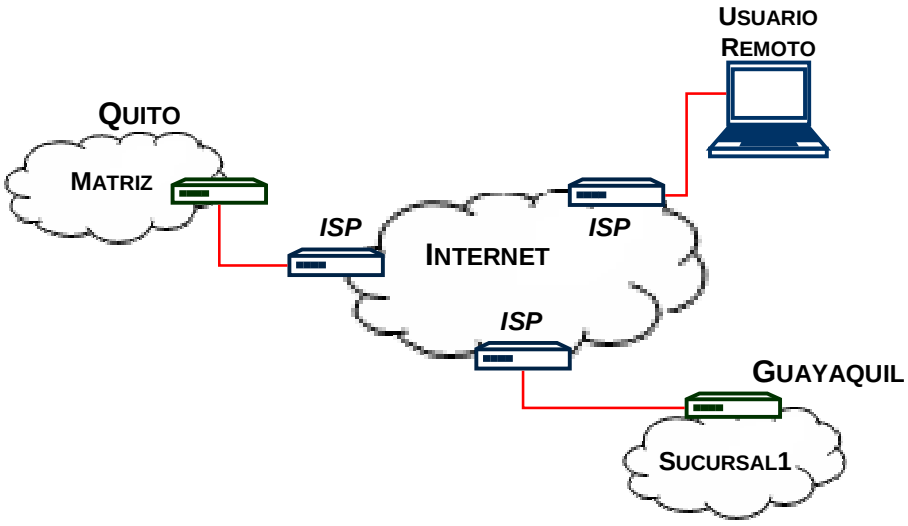


Figura 2-1 Esquema General De Red Empresarial Propuesto

El propósito del Capítulo 2 es definir pautas, tanto técnicas como legales, para realizar un túnel VPN a través de una nube WAN, formada por varios ruteadores interconectados entre sí, simulando el ambiente de Internet.

La red diseñada prestará servicios de seguridad, integridad, confidencialidad y autenticación, para las comunicaciones telefónicas entre la oficina matriz y las sucursales, además de brindar la comodidad de acceso a clientes remotos ubicados en diferentes localidades fuera de las dependencias de la empresa; es decir, fuera de la oficina matriz o la oficina sucursal.

2.1 DESCRIPCIÓN DEL ESCENARIO [1]

Una VPN puede ser construida en diferentes escenarios como: Internet VPN, Intranet VPN y Extranet VPN. En el caso de una Intranet VPN se crea un canal de comunicaciones privado sobre las redes abiertas de Internet. Este tipo de VPN cumple con las siguientes funciones:

- Brindar conectividad a oficinas remotas a través de Internet.
- Brindar conectividad remota a usuarios dial up a través de un ISP.

En una Intranet VPN se habilita un canal de comunicaciones privado sobre la infraestructura de la red LAN de una empresa, entidad bancaria, campus universitario, etc. Se utiliza una Intranet VPN para brindar acceso seguro a información privilegiada y a sitios confidenciales dentro de la empresa o entidad.

Por otra parte, en una Extranet VPN se maneja un canal de comunicaciones privado entre dos o más sitios separados. Esto implica transmisión de datos a través de un enlace WAN, como Internet. Se utiliza una Extranet VPN para comunicar la red de una entidad con redes de clientes o entidades afines.

2.1.1 REQUISITOS

El presente proyecto esta encaminado a crear una conexión entre la oficina Matriz de una empresa genérica, en Quito, con su respectiva oficina sucursal, en Guayaquil; por lo tanto, la información a transmitir será siempre concerniente a la misma empresa. Este es un ambiente de trabajo asociado a una Intranet VPN que cumple con relacionar dependencias u oficinas remotas de la misma entidad.

Entre las empresas que podrían tener una infraestructura como la que aquí se cita, se destacan: cadenas de supermercados, de farmacias, universidades como la Universidad Técnica Particular de Loja, etc. y todas aquellas entidades que mantienen oficinas sucursales y empleados que requieran trabajar remotamente.

Se utiliza para el presente proyecto información suministrada por la empresa SONDA del Ecuador S.A., aunque de manera parcial. Esto debido a que la empresa no cuenta con otros datos que también se requieren para el presente trabajo como: información relacionada con la PBX local, así como de la ocupación de las extensiones existentes en términos de tiempo y demanda. Por lo mismo, la

información proporcionada está limitada al número de usuarios de la central PBX existente.

SONDA se dedica a la venta de equipos y suministros informáticos, computadoras, impresoras y accesorios, así como también brinda servicios de mantenimiento y monitoreo de redes. La oficina sucursal en Guayaquil se encarga, eventualmente, de proveer y suministrar inventario faltante a la oficina matriz en Quito. Para ello se necesita coordinar el trabajo entre sus empleados, tanto en Quito como en Guayaquil. Obviamente, la oficina sucursal está subordinada a la oficina matriz por lo que las comunicaciones entre los ejecutivos y empleados de ambas oficinas son habituales.

SONDA cuenta además con empleados que laboran permanentemente en dependencias de empresas en las que se brinda asistencia o servicios afines, además de empleados que realizan labores concernientes a visitas técnicas dentro y fuera de la ciudad; de igual manera, otros que llevan a cabo visitas concernientes al área de ventas. Para llevar a cabo estas funciones los empleados necesitan mantener contacto con las oficinas respectivas tanto en Quito como en Guayaquil.

El tráfico telefónico a cruzar será únicamente entre las extensiones pertenecientes a la empresa; es decir, entre terminales tanto de Quito como de Guayaquil y eventualmente con empleados remotos debidamente autorizados relacionados de igual manera.

2.1.1.1 Descripción de la red en la oficina Matriz [2]

SONDA, por ser una empresa plenamente en plena actividad, que presta servicios de planificación y monitores de redes, debería contar con un esquema LAN como se muestra en la Figura 2-2. Éste esquema se denomina de 3 capas.

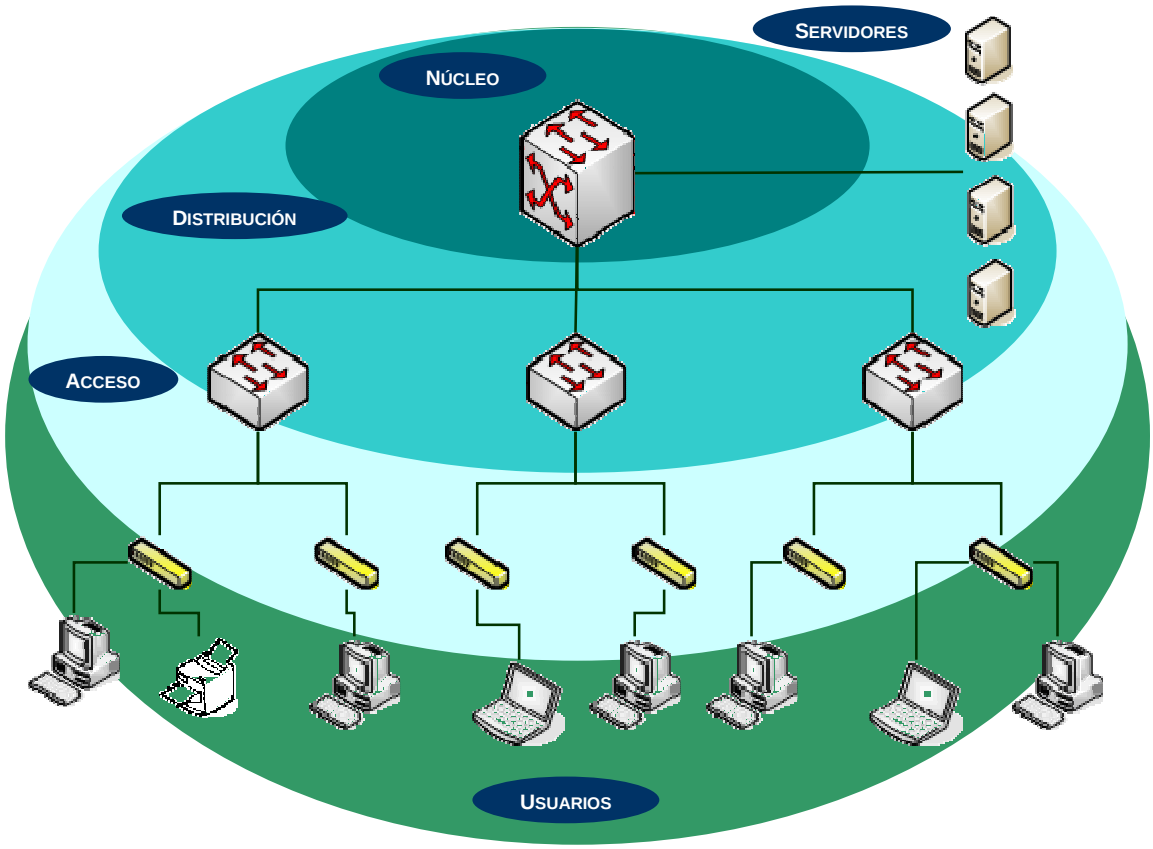


Figura 2-2 Diagrama De Red De La Oficina Matriz.

En resumen, la capa de acceso proporciona a los usuarios de grupos de trabajo acceso a la red. La capa de distribución por otro lado brinda conectividad a los usuarios basada en políticas, mientras que la capa núcleo denominada también backbone proporciona transporte óptimo entre sitios.

Los switches de la capa de acceso operan en la Capa 2 del modelo OSI y ofrecen servicios como el de asociación de VLAN. El principal propósito de un switch de capa de acceso es permitir a los usuarios finales el acceso a la red. Un switch de capa de acceso debe proporcionar esta funcionalidad con bajo costo y una alta densidad de puerto acorde al número de usuarios que se tengan proyectados. En los switches de acceso es donde se conectaran los teléfonos IP o softphones que funcionan sobre PCs.

El switch de la capa de distribución es un punto en el cual se encuentra limitado el dominio de broadcast. Se pueden aplicar políticas de seguridad a través de listas de control de acceso que se encargan de filtrar paquetes. La capa de distribución aísla los problemas de red dentro de los grupos de trabajo en los cuales se producen. La capa de distribución también evita que estos problemas afecten la capa núcleo. La capa de distribución combina el tráfico VLAN y es un punto focal para las políticas empresariales sobre flujo de tráfico. Por estas razones, los switches de la capa de distribución operan tanto en la Capa 2 como en la Capa 3 del modelo OSI. Los switches en esta capa se conocen como switches multicapa.

Sonda es una empresa que cuenta con departamentos Financiero, Administrativo, Técnico y de Ventas. Para ello cuenta con VLANs y políticas que van de acuerdo a cada área de trabajo, dando una mejor administración y servicios a los usuarios de la red.

La capa núcleo es un backbone de conmutación de alta velocidad. Esta capa no debería realizar ninguna manipulación de paquetes. La manipulación de paquetes, como por ejemplo el filtrado mediante listas de acceso, hace que la conmutación de paquetes se vuelva lenta. Una infraestructura central con rutas alternadas redundantes ofrece estabilidad a la red en caso de que se produzca una única falla en un dispositivo. Esto garantiza a los usuarios el acceso permanente a los servidores que dispone la empresa.

En la oficina Matriz funciona actualmente una red LAN que permite a todos sus usuarios una conexión a Internet. La oficina matriz cuenta con un número de 70 usuarios que mantienen extensiones telefónicas activas, y que a su vez requieren acceso telefónico con las extensiones de la oficina sucursal en Guayaquil.

Los usuarios en la red LAN de la oficina matriz requieren mantener los siguientes servicios o aplicaciones:

- ✓ Correo Electrónico.
- ✓ Descarga de archivos.
- ✓ Navegación Web.
- ✓ Acceso a bases de datos.

Los servidores deben ir lo más próximo a la capa núcleo. Esto permite a los usuarios el rápido acceso a los servicios mencionados anteriormente. El servidor de telefonía IP se conectará a esta capa.

2.1.1.2 Descripción de la red de la Oficina Sucursal

SONDA cuenta en Guayaquil con una red LAN como se muestra en la Figura 2-3. Esta red cuenta con menor número de usuarios y menor requerimiento de recursos de red, por lo que utiliza un esquema reducido de 2 capas, acceso y distribución. En este caso la capa de distribución realiza las funciones de la capa núcleo.

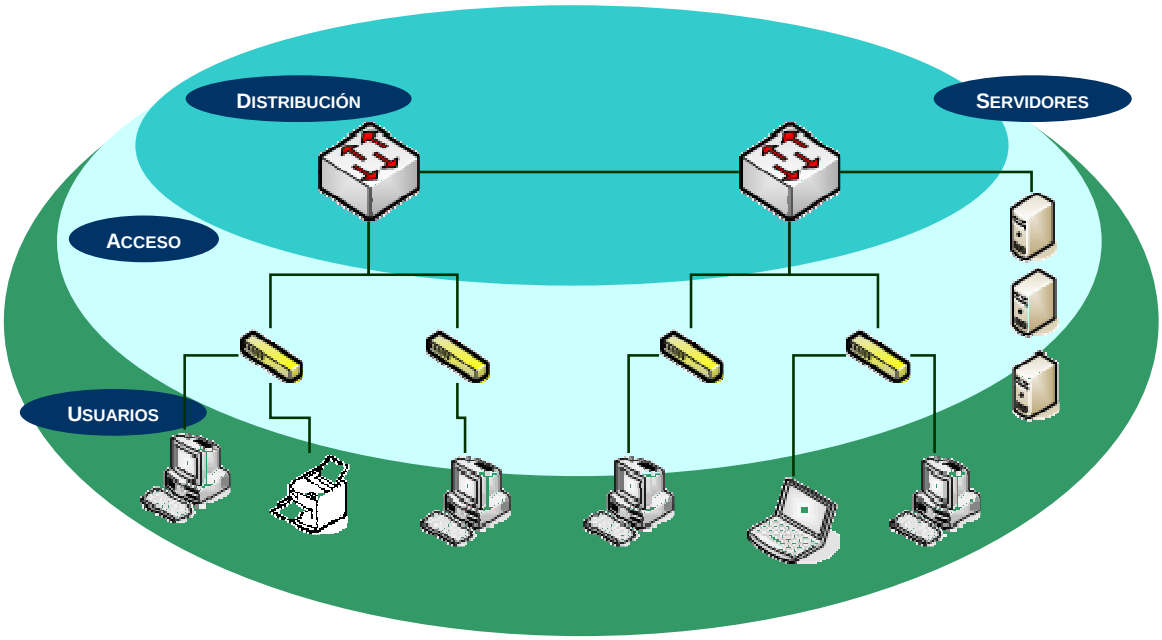


Figura 2-3 Diagrama De Red Sucursal

Los usuarios en esta dependencia mantienen los mismos servicios que los usuarios en la oficina matriz, a saber:

- ✓ Correo Electrónico.
- ✓ Descarga de archivos.
- ✓ Navegación Web.
- ✓ Acceso bases de datos.

En el caso de la oficina sucursal se cuenta con un total de 23 extensiones. De igual manera, las extensiones en esta dependencia tendrán acceso a las extensiones en la oficina matriz.

2.1.1.3 Acceso Remoto

A nivel empresarial muchas compañías buscan expandir sus fronteras permitiendo que personal de la empresa se desplace fuera de los límites ya constituidos en términos comerciales, o simplemente, permitiéndoles flexibilidad en cuanto a su lugar de trabajo. SONDA cuenta con vendedores y empleados que trabajan fuera de sus dependencias más de la mitad del tiempo de trabajo.
En este caso se habilitará una extensión para cada usuario remoto, para ello la persona que haga uso de esta extensión deberá tener acceso a Internet.

Uno de los requisitos fundamentales es que la empresa cuente con un equipo con la capacidad de montaje y administración para redes VPN. Los equipos Cisco Systems se consideran para el diseño puesto que dentro de las telecomunicaciones y equipos de networking, Cisco ocupa un lugar privilegiado en el mercado a nivel mundial y presenta una gran variedad e información acerca de tecnologías y equipos. Adicionalmente, Cisco es una firma dedicada al desarrollo de tecnologías y equipos de comunicaciones, que cuenta con protocolos propietarios.

2.1.2 ESCENARIOS VPN [1]

De acuerdo con los requisitos planteados se proponen las siguientes soluciones VPN.

2.1.2.1 Intranet VPN Sitio A Sitio

En este esquema se puede acceder a los recursos de una red LAN desde otra. En este caso se permitirá el acceso de las terminales de Quito y Guayaquil indistintamente de donde se origine la llamada.

En la Figura 2-4 se muestra un ejemplo de una conexión de tipo sitio a sitio. Como se aprecia, es una conexión independiente de la distancia entre cada una de las redes.

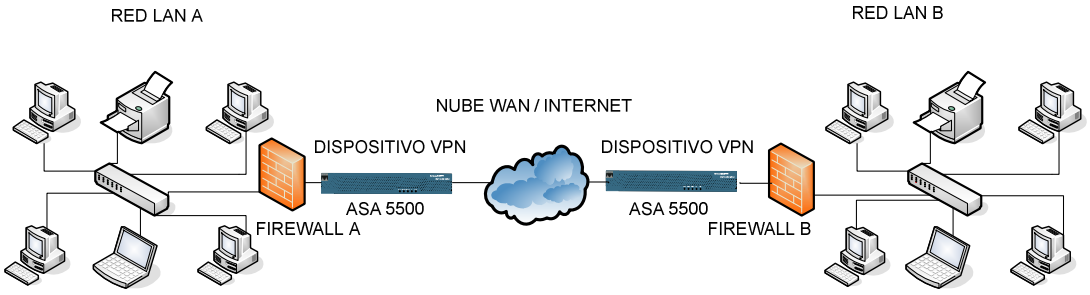


Figura 2-4 Conexión Sitio A Sitio

Para este tipo de escenario se plantea el uso de 2 equipos de borde, que soportarán el túnel VPN. Un equipo ubicado en Quito y otro en Guayaquil, en ellos se configuraran los comandos necesarios para poder procesar y transmitir información encriptada, previo a la autenticación y acreditación del par respectivo. De esta manera, la red telefónica tendrá una administración centralizada ubicada en la oficina matriz en Quito porque contiene el mayor número de extensiones.

Las aplicaciones y servicios de otros empleados que no hagan uso del túnel VPN no se verán afectadas de ninguna manera en el momento en que el túnel empiece a operar. De esta manera se permite independencia al nuevo servicio IP del

normal desempeño de los otros servicios y aplicaciones en curso. Para cumplir esta finalidad se limita a los usuarios el acceso al túnel mediante listas de acceso permitiendo el uso únicamente a los usuarios que transmiten paquetes VoIP.

2.1.2.2 Acceso Remoto

En este escenario se tendrá un servidor VPN en el equipo de frontera, en este caso el usuario remoto se autenticará en el equipo en Quito que le permitirá acceso a cualquier terminal en la red tanto en Quito como Guayaquil. Además se dispondrá de un software aplicativo de CISCO para clientes VPN instalado en la respectiva PC de cada usuario remoto.

En este tipo de esquema, una máquina remota tendrá acceso a los recursos de una red a través de un túnel y podrá realizar llamadas telefónicas con los usuarios de la red. Para realizar una llamada tendrá que estar autorizado por el servidor Asterisk que controla las extensiones dentro de la matriz y las sucursales, pero previamente deberá ser identificado y autorizado por el equipo responsable de la administración del túnel VPN.

Un ejemplo de este escenario se muestra en la Figura 2-5, en que el cliente accede a la red a través de un ISP:

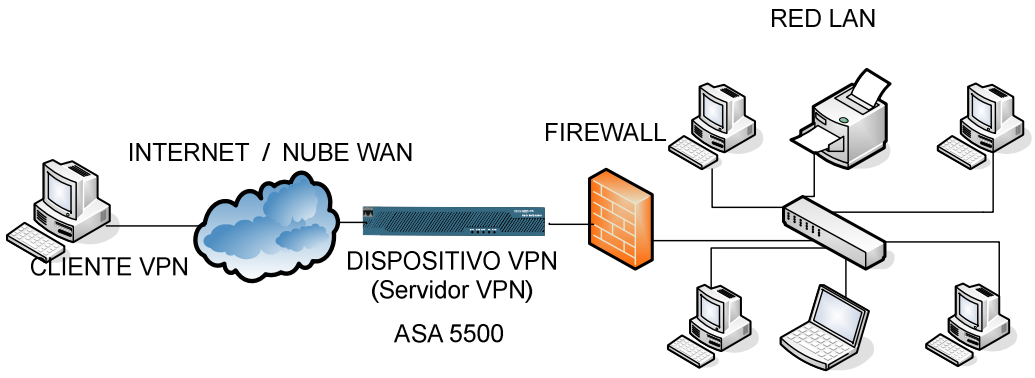


Figura 2-5 Acceso Remoto

2.2 DISEÑO DE LA VPN

Para el diseño de la VPN se deben cumplirse con ciertos pasos los mismos que se describen a continuación.

2.2.1 ASIGNACIÓN DE DIRECCIONES [1]

El direccionamiento de las redes LAN internas se realiza de acuerdo a la norma RFC 1918[12]. Se indica el rango de direcciones privadas en la Tabla 2-1.

CLASE	DESDE	HASTA	BITS DE RED	BITS DE HOST
A	**10.0.0.0**	**10.255.255.255**	**8**	24
B	**172.16.0.0**	**172.31.255.255**	**16**	16
C	192.168.0.0	192.168.255.255	24	8

Tabla 2-1 Direcciones Privadas.

Cuando se utiliza direcciones IP privadas no es posible conectase directamente a Internet por lo que se necesita la traducción de direcciones de red (NAT) con una dirección pública enrutable.

El rápido crecimiento de la Internet ha sorprendido a la mayoría de los observadores. Una de las razones por las que Internet ha crecido tan rápidamente es debido a la flexibilidad del diseño original. Sin el desarrollo de nuevas tecnologías de asignación de direcciones IP, el rápido crecimiento de Internet habría agotado la cantidad actual de direcciones IP. Para poder compensar esta falta de direcciones IP, se buscaron diferentes soluciones. Una solución ampliamente implementada, es la Traducción de direcciones de red.

[12] RFC 1918. Define los rangos de direcciones IP a utilizar en redes privadas.

NAT es un mecanismo para conservar direcciones IP registradas en las grandes redes y simplificar las tareas de administración de direccionamiento IP. Mientas se enruta un paquete a través de un dispositivo de red, por lo general un firewall o router fronterizo, la dirección IP fuente se traduce de una dirección de red interna privada a una dirección IP pública enrutable. Esto permite que se transporte el paquete a través de redes externas públicas como la Internet. La dirección pública de la respuesta se traduce de nuevo a la dirección interna privada para su entrega dentro de la red interna. Una variación de NAT, conocida como Traducción de direcciones de puerto (PAT), permite la traducción de muchas direcciones privadas internas con una sola dirección pública externa como se puede ver en la Figura 2-6.

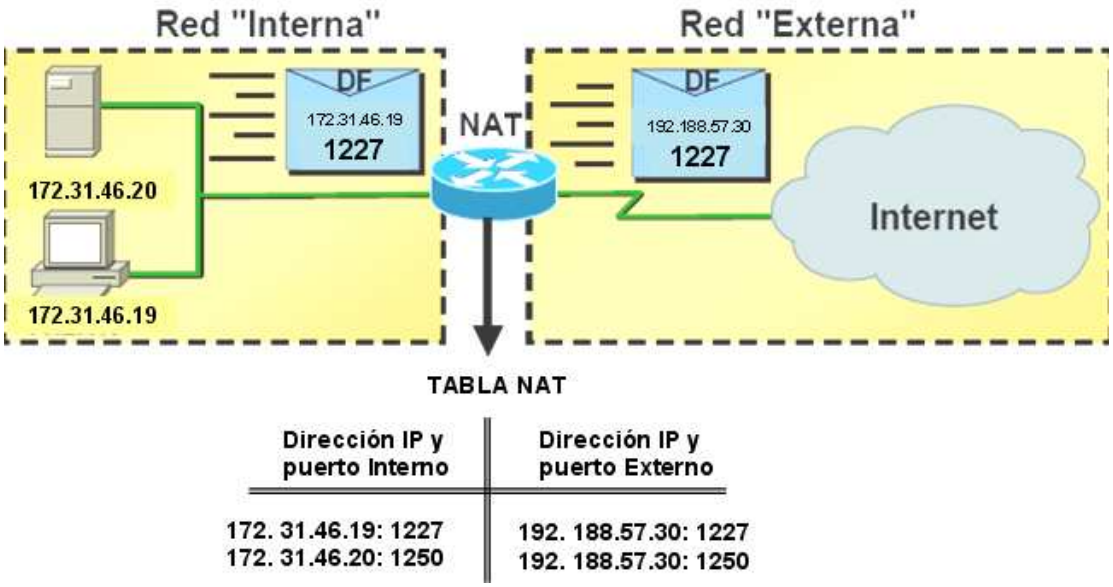


Figura 2-6 Proceso PAT Oficina Sucursal.

En la Tabla 2-2 se describe el esquema de direcciones IP que se utilizan en las respectivas redes LAN. Así mismo se describe la dirección que utilizan las direcciones IP privadas para comunicarse a Internet, en el caso en que no se encuentren conectadas a la red VPN.

RED	RANGO DE DIRECCIONES	TRADUCCIÓN DE DIRECCIONES	PUERTA DE ENLACE	MÁSCARA DE RED
MATRIZ	192.188.57.242 hasta 192.188.57.254	-	192.188.57.241	255.255.255.240
SUCURSAL	172.31.46.2 hasta 172.31.46.63	192.188.57.30 /27	172.31.46.1	255.255.255.192

Tabla 2-2 Asignación De Direcciones.

Un usuario remoto estará sometido a un proceso de asignación dinámica de direcciones llevado a cabo por el equipo encargado de realizar la autenticación y control de acceso a la red, que en este caso se localizará en Quito, y tendrá una dirección en el rango de direcciones de la matriz.

2.2.2 PROTOCOLO PARA EL ESTABLECIMIENTO VPN [5] [6]

Existen algunos protocolos para el establecimiento de túneles VPN, como PPTP[13], L2F[14], L2TP[15], que funcionan en capa 2 del modelo de referencia OSI, y que permiten establecer conexiones remotas. Además existen protocolos como IPSec que también permite mantener sesiones remotas y que, a diferencia de los mencionados anteriormente, funciona en capa 3; paro lo mas importante, IPSec permite autenticar los paquetes mientras viajan por la red, a diferencia de los protocolos mencionados anteriormente que permiten autenticar los paquetes únicamente en los extremos del túnel.

Por lo tanto el protocolo que se utilizará para el túnel VPN es IPSec que permite brindar seguridad a nivel de capa 3, lo que significa que cada paquete IP se encapsula con una cabecera IPSec.

[13] PPTP, Point to Point Tunneling Protocol
[14] L2F, Layer 2 Forwarding
[15] L2TP, Layer 2 Tunneling Protocol

IPSec provee un mecanismo para brindar seguridad en la transmisión de datos, a través de redes IP, brindando confidencialidad, integridad y autenticación de datos para comunicaciones sobre redes no protegidas tal como es el Internet. IPSec para ambientes VPN se caracteriza por:

- ✓ *Confidencialidad de datos:* El dispositivo que envía los datos puede encriptar los paquetes antes de transmitir éstos a través de la red.
- ✓ *Integridad de los datos*: El dispositivo que recibe los datos puede autenticar el otro equipo (peer) y paquetes IPSec recibidos para asegurarse que los datos no han sido alterados durante la transmisión.
- ✓ *Autenticación del origen de los datos:* El dispositivo IPSec receptor puede autenticar la fuente de los paquetes IPSec que son enviados de forma independiente de la integridad de los datos; es decir, que se verifica el origen de los datos independientemente de la cantidad de errores.
- ✓ *Anti-Replay:* El dispositivo IPSec receptor puede detectar y rechazar paquetes repetidos ayudando a prevenir spoofing y ataques errados.

Por otra parte, los dispositivos de seguridad que se vayan a utilizar deberán soportar, además de IPSec, otros protocolos como:

- ✓ ESP (Encapsulation Security payload)
  Los dispositivos IPSec utilizan ESP para encapsular paquetes IP.
- ✓ IKE (Internet key Exchange)
  IKE es un protocolo híbrido que provee servicios útiles para IPSec como:
  - ➢ Autenticación de los pares IPSec
  - ➢ Negociación IKE y asociaciones de seguridad IPSec (SAs)
  - ➢ Establecimiento de llaves por algoritmos de encripción usados por IPSec

De igual manera se requiere de algoritmos criptográficos como:

- ✓ DES (Data Encryption Standard)

  DES es usado para encriptar y desencriptar paquetes de datos. DES es usado tanto por IPSec como por IKE.
- ✓ 3DES (TripleData Encryption Standard)

  3DES es una variación de DES y tiene tres llaves separadas. 3DES triplica la fuerza de encripción de DES; es decir, tiene una llave de 168 bits. 3DES es usado para encriptar y desencriptar el tráfico de datos.
- ✓ AES (Advanced Encryption Standard)

  AES provee mayor seguridad que DES y es más eficiente que 3DES.

  The National Institute of Standars for Technology (NIST) recientemente adoptó el nuevo algoritmo de encripción AES para reemplazar a DES en dispositivos criptográficos.
- ✓ DH (Deffie - Hellman)

  DH es un protocolo criptográfico de llaves públicas. Este permite dos partes para establecer una llave secreta compartida sobre un canal de comunicaciones inseguro.
- ✓ MD5 (Message Digest 5)

  MD5 es un algoritmo hash usado para autenticar paquetes de datos. Un hash es una forma de algoritmo de encripción que toma un mensaje de entrada de una longitud arbitraria y produce una variación de la longitud en el mensaje de salida.
- ✓ IKE y ESP usan MD5 para la autenticación.
- ✓ SHA (Secure Hash Algorithm-1)

  SHA es un algoritmo hash usado para autenticar paquetes de datos.

  IKE y ESP usan SHA-1 para la autenticación.

Se consideró para seguridad en este proyecto el uso del algoritmo de encripción AES, porque permite el uso de llaves de diferente tamaño, además porque ha demostrado ser mucho más eficiente que su predecesor DES. AES ha sido adoptado por organizaciones y entidades a nivel internacional y desde su

nacimiento no se conoce ningún ataque que haya podido burlar la seguridad que ofrece este algoritmo.

2.2.3 SELECCIÓN DE LOS EQUIPOS [7]

Para conseguir una conexión VPN se puede utilizar cualquiera de los routers indicados a continuación, cargados con la versión de IOS 12.2 o superior,

- ✓ Cisco 806, Cisco 826, Cisco 827, y Cisco 828 Routers.
- ✓ Cisco 1700 Series Routers.
- ✓ Cisco 2600 Series Routers.
- ✓ Cisco 3620 Router.
- ✓ Cisco 3640 Routes.
- ✓ Cisco 3660 Router.
- ✓ Cisco 7100 Series VPN Routers.
- ✓ Cisco 7200 Router.
- ✓ Cisco 7500 Series Routers.
- ✓ *Cisco 5500 Series ASA.*

Al momento de elegir uno u otro equipo se debe tomar en cuenta las aplicaciones previas que tiene la empresa, básicamente el acceso a Internet y la compartición de recursos con el fin de mantener la Intranet funcional, como venia operando previo a la implementación del túnel VPN; es decir, que la implementación del túnel sea transparente a los usuarios dentro de la LAN que no requieran de acceso a través del túnel VPN.

Para propósitos de prueba de la conexión VPN se utilizan dos equipos Cisco ASA (Adaptive Security Appliance) Serie 5500.

Los equipos ASA son firewalls con varias funciones y características, de las cuáles se consideran importantes para el presente proyecto las siguientes:

- ✓ Dispositivo para medianas y grandes empresas que brindan seguridad y aplicaciones VPN.
- ✓ Interfaces Giga ethernet10 / 100 / 1000 Mbps
- ✓ Soporte superior a 25 VLANs
- ✓ Soporta VPN sitio a sitio (LAN to LAN)
- ✓ Soporta VPN de Acceso Remoto
- ✓ Soporta WebVPN
- ✓ Virtual Firewalls

Para ver características y detalles del equipo ASA 5500 consultar el Anexo A, Características ASA 5500.

2.2.4 PASOS PARA ESTABLECER UNA SESIÓN VPN UTILIZANDO IPSEC [1]

Para establecer una comunicación telefónica, debe previamente establecerse un túnel VPN, que en el presente proyecto es un requisito de seguridad importante y necesario para acceder mediante una red pública, Internet. En una secuencia de cinco pasos, resumidos de acuerdo a los procedimientos que se van ejecutando, IPsec levanta él túnel VPN que servirá de enlace entre la oficina Matriz y la oficina Sucursal, o a su vez entre una oficina, ya sea Matriz o Sucursal, y un Usuario Remoto.

2.2.4.1 Definir el tráfico interesante

El tráfico se denomina interesante cuando el dispositivo VPN reconoce que el tráfico que se quiere enviar necesita ser protegido. En este caso se define como tráfico interesante a los paquetes de voz.

La manera de definir el tráfico interesante es por medio de listas de acceso, ya que de esta manera se habilitarán los puertos tanto TCP como UDP que sean

necesarios para la transmisión de voz y, de ser necesario, algún otro puerto que necesite de encripción. A pesar de que el protocolo ICMP no necesita ser encriptado, se requiere para probar conectividad, por lo que se habilitaría como tráfico interesante, aunque temporalmente.

Los puertos que no se vayan a utilizar deben ser bloqueados de tal manera que el tráfico que pase a través del túnel sea exclusivamente el que requiere ser encriptado y autenticado.

Políticas empresariales son las que definen que tráfico necesita ser protegido y cuál tráfico debe ser enviado en forma plana; es decir, sin la necesidad de encriptar.

Como se puede apreciar en la Figura 2-7, los usuarios de la Intranet pueden comunicarse con los usuarios de la Intranet asociada a través del túnel VPN, o pueden, simplemente, navegar por la Internet para lo cual no es necesario acceder al túnel VPN. El control de acceso al túnel se realiza en el equipo de borde y es aquí donde se identifica el tráfico interesante y se conduce por el túnel VPN, mientras que el tráfico no interesante se desplaza abiertamente por la red pública.

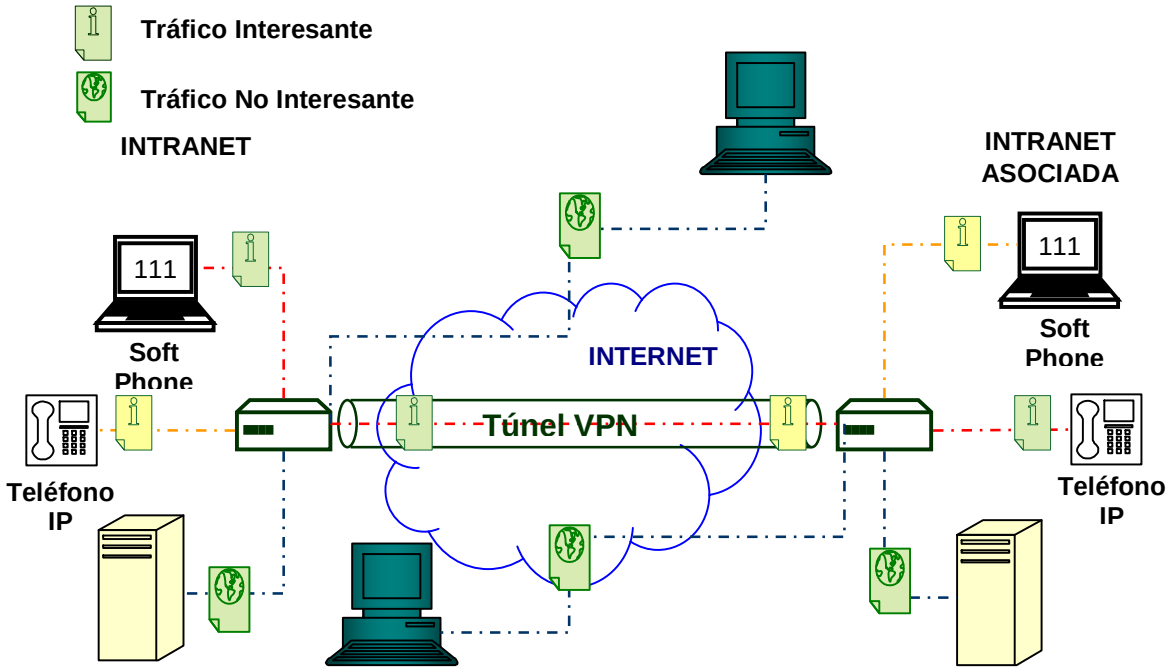


Figura 2-7 Enrutamiento del Tráfico Interesante

2.2.4.2 Establecimiento de la conexión

En esta fase se establece la conexión entre los extremos del túnel. Para el establecimiento de la conexión se necesita una configuración básica de servicios de seguridad que son negociados y acordados previamente entre los pares (peers) de la VPN. Estos servicios de seguridad protegen todas las subsecuentes comunicaciones entre los pares.

Para este proyecto se utilizará el protocolo IKE para el establecimiento de la conexión, para ello se dice que IKE actúa en dos fases. El propósito básico de IKE fase 1 es negociar políticas de configuración IKE (algoritmo de encripción, de autenticación, tiempo de vida del túnel), autenticación de los pares y configurar un canal seguro entre los mismos.

2.2.4.3 Establecimiento de las Políticas de Seguridad

Las políticas de seguridad se establecen para definir el grado de seguridad que se debe brindar a los datos a transmitir. Empieza por discriminar entre los datos que

necesitan seguridad y los que no; por ejemplo, al momento de definir el tráfico interesante, que es cuando se define el tipo de paquetes que requieren seguridad, y una vez definido el tráfico interesante se define que parámetros son necesarios para cumplir los requisitos de seguridad impuestos por la empresa.

Las políticas de seguridad se establecen en la segunda fase de IKE. El propósito en ésta fase de IKE es negociar los parámetros de seguridad de IPSec que son usados para asegurar el túnel VPN.

IKE fase 2 cumple con las siguientes funciones:

- ✓ Negociar parámetros de seguridad IPSec.
- ✓ Establecer Asociación de seguridad IPSec
- ✓ Periódicamente renegocia asociaciones de seguridad para IPSec de esta manera cumple con aspectos de seguridad como integridad confidencialidad, etc.
- ✓ Opcionalmente mantiene un intercambio DH.

2.2.4.4 Transmisión de datos

Una vez negociadas las políticas de seguridad; es decir, luego de que la segunda fase de IKE ha sido completada, se establece una sesión IPSec para lo cual se establecen asociaciones de seguridad IPSec. El tráfico se intercambia entre los host de las diferentes redes a través de un túnel seguro. El tráfico interesante es encriptado y desencriptado de acuerdo con los servicios de seguridad especificados en el IPSec SA.

2.2.4.5 Terminación de la conexión

Una vez realizada la comunicación la sesión del túnel puede darse por terminada por las siguientes razones:

- ✓ Cuando el tiempo de la conexión Lifetime configurado en los parámetros SA llega a su fin.
- ✓ Si el contador de paquetes es excedido.
- ✓ Cuando el IPSec SA es removido.

2.3 DIMENSIONAMIENTO DEL CANAL TELEFÓNICO

2.3.1 ANÁLISIS DEL TRÁFICO TELEFÓNICO [6] [7]

El tráfico telefónico se asocia al concepto de ocupación. Se dice que un circuito telefónico esta cursando tráfico cuando esta ocupado, nunca si esta libre. El tráfico telefónico es medible en términos de tiempo, entiéndase como tiempo de ocupación, y depende del número de comunicaciones y de la duración de las mismas. Algunas empresas o entidades limitan el tiempo de ocupación de sus extensiones cuando la llamada se genera desde terminales en la red privada hacia la red pública. Se aplica este concepto en el diseño de la red debido a que es necesario rentar ancho de banda para cumplir con el servicio en mención.

Para la determinación del tráfico la ITU[16] establece la realización de mediciones durante un período de cinco a diez días, con una demanda de quince minutos. Del análisis estadístico de las mediciones debe surgir el valor correspondiente tanto a la hora cargada como de los cuartos de hora que posean el mayor tráfico. EL concepto de hora cargada se creó debido a que el comportamiento del tráfico no presenta el mismo volumen durante el transcurso del día pero puede ser representativo a ciertas horas.

Debido a la falta de información pertinente por parte de la empresa; es decir, estadísticas del tiempo de ocupación de las extensiones, se realiza un ejemplo de cálculo asumiendo un *tiempo medio de ocupación* de 2 minutos por llamada.

[16] ITU, International Telecomunication Union

También se debe considerar el *número de ocupaciones* de las extensiones en la hora pico, que en promedio cada extensión ocupa 5 veces la línea para comunicarse a la sucursal desde la matriz o viceversa.

Las consideraciones anteriores se realizan tomando en cuenta que estadísticamente el 80% del tráfico en una red es interno y el 20% externo, regla conocida como 80-20. Dicho de otra manera, gran mayoría de las llamadas entre empleados, tanto de la matriz como de la sucursal, se llevan a cabo dentro de las dependencias, bien dentro de la matriz o bien dentro de la sucursal, mientras que el tráfico restante se cruza hacia la sucursal desde la matriz o viceversa.

Se tiene entonces, para un abonado promedio, la Ecuación 2-1.

$$A = c_A t_m \qquad \textbf{Ecuación 2-1}$$

donde:

t_m representa el tiempo medio de ocupación de una línea de salida,

c_A es el número de ocupaciones ofrecidas por término medio en la unidad de tiempo. En este caso corresponde a 5 ocupaciones durante una hora:

$$c_A = \frac{5}{3600} \qquad \textbf{Ecuación 2-2}$$

Reemplazando C_A en la Ecuación 2-1:

$$A = \frac{5}{3600} 120 \qquad \textbf{Ecuación 2-3}$$

A_i = 0,17 Erlangs**,**

donde **A_i** representa la cantidad de tráfico en Erlangs en promedio para cada terminal telefónica.

Para un total de 93 usuarios:

A = 93 * 0,17

A = 15,81 Erlangs

Gran parte de las centrales telefónicas están construidas bajo el *sistema de pérdida*. En los sistemas de pérdida**,** mostrado en la Figura 2-8, el abonado que solicita una comunicación y encuentra congestión; es decir, falta de enlaces libres en la red, recibe tono de ocupado.

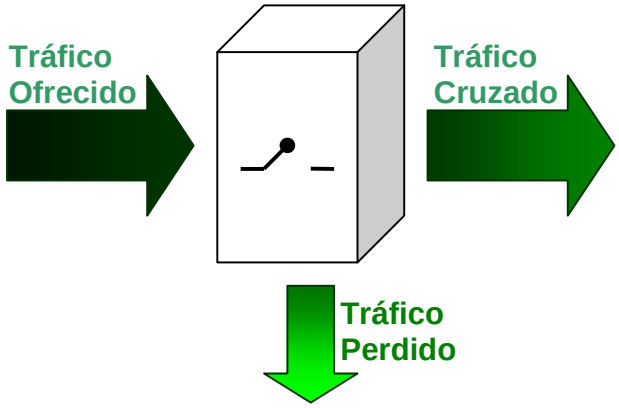


Figura 2-8 Sistema De Pérdidas

Si se considera un porcentaje de pérdida del 10%, 10 de cada 100 llamadas no se podrán cruzar en la hora pico, y recurriendo a las tablas de Erlang, en el sitio http://www.erlang.com/calculator/erlb, se determina que se requieren de 19 líneas o canales para cruzar el tráfico calculado, 15.81 Erlangs. Como se puede apreciar en la Figura 2-9, para calcular el número de líneas se requiere el valor total del tráfico a cruzar, BHT (Erl.), además del porcentaje de bloqueo de llamadas, de 0 a 1, en este caso 0.1.

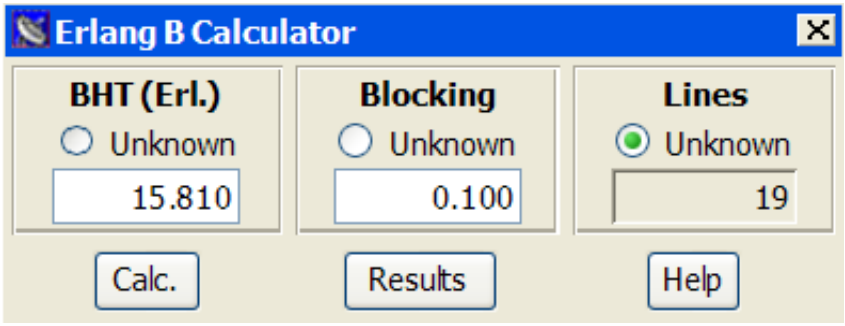


Figura 2-9 Calculadora Erlang B.

De acuerdo con los cálculos realizados, la red tendría un comportamiento caracterizado en la Tabla 2-3.

Número de abonados	**93**
Tiempo medio de ocupación en la hora pico por extensión	**600 segundos**
Volumen de tráfico de la red en la hora pico	**55800 segundos**
Intensidad de Tráfico total	**15,81 Erlangs**
Probabilidad de Perdida	**10 %**
Número de canales estimado**	**19 canales**

Tabla 2-3 Consideraciones De Tráfico Telefónico

Dado que los datos en esta sección son estimados de declaraciones verbales por el administrador de la central PBX de la empresa SONDA, se debe considerar un proceso de medición del tráfico generado por las extensiones tanto en la matriz como en la sucursal, previa implementación de este sistema. Vale aclarar que el proceso de medición de tráfico no es parte del alcance del proyecto planteado.

2.3.2 ESTIMACIÓN DE ANCHO DE BANDA [8]

El ancho de banda requerido para una aplicación VoIP depende mucho del códec que se utilice. Existen algunas normas y estándares de compresión, caracterizados por el Mean Opinion Score (MOS) que es un valor con escala del 1 al 5, como se muestra en la Tabla 2-4. Este parámetro se utiliza para resaltar la calidad presente en un determinado códec, pero pese a que los diferentes códecs requieren de diferentes velocidades de transmisión, la calidad en términos de MOS no se ve considerablemente disminuida entre el de menor y mayor MOS. Por ejemplo, en el caso de G.711 el MOS indicado es de 4.1, mientras que para el caso de G.729 el MOS es de 3.92.

La principal diferencia está en las capacidades de transmisión requeridas en los diferentes códecs; en el caso de G.711 se requiere de 64 Kbps, en tanto que para G.729 se requiere una capacidad de 8 Kbps, Para hacer un mejor uso del ancho de banda se considera el estándar G.729 como norma para este proyecto, que por una parte ofrece un MOS bastante aceptable y por otra disminuye considerablemente los requerimientos de ancho de banda para una aplicación VoIP.

NOMBRE	ESTANDARIZADO	DESCRIPCIÓN	BIT RATE (KB/S)	FRAME SIZE (MS)	MOS (MEAN OPINION SCORE)
G.711	ITU-T	Pulse code modulation (PCM), Ley A y Ley μ	**64**	Muestreada	**4.1**
G.722	ITU-T	7 kHz audio-coding within 64 kbit/s	**64**	Muestreada	**-**
G.723	ITU-T	Extensión de la norma G.721 a 24 y 40 kbit/s para aplicaciones	**24/40**	Muestreada	**-**
G.723.1	ITU-T	Dual rate speech coderFor multimedia Communications transmitting at 5.3 and 6.3 kbit/s	**5.6/6.3**	30	**3.8-3.9**
G.726	ITU-T	40, 32, 24, 16 kbit/s adaptive differential pulse code modulation	**16/24/32/40**	Muestreada	**3.85**

Nombre	Estandarizado	Descripción	Bit rate (kb/s)	Frame size (ms)	MOS (Mean Opinion Score)
		(ADPCM)			
G.728	ITU-T	Coding of speech at 16 kbit/s using low-delay code excited linear prediction	**16**	2.5	**3.61**
G.729	ITU-T	Coding of speech at 8 kbit/s using conjugate-structure lgebraic-code-excited linear-prediction (CS-ACELP)	**8**	10	**3.92**
GSM	**ETSI**	**RegularPulse Excitation LongTerm Predictor (RPE-LTP)**	**13**	**22.5**	**-**

Tabla 2-4 Códecs que soporta Asterisk

Una vez escogido el códec a utilizar, se procede a calcular el ancho de banda requerido para un canal de voz. En esta parte se tiene que considerar los protocolos que intervienen en la transmisión de un paquete de voz. A saber:

- ✓ Cabecera UDP y RTP, que en conjunto suman 20 bytes (8 bytes UDP y 12 bytes RTP). Cabe recalcar que SIP, protocolo utilizado para señalización de voz, se ubica dentro de RTP.
- ✓ Cabecera IP, que tiene un tamaño de 20 bytes.
- ✓ Cabecera IPsec., de acuerdo al protocolo que se utilice, ESP o AH.
- ✓ Protocolo de capa 2, que puede ser PPP.

En la Figura 2-10 se puede observar el proceso de encapsulado para una aplicación VoIP.

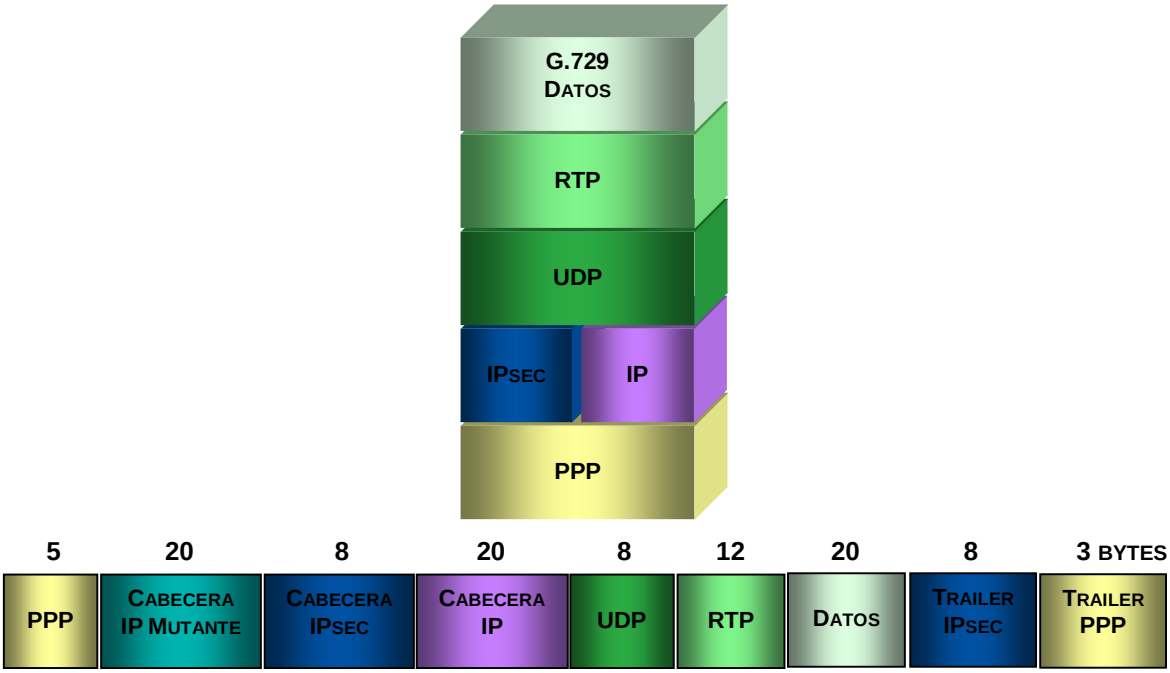


Figura 2-10 Proceso De Encapsulamiento VoIP

Considerando que un códec G.729 transmite paquetes de 20 bytes a una velocidad de 8 Kbps se calcula que transmite 50 paquetes por segundo (PPS), se tiene la Ecuación 2-2.

$$PPS = \frac{8kbps}{20bytes * 8bits}$$
$$PPS = 50$$

Ecuación 2-4

Entonces para realizar una transmisión de 50 paquetes por segundo se calcula el ancho de banda, considerando las cabeceras y trailers de los protocolos que intervienen en el proceso de encapsulamiento:

$$20\ bytes\ Datos$$
$$84\ bytes\ Cabecera\ y\ Trailers$$
$$AB(Kbps) = 104\ bytes * 8\ bits * 50\ PPS$$
$$AB(Kbps) = 41.600\ bps$$
$$AB = 41{,}6\ Kbps$$

Ecuación 2-5

El valor anteriormente calculado representa el ancho de banda que debe tener un canal VoIP considerando los protocolos de seguridad y de encapsulamiento ya mencionados. Para cumplir con la demanda de 15.85 Erlangs, se requiere de 19 canales de 41.6 Kbps, que significa un ancho de banda de 790.4 Kbps.

El proceso de cálculo realizado anteriormente se puede aproximar con la ayuda de una calculadora de ancho de banda para aplicaciones VoIP en el sitio http://site.asteriskguide.com/bandcalc/bandcalc.php, en la que se puede aproximar el cálculo dependiendo del protocolo utilizado. Se puede así mismo estimar un ancho de banda de acuerdo al número de llamadas simultáneas. La Figura 2-11 muestra el cálculo utilizando una conexión VPN, se toma en cuenta al protocolo IPsec como herramienta de seguridad, además se elige PPP como protocolo de capa 2.

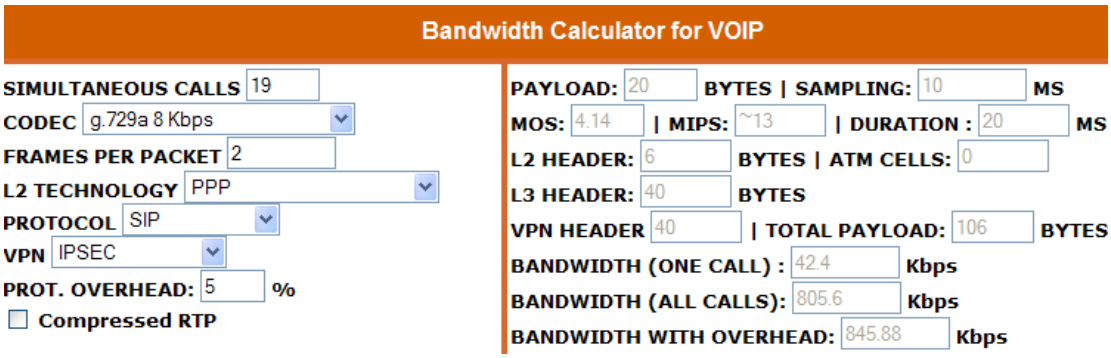


Figura 2-11 Calculadora De Ancho De Banda Para VoIP

Según la estimación de ancho de banda se deberá contratar con un proveedor de Internet, una conexión acorde a lo presupuestado que es de 1024 Kbps. Esta conexión se debe contratar tanto para la oficina matriz como para la sucursal.

SONDA es una empresa que ha alcanzado un nivel comercial que mantiene en competencia frente a otras empresas de propósitos similares. En este sentido la empresa maneja un número 10 de extensiones disponibles en caso de necesitarse en ciertas áreas o departamentos. Un ancho de banda de 1024 Kbps admite 5

canales adicionales, que a su vez permitirán el uso adicional de 10 extensiones más.

Es importante resaltar que mientras se tenga un excedente de ancho de banda se tendrá un menor porcentaje de pérdidas al inicialmente considerado, mientras que al acercarse o exceder al numero de abonados, la posibilidad de pérdida será aún mayor.

Existen otras herramientas para estimar ancho de banda para aplicaciones de Telefonía IP. Se puede recurrir a la página de Erlang, www.erlang.com/calculator, pero en este caso esta aplicación no pemite estimar un ancho de banda que incluya otro tipo de protocolos además de IP/UDP/RTP. Se puede ver en la Figura 2-12 que para el códec G.729 considerando un tráfico de 15.85 Erlang, el ancho de banda calculado por esta herramienta es de 456 Kbps.

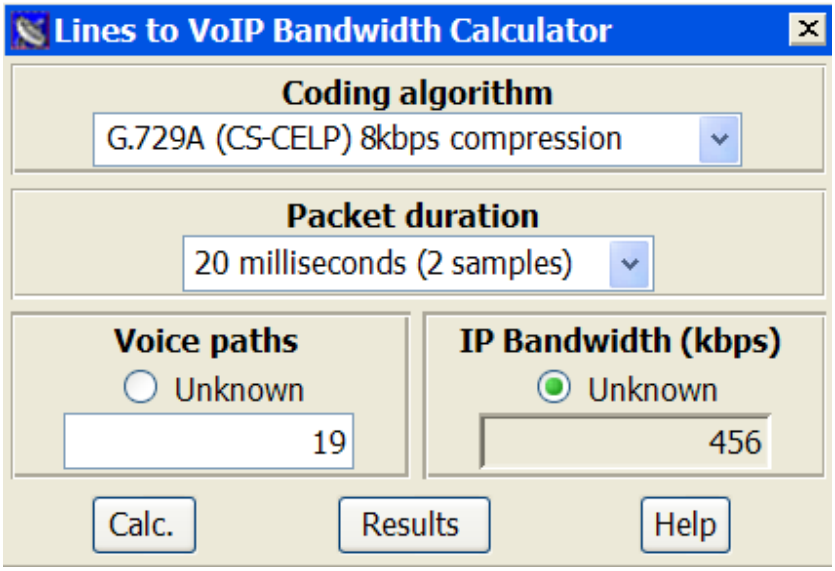


Figura 2-12 Calculadora Erlang VoIP

2.4 MARCO REGULATORIO VOIP [9]

El marco legal que rige a las telecomunicaciones en el país esta ligado, hasta la presente fecha, a la Ley de Telecomunicaciones Reformada y al Reglamento

General a la Ley Especial de Telecomunicaciones Reformada, cuyo ente encargado de vigilar el cumplimiento de dicha ley y del reglamento asociado es el Consejo Nacional de Telecomunicaciones (CONATEL).

En lo concerniente al tráfico de voz sobre Internet el CONATEL expone en la Resolución 491-21 del 8 de Septiembre del 2006 Regulaciones de VoIP Internas y Externas, que se puede apreciar en su totalidad en el Anexo B. En esta resolución se destaca el artículo cinco relacionado a la legalidad del uso y/o prestación del servicio en mención.

ARTICULO CINCO. *Ninguna persona natural o jurídica, incluyendo a los Proveedores de Servicio de Valor Agregado de Internet, podrán usar, dentro del territorio nacional, dispositivos de conmutación, tales como interfaces o compuertas (gateways) o similares, que permitan conectar las comunicaciones de Voz sobre Internet o las llamadas sobre Internet a las Redes Públicas de Telecomunicaciones del Ecuador.*
Se exceptúan de esta limitación a los operadores de telecomunicaciones debidamente autorizados.

De acuerdo con el artículo en mención, no es permitido cruzar comunicaciones de voz sobre Internet a través de redes públicas dentro del territorio nacional. Es por esto que el presente proyecto busca comunicar terminales telefónicas pertenecientes a una misma entidad a través de la Internet, para no contradecir de ninguna forma la norma legal establecida. En este caso, el tráfico cruzado se mantendrá dentro de la red de dicha entidad y la información que se cruce será de índole privada y exclusiva de sus miembros.

2.5 ADMINISTRACIÓN DE LA RED TELEFÓNICA EN UN ENTORNO LINUX. [10] [11]

La principal diferencia entre VoIP y Telefonía IP (IPtel, IP telephony) es el área de

cobertura que puede limitar uno u otro servicio. En el caso del servicio tradicional VoIP, la cobertura de una llamada no se limita a un espacio físico específico; es decir, que la llamada puede acceder a cualquier punto sobre el Internet. En éste caso se requerirá de una dirección IP pública, por lo que se considera a VoIP como una cobertura a nivel de WAN. Telefonía IP ocupa un campo más específico, que se podría considerar un servicio del tipo LAN. En esencia esta seria una de las principales diferencias con VoIP, pero en realidad la más importante es que Telefonía IP conlleva un manejo administrativo tanto de recursos como de usuarios más detallado y centralizado.

Con la aplicación de Telefonía IP sobre redes privadas virtuales es posible conectar a usuarios remotos a una red local, permitiendo de esta manera mantener una comunicación con la entidad central sin perder el control sobre los terminales remotamente conectados.

Existen herramientas creadas para soportar aplicaciones a nivel de Telefonía IP como Asterisk que, desarrollado por Mark Spencer, brinda cobertura telefónica a nivel de central telefónica, PBX. Asterisk ha sido diseñada para trabajar en diferentes escenarios en cuanto a cobertura se refiere.

En un ambiente WAN, Asterisk administra a un grupo de extensiones ubicadas en localidades diferentes, por ello se utiliza como herramienta para manejar una central PBX que satisfaga las necesidades planteadas. En la Figura 2-12 se observa que el servidor Asterisk se ubica en la matriz; es decir, en Quito, esto debido a que la matriz cuenta con un mayor número de extensiones pero, lo más importante, mantiene un esquema de red de 3 capas que permite un rápido acceso y mejor manejo de los servidores, particularmente Asterisk. Las extensiones en la oficina matriz, sucursal y usuarios remotos se registran en el servidor Asterisk quedando disponibles para hacer o recibir llamadas entre los usuarios.

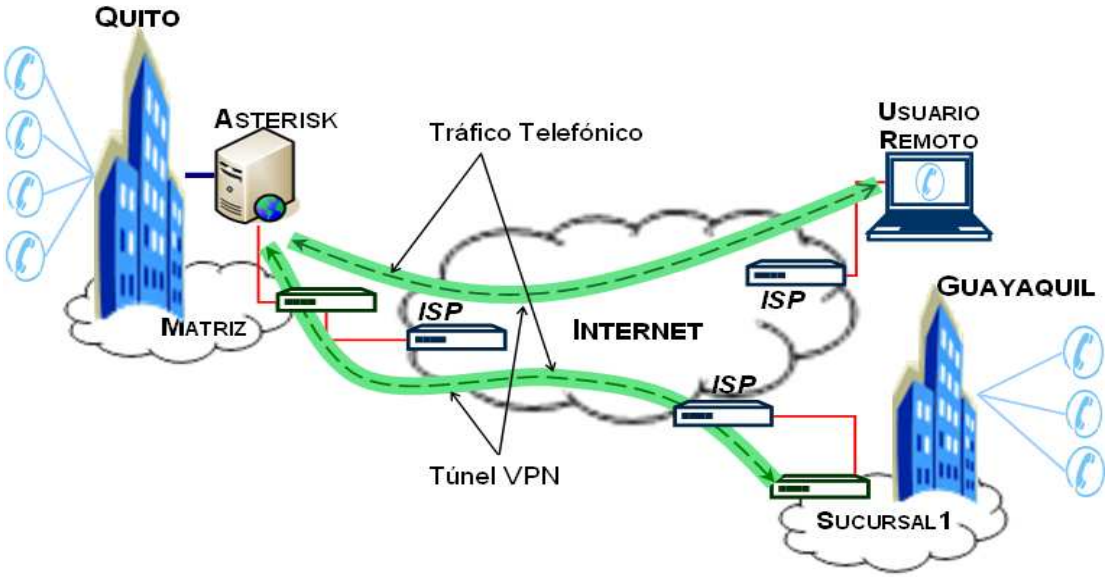


Figura 2-13 Esquema Teléfonico de la Red

En el esquema propuesto en la Figura 2-13 se pueden realizar llamadas entre usuarios de la matriz, sucursal y remoto, como se indica en la Tabla 2-5.

ORIGEN	DESTINO
Usuario Remoto	Matriz
Usuario Remoto	Sucursal
Matriz	Matriz
Matriz	Sucursal
Matriz	Usuario remoto
Sucursal	Matriz
Sucursal	Sucursal
Sucursal	Usuario remoto

Tabla 2-5 Origen Y Destino De Llamadas

2.5.1 ASTERISK

Asterisk es una plataforma de protocolo abierto de distribución libre que

implementa una PBX completa en software. Esta plataforma se soporta principalmente sobre sistemas operativos basados en UNIX[17], como Linux, FreeBSD, Solaris entre otros.

Asterisk es distribuido bajo los términos de licencia GPL *(General Public Licens*e). Esta licencia permite distribuir libremente Asterisk en forma de código fuente y binario con o sin modificaciones y sin restricciones de uso. La GPL no está referida al hardware o software con el que Asterisk se comunica; por ejemplo, si se utiliza un *softphone* SIP, teléfono que soporta protocolo SIP, como cliente de Asterisk, este no requiere que el software también sea distribuido bajo los términos de la GPL.

Asterisk esta diseñada para ofrecer una interfase entre cualquier parte del software o hardware telefónico y los servicios telefónicos que esta ofrece de forma transparente. Tradicionalmente, los productos telefónicos son diseñados para resolver una necesidad específica dentro de la red; sin embargo, muchas de las aplicaciones y servicios telefónicos más usados necesitan implementar gran cantidad de tecnología que no siempre está incluida en el precio de la PBX.

Asterisk toma ventaja de esta sinergia, para crear un único ambiente que puede amoldarse y encajar adecuadamente en cualquier aplicación, ofreciendo todos los servicios que el usuario estime conveniente.

2.5.1.1 Arquitectura Asterisk

Asterisk actúa como intermediario, conectando tecnologías telefónicas con aplicaciones y servicios telefónicos de forma transparente creando de esta manera un ambiente que permite unificar varias tecnologías y poder desplegar una telefonía mixta.

[17] UNIX, sistema operativo multitarea y multiusuario.

El núcleo de Asterisk contiene varias *engines* (máquinas) las cuales participan en la operación del software. Las Interfaces de Programas de Aplicación API[18] específicas, como se muestran en la Figura 2-14, son definidas alrededor del núcleo del sistema. El núcleo se ocupa de la interconexión interna de la plataforma, separándose de los protocolos específicos, códec, interfaces de hardware y de las aplicaciones telefónicas. Lo anterior le permite a Asterisk usar cualquier hardware conveniente y tecnología disponible ahora o en el futuro para realizar sus funciones esenciales, conectando hardware y aplicaciones.

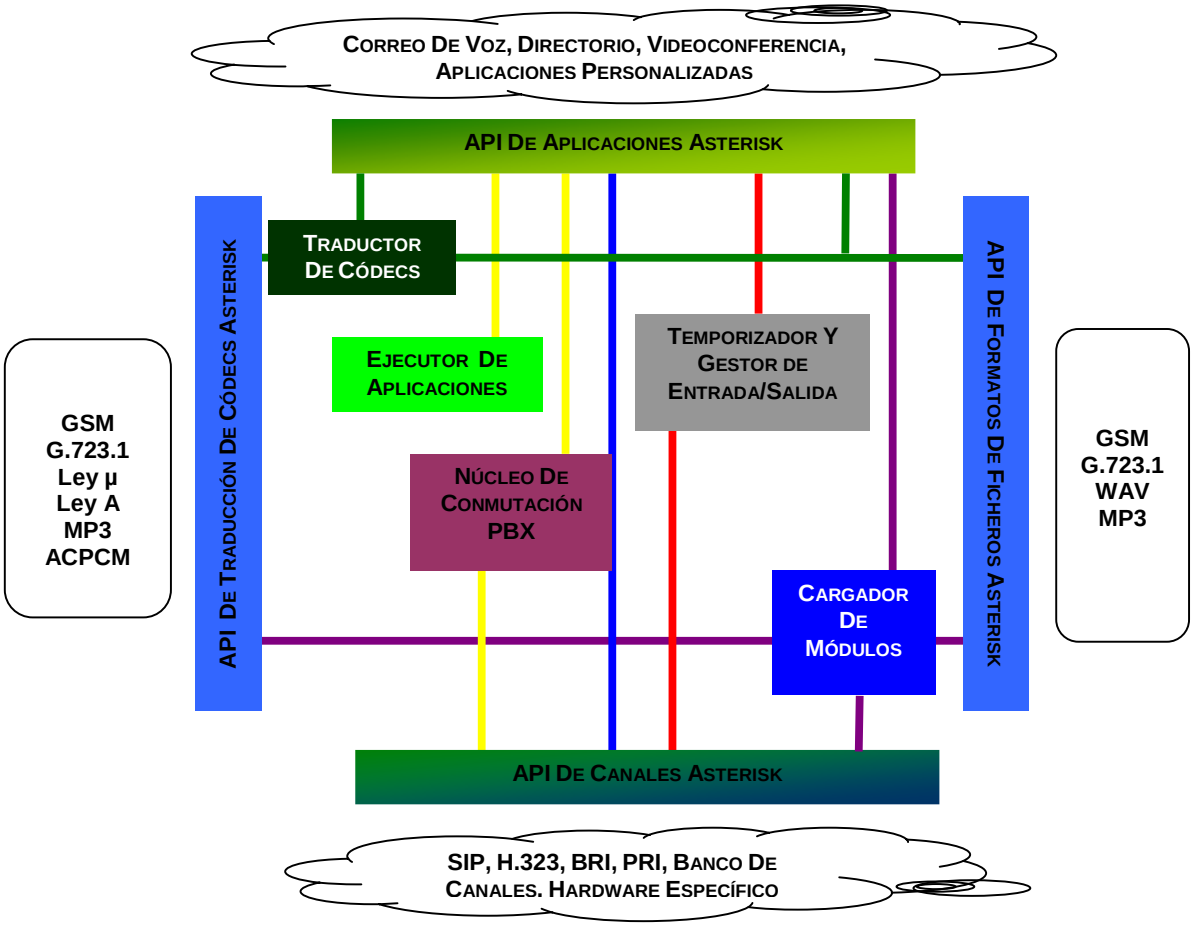


Figura 2-14 Arquitectura Asterisk

Al iniciar Asterisk, el Cargador de Módulos Dinámicos carga e inicializa cada uno de los *drivers* de los diferentes canales, los formatos de los archivos, codecs,

[18] *Aplication Program Interface*

aplicaciones y más, enlazándolos con las apropiadas API internas. Esto permite al Núcleo de Conmutación de la PBX Asterisk comenzar a aceptar llamadas desde las interfaces y responderlas de acuerdo con el plan de marcado, usando el Ejecutor de Aplicaciones. Este ejecuta aplicaciones, que a su vez realizan servicios para los usuarios, como llamar a los teléfonos, correo de voz, reproducción de archivos, etc.

Para facilitar la abstracción de protocolos y de hardware se definen cuatro módulos que tienen la capacidad de cargar cuatro interfaces de programas de aplicación. Usando este sistema de cargar módulos, el núcleo de Asterisk no tiene que preocuparse por los detalles de como el llamador se ha conectado, que códecs esta usando, etc.

1. API para los canales, sirve para controlar todas las llamadas del sistema, sean Voz IP, analógicas cualquier otra tecnología pudiendo desarrollar nuevos canales
2. La API para la Traducción de Códec, carga los módulos de códec que le permiten soportar varios formatos de codificación y decodificación de la voz como pueden ser GSM, Ley µ, Ley A, MP3. Por lo general son códecs que no requieren patentes.
3. API de Formato de Ficheros, sirve para controlar el formato de ficheros que pueden ser administrados por el sistema.
4. API de Aplicaciones, son herramientas desarrollados como complemento a las ya tradicionales existentes en la telefonía analógica tradicional

2.5.1.2 Características de una extensión Asterisk

En Asterisk una extensión se define como una lista de aplicaciones y argumentos para ejecutar. Cada paso de una extensión está referido a una prioridad y ejecuta una aplicación. Cada operación en una llamada es manejada invocando una aplicación. Hay disponibles un gran número de aplicaciones para realizar varias

funciones de una PBX. Las aplicaciones de Asterisk proporcionan tanto características básicas como avanzadas. Asterisk tiene aplicaciones para marcar, descolgar, responder o reproducir un archivo de sonido. Las aplicaciones más avanzadas proporcionan la creación de correos de voz, conferencia y servicios de directorio. Cada prioridad generalmente es ejecutada por orden aunque algunas aplicaciones como *"Dia*l" y *"Goto*" pueden remitir una llamada a una prioridad diferente. Cada paso en una extensión, típicamente se hace como sigue.

La estructura de Asterisk permite la integración de gran parte de códecs de audio además de proveer de todas las aplicaciones de la telefonía analógica tradicional. Asterisk da paso a la creación de nuevas aplicaciones y servicios que un usuario o empresa pueda requerir sobre una PBX, esto se debe a que Asterisk fue creado en un ambiente de fuente abierto. Por todo esto, Asterisk es una herramienta versátil que permite caracterizar cada una de las extensiones de forma individual.

Al momento de configurar una extensión, se debe completar las características mostradas en la Tabla 2-6.

CARACTERÍSTICA	FUNCIÓN
Seguridad	**Permitir llamadas de larga distancia solo desde teléfonos seguros**
Ruteo	**Encaminar las llamadas basadas en extensiones**
Contestadora	**Saludar a los llamadores y preguntarles para entrar a las extensiones.**
Autenticación	**Preguntar por la palabra clave al entrar a las extensiones asignadas**
Privacidad	**Lista negra de llamadores fastidiosos**
Macros	**Crear aplicaciones para las funciones mas comúnmente utilizadas**

Tabla 2-6 Características comunes de una extensión Asterisk.

2.5.1.3 Asignación Numérica A Los Terminales IP

Asterisk permite extensiones de hasta 5 dígitos, pudiendo de esta manera diferenciar entre grupos de extensiones pertenecientes a un mismo departamento dentro de la matriz o de la sucursal, o, en su defecto, para asociar extensiones a grupos de similares funciones o características.

Para distinguir una extensión en la matriz de una en la oficina sucursal, se utiliza una extensión de 4 dígitos, el primer digito como indicador, 1 en el caso de la matriz y 2 para la sucursal. La Tabla 2-7 muestra el rango de direcciones posibles.

ÁREA	PRIMER DÍGITO	RANGO DE EXTENSIONES
Matriz	**1**	**1001-1999**
Sucursal	**2**	**2001-2999**
Remoto	**3**	**3001-3999**

Tabla 2-7 Numeración

De esta manera se procede a asignar la numeración tomando en cuenta a los 93 usuarios presentes, y permitiendo extensiones para usuarios remotos.

2.5.1.4 Herramientas de Administración

La mayor parte de la flexibilidad de Asterisk es controlada a través de los archivos de configuración que se localizan en el directorio *etc/Asteris*k. La sintaxis de la configuración está diseñada de forma que le sea más fácil analizarla tanto al software, como a la persona que opera el sistema. Mediante los archivos de configuración se establecen todos los servicios que ofrece Asterisk, los canales (SIP, H.323), las interfaces y principalmente el “Plan de Marcación” que a la postre es el que va a permitir la comunicación a través de Asterisk.

El Plan de Marcación es configurado en el archivo *extension.con*f. La configuración de este archivo permite encaminar todas las llamadas en el sistema, desde la fuente hasta el destino final, mediante varias aplicaciones.

Asterisk permite administrar usuarios por nombre o por número de extensión, de esta manera se configura el protocolo VoIP para cada usuario, puede ser SIP o H.323, teniendo en cuenta que las extensiones se podrán comunicar únicamente si utilizan el mismo protocolo.

Para limitar el número de usuarios y garantizar la comunicación con la central telefónica se asigna una ID de usuario a la par con una contraseña, restringiendo el acceso a usuarios no autorizados.

Asterisk cuenta con la herramienta *Asterisk Logs* que permite monitorear llamadas concurrentes y mantener un registro de las llamadas de cada una de las extensiones, además muestra el protocolo utilizado, el número de extensión, dirección IP origen y destino y el tiempo de duración.

El diseño presentado en este capítulo determina las pautas a seguir en un proceso de configuración e instalación de equipos, servidores y elementos de software. Se detalla un proceso de estimación de ancho de banda requerido para la aplicación que se tendrá sobre la red diseñada, de esta manera se pretende optimizar el uso de recursos sin afectar el desempeño de las aplicaciones o el acceso a los recursos de red.

La conexión VPN propuesta en esta sección describe un proceso de acuerdo al protocolo de seguridad utilizado. IPSec establece en 5 fases el túnel VPN, que luego se utilizará para transmitir conversaciones telefónicas, para ello durante el proceso se realizan intercambios de contraseñas con sus respectivas identificaciones de usuario o de túnel, además se procede con diferentes procesos de verificación y autenticación.

Una vez establecido el túnel VPN, todos los usuarios podrán acceder al servidor Asterisk, que administra el tráfico telefónico. Los usuarios registrados en éste

servidor podrán comunicarse entre ellos, independientemente de donde se encuentren. Dado que el tráfico telefónico generado se mantiene dentro de la red de la empresa no se infringe la ley de regulación para VoIP.

BIBLIOGRAFÍA-CAPÍTULO 2

[1] Knowledgenet.Cisco.Securing.Networks.with.PIX.and.ASA.SNPA.Student. Guide.V4.0.eBook-DDU.pdf

[2] Curriculum Académico, ***Cisco*** Certified ***Network*** Associate, Modulo 3

[3] Curriculum Académico, ***Cisco*** Certified ***Network*** Associate, Modulo 4

[4] URL: http://seguridad.internet2.ulsa.mx/congresos/2001/cudi2/tutorial_ipsec.pdf

[5] URL: http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1218461,00.html

[6] CRRION Hugo, Ingeniería de tráfico de telecomunicaciones, Carrión & Carrión Consultores, Julio 2005.

[7] Tecnologías de Banda Ancha Tráfico, Universidad Nacional de rosario, Facultad de Ciencias Exactas y Agrimensura,

[8] URL: http://www.teldat.es/docs/products/pdf/ancho_banda.pdf

[9] URL: http://www.supertel.gov.ec

[10] URL: http://linux.pucp.edu.pe/downloads/linuxweek2006/lwp-asterisk.pdf Handbook.- http://www.digium.com/handbook-draft.pdf

[11] URL:
http://www.investigacion.frc.utn.edu.ar/labsis/Publicaciones/QueEsLinux/QueEsLinux.html

CAPÍTULO 3

3 IMPLEMENTACIÓN DE LA RED

De acuerdo al diseño y a las consideraciones realizadas en el Capítulo 2 para el túnel VPN y para el servicio de VoIP, se procede a la implementación del proyecto donde se incluyen las configuraciones de los equipos utilizados para la implementación del túnel VPN, cliente VPN, servidor de VoIP, softphone y teléfono IP.

Para el presente proyecto se requiere realizar llamadas a través de un túnel VPN, en dos escenarios: LAN a LAN y Acceso Remoto. En el escenario LAN a LAN se configura el túnel en un equipo de frontera en cada una de las redes LAN, que se encuentran separadas por una nube WAN simulada. En el escenario de Acceso Remoto se configura el túnel en uno de los equipos de frontera en las redes LAN.

Una vez implementado el túnel VPN, se realiza la instalación y configuración del servidor de VoIP, Asterisk Now. Luego de lo cual se podrán realizar llamadas entre usuarios en la LAN y usuarios remotos. Por último se describe la configuración de un softphone y de un Teléfono IP.

3.1 PASOS PARA LA IMPLEMENTACIÓN DE IPSEC [1]

En el siguiente diagrama de bloques se describe los pasos a seguir para la configuración de una VPN mediante el protocolo IPSec (Figura 3-1).

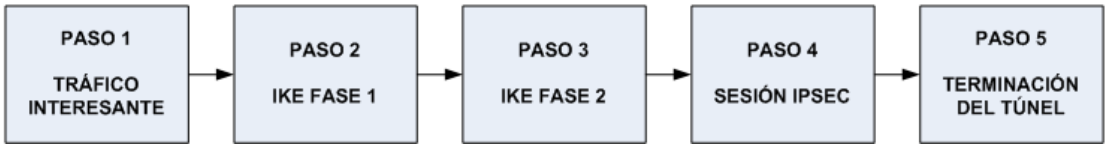


Figura 3-1 Diagrama De Bloques IPSec

3.1.1 TRÁFICO INTERESANTE

El tráfico definido como interesante es el tráfico que va a atravesar el túnel VPN, y necesita ser encriptado. En este caso se define como tráfico interesante los paquetes de VoIP, debido a que los paquetes de voz se envían a través del túnel, permitiendo realizar llamadas entre usuarios remotos y usuarios locales y viceversa.

En la red se tiene políticas para enviar el tráfico cifrado entre las terminales VPN, y en texto plano el tráfico para otras conexiones que no requieran encripción. Esta diferenciación se realiza en los puntos de frontera entre la red pública, Internet, y la red privada, como se muestra en la Figura 3-2.

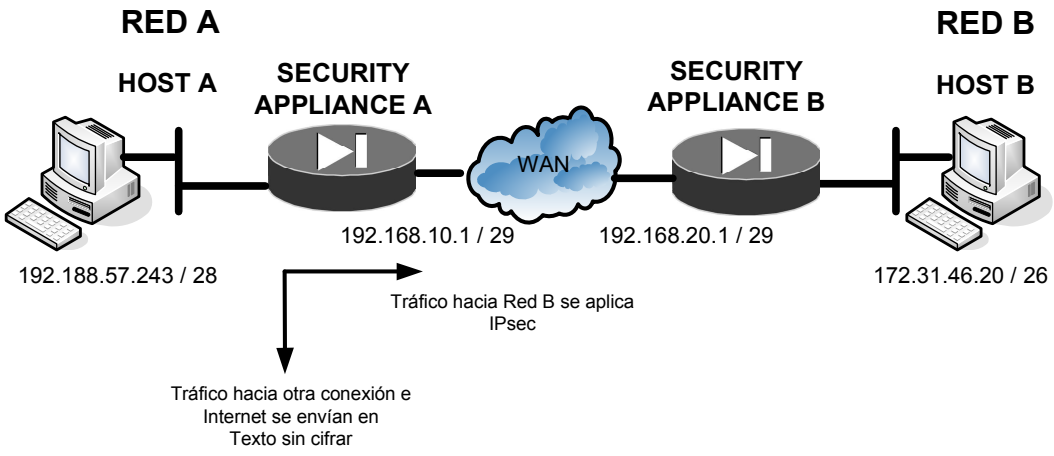


Figura 3-2 Tráfico Interesante

Se define el tráfico interesante en cada uno de los equipos ASA por medio de listas de acceso habilitando los puertos necesarios para enviar el tráfico entre los extremos del túnel.

Las listas de acceso configuradas son del tipo extendidas y tienen el siguiente formato.

fw1(config)# access-list *(name) (tipo de access-list) (permiso) (protocolo) (origen) (destino)* ***eq*** *(puerto)*

En la Tabla 3-1 se describe los comandos de la instrucción anterior y su respectiva descripción.

Name	**---**	**Palabra o número menor a 241 caracteres**
Tipo de access-list	**Standard**	**Configura una lista de acceso del tipo estándar**
	Extended	**Configura una lista de acceso del tipo extendida**
Permisos	**Permit**	**Especifica los tipos de paquetes que se van a enviar**
	Deny	**Especifica los tipos de paquetes que se van a rechazar**
Protocolo	**Ip**	**Configura Internet Protocol**
	Tcp	**Configura Transmission Control Protocol**
	Udp	**Configura User Datagram Protocol**
	Ipsec	**Configura IP Security**
	Icmp	**Configura Internet Control Message Protocol**
Origen	**Hostname or A.B.C.D**	**Dirección o nombre del host de origen**
	Any	**Desde cualquier origen**
	Host	**Se configura un host como origen**
	Interface	**Usa la dirección de la interfaz como dirección origen**
	object-group	**Especifica un grupo de máquinas o redes como dirección origen**
Destino	**Hostname or A.B.C.D**	**Dirección o nombre del host de destino**
	Any	**Hacia cualquier destino**
	Host	**Se configura un host como destino**
	Interface	**Usa la dirección de la interfaz como dirección**

		destino
	object-group	**Especifica un grupo de máquinas o redes como dirección destino**
Puerto	**nombre o número de puerto**	**El número de puerto entre 0 y 65535**

Tabla 3-1 Comandos Para Definir Tráfico Interesante

En el caso particular del presente proyecto los paquetes que requieren encripción son los paquetes de voz. A continuación se tiene un ejemplo de la configuración del protocolo SIP (puerto UDP 5060) como tráfico interesante. Estos comandos se deben configurar en cada equipo VPN.

fw1(config)# access-list 101 permit udp 192.188.57.240 255.255.255.240 172.31.46.0 255.255.255.192 eq 5060

fw2(config)# access-list 101 permit udp 172.31.46.0 255.255.255.192 192.188.57.240 255.255.255.240 eq 5060

En caso que se requiera de otras aplicaciones, diferentes de la de voz, se puede definir como tráfico interesante los puertos requeridos o en su defecto a todo el conjunto de protocolos IP entre los extremos del túnel. A continuación se indica la configuración del conjunto de protocolos IP como tráfico interesante.

fw1(config)# access-list 101 permit ip 192.188.57.240 255.255.255.240 172.31.46.0 255.255.255.192
fw1(config)# nat (inside) 0 access-list 101

fw2(config)# access-list 101 permit ip 172.31.46.0 255.255.255.192 192.188.57.240 255.255.255.240
fw2(config)# nat (inside) 0 access-list 101

Otro comando que se utiliza es el “nat 0”, que se utiliza para que las redes definidas en las listas de acceso no se traduzcan por el protocolo NAT, que normalmente se define para que las redes tengan salida a Internet, de tal manera

que al acceder a la VPN las máquinas terminales se las pueda ver con las direcciones IP originales en cualquier punto del túnel.

3.1.2 INTERNET KEY EXCHANGE FASE 1

En este paso se configuran políticas que se mantendrán durante la conexión del túnel VPN. Éstas políticas deben ser iguales en cada uno de los equipos para que se establezca el túnel.

Los parámetros que se definen en la política son los siguientes:

- ✓ Método de Autenticación
- ✓ Algoritmo de Encripción
- ✓ Grupo DH
- ✓ Algoritmo Hash
- ✓ Lifetime (Tiempo de vida del túnel)

Los comandos que se utilizan tienen el siguiente formato:

fw1(config)# crypto iskmp policy *(número de política) (autenticación / encripción / grupo / hash / lifetime) (opción)*

En la Tabla 3-2 a continuación se muestra los comandos y los parámetros de configuración.

Política	**crypto isakmp policy**	**---**	**Configura las políticas con el protocolo ISAKMP**
Número de política	**1 – 65535**	**---**	**Prioridad de la política (1 es la más alta)**
Autenticación del Peer	**Authentication**	**pre-share**	**Configura clave pre-confgurada manualmente**
		rsa-sig	**Configura el algoritmo rsa-sig**
		dsa-sig	**Configura el algoritmo dsa-sig**
Algoritmo de Encripción	**Encryption**	**Des**	**Configura des (56 bits)**
		3des	**Configura 3des (168 bits)**

		Aes	**Configura aes (128 bits)**
		aes-192	**Configura aes (192 bits)**
		aes-256	**Configura aes (256 bits)**
Grupo	**Group**	**1**	**Diffie-Hellman group 1 (768 bits)**
		2	**Diffie-Hellman group 2 (1024 bits)**
		5	**Diffie-Hellman group 5 (1536 bits)**
		7	**Diffie-Hellman group 7 (mayor 1536 bits)**
Algoritmo de Integridad de mensajes	**Hash**	**md5**	**Configura hash md5**
		Sha	**Configura hash sha**
Tiempo de vida	**Lifetime**	**tiempo**	**Se escribe el tiempo de duración del túnel en segundos**
		None	**Se tiene un túnel con un tiempo de duración ilimitado**

Tabla 3-2 Comandos Para Definir Políticas

A continuación se tiene un ejemplo para configurar pre-share, aes, group 2, md5, lifetime de 86400 segundos (1 día):

Fw1(config)# crypto isakmp policy 10 authentication pre-share
Fw1(config)# crypto isakmp policy 10 encryption aes
Fw1(config)# crypto isakmp policy 10 group 2
Fw1(config)# crypto isakmp policy 10 hash md5
Fw1(config)# crypto isakmp policy 10 lifetime 86400

3.1.3 INTERNET KEY EXCHANGE FASE 2

En este paso se configura el encapsulamiento de paquetes con los protocolos de encripción y de autenticación establecidos previamente en la fase 1 de IKE. Los comandos a configurar tienen el siguiente formato:

Fw1(config)# crypto ipsec transform-set (name) (encapsulamiento-protocolo)

La Tabla 3-3 siguiente muestra los protocolos que se pueden utilizar.

Name	**Palabra menor a 64 caracteres**

esp-des	**ESP transform using DES cipher (56 bits)**
Esp-3des	**ESP transform using 3DES cipher(168 bits)**
esp-aes	**ESP transform using AES-128 cipher**
esp-aes-192	**ESP transform using AES-192 cipher**
esp-aes-256	**ESP transform using AES-256 cipher**
esp-md5-hmac	**ESP transform using HMAC-MD5 auth**
esp-sha-hmac	**ESP transform using HMAC-SHA auth**
Esp-none	**ESP no authentication**
Esp-null	**ESP null encryption**

Tabla 3-3 Parámetros De Encapsulamiento

La siguiente línea es un ejemplo de configuración de seguridad para una VPN

fw1(config)# crypto ipsec transform-set equipo_vpn esp-aes esp-md5-hmac

El comando anterior significa, que se encapsula los paquetes con ESP y que además se utiliza como algoritmo de autenticación MD5 y como algoritmo de encripción AES. En el presente proyecto esta configuración se aplicó para ejecutar las políticas de seguridad requeridas por la empresa.

3.1.4 SESIÓN IPSEC

Una vez configurado todos los parámetros para el túnel IPSec, se establece la sesión IPSec y se pueden transmitir información entre los extremos del túnel.

3.1.5 TERMINACIÓN DE LA SESIÓN DEL TÚNEL

En la figura 3-3 se muestra un esquema de la terminación del túnel.

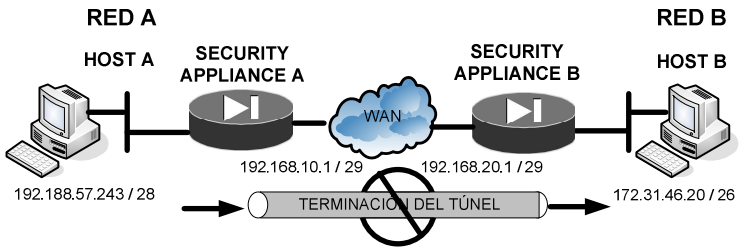


Figura 3-3 Terminación Del Túnel

La sesión del túnel VPN puede terminar por tres causas:

1. Por que venció el tiempo de vida o lifetime para el que fue configurado el túnel.
El tiempo de vida se establece con el siguiente comando:

fw1 (config)# isakmp policy 10 lifetime (*tiempo en segundos*)

El lifetime se puede configurar desde un tiempo mínimo de 120 segundos hasta 2147483647 segundos que equivale aproximadamente a 68 años.

Además se tiene la opción de “none”, esto permite que el tiempo de vida del túnel sea ilimitado.

2. Si los parámetros de SAs son diferentes, el túnel no se establece.

3. Si los parámetros de SAs son removidos o se cambian, se pierde la comunicación establecida.

Una vez definidos los pasos a seguir para configurar el túnel se procede a continuación con la descripción de los escenarios implementados y las configuraciones respectivas.

3.2 VPN LAN-TO-LAN IPSEC USANDO EQUIPOS CISCO [1]

Para el establecimiento del escenario VPN LAN a LAN se tienen las siguientes características:

Topología: LAN-to-LAN
Tecnología de tunel: IPSec
Plataforma: Por hardware usando equipos CISCO ASA serie 5500
Equipos utilizados:

- ✓ Dos Equipos Cisco ASA serie 5500.
- ✓ Dos computadores Pentium IV

3.2.1 ESCENARIO MONTADO

La implementación de la VPN y el desempeño del servicio de VoIP se realizaron en la Unidad de Gestión de Información (UGI) de la Escuela Politécnica Nacional gracias a la colaboración de dicha unidad y por la prestación de los equipos ASA para crear una red VPN sobre la infraestructura de red ya constituida.

El túnel conecta la red de la UGI, y la red de servidores públicos de la Universidad. La red de servidores públicos cuenta con direcciones públicas y no puede tener acceso a ningún equipo en la red LAN.

En la Figura 3-4 se muestra la Polired y la implementación del túnel VPN entre dos redes LAN.

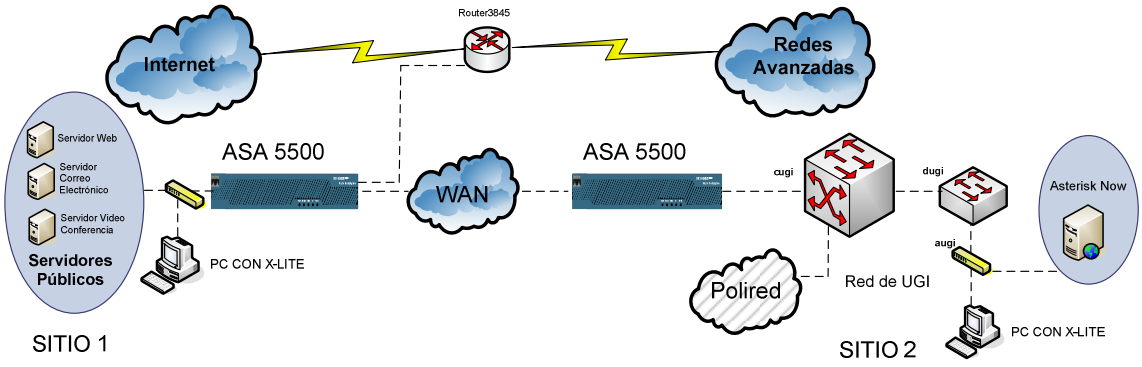


Figura 3-4 Diseño Lógico De Una Red VPN Sobre La Polired

3.2.2 DIRECCIONAMIENTO DE LA RED

En la Figura 3-5 se describe el direccionamiento de los equipos a utilizar en la implementación.

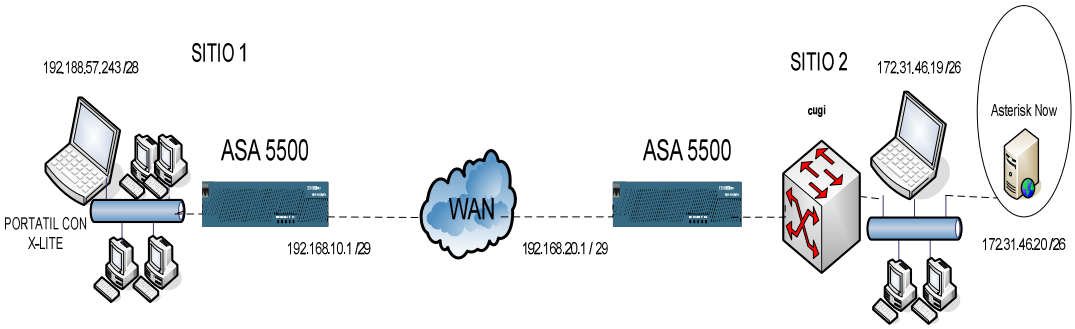


Figura 3-5 Diseño Implementado De Una VPN LAN a LAN

3.2.3 INSTALACIÓN Y CONFIGURACIÓN

Se parte del hecho de tener operativas las dos redes de área local (sitio1 y sitio2). En el Sitio1 (Red de Servidores Públicos) la dirección de la red es 192.188.57.240 con máscara 255.255.255.240, y en Sitio2 (Subred de la Unidad de Gestión de Información) la dirección de la red es 172.31.46.0 con máscara de 255.255.255.192.

La red de servidores públicos cuenta con varios equipos entre los cuáles se encuentra servidores de correo electrónico, DNS público, servidor de video conferencia. Todos estos equipos y la interfaz del equipo ASA se conectan a un Switch de 24 puertos. Por otro lado, la interfaz del otro equipo ASA en el Sitio2 se conecta directamente al Switch de Core que se tiene en el centro de computo y éste a su vez se conecta a la red de la UGI.

En el Sitio1, la dirección IP de la estación de trabajo es 192.188.57.243 / 28 y en el Sitio2, la dirección IP de la estación de trabajo es 172.31.46.19 / 26 y el servidor Asterisk con la dirección 172.31.46.20 / 26.

La configuración de los equipos ASA para el establecimiento de la VPN IPSec entre las dos LANs es la siguiente;

Sitio1, Red de Servidores Públicos.

```
ASA1(config)# tunnel-group 192.168.10.1 type ipsec-l2l
ASA1 (config)# isakmp enable outside
ASA1 (config)# isakmp identity address
ASA1(config)# isakmp policy 10 encryption aes
ASA1(config)# isakmp policy 10 hash md5
ASA1(config)# isakmp policy 10 authentication pre-share
ASA1(config)# isakmp policy 10 group 1
ASA1(config)# isakmp policy 10 lifetime none
ASA1(config)# tunnel-group 192.168.10.1 ipsec-attributes
ASA1(config-tunnel-ipsec)# pre-shared-key cisco123
ASA1(config)# access-list 101 permit ip 192.188.57.240 255.255.255.240 172.31.46.0 255.255.255.192
ASA1(config)# nat (inside) 0 access-list 101
ASA1(config)# crypto ipsec transform-set equipo_vpn esp-des esp-md5-hmac
ASA1(config)# crypto map EQUIPO_1_MAP 10 match address 101
ASA1(config)# crypto map EQUIPO_1_MAP 10 set peer 192.168.20.1
ASA1(config)# crypto map EQUIPO_1_MAP 10 set transform-set equipo_vpn
ASA1(config)# crypto map EQUIPO_1_MAP 10 set security-association lifetime seconds 48000
ASA1(config)# crypto map EQUIPO_1_MAP interface outside
ASA1(config)# route outside 0.0.0.0 0.0.0.0 192.168.10.1
```

```
ASA1(config)# crypto ipsec transform-set remoteuser1 esp-des esp-sha hmac
ASA1(config)# crypto dynamic-map rmt-dyna-map 10 set transform-set remoteuser1
ASA1(config)# crypto map rmt-user-map 10 ipsec-isakmp dynamic rmt-dyna-map
ASA1(config)# crypto map rmt-user-map interface int_vpn
```

Sitio 2, Polired.

```
ASA2(config)# tunnel-group 192.168.20.1 type ipsec-l2l
ASA2(config)# isakmp enable outside
ASA2(config)# isakmp identity address
ASA2(config)# isakmp policy 10 encryption aes
ASA2(config)# isakmp policy 10 hash md5
ASA2(config)# isakmp policy 10 authentication pre-share
ASA2(config)# isakmp policy 10 group 1
ASA2(config)# isakmp policy 10 lifetime none
ASA2(config)# tunnel-group 192.168.20.1 ipsec-attributes
ASA2(config-tunnel-ipsec)# pre-shared-key cisco123
ASA2(config)# access-list 101 permit ip 172.31.46.0 255.255.255.192 192.188.57.240 255.255.255.240
ASA2(config)# nat (inside) 0 access-list 101
ASA2(config)# crypto ipsec transform-set equipo_vpn esp-des esp-md5-hmac
ASA2(config)# crypto map EQUIPO_1_MAP 10 match address 101
ASA2(config)# crypto map EQUIPO_1_MAP 10 set peer 192.168.10.1
ASA2(config)# crypto map EQUIPO_1_MAP 10 set transform-set equipo_vpn
ASA2(config)# crypto map EQUIPO_1_MAP 10 set security-association lifetime seconds 48000
ASA2(config)# crypto map EQUIPO_1_MAP interface outside
ASA2(config)# route outside 0.0.0.0 0.0.0.0 192.168.20.1
ASA2(config)# crypto ipsec transform-set remoteuser1 esp-des esp-sha hmac
ASA2(config)# crypto dynamic-map rmt-dyna-map 10 set transform-set remoteuser1
ASA2(config)# crypto map rmt-user-map 10 ipsec-isakmp dynamic rmt-dyna-map
ASA2(config)# crypto map rmt-user-map interface int_vpn
```

En resumen las políticas configuradas para el establecimiento del túnel son las siguientes:

- ✓ Método de Autenticación: md5
- ✓ Algoritmo de Encripción: aes (128 bits)
- ✓ Grupo DH: Grupo 1 (768 bits)

- ✓ Lifetime: none (ilimitado)
- ✓ Contraseña: cisco123

3.2.4 CONFIGURACIÓN DE LA NUBE WAN

La nube WAN esta formada por routers Cisco configurados en varias topologías de red. El propósito de la nube WAN es simular la red mundial de Internet, para obtener un escenario propicio para probar el diseño y configuración propuestos. Las topologías que se implementan son las siguientes:

3.2.4.1 Topología Tipo Bus Punto A Punto

En esta topología se utiliza dos ruteadores Cisco de la serie 1841 conectados en serie y configurados para que la red 192.168.10.1/29, Sitio1, tenga conectividad con la red 192.168.20.1/29, Sitio2.

Las direcciones de cada equipo se muestran en la Figura 3-6

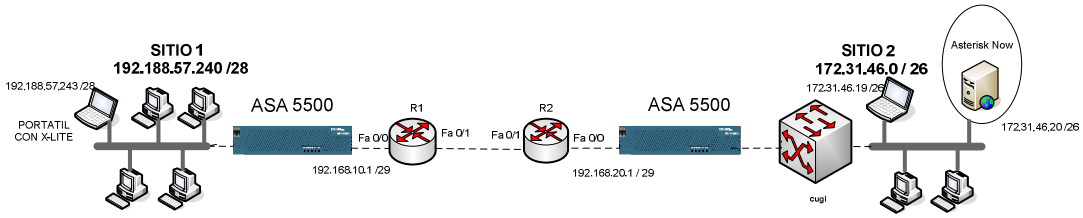


Figura 3-6 Topología Tipo Bus

En la Tabla 3.4 se muestra un resumen de los parámetros configurados en los ruteadores.

Nombre de Host	**Router1**	**Router2**
Contraseña de la consola	**Cisco**	**Cisco**

Contraseña vty	**Cisco**	**Cisco**
Int Fa 0/0	**192.168.10.2 / 29**	**192.168.20.2 / 29**
Int Fa 0/1	**10.10.10.10.1 / 28**	**10.10.10.10.2 / 28**
Protocolo de enrutamiento	**OSPF**	**OSPF**
Descripción Interfaz fa 0/0	**Puerta de enlace ASA1**	**Puerta de enlace ASA2**
Descripción Interfaz fa 0/1	**Conexión con Router2**	**Conexión con Router1**

Tabla 3-4 Topología Tipo Bus: Configuración De Routers

3.2.4.2 Topología Tipo Estrella

En esta topología se utiliza tres ruteadores Cisco conectados en estrella y configurados para que la red 192.168.10.1/29, Sitio1, tenga conectividad con la red 192.168.20.1/29, Sitio 2.

El esquema implementado se lo muestra en la Figura 3-7.

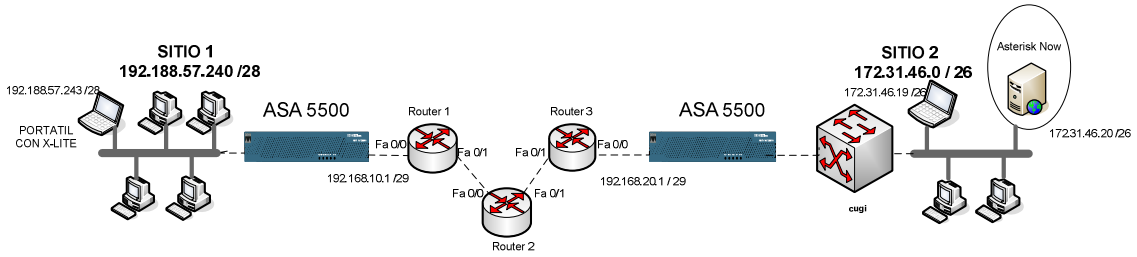


Figura 3-7 Topología Tipo Estrella

En la Tabla 3-5 se muestra un resumen de los parámetros configurados en cada uno de los ruteadores.

Nombre de Host	**Router1**	**Router2**	**Router2**
Contraseña de la consola	**Cisco**	**cisco**	**cisco**
Contraseña vty	**Cisco**	**cisco**	**cisco**
Int Fa 0/0	**192.168.10.2 / 29**	**10.10.10.10.2 / 28**	**192.168.20.2 / 29**
Int Fa 0/1	**10.10.10.10.1 / 28**	**10.10.11.1 / 28**	**10.10.11.2 / 28**
Protocolo de enrutamiento	**OSPF**	**OSPF**	**OSPF**
Descripción Interfaz fa 0/0	**Puerta de enlace ASA1**	**Conexión con Router1**	**Puerta de enlace ASA2**

Descripción Interfaz fa 0/1	Conexión con Router2	Conexión con Router3	Conexión con Router2

Tabla 3-5 Topología Tipo Estrella: Configuración De Routers

3.2.4.3 Topología En Malla Parcial

En esta topología utilizamos cuatro ruteadores Cisco conectados en una topología en malla parcial, configurada de manera que la red 192.168.10.1/29, Sitio1, tenga conectividad con la red 192.168.20.1/29, Sitio2.

El esquema implementado se lo muestra en la Figura 3-8

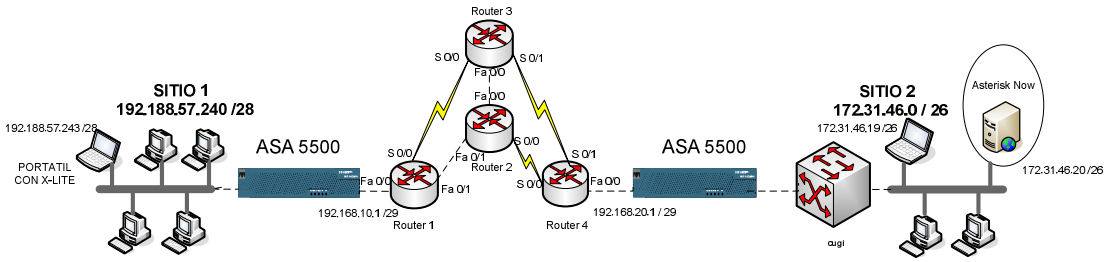


Figura 3-8 Topología En Malla Parcial

En la Tabla 3-6 se muestra un resumen de los parámetros configurados en los Router.

Nombre de Host	**Router1**	**Router2**	**Router3**	**Router4**
Contraseña de la consola	**cisco**	**cisco**	**cisco**	**cisco**
Contraseña vty	**cisco**	**cisco**	**cisco**	**cisco**
Int Fa 0/0	**192.168.10.2 / 29**	**10.10.11.1 / 28**	**10.10.11.2 / 28**	**192.168.20.2 / 29**
Int Fa 0/1	**10.10.10.2 / 28**	**10.10.10.1 / 28**	**---**	**---**
Int S 0/0	**10.10.13.1 / 28**	**10.10.12.1 / 28**	**10.10.13.2 / 28**	**10.10.12.2 / 28**
Int S 0/1	**---**	**---**	**10.10.14.1 / 28**	**10.10.14.2 / 28**
Protocolo de enrutamiento	**OSPF**	**OSPF**	**OSPF**	**OSPF**
Descripción Interfaz fa 0/0	**Puerta de enlace ASA1**	**Conexión con Router3**	**Conexión con Router2**	**Puerta de enlace ASA2**
Descripción Interfaz fa 0/1	**Conexión con Router2**	**Conexión con Router1**	**---**	**---**
Descripción Interfaz S 0/0	**Conexión con Router3 (DCE)**	**Conexión con Router4 (DCE)**	**Conexión con Router1 (DTE)**	**Conexión con Router2 (DTE)**

Descripción Interfaz S 0/1	**---**	**---**	**Conexión con Router4 (DTE)**	**Conexión con Router3 (DCE)**

Tabla 3-6 Topología Tipo Malla Parcial: Configuración De Routers

3.3 ACCESO REMOTO IPSEC CON EQUIPO CISCO [1]

Para el establecimiento del escenario VPN de Acceso Remoto se tienen las siguientes características:

Topología: Acceso Remoto

Tecnología de tunel: IPSec

Plataforma: Para servidor VPN usando un ASA serie 5500 con un IOS asa712-k8.bin y para cliente VPN un software propietario de cisco.

Equipos utilizados:

- ✓ 1 equipo ASA 5520
- ✓ Dos computadores Pentium IV

3.3.1 ESCENARIO MONTADO

La implementación del Acceso Remoto VPN se lo realizo mediante un equipo ASA configurado como servidor VPN y designando un pool de direcciones que pertenecen a la Intranet, para que desde una conexión WAN o vía Internet se pueda acceder a la Polired.

Por seguridad, el acceso remoto se restringe a una determinada subred de la LAN de la Polired en este caso la subred 172.31.46.0 / 26, que es la subred donde se encuentra el servidor de VoIP, además se puede habilitar y bloquear los puertos tanto TCP como UDP según sea necesario.

EL cliente VPN accede a la LAN por medio de un software propietario de Cisco mediante el protocolo IPSec. Se necesita tener salida a Internet y tener habilitado

el puerto IPSec y el ISAKMP (puerto UDP 500). Otro requisito es tener conectividad al servidor VPN que tiene la dirección IP pública 192.188.57.2 / 27.

En la Figura 3-9 se muestra el diseño lógico de la red VPN a implementar sobre la Polired.

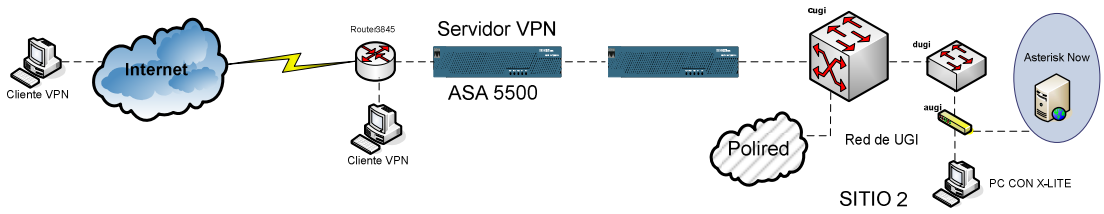


Figura 3-9 Diseño de la Topología Lógica Para Acceso Remoto

3.3.2 DIRECCIONAMIENTO DE LA RED

En la Figura 3-10 se describe el direccionamiento de los equipos a utilizar en la implementación del *acceso remoto*. La Figura 3-10 muestra 2 escenarios, en el primero se conecta el cliente VPN desde una máquina fuera de la Polired, a través de un ISP. El segundo escenario se realizó utilizando un Host conectado a una interfaz del router de frontera de la Institución, facilitada por el departamento UGI, con el propósito de tener una máquina fuera de la red LAN local.

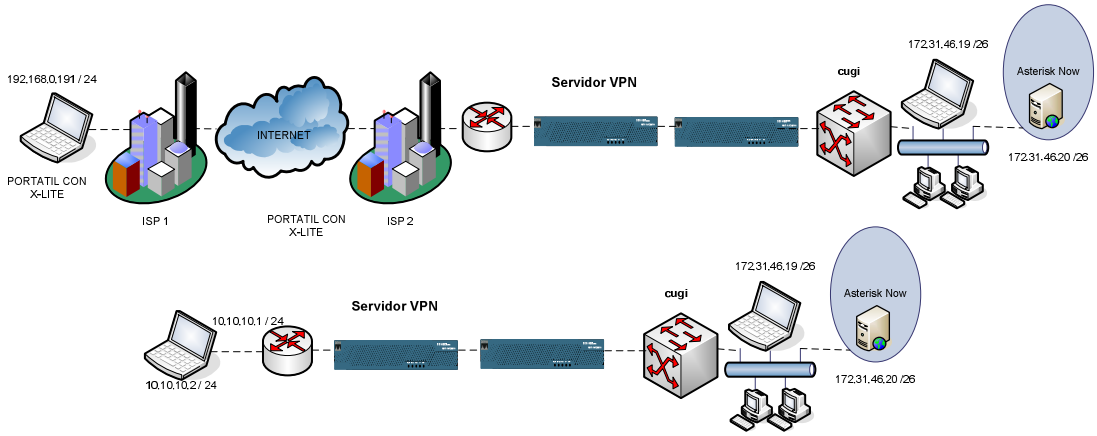


Figura 3-10 Diseño Implementado Para Acceso Remoto

3.3.3 INSTALACIÓN Y CONFIGURACIÓN

Para el caso del acceso remoto, la instalación y configuración se divide en dos partes una para el servidor y otra para el cliente VPN.

3.3.3.1 Instalación y configuración del Servidor VPN

En este escenario se configura uno de los dos equipos usados en el escenario anterior como servidor VPN para clientes remotos. Se define el protocolo VPN, protocolos de encripción, el usuario, contraseña para el cliente VPN, el tiempo de vida del túnel, el pool de direcciones asignadas para los clientes VPN que se conecten a la red.

La configuración del servidor VPN se detalla a continuación:

```
ASA1(config)# interface GigabitEthernet0/0
ASA1(config-if)# nameif outside
ASA1(config-if)#  security-level 0
ASA1(config-if)#  ip address 192.188.57.2 255.255.255.224

ASA1(config)# interface GigabitEthernet0/1
ASA1(config-if)#  nameif inside
ASA1(config-if)#  security-level 100
ASA1(config-if)#  ip address 172.31.6.3 255.255.255.0

ASA1(config)# crypto ipsec transform-set SET-EPN esp-aes esp-md5-hmac
ASA1(config)# crypto dynamic-map DYNAMIC-EPN 20 set transform-set SET-EPN
ASA1(config)# crypto map MAP-EPN 20 ipsec-isakmp dynamic DYNAMIC-EPN
ASA1(config)# crypto map MAP-EPN interface outside
ASA1(config)# isakmp enable outside
ASA1(config)# isakmp policy 20 authentication pre-share
ASA1(config)# isakmp policy 20 encryption aes
ASA1(config)# isakmp policy 20 hash md5
ASA1(config)# isakmp policy 20 group 2
ASA1(config)# isakmp policy 20 lifetime 86400
```

```
ASA1(config)# ip local pool poolvpn 172.31.7.1-172.31.7.254 mask 255.255.255.0
ASA1(config)# tunnel-group acceso-remoto-epn type ipsec-ra
ASA1(config)# tunnel-group acceso-remoto-epn general-attributes
ASA1(config)#  address-pool ippool-acceso-remoto-epn
ASA1(config)#  default-group-policy acceso-remoto-epn
ASA1(config)# tunnel-group acceso-remoto-epn ipsec-attributes
ASA1(config-ipsec)# pre-shared-key cisco123
ASA1(config-ipsec)# isakmp keepalive threshold 30 retry 10
ASA1(config)# username cliente-vpn-epn password cisco123**
ASA1(config)# access-list 101 extended permit ip 172.31.6.0 255.255.255.0 172.31.7.0
255.255.255.0
```

3.3.3.2 Instalación y configuración del cliente VPN [1]

Para la conexión de usuarios remotos se utiliza el software Cisco Systems VPN Client, propietario de la empresa en mención. Este software se caracteriza por:

- ✓ Soportar protocolos para creación de túneles como IPSec además del protocolo ESP.
- ✓ Soportar Autenticación y Enpcripción a través de algoritmos de encripción como: DES, 3DES y AES, combinados con otros algoritmos como MD5 o SHA que cumplen funciones de autenticación.
- ✓ Soportar técnicas de administración o manejo de llaves a través del protocolo IKE en modo agresivo o modo principal.
- ✓ Soportar técnicas de compresión de datos.
- ✓ Soportar Certificados Digitales.
- ✓ Políticas de Administración que se manejan mediante el protocolo ISAKMP

Este programa, VPN CLIENT, viene en la versión 4.0.5 y en la versión 4.6 y sirve para los siguientes sistemas operativos:

- ✓ Linux
- ✓ Macintosh OS X
- ✓ Solaris

- ✓ Windows

Las pruebas se realizaron mediante clientes instalados en un ambiente Windows y para su instalación y configuración se detallan los siguientes pasos:

1. Una vez introducido el Cd de Instalación del VPN Client se despliega la pantalla mostrada en la Figura 3-11.

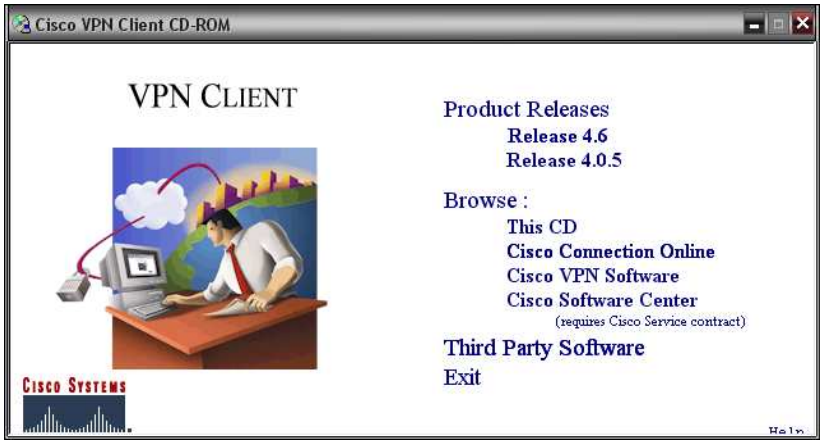


Figura 3-11 Ventana De Inicio De Instalación

2. Las versiones disponibles del VPN Client son la 4.6 y 4.0.5, por ser la versión más reciente se elige la versión 4.6, luego de lo cual se despliega la ventana mostrada en la Figura 3.12.

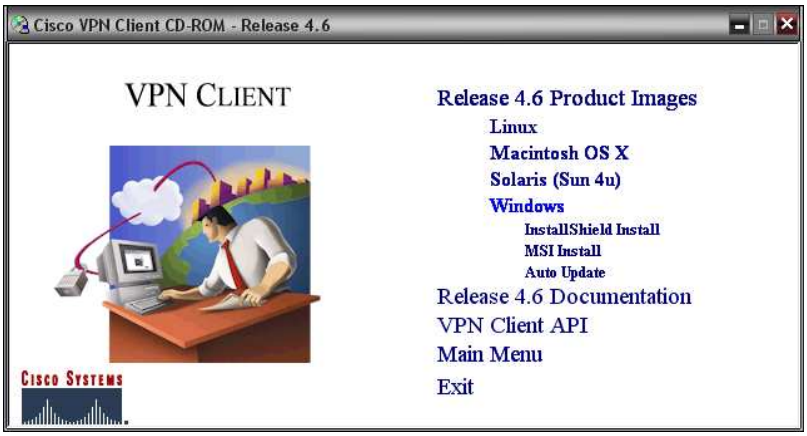


Figura 3-12 Versión del cliente VPN

3. El siguiente paso es escoger el sistema operativo donde se desea instalar el Cliente VPN, en este caso se escoge Windows y la opción de instalar, posteriormente se despliega la carpeta que contiene el archivo de instalación para Windows.

4. A continuación se ejecuta el archivo setup.exe y se da paso a la configuración por defecto.

5. Una vez instalado el software se reinicia el computador y se crea una tarjeta de red virtual para el acceso a la VPN. Una vez reiniciado el computador se ejecuta el Cliente VPN y se despliega la siguiente ventana de conexión a la VPN, Figura 3-13.

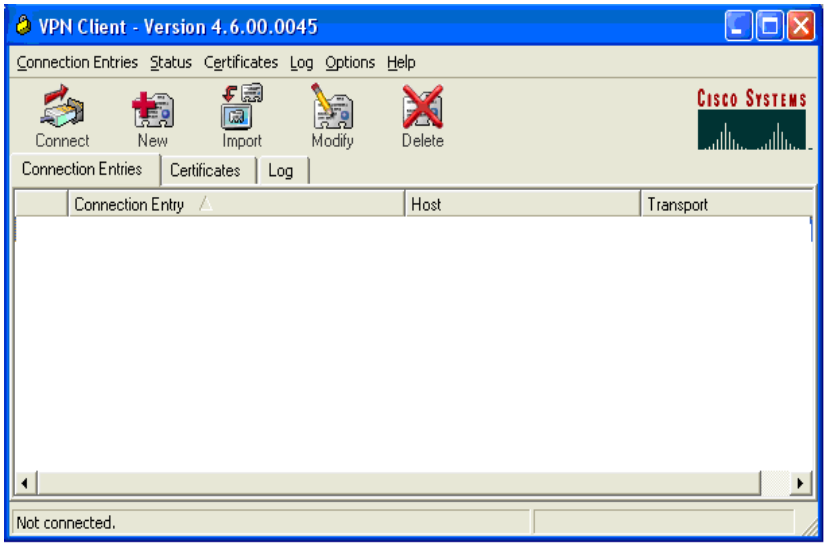


Figura 3-13 Ventana De Conexión VPN

6. Para establecer una nueva conexión se elige el icono New y se despliega la ventana de configuración de una nueva red VPN, Figura 3-14.

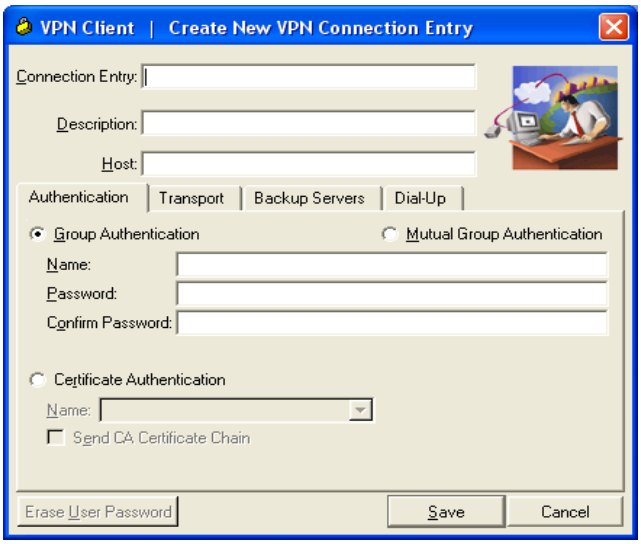


Figura 3-14 Ventana Para Crear Una Conexión VPN

7. Se completa los espacios en blanco con los parámetros requeridos de acuerdo a los configurados en el servidor VPN que se vieron en el segmento 3.3.3.1. Se muestra un ejemplo de configuración del cliente remoto en la Figura 3-15.

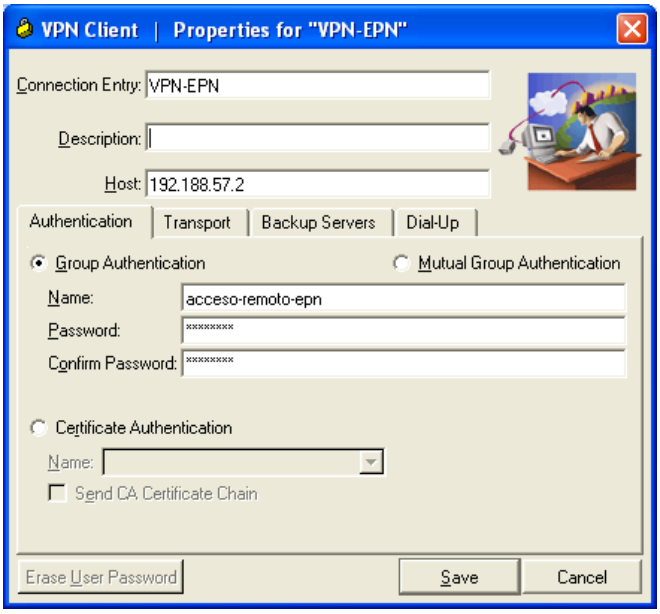


Figura 3-15 Configuración Cliente VPN.

8. Las otras configuraciones (Transport, Backup Servers, Dial-Up) son opcionales por lo que una vez realizada la configuración esencial se guardan los cambios y aparece una nueva conexión en la ventana principal, Figura 3.16.

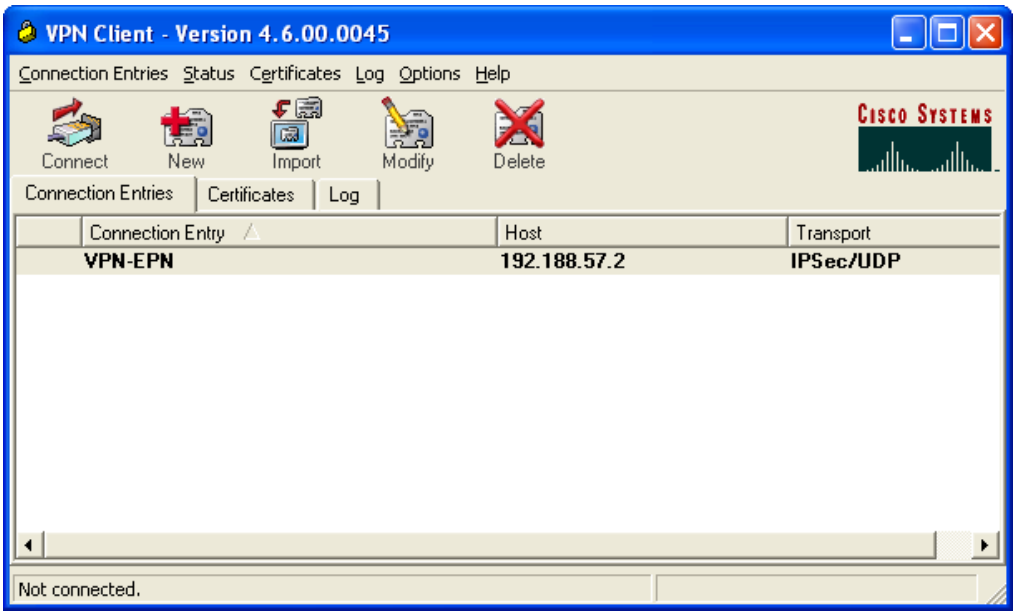


Figura 3-16 Conexión VPN

9. Se da doble click en la etiqueta creada, VPN-EPN, y se inicia la conexión al túnel VPN.

10. Si todos los parámetros configurados se encuentran correctos, se despliega una ventana donde se solicita la autenticación del usuario VPN, donde se requiere ingresar el nombre de usuario y la contraseña para la conexión a la VPN, Figura 3-17.

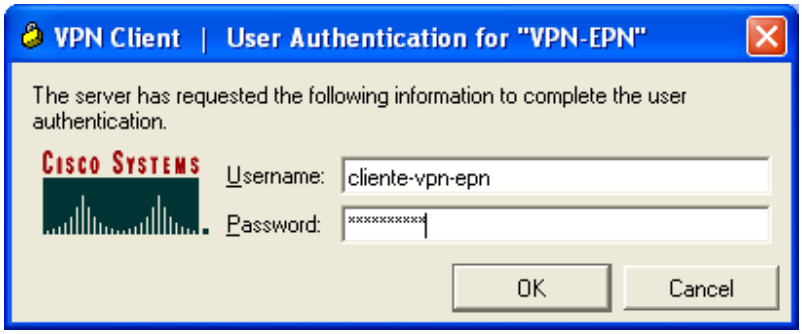


Figura 3-17 Autenticación de Usuario VPN

11. Una vez que se ingresa a la VPN se tiene acceso a servicios y servidores en la Intranet, de acuerdo a la configuración del servidor VPN. Por ejemplo se puede acceder remotamente a una máquina que se encuentre en la LAN y monitorear la red, configurar equipos. En este caso, se tendrá acceso al servidor Asterisk Now, que permite la comunicación telefónica entre usuarios remotos con usuarios locales y viceversa.

3.4 IMPLEMENTACIÓN DEL SERVICIO DE VOIP [2]

Para la implementación del servicio de VoIP se tiene varias alternativas tanto en software como en hardware. Por las diferentes ventajas que presenta Asterisk Now y por ser un sistema operativo basado en Linux se lo utiliza para la instalación de la Central IP.

Para mayor referencia, el proceso de instalación del servidor Asterisk se detalla en el Anexo C. A continuación se detalla la configuración de Asterisk como central telefónica.

Una vez instalado y reiniciado el servidor Asterisk Now se despliega una ventana que muestra la dirección IP del servidor, esta dirección puede ser fija o dinámica, además se despliega un menú donde se encuentran opciones para actualizar el sistema, acceder al servidor vía consola, reiniciar el servicio de Asterisk, reiniciar y apagar el servidor, como se indica en la Figura 3-18.

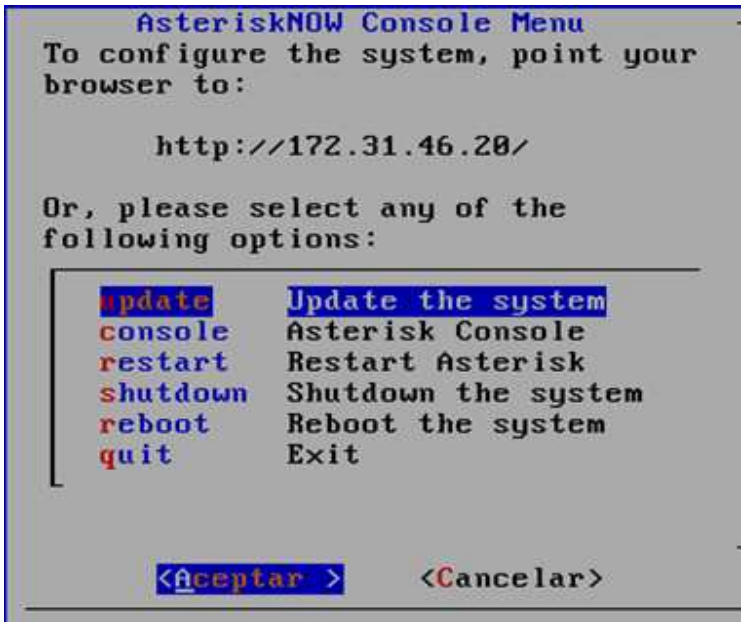


Figura 3-18 Menú para la consola de Asterisk Now

3.4.1 ADMINISTRACIÓN DEL SERVIDOR ASTERISK

Para administrar la central Asterisk se tienen dos alternativas:

- ✓ Vía HTTP[19].
- ✓ Vía SSH[20].

3.4.1.1 Administración De Asterisk Vía HTTP

Para una administración vía HTTP o WEB se debe disponer de un ordenador en red con el servidor Asterisk y mediante un navegador web, como Firefox o Internet Explorer, se accede tipiando la dirección IP del servidor en la barra de búsqueda del navegador.

A continuación se debe ingresar el usuario y la contraseña, que son configurados en la instalación del servidor Asterisk, Figura 3-19.

[19] HTTP, El protocolo de transferencia de hipertexto es el protocolo usado en cada transacción de la Web (WWW).

[20] SSH (Secure SHell) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red de manera segura.

Usuario: *admin*.

Password: *asterisk*

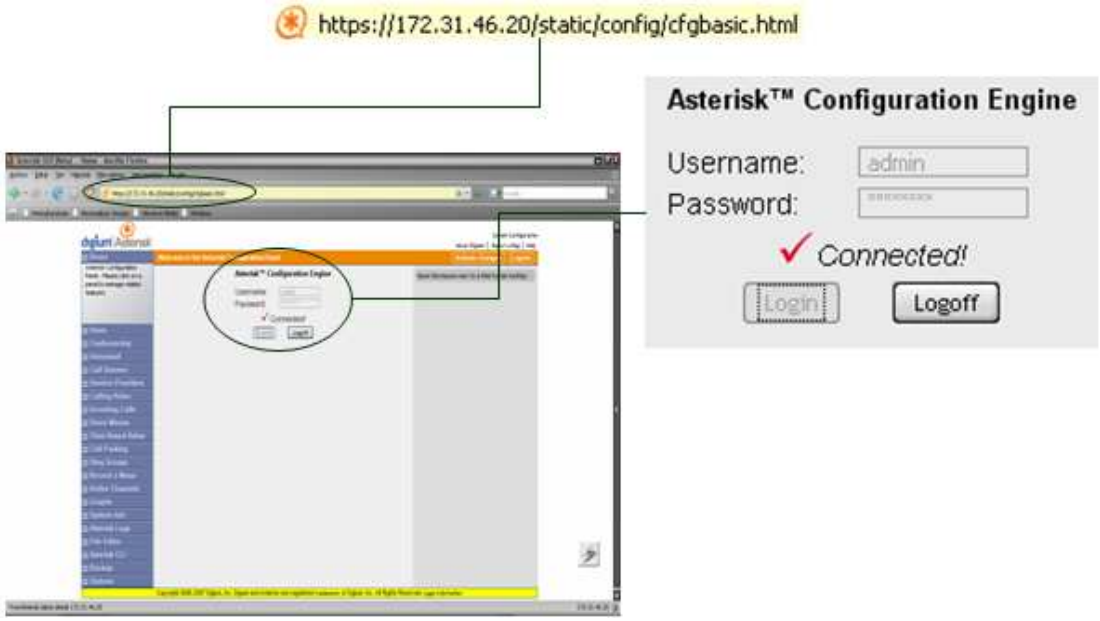


Figura 3-19 Ingreso Al Servidor Asterisk Now

Una vez ingresada a la página de configuración de Asterisk, se despliega un menú con varias opciones. Para crear, editar y borrar usuarios, se ingresa a la opción de ***users*** donde se registran los usuarios, número de extensión, contraseña y el protocolo para VoIP. Para el proyecto en particular se utiliza el protocolo SIP.

En la Figura 3-20 a continuación se indica los parámetros a configurar para crear un usuario con su extensión telefónica.

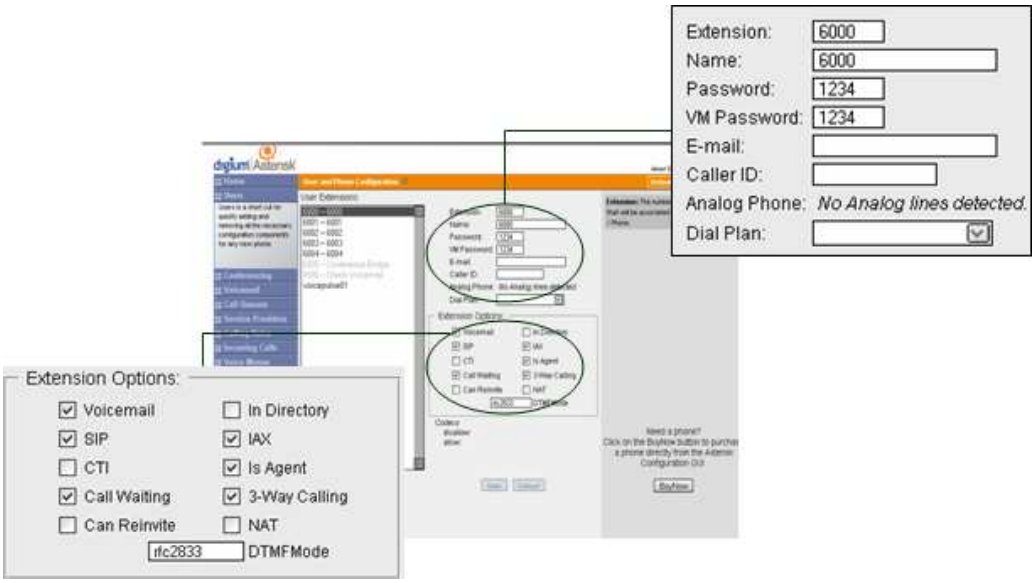


Figura 3-20 Configuración De Usuarios Y Extensiones Digitales

Para configuraciones avanzadas del sistema como cambiar la dirección IP y el tipo de usuario del sistema, se accede en el link ***"system configuration"*** donde se despliega una pantalla de autenticación de usuario, se digita el usuario *"admin"* y la clave por defecto *"password".*

Una vez autenticado el usuario se despliega un menú en el que se puede configurar una dirección IP fija o dinámica para el servidor, la contraseña del usuario privilegiado (root), entre otros parámetros, que no inciden en el desarrollo del proyecto.

En la Figura 3-21 se indica la configuración de la contraseña del usuario root. Se configuró ***asterisk*** como contraseña del usuario root, como se muestra a continuación.

Figura 3-21 Configuración de contraseña del usuario Root

3.4.1.2 Administración de Asterisk vía SSH

Para configuraciones más avanzadas, se accede al servidor Asterisk vía SSH. Se utiliza el software PuTTY que sirve para acceder a un equipo en la red vía telnet, vía ssh o vía serial.

Para acceder al servidor Asterisk, se debe configurar la dirección del servidor o en su defecto el nombre del servidor, si se dispone de un servidor DNS como se muestra en la Figura 3-22.

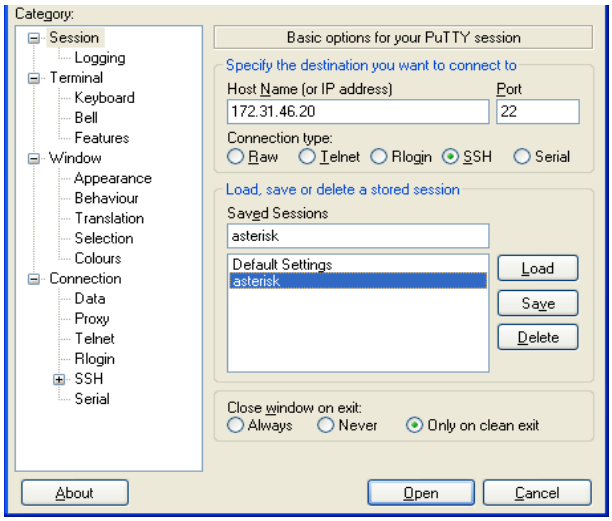


Figura 3-22 Configuración De PuTTY Para Acceder Al Servidor Vía SSH.

Una vez ingresado al servidor se despliega una ventana igual a cualquier sistema Linux en donde se solicita el usuario y contraseña, configurados en la instalación. Para ingresar como “root”, que es el usuario administrador, se digita el comando “*su”* y la contraseña “*asterisk”,* Figura 3.23.

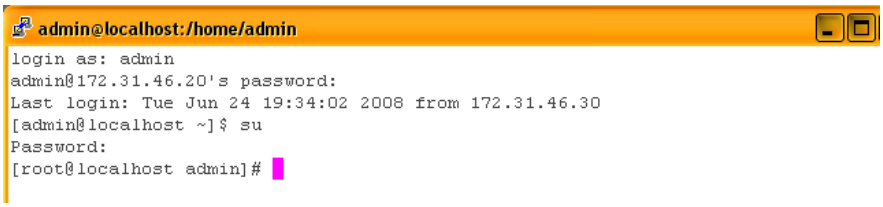


Figura 3-23 Ingreso al Servidor Asterisk Now vía ssh

El directorio de los archivos de configuración tanto de SIP como de otros parámetros de Asterisk, se encuentran en el directorio cd /etc/asterisk, Figura 3-24.

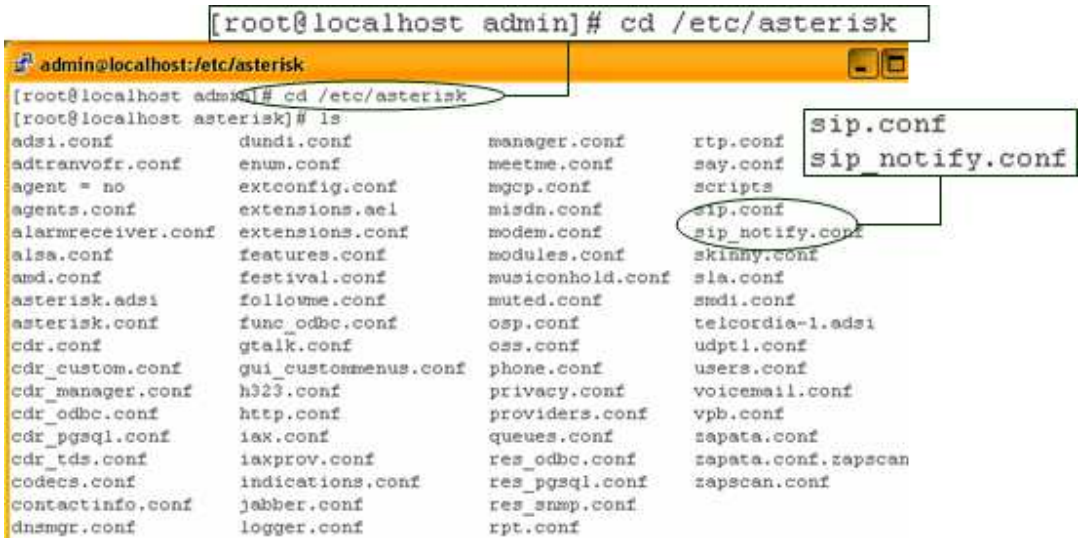


Figura 3-24 Archivos De Configuración De Asterisk

Para tener servicios adicionales como video llamada a través del protocolo SIP se debe acceder al archivo sip.conf, con el comando **"vi sip.conf",** y habilitar el servicio de video llamada con el comando **"videosupport=yes",** como se muestra en la Figura 3-25.

Para guardar los cambios configurados en el archivo sip.conf se digita las teclas "Shift ZZ " o las teclas "wq!".

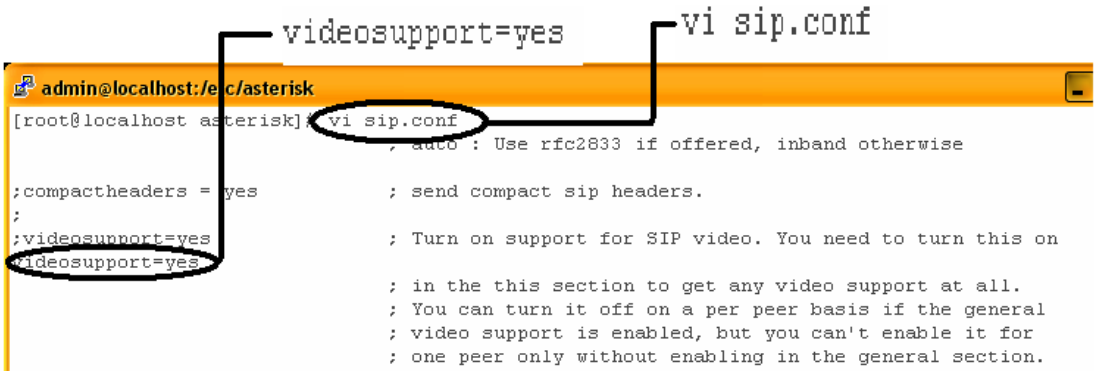


Figura 3-25 Configuración De Video Llamada Con SIP

Para crear, editar y borrar usuarios, se edita el archivo users.conf, en este archivo se debe ingresar entre corchetes el número de extensión, el usuario, la contraseña

```
[6006]
callwaiting    = yes
cid_number     =
context        =
```

y los protocolos para realizar llamadas. A continuación se indica un ejemplo de los comandos que se deben tener para la creación de la extensión 6006.

3.4.2 INSTALACIÓN Y CONFIGURACIÓN DEL SOFTPHONE [3]

Para manejar la central IP y hacer llamadas, se necesita teléfonos IP o en su defecto PCs equipadas con softphones. El softphone utilizado para las pruebas es X-lite que sirve para realizar llamadas a través del protocolo SIP.

La instalación de este softphone es como cualquier aplicación sobre Windows, donde se aceptan los parámetros por defecto, y se instala.

Una vez instalado el softphone se debe configurar los parámetros, para que el softphone se registre en el servidor Asterisk, y pueda realizar llamadas a otros usuarios registrados.

En la parte superior del programa, se encuentra un botón, en el cual se encuentra la opción “SIP Account settings”, en donde se configurará el softphone con los parámetros definidos para las extensiones, las cuáles son configuradas en el servidor Asterisk Figura 3.26.

Figura 3-26 Softphone X-lite.

Después de seleccionar “SIP Account Settings”, se despliega una ventana y se selecciona la opción de Add. A continuación se despliega otra ventana donde se configura los parámetros de la extensión. A continuación en la Figura 3.27, se indica un ejemplo de configuración de una extensión.

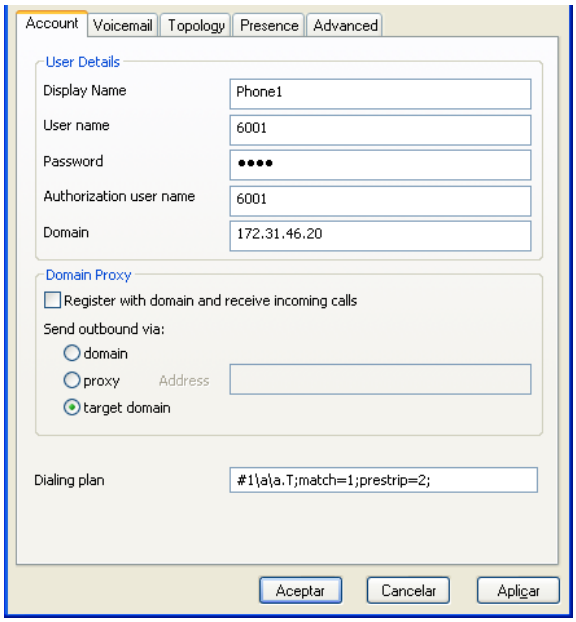


Figura 3-27 Configuración De La Extensión Telefónica

Detalle de los campos:

- Display Name: Nombre o alias del usuario para mostrar en pantalla.

- User Name: Nombre o extension que nos ha asignado el administrador de Asterisk (sip.conf parámetro entre corchetes)

- Password: La contraseña asignada por el administrador de Asterisk (sip.conf el parámetro secret)

- Authorization user name: Número de la extensión

- Domain: La dirección Ip del servidor Asterisk

Si todos los parámetros configurados para una extensión, se encuentran correctos, en la pantalla del Softphone se despliega el mensaje "**Ready**", como se indica en la Figura 3-28.

Figura 3-28 Registro exitoso de la extensión

Por otro lado, si un parámetro se encuentra mal configurado, o si el PC con el softphone instalado no tiene conexión con el servidor Asterisk, se muestra en la pantalla del softphone el mensaje “Registration error 404 – Not found”, como se indica en la Figura 3-39.

Figura 3-29 Falla en el registro de la extensión

Una vez resuelto todos los inconvenientes de registro del softphone, se puede realizar llamadas telefónicas entre los softphones registrados. De esta manera se pueden realizar llamadas entre usuarios en la LAN de la oficina matriz, de la Sucursal, y Hosts remotos.

3.4.3 CONFIGURACIÓN DEL TELÉFONO IP CISCO 7960 [4]

La configuración de la extensión telefónica en el teléfono IP, es similar a la configuración del softphone, se necesita tener en red el teléfono IP con el servidor Asterisk. El teléfono por defecto se encuentra configurado para obtener una dirección IP dinámicamente, pero se lo puede configurar con una dirección fija.

El teléfono IP cuenta con varios botones entre los cuales se accede a mensajes, servicios, directorios y configuraciones del equipo, como se indica en la Figura 3-30.

Figura 3-30 Teléfono IP 7960

Para configurar el teléfono IP se presiona el botón ***settings***, donde se despliega una pantalla con un menú, con los parámetros de configuración, los cuáles se indican en la Figura 3-31.

- ✓ Contraste: En este parámetro se regula el contraste de la pantalla, para tener una mejor visualización.

- ✓ Tipo de Timbre: En este parámetro se escoge el tipo de tono para el teléfono.

- ✓ Configuración de red: En este parámetro se configura una dirección IP fija o dinámica, servidor DNS, gateway, entre otros parámetros de red.

- ✓ Configuración SIP: en este parámetro se configura la extensión telefónica, el usuario, la contraseña, la dirección del servidor de VoIP.

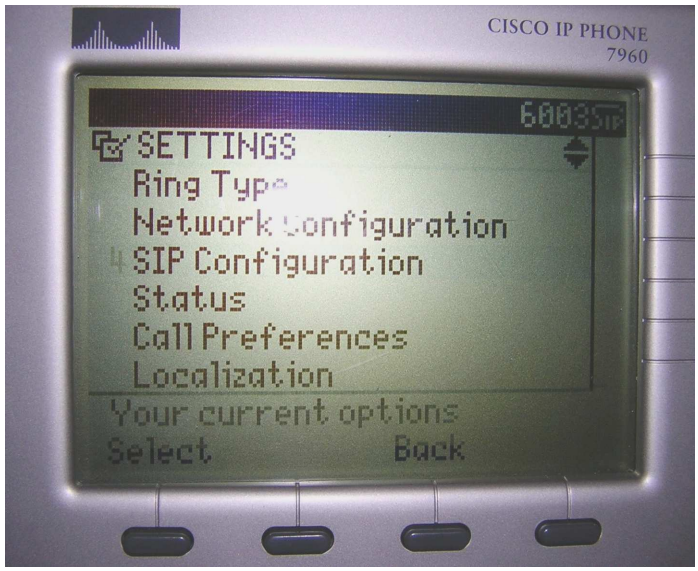


Figura 3-31 Menú de configuración del Teléfono IP

En la Figura 3-32, se da un ejemplo de cómo configurar una dirección fija para el teléfono IP en la subred de la UGI. Se configura al teléfono con la dirección 172.31.46.30 / 26, de esta manera el teléfono se encontrará en la misma red que el servidor VPN que tiene la dirección 172.31.46.30 / 26.

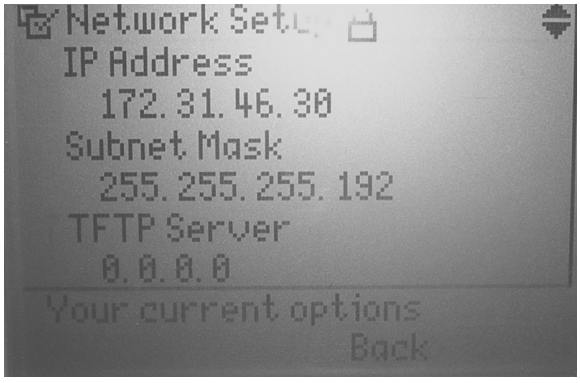


Figura 3-32 Configuración de una dirección IP fija del Teléfono IP

En la Figura 3-33, se da un ejemplo de cómo configurar una extensión telefónica en el teléfono IP. Los parámetros configurados, son iguales al softphone, se necesita configurar el nombre de usuario, la extensión, la clave, y la dirección del servidor Asterisk.

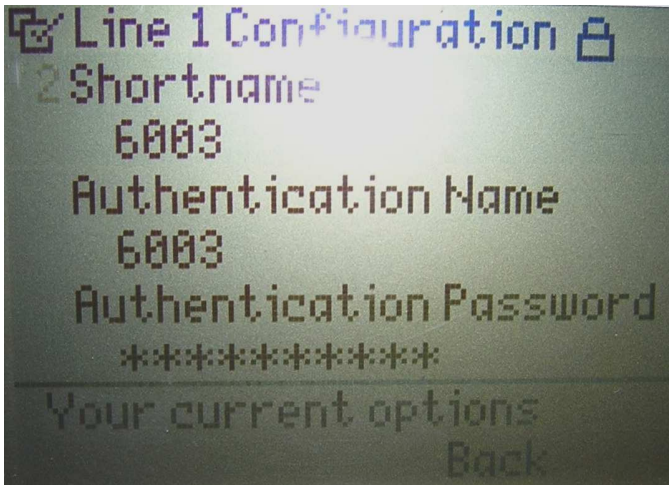


Figura 3-33 Configuración de una dirección IP fija del Teléfono IP

Con el proceso de implementación y configuración realizados, tanto de los equipos y software que intervienen en el túnel VPN y la central telefónica, se da paso al Capítulo 4, donde se muestran una serie de pruebas y resultados para determinar el funcionamiento y la validez de la red implementada.

BIBLIOGRAFÍA - CAPITULO 3

[1] Knowledgenet.Cisco.Securing.Networks.with.PIX.and.ASA.SNPA.Student. Guide.V4.0.eBook-DDU.pdf

[2] URL: http://www.balearsinnovacio.com/blog/wpcontent/uploads/2007/07/ ManualAsterisk_innova.pdf

[3] URL: http://garvanet.com/xten/

[4] URL: http://www.sistemasyenlaces.com.ar/Cisco7960_7940_IPPhone.html

CAPÍTULO 4

4 PRUEBAS Y RESULTADOS DE LA SIMULACIÓN

Luego de haber realizado la configuración, tanto de los equipos de red como de aquellos que intervienen en la administración de las terminales telefónicas, se procede a una serie de pruebas para determinar la validez del diseño y configuración realizados. Con este propósito se recrea un ambiente similar a un escenario VPN de acceso remoto, sobre Internet a través de un ISP. Se determinará también si se pueden realizar llamadas mediante IP en la LAN con las herramientas y facilidades de la administración telefónica Asterisk.

Con los objetivos indicados se procederá a levantar un túnel VPN, seguido de una comunicación telefónica que se lleva a cabo sobre el túnel previamente establecido. En la comunicación telefónica se utiliza software telefónico, en este caso X-Lite, y un teléfono IP CISCO, operando ambos con protocolo SIP. Para el túnel VPN se utiliza un equipo de frontera y software propietario para usuario remoto VPN.

Para mantener la confidencialidad sobre la Polired, se omite las direcciones IP específicas de los equipos de seguridad y de acceso utilizados durante la implementación y el periodo de pruebas del proyecto. En su defecto se mencionan los dos primeros campos que conforman la dirección IPv4.

4.1 DESCRIPCIÓN DE LOS ESCENARIOS DE PRUEBA

Tal como se indicó hasta aquí, gracias a la colaboración de la Unidad de Gestión de Información (UGI) que facilitó el acceso a los equipos de red pertinentes. El proceso de prueba se llevó a cabo en los predios de la Escuela Politécnica Nacional, sobre la Polired. Además se utilizó una conexión doméstica de Internet

ubicada en el sector de la Mariscal, para simular un ambiente de acceso remoto.

La Polired es una red jerárquica de 3 capas, acceso, distribución y núcleo, además cuenta aproximadamente con 1000 usuarios. Es por esta razón que el proceso de pruebas realizado permite obtener resultados aproximados a la realidad de una empresa como SONDA; en la que no es posible realizar pruebas debido a políticas y restricciones propias, además de no contar con los equipos necesarios para llevar a cabo la implementación del proyecto.
Dicho esto se proponen 2 escenarios para llevar a cabo la conexión VPN.

4.1.1 ESCENARIO SOBRE UNA RED WAN

Este escenario se divide en tres segmentos, como se indica en la Figura 4-1, los mismos que se indican a continuación.

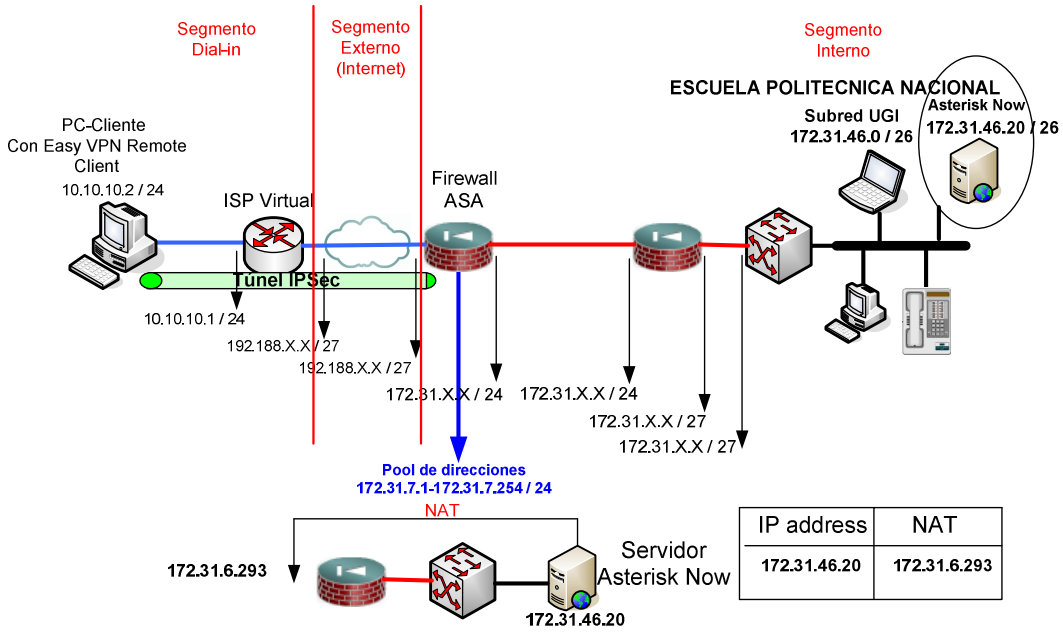


Figura 4-1 Acceso Remoto sobre una WAN

4.1.1.1 Segmento Dial-in

Es el segmento que permite a un usuario el acceso desde el PC-Cliente hacia servidores y equipos de la Institución, que cuentan con direcciones públicas, simulando a un usuario en Internet. Entre los servidores públicos a los que se tiene acceso se destaca el servidor Web, el servidor de Correo Electrónico, y el servidor VPN.

El PC-Cliente tiene la dirección 10.10.10.2 /24 y se conecta directamente a una interfaz del Router de Borde de la Institución, configurado con la dirección 10.10.10.1/24. El Router de Borde constituye en un ISP virtual para el PC-Cliente, simulando lo que sería un acceso sobre Internet, con la diferencia de que el acceso remoto se lo hace a través de un ancho de banda de 100 Mbps.

Antes del túnel el usuario remoto no podrá conectarse con usuarios en la Intranet debido a que el PC-Cliente y la Intranet están en redes privadas diferentes, de esta manera se crea un ambiente WAN.

4.1.1.2 Segmento Externo (WAN)

En este escenario, que simula al Internet, se utiliza una red WAN formada por un Router de Borde conectado al Firewall ASA de la Institución.

El router se conecta a la interfaz de salida del Firewall (Servidor VPN). El Firewall, al configurarlo como servidor VPN permite a usuarios remotos acceder a la Intranet. En el Firewall se configuran las políticas y los puertos necesarios para realizar las llamadas mediante VoIP. El usuario remoto, para las pruebas, sólo podrá acceder a ciertas máquinas en la UGI que se encuentran en la subred 172.31.46.0 / 26. El servidor Asterisk se encuentra en esta subred y se lo configura con una dirección IP estática 172.31.46.20 / 26.

4.1.1.3 Segmento Interno (Polired)

La Polired cuenta con varias subredes divididas de acuerdo a las políticas de la Institución, agrupadas dentro de la red 172.31.0.0 / 16. La Polired se conecta a través del switch de Core, ubicado en la UGI, a la interfaz del Firewall, que brinda seguridad a la Intranet a través de filtros, y a su vez se conecta al Firewall servidor VPN. Este equipo realiza la función de NAT y de PAT para que los usuarios y subredes en la Polired tengan salida a Internet.

El usuario remoto al conectarse a la VPN tendrá conectividad con cualquier host que se encuentre en la red 172.31.6.0, ya que la interfaz del servidor VPN se encuentra en esta red. Por esta razón se requiere realizar la traducción de dirección del servidor Asterisk Now, con la dirección 172.31.6.239, como se indicó en la Figura 4-1. El usuario remoto podrá realizar llamadas a cualquier extensión que se encuentre registrada en el servidor Asterisk.

4.1.2 ESCENARIO SOBRE INTERNET

En este escenario se realiza una prueba real del proyecto, en la que un usuario autorizado sobre Internet podrá acceder a la red interna de la Escuela Politécnica Nacional. Por motivo de pruebas se limita el acceso a ciertas máquinas en la subred de la UGI, que es donde se encuentran los servidores y en particular el servidor VPN.

El objetivo es que un usuario sobre Internet se conecte al túnel VPN y pueda realizar llamadas mediante VoIP, hacia usuarios dentro de la Institución y viceversa. No está por demás recalcar que las llamadas se realizarán con mayor seguridad y confidencialidad, entre otras ventajas de utilizar VPNs.

Este escenario también se divide en tres segmentos, como se indica en la Figura 4-2, los mismos que se indican a continuación.

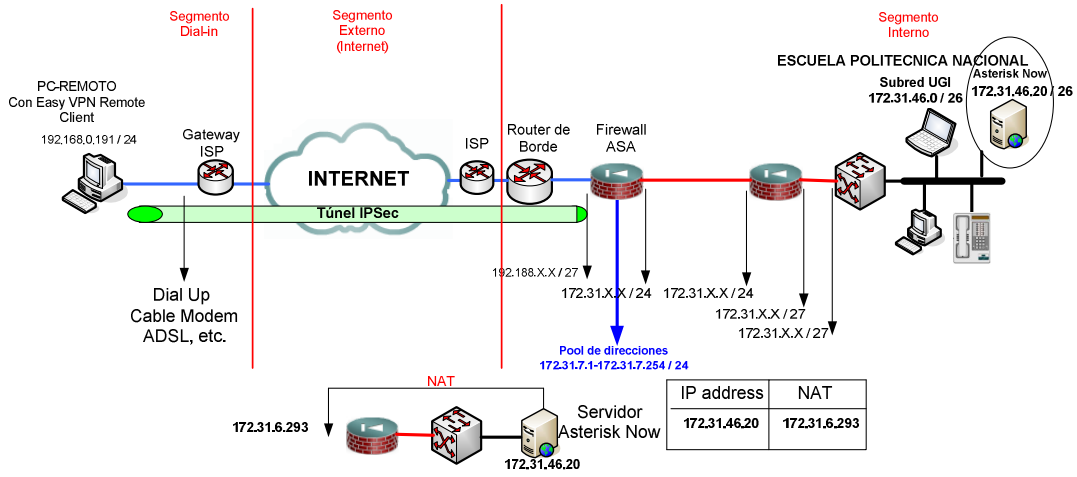


Figura 4-2 Acceso Remoto sobre Internet

4.1.2.1 Segmento Dial-in

Este segmento se caracteriza por permitir al usuario el acceso a Internet a través de un ISP. Para el proyecto las pruebas se realizaron con un Host que tiene salida a Internet a través de la empresa TV Cable con un ancho de banda de 256 kbps.

El ISP le asigna al Host la dirección 192.168.0.191 / 24 y a través de Internet tendrá conectividad con las direcciones públicas de la Institución. Debido a que tanto el Host remoto como la LAN de la Polired cuentan con direcciones privadas, inicialmente no se tendrá conectividad entre el host remoto y la LAN de la Polired y viceversa.

Una vez establecido el túnel, el usuario remoto podrá acceder a la LAN de la Institución y además podrá realizar llamadas a usuarios dentro de la Polired.

4.1.2.2 Segmento Externo (Internet)

Este segmento, conocido como Internet, es una gran nube de nodos, que por su magnitud y complejidad se vuelve impredecible. El ISP del usuario remoto es TV

Cable con el servicio de Cable MODEM y el de la Escuela Politécnica Nacional es Telconet. Al ejecutar el comando tracert[21] en el usuario remoto se determina que existen 15 saltos entre el usuario remoto y el servidor VPN, como se observa en la Figura 4-3; es decir que entre ambos extremos del túnel el tráfico atraviesa 15 nodos hasta llegar a su destino. La ventaja de implementar la VPN en los predios de la Institución es que se podrá acceder a equipos dentro de la Polired, vía Internet, sin importar el lugar geográfico donde se encuentre el usuario remoto.

4.1.2.3 Segmento Interno (Polired)

Es el segmento en el que se filtra el tráfico desde Internet hacia la Intranet y viceversa, brindando seguridad a los usuarios, protección de la información y de los equipos en la red interna.

En este segmento se tiene a la red LAN que sale a Internet a través del Router de borde que se comunica con los equipos de Telconet. Las funciones de seguridad y de la traslación de direcciones se las realiza en los Firewalls de la Institución. En este caso el segmento interno es el mismo señalado en el punto 4.1.1.3

4.2 PROCESO PARA EL ESTABLECIMIENTO DE LA VPN

El establecimiento del acceso remoto es igual para los dos escenarios anteriores. A continuación se indican los pasos a seguir para que un usuario acceda remotamente.

4.2.1 CONEXIÓN AL SERVIDOR VPN

El túnel se establece entre el usuario remoto y el servidor VPN. Para poder ingresar a la red privada virtual se debe tener conectividad (ping) al servidor VPN,

[21] Tracert es un utilitario del conjunto de protocolos TCP/IP que determina la ruta tomada, determinando el número de nodos que atraviesa un paquete desde su origen hasta su destino

ya sea vía WAN o vía Internet, y se debe tener instalado el cliente VPN en el Host Remoto.

En la configuración del software VPN Client se deberá configurar la dirección del servidor VPN, el nombre del túnel y la contraseña de la autenticación del cliente VPN. Estos parámetros son configurados en el servidor VPN como se indicó en el Capitulo 3 y se indica en la Figura 4-3.

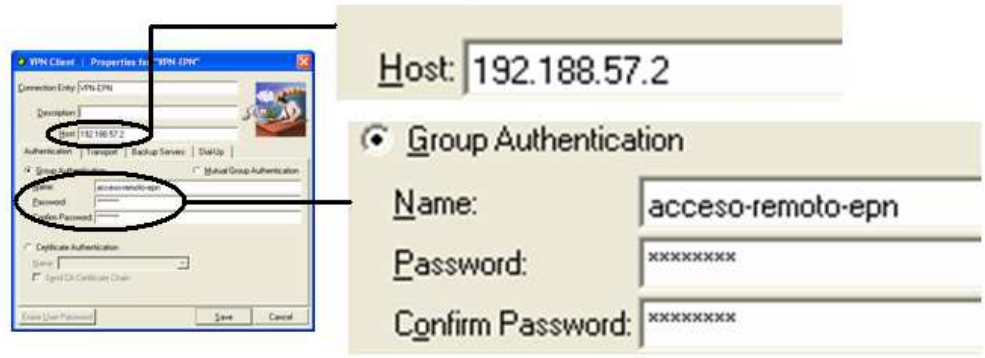


Figura 4-3 Parámetros configurados en el VPN Client

4.2.2 AUTENTICACIÓN DE USUARIO

Para acceder al túnel se debe ser un usuario autorizado. Una vez autenticado el Cliente con el servidor VPN, se deberá autenticar el usuario para acceder al túnel y a la red LAN.

Este usuario puede ser configurado localmente en el servidor VPN o se podrá tener un servidor externo de autenticación que puede ser un servidor Radius[22] o TACACS[23]. Para el proyecto se configuró un usuario localmente.

En la Figura 4-4 se muestra la ventana de autenticación de usuario y se ingresó

---

[22] Radius (*Remote Authentication Dial-In User Server*). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP.

[23] TACACS (*Terminal Access Controller Access Control System) es* un protocolo de autenticación remota que se usa para comunicarse con un servidor de autenticación Cisco.

el nombre del usuario remoto autorizado y la contraseña.
El usuario y contraseña configurados son “cliente-vpn-epn” y “cisco123**” respectivamente.

Figura 4-4 Autenticación de Usuario

4.2.3 ESTABLECIMIENTO DEL TÚNEL

Una vez autenticado el cliente VPN y el usuario remoto, se establece un túnel mediante el protocolo IPSec de acuerdo a los parámetros configurados en el Capítulo 3.

4.2.4 ASIGNACIÓN DE DIRECCIÓN IP

Al conectarse el usuario remoto al túnel se asigna una dirección IP dinámica al host remoto. El pool de direcciones configuradas tiene el siguiente rango de direcciones 172.31.7.1 – 172.31.7.254 y la máscara de red 255.255.255.0.

Conforme se vayan conectando clientes a la VPN se les asigna dinámicamente direcciones IP del pool configurado en el servidor.

4.2.5 TRANSMISIÓN DE DATOS

Una vez establecido el túnel y asignada la dirección IP se pueden realizar llamadas entre el usuario remoto y usuarios dentro de la Polired y viceversa.

4.2.6 TERMINACIÓN DEL TÚNEL

La comunicación del túnel puede terminar por que el usuario se desconecta del túnel manualmente o por que se termina el tiempo de vida de la conexión configurada en el servidor VPN.

4.3 PRUEBAS DE LA CONEXIÓN A LA VPN

4.3.1 ACCESO REMOTO SOBRE UNA WAN SIMULADA

4.3.1.1 Antes del túnel

Antes de establecer el túnel VPN sobre la red WAN simulada, se realizó pruebas de conectividad hacia direcciones públicas y privadas de la Institución. Además se determinó el número de saltos desde el Host remoto hacia servidores públicos de la Polired.

En la Tabla 4-1 se indica los resultados obtenidos antes de establecer el túnel VPN.

Ping direcciones públicas	**192.188.57.254**	**Exitoso**	Servidor Web de la Institución
Ping direcciones privadas	**172.31.6.239**	**Fallido**	Servidor Asterisk interno
Tracert direcciones públicas	**192.188.57.254**	**2 saltos**	Servidor Web de la Institución
Tracert direcciones privadas	**172.31.6.239**	**Fallido**	Servidor Asterisk interno

Tabla 4-1 Resultados de las pruebas antes de establecer el túnel sobre una red WAN

En la Figura 4-5 se muestra los saltos desde el Host remoto hacia el servidor WEB 192.188.57.254 / 28. Se realiza esta prueba con el fin de comparar el número de saltos una vez establecido el túnel.

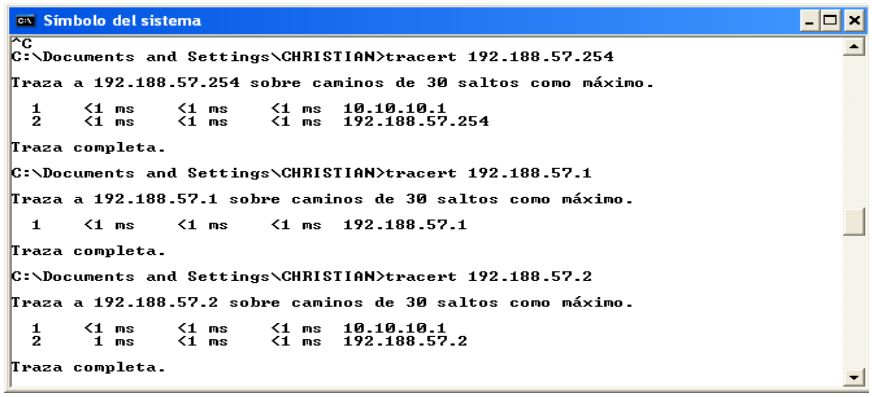


Figura 4-5 Saltos hacia servidores públicos de la Polired

En la Figura 4-5 se puede ver que se tiene dos saltos entre el host conectado al Router y los servidores públicos.

4.3.1.2 Después del túnel

Una vez que el Host remoto se conecta al túnel, el cliente adquiere una dirección dinámica del pool de direcciones disponible. De esta manera el host remoto tendrá la dirección local 10.10.10.2 / 24 y la dirección del túnel 172.31.7.1 / 24, como se indica en la Figura 4-6. Con la dirección 172.31.7.1 / 24 el usuario remoto es virtualmente parte de la LAN y podrá acceder a PCs y servicios dentro de la LAN y realizar llamadas a través de VoIP a usuarios en la LAN y viceversa.

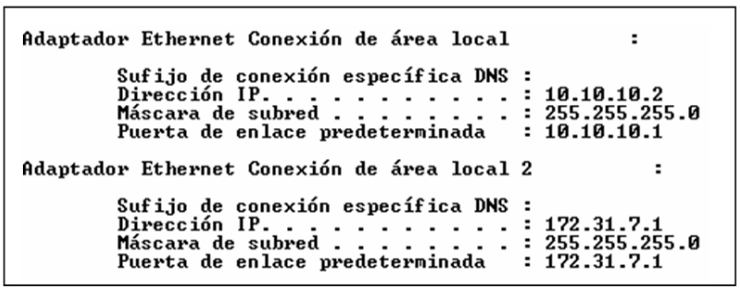


Figura 4-6 Dirección IP Asignada al Host conectado remotamente

Una vez que el host es virtualmente parte de la red LAN, se realizan pruebas de conectividad hacia direcciones públicas y privadas en la Polired. De igual manera,

se determina el número de saltos hacia servidores públicos e internos de la Institución, obteniéndose los resultados que se indican en la Tabla 4-2.

Ping direcciones públicas	**192.188.57.254**	**Exitoso**	Servidor Web de la Institución
Ping direcciones privadas	**172.31.6.239**	**Exitoso**	Servidor Asterisk interno
Tracert direcciones públicas	**192.188.57.254**	**1 salto**	Servidor Web de la Institución
Tracert direcciones públicas	**192.188.57.2**	**1 salto**	Servidor VPN de la Institución
Tracert direcciones privadas	**172.31.6.239**	**1 salto**	Servidor Asterisk interno

Tabla 4-2 Resultados después de establecer el túnel sobre la red WAN

En la Figura 4-15 se indica los saltos hacia host internos, entre ellos el servidor Asterisk 172.31.6.239 y en todos los casos tiene un solo salto, esto es debido a que el host remoto forma virtualmente parte de la LAN.

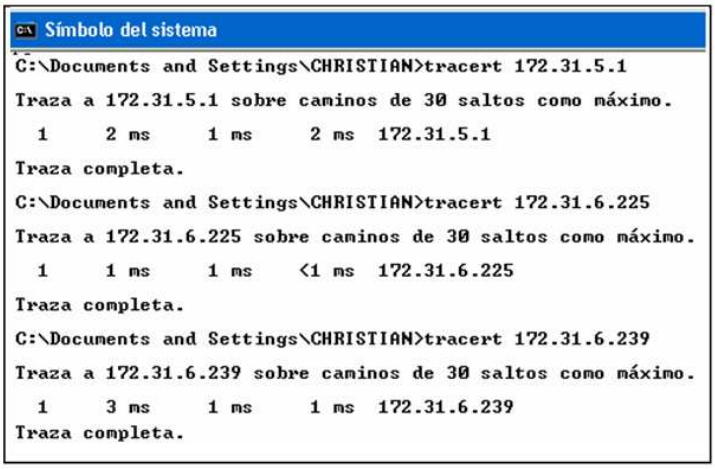


Figura 4-7 Saltos hacia PCs dentro de la LAN desde el Host remoto

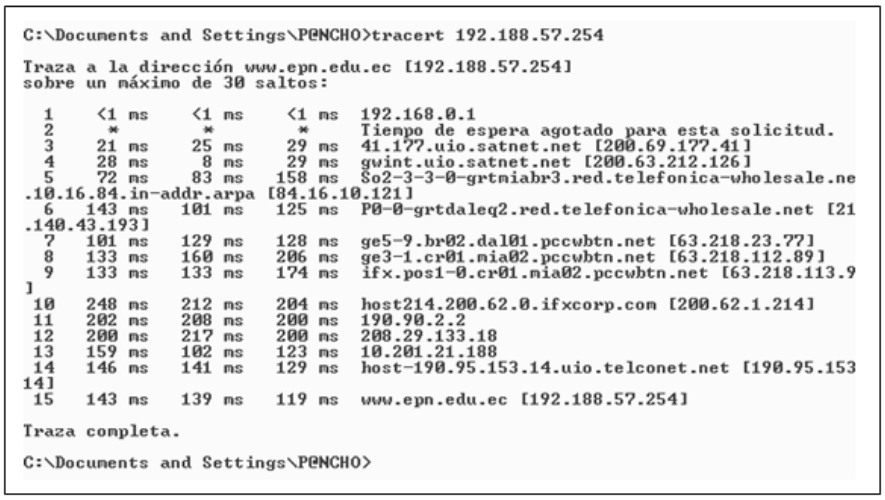
4.3.2 ACCESO REMOTO SOBRE INTERNET

Para determinar que un Host con salida a Internet se conecta a un túnel mediante acceso remoto se debe hacer pruebas de la conexión antes y después del túnel.

4.3.2.1 Antes del Túnel

Antes de establecer el túnel, el host tiene únicamente la IP asignada por el proveedor de Internet, 192.168.0.100 / 24, y solo podrá tener acceso a las máquinas de la Institución con direcciones públicas, como por ejemplo servidor Web, servidor de correo, DNS público, Router de borde y servidor VPN.

En la Figura 4-8 se muestra el retardo y el número de saltos desde el PC-Remoto hacia el servidor Web de la Institución cuya dirección IP pública es 192.188.57.254 / 28. Luego de lo cual se determina que en promedio se tiene un retardo de 134 ms y un total de 15 saltos hacia el servidor Web.



```
C:\Documents and Settings\P@NCHO>tracert 192.188.57.254

Traza a la dirección www.epn.edu.ec [192.188.57.254]
sobre un máximo de 30 saltos:

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2     *        *        *     Tiempo de espera agotado para esta solicitud.
  3    21 ms    25 ms    29 ms  41.177.uio.satnet.net [200.69.177.41]
  4    28 ms     8 ms    29 ms  gwint.uio.satnet.net [200.63.212.126]
  5    72 ms    83 ms   158 ms  So2-3-3-0-grtmiabr3.red.telefonica-wholesale.ne
.10.16.84.in-addr.arpa [84.16.10.121]
  6   143 ms   101 ms   125 ms  P0-0-grtdaleq2.red.telefonica-wholesale.net [21
.140.43.193]
  7   101 ms   129 ms   128 ms  ge5-9.br02.dal01.pccwbtn.net [63.218.23.77]
  8   133 ms   160 ms   206 ms  ge3-1.cr01.mia02.pccwbtn.net [63.218.112.89]
  9   133 ms   133 ms   174 ms  ifx.pos1-0.cr01.mia02.pccwbtn.net [63.218.113.9
]
 10   248 ms   212 ms   204 ms  host214.200.62.0.ifxcorp.com [200.62.1.214]
 11   202 ms   208 ms   200 ms  190.90.2.2
 12   200 ms   217 ms   200 ms  208.29.133.18
 13   159 ms   102 ms   123 ms  10.201.21.188
 14   146 ms   141 ms   129 ms  host-190.95.153.14.uio.telconet.net [190.95.153
14]
 15   143 ms   139 ms   119 ms  www.epn.edu.ec [192.188.57.254]

Traza completa.

C:\Documents and Settings\P@NCHO>
```

Figura 4-8 Tracert al servidor WEB de la Institución

A continuación se prueba que antes de la conexión VPN no se tiene conectividad a PCs dentro de la LAN de la Polired. En la Figura 4.9 se muestra el resultado negativo del comando ping a la dirección 172.31.5.1 / 27.

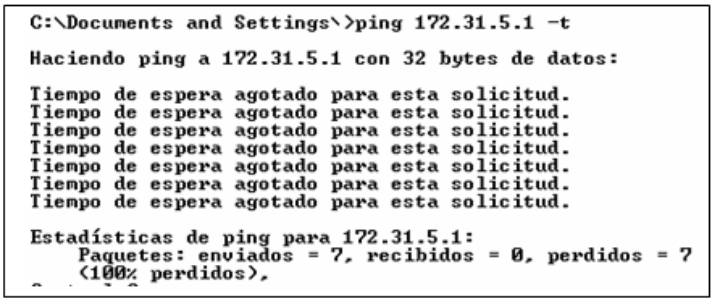


Figura 4-9 Ping a una IP interna

4.3.2.2 Después del Túnel

Una vez establecido el túnel, el servidor VPN le asigna una dirección IP dinámica del pool configurado. Por consiguiente el Host remoto tendrá la dirección IP local y la dirección asignada por el servidor VPN 172.31.7.2/24 como se muestra en la Figura 4-10.

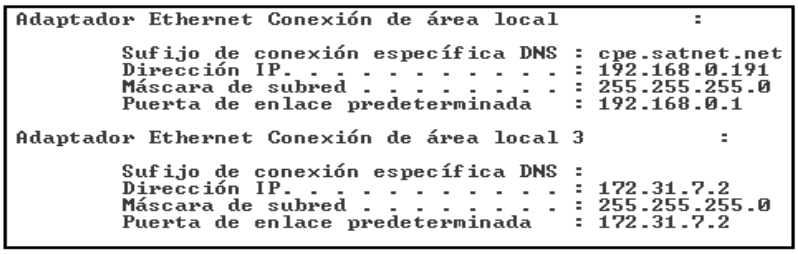


Figura 4-10 Direccionamiento después de conectarse al túnel

Una vez que el cliente VPN se conecta al túnel puede tener acceso a la red LAN de la Institución, se muestra en la Figura 4-11, el ping exitoso a la dirección 172.31.5.1.

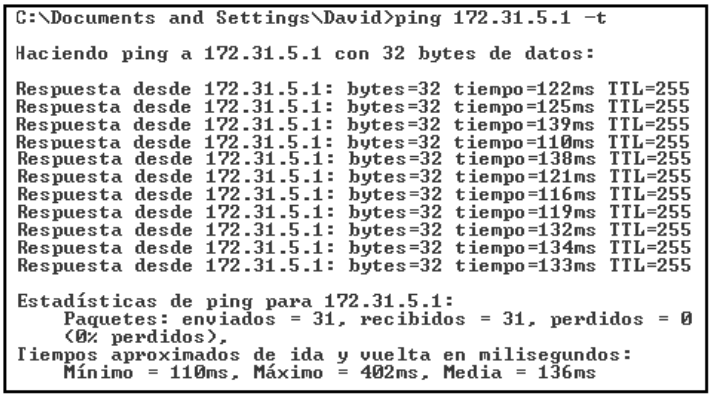


Figura 4-11 Retardo hacia una IP interna después del túnel

Una vez que el host remoto es parte de la red LAN se analiza los saltos hacia direcciones públicas e internas de la Polired. En la Figura 4-12 se indica el salto hacia el servidor Web de la Institución 192.188.5.254 después del túnel y, como se puede observar, es de un solo salto a diferencia de los 15 saltos que se obtuvo antes del túnel. De igual manera se tiene un solo salto hacia direcciones internas, como se indica en la Figura 4-13.

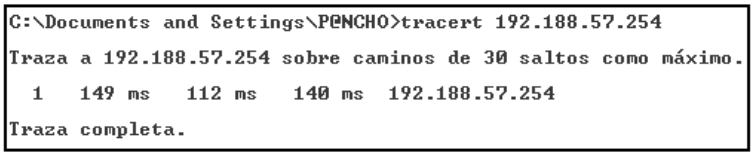


Figura 4-12 Saltos hacia el servidor Web después del túnel

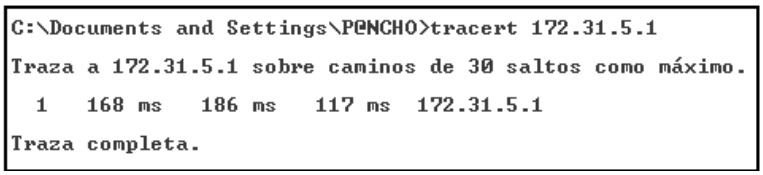


Figura 4-13 Saltos hacia IPs internas después del túnel

A continuación en la Tabla 4-1 se indica un resumen de las pruebas realizadas sobre la conexión VPN a través de Internet.

Item	Antes del Túnel	Después del Túnel
Dirección IP Local	**192.168.0.191 / 24**	192.168.0.191 / 24
Dirección IP del túnel	**---**	172.31.7.2 / 24
Ping Direcciones Públicas en la Polired	**Si**	Si
Retardo promedio hacia Servidor Web	**125 ms**	125 ms
Número de Saltos hacia Servidor Web	**15**	1
Ping Direcciones Privadas	**No**	Si
Retardo promedio hacia Switch de Core	**----**	136 ms
Número de Saltos hacia Switch de Core	**----**	1

Tabla 4-3 Resumen de los resultados de las pruebas de conectividad

4.4 PRUEBAS DE TELEFONÍA IP

Luego de establecida la conexión VPN el usuario remoto puede acceder a la Polired, específicamente a la subred de la UGI, de igual manera a los servidores y otros recursos de red disponibles. Para llevar a cabo una comunicación telefónica es necesario que el usuario este registrado en el servidor Asterisk, luego de lo cual podrá realizar y recibir llamadas con usuarios dentro de la LAN. Se considera que en este caso cada usuario registrado cuenta con un teléfono IP o en su defecto un PC equipado con software telefónico.

4.4.1 DESCRIPCIÓN DEL PROCESO DE UNA LLAMADA

Existen varios pasos que se deben cumplir previa la comunicación entre 2 terminales telefónicas. En una llamada utilizando protocolo SIP hay varias transacciones entre el equipo terminal y el equipo servidor. Una transacción consta de varias peticiones y respuestas desde y hacia el servidor como en la Figura 4-14.

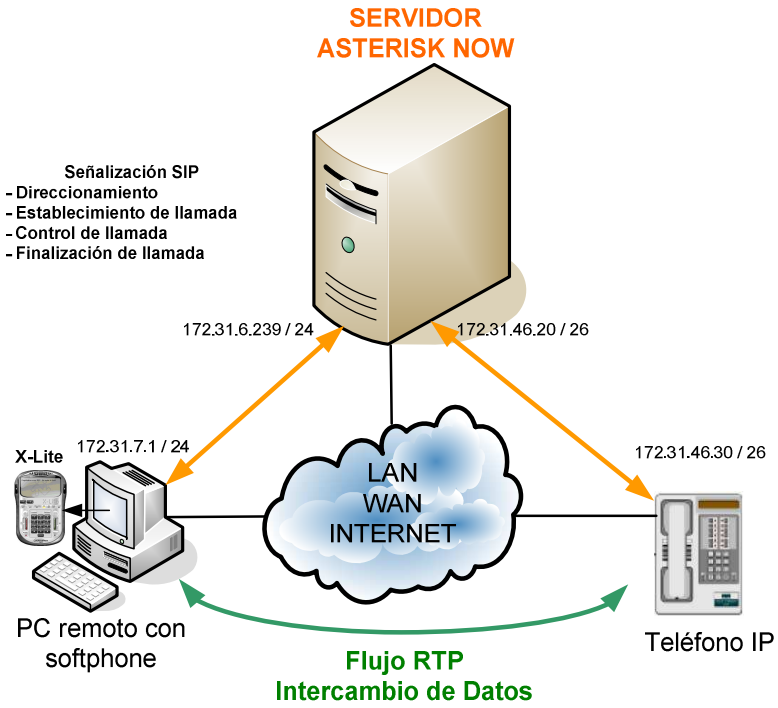


Figura 4-14 Procesos en una llamada IP.

Los siguientes procesos deben cumplirse previo la transmisión de paquetes de voz:

4.4.1.1 Registro

Los usuarios deben registrarse para poder ser encontrados por otros usuarios dentro de la red. Como se observa en la Figura 4-15 el softphone X-lite realiza un proceso de registro una vez configurado.

Figura 4-15 X-Lite Registrándose

En este caso, los terminales envían una petición REGISTER al servidor Asterisk, a la dirección 172.31.46.20 visto dentro de la LAN, mientras que visto para desde un

usuario remoto tendrá la dirección 172.31.6.239, por políticas de la Polired. El servidor consulta en su base, si el usuario puede ser autenticado y envía un mensaje de OK en caso positivo, de esta manera queda registrada la extensión como en la Figura 4-16, A continuación el servidor Asterisk asocia la dirección IP con el número de extensión telefónica, por ejemplo:

- ✓ El host en la LAN con dirección 172.31.46.19 se lo registra con la extensión 6001.
- ✓ El host en la LAN con dirección 172.31.46.30 se lo registra con la extensión 6007.
- ✓ El host remoto con dirección 172.31.7.1 se lo registra con la extensión 6005.

Figura 4-16 Extensión 6001 Registrada

Las direcciones en la LAN se asignan de manera estática y dinámica, mientras que los números de extensión se registran únicamente de forma estática, primero en el servidor Asterisk y luego en las terminales. Como se observa en la Figura 4-14 las terminales se registran en el servidor Asterisk, de esta manera la señalización y el control de la llamada queda bajo su dominio.

4.4.1.2 Establecimiento de sesión

Previo al establecimiento de una llamada, se envía una solicitud INVITE del usuario que realiza la llamada, hacia el servidor. Por ejemplo, el usuario 172.31.46.19, que en este caso tiene la extensión 6001, como se muestra en la

Figura 4-17, trata de comunicarse con la extensión 6007. Inmediatamente el servidor envía un TRYING al usuario 6001 para parar las retransmisiones de solicitud, y luego reenvía la petición al usuario con IP 172.31.46.30, extensión 6007.

Figura 4-17 Llamando a extensión 6007

El usuario 6007 envía un Ringing que es cuando el teléfono empieza a sonar, como se ve en la Figura 4-18 y también es reenviado por el servidor hacia el usuario 6001. Por ultimo se envia el mensaje OK que corresponde a aceptar la llamada por parte del usuario 6007.

Figura 4-18 Llamada Entrante desde 6001

4.4.1.3 Intercambio de Información

En este momento la llamada está establecida, y pasa a funcionar el protocolo de transporte en tiempo real (RTP) con los parámetros establecidos en la negociación mediante el protocolo SDP[24].

[24] Sesión Description Protocol, SDP se usa para la negociación de las capacidades de los participantes, tipo codificación.

Usuario 6007 Usuario 6001

Figura 4-19 Llamada En Progreso

4.4.1.4 Fin de Sesión

Esta finalización de la sesión o llamada se lleva a cabo con una única petición BYE enviada al servidor por cualquiera de los usuarios, y posteriormente reenviada al par respectivo. Este usuario contesta con un OK para confirmar que se ha recibido el mensaje final correctamente, como se muestra en la Figura 4-20.

Figura 4-20 Llamada finalizada

4.4.2 TIEMPO DE LATENCIA

La calidad de servicio de las llamadas realizadas durante las pruebas se puede determinar analizando la latencia y el jitter. Para lo cual se hace distinción entre una llamada dentro de la red LAN y una llamada sobre una red WAN, específicamente sobre Internet.

En la red WAN simulada, planteada en el punto 4.1.1, no se presentan mayores retardos pese a realizarse un proceso de encripción y por ende estar asociada a

un túnel VPN, por lo que se asemeja a un ambiente LAN.

4.4.2.1 Ambiente LAN

Al realizar una llamada entre 2 terminales dentro de una red LAN, como se indica en la Figura 4-21, se dispone normalmente de un ancho de banda de 100 Mbps, como en el caso de la UGI. En este ambiente se realizaron pruebas de conectividad utilizando el comando *ping* en la ventana DOS mientras se mantenían comunicaciones VoIP activas.

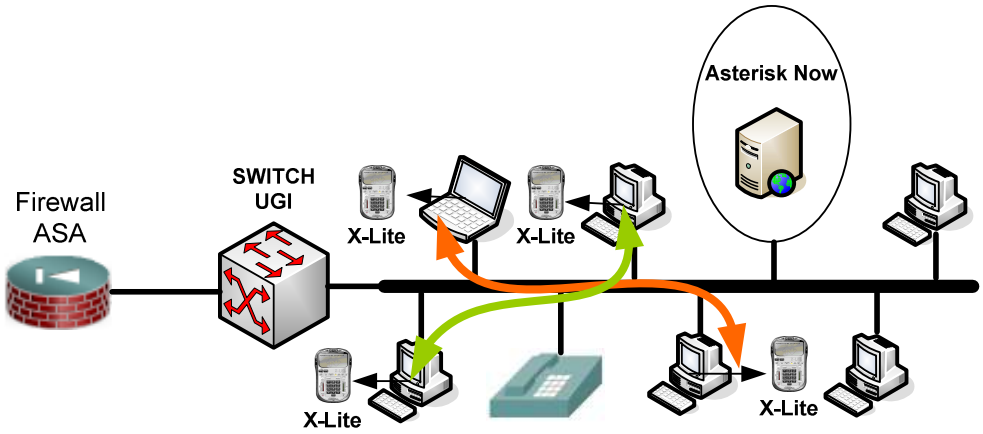


Figura 4-21 Comunicación LAN

Como se puede apreciar en la Figura 4-22, los tiempos de llegada de los paquetes ICMP, utilizados por el comando ping, son mínimos y se aproximan a 1 ms, muy por debajo de la recomendación de 150 ms, además cumple con un nivel de variación mínimo cero, esto al mantenerse un retardo constante de 1 ms.

```
C:\Documents and Settings\Usuario>ping 172.31.46.20

Haciendo ping a 172.31.46.20 con 32 bytes de datos:

Respuesta desde 172.31.46.20: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.31.46.20: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.31.46.20: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.31.46.20: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 172.31.46.20:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Documents and Settings\Usuario>
```

Figura 4-22 Ejecución comando Ping

4.4.2.2 Ambiente WAN

En un ambiente de Internet la calidad de servicio de las llamadas depende del ancho de banda disponible contratado con un proveedor de Internet. Para el desarrollo de estas pruebas se utiliza una conexión de 256 Kbps.

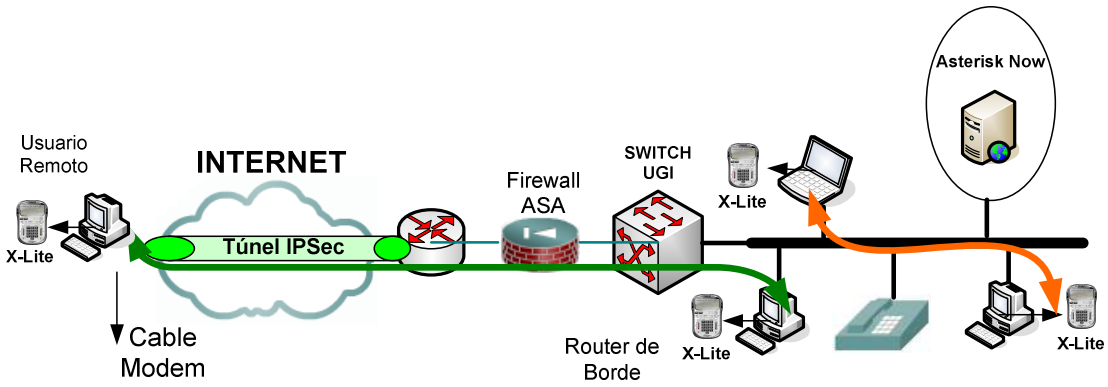


Figura 4-23 Comunicación sobre Internet

Se considera para este escenario realizar una estimación de calidad de servicio de acuerdo a la variación de latencia o *jitter* utilizando para ello la Ecuación 4-1.

$$D_i = (R_i - S_i) - (R_{i-1} - S_{i-1})$$
$$D_i = (R_i - R_{i-1}) - (S_i - S_{i-1})$$ **Ecuación 4- 1**
$$Jitter = \frac{\sum_{i}^{n} |D_i|}{n}$$

El factor (R_i - S_i) en la Ecuación 4-1 es el intervalo de tiempo que tarda un paquete desde que se envió hasta que se recibió, y se define como tiempo de latencia del paquete. La latencia en un ambiente de Internet es de alrededor de 200 ms, muy superior al de un ambiente LAN. Pese a ello, la calidad de voz se mantiene, como se puede observar en la Tabla 4-3 el valor de latencia está próximo a los 125 ms lo que se refleja en un *jitter* de 20 ms.

	Latencia i [ms]	**Variación i [ms]**	**Latencia i [ms]**	**Variación i [ms]**
	123	0	110	11
	123	0	128	18
	130	7	125	3
	119	11	118	7
	135	14	126	8
	135	0	123	3
	116	19	120	3
	147	31	119	1
	121	26	119	0
	137	16	147	28
	126	11	129	18
	125	1	136	7
	121	4	113	23
Media	**125**	**20**		

Tabla 4-4 Latencia Jitter

Los resultados obtenidos en las llamadas entre dos extensiones con softphones, son similares a las llamadas realizadas entre un teléfono IP y un softphone o entre dos teléfonos IP.

4.5 MONITOREO DE LA RED

El monitoreo de la red se realiza con el fin de determinar paso a paso el intercambio de paquetes en el proceso de registro, comunicación con el servidor Asterisk y establecimiento de una llamada, además se lo utiliza para analizar el proceso de establecimiento del túnel VPN y la encripción de los datos que se transmiten sobre el mismo.

Para realizar este proceso se utiliza un software de monitoreo de red, Wireshark, cuya descripción se indica en el Anexo D. A continuación se describe los monitoreos realizados.

4.5.1 MONITOREO DEL TÚNEL

El propósito de monitorear el túnel es determinar la encripción de los datos que se transmiten a través del túnel. El monitoreo se lo realiza a nivel local en el Host remoto y a nivel externo en el Host-Hacker, para comparar los resultados y determinar la encripción de los paquetes.

El Host-Hacker se conecta en red con el Host remoto a través de un HUB. Se procedió así debido a que en el HUB retransmite la información a todos los puertos, permitiendo el monitoreo de la red desde algún otro Host, simulando lo que haría un Hacker desde un punto sobre la gran nube de Internet. El escenario para el Host-Hacker es el que se indica en la Figura 4-24.

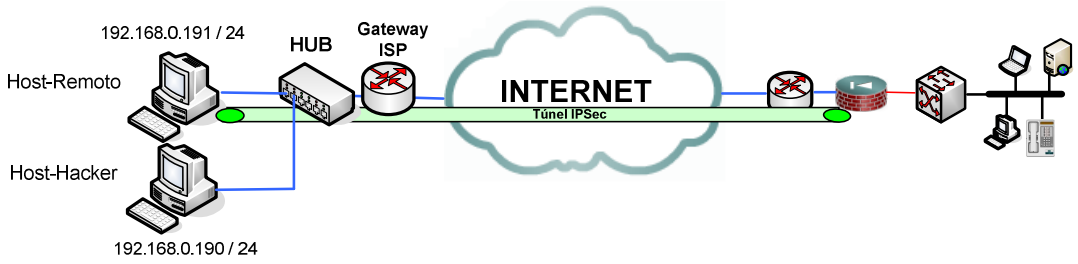
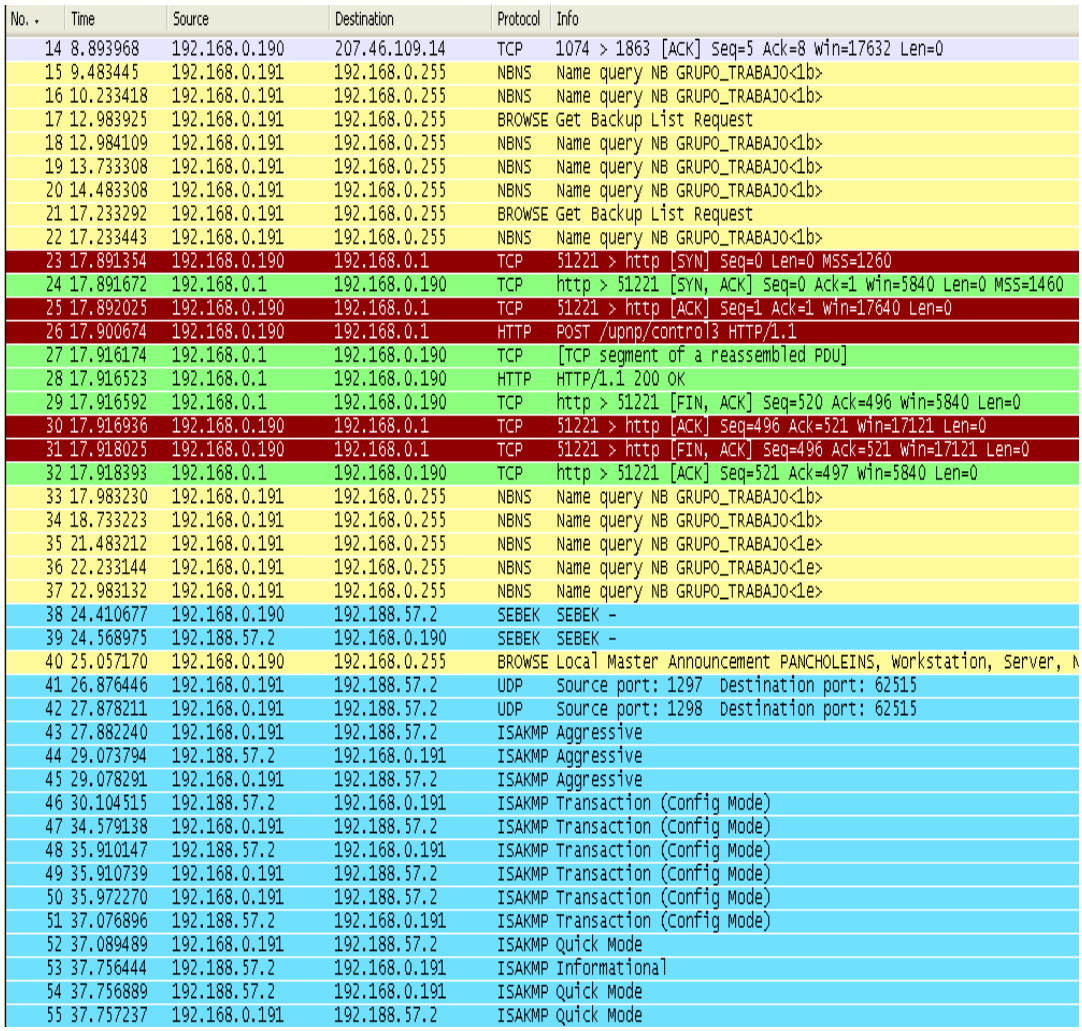


Figura 4-24 Escenario del Host-Hacker para el monitoreo de la red

Antes de establecer el túnel, el Host remoto, al igual que el Host-Hacker, podrán visualizar los datos que el host remoto está transmitiendo.

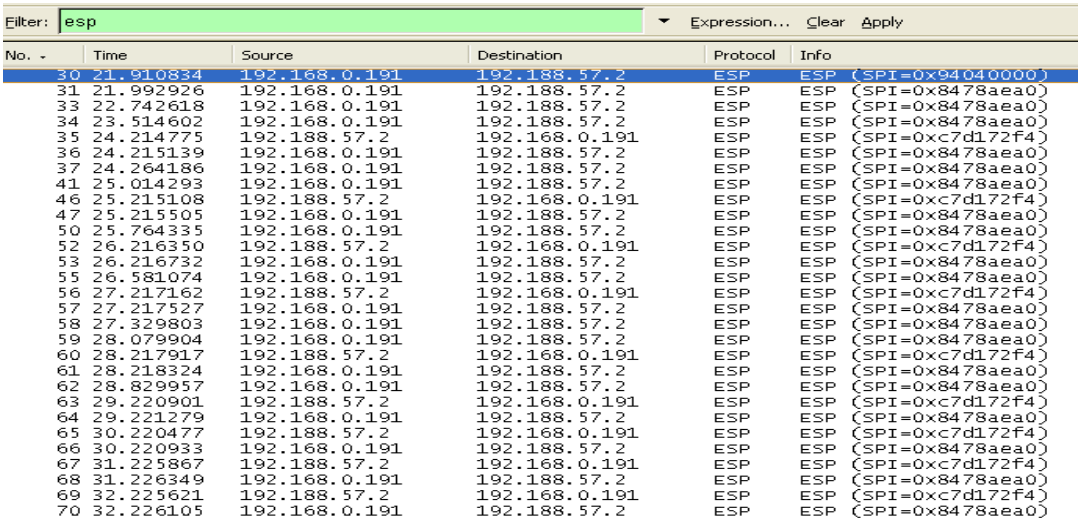
El Host remoto establece la sesión del túnel, luego de lo cual transmite datos a través del mismo (llamada telefónica). Los protocolos de encripción a nivel local son transparentes para el usuario, es decir que el monitoreo realizado muestra los protocolos utilizados en las aplicaciones del usuario, como por ejemplo SIP.

Por otra parte, el monitoreo en el Host-Hacker visualiza los paquetes transmitidos por el host remoto, como paquetes ESP, indistintamente del contenido del paquete; es decir, mientras el Host remoto transmite paquetes SIP, el Host-Hacker monitoriza la transmisión como paquetes ESP. Esto se indica en la Figura 4-25 y 4-26 respectivamente.



No.	Time	Source	Destination	Protocol	Info
14	8.893968	192.168.0.190	207.46.109.14	TCP	1074 > 1863 [ACK] Seq=5 Ack=8 Win=17632 Len=0
15	9.483445	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1b>
16	10.233418	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1b>
17	12.983925	192.168.0.191	192.168.0.255	BROWSE	Get Backup List Request
18	12.984109	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1b>
19	13.733308	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1b>
20	14.483308	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1b>
21	17.233292	192.168.0.191	192.168.0.255	BROWSE	Get Backup List Request
22	17.233443	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1b>
23	17.891354	192.168.0.190	192.168.0.1	TCP	51221 > http [SYN] Seq=0 Len=0 MSS=1260
24	17.891672	192.168.0.1	192.168.0.190	TCP	http > 51221 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
25	17.892025	192.168.0.190	192.168.0.1	TCP	51221 > http [ACK] Seq=1 Ack=1 Win=17640 Len=0
26	17.900674	192.168.0.190	192.168.0.1	HTTP	POST /upnp/control3 HTTP/1.1
27	17.916174	192.168.0.1	192.168.0.190	TCP	[TCP segment of a reassembled PDU]
28	17.916523	192.168.0.1	192.168.0.190	HTTP	HTTP/1.1 200 OK
29	17.916592	192.168.0.1	192.168.0.190	TCP	http > 51221 [FIN, ACK] Seq=520 Ack=496 Win=5840 Len=0
30	17.916936	192.168.0.190	192.168.0.1	TCP	51221 > http [ACK] Seq=496 Ack=521 Win=17121 Len=0
31	17.918025	192.168.0.190	192.168.0.1	TCP	51221 > http [FIN, ACK] Seq=496 Ack=521 Win=17121 Len=0
32	17.918393	192.168.0.1	192.168.0.190	TCP	http > 51221 [ACK] Seq=521 Ack=497 Win=5840 Len=0
33	17.983230	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1b>
34	18.733223	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1b>
35	21.483212	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1e>
36	22.233144	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1e>
37	22.983132	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1e>
38	24.410677	192.168.0.190	192.188.57.2	SEBEK	SEBEK -
39	24.568975	192.188.57.2	192.168.0.190	SEBEK	SEBEK -
40	25.057170	192.168.0.190	192.168.0.255	BROWSE	Local Master Announcement PANCHOLEINS, Workstation, Server, N
41	26.876446	192.168.0.191	192.188.57.2	UDP	Source port: 1297 Destination port: 62515
42	27.878211	192.168.0.191	192.188.57.2	UDP	Source port: 1298 Destination port: 62515
43	27.882240	192.168.0.191	192.188.57.2	ISAKMP	Aggressive
44	29.073794	192.188.57.2	192.168.0.191	ISAKMP	Aggressive
45	29.078291	192.168.0.191	192.188.57.2	ISAKMP	Aggressive
46	30.104515	192.188.57.2	192.168.0.191	ISAKMP	Transaction (Config Mode)
47	34.579138	192.168.0.191	192.188.57.2	ISAKMP	Transaction (Config Mode)
48	35.910147	192.188.57.2	192.168.0.191	ISAKMP	Transaction (Config Mode)
49	35.910739	192.168.0.191	192.188.57.2	ISAKMP	Transaction (Config Mode)
50	35.972270	192.168.0.191	192.188.57.2	ISAKMP	Transaction (Config Mode)
51	37.076896	192.188.57.2	192.168.0.191	ISAKMP	Transaction (Config Mode)
52	37.089489	192.168.0.191	192.188.57.2	ISAKMP	Quick Mode
53	37.756444	192.188.57.2	192.168.0.191	ISAKMP	Informational
54	37.756889	192.188.57.2	192.168.0.191	ISAKMP	Quick Mode
55	37.757237	192.168.0.191	192.188.57.2	ISAKMP	Quick Mode

Figura 4-25 Monitoreo del Host remoto antes de establecer el túnel



Filter: esp — Expression... Clear Apply

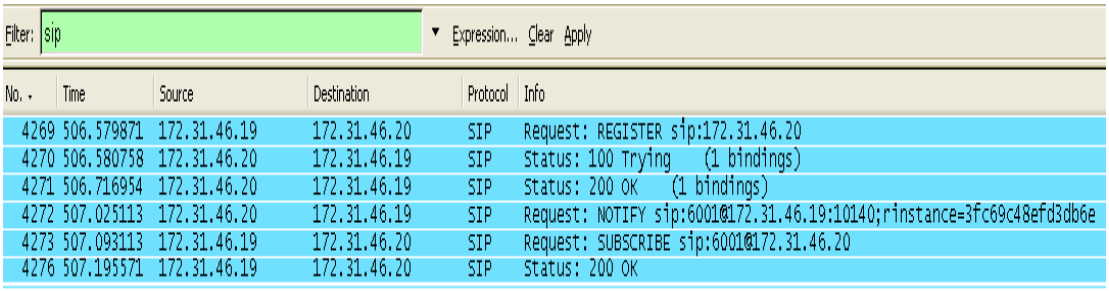
No.	Time	Source	Destination	Protocol	Info
30	21.910834	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x94040000)
31	21.992926	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
33	22.742618	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
34	23.514602	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
35	24.214775	192.188.57.2	192.168.0.191	ESP	ESP (SPI=0xc7d172f4)
36	24.215139	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
37	24.264186	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
41	25.014293	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
46	25.215108	192.188.57.2	192.168.0.191	ESP	ESP (SPI=0xc7d172f4)
47	25.215505	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
50	25.764335	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
52	26.216350	192.188.57.2	192.168.0.191	ESP	ESP (SPI=0xc7d172f4)
53	26.216732	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
55	26.581074	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
56	27.217162	192.188.57.2	192.168.0.191	ESP	ESP (SPI=0xc7d172f4)
57	27.217527	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
58	27.329803	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
59	28.079904	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
60	28.217917	192.188.57.2	192.168.0.191	ESP	ESP (SPI=0xc7d172f4)
61	28.218324	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
62	28.829957	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
63	29.220901	192.188.57.2	192.168.0.191	ESP	ESP (SPI=0xc7d172f4)
64	29.221279	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
65	30.220477	192.188.57.2	192.168.0.191	ESP	ESP (SPI=0xc7d172f4)
66	30.220933	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
67	31.225867	192.188.57.2	192.168.0.191	ESP	ESP (SPI=0xc7d172f4)
68	31.226349	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
69	32.225621	192.188.57.2	192.168.0.191	ESP	ESP (SPI=0xc7d172f4)
70	32.226105	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)

Figura 4-26 Monitoreo del Host remoto después de establecer el túnel

4.5.2 MONITOREO DEL PROCESO DE REGISTRO DE UNA EXTENSIÓN

El proceso de registro de una extensión en el servidor Asterisk es idéntico para un usuario en la LAN como para un usuario remoto, y se realiza como se indica en la Figura 4-27, respectivamente.

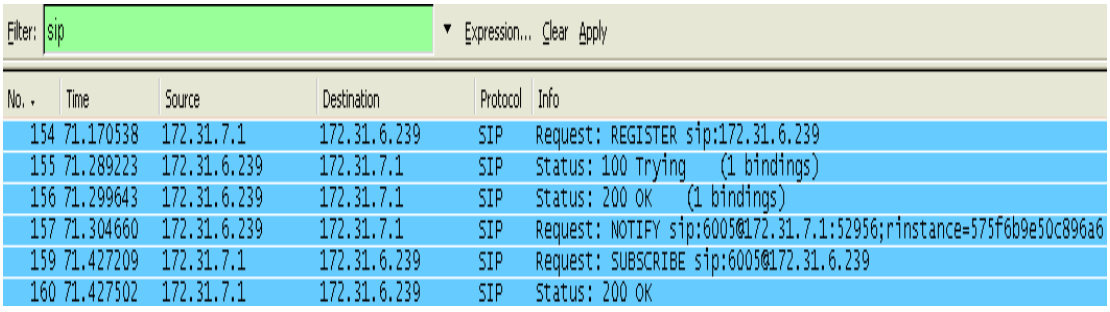
Usuario dentro de la LAN



Filter: sip — Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
4269	506.579871	172.31.46.19	172.31.46.20	SIP	Request: REGISTER sip:172.31.46.20
4270	506.580758	172.31.46.20	172.31.46.19	SIP	Status: 100 Trying (1 bindings)
4271	506.716954	172.31.46.20	172.31.46.19	SIP	Status: 200 OK (1 bindings)
4272	507.025113	172.31.46.20	172.31.46.19	SIP	Request: NOTIFY sip:6001@172.31.46.19:10140;rinstance=3fc69c48efd3db6e
4273	507.093113	172.31.46.19	172.31.46.20	SIP	Request: SUBSCRIBE sip:6001@172.31.46.20
4276	507.195571	172.31.46.19	172.31.46.20	SIP	Status: 200 OK

Usuario remoto



Filter: sip — Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
154	71.170538	172.31.7.1	172.31.6.239	SIP	Request: REGISTER sip:172.31.6.239
155	71.289223	172.31.6.239	172.31.7.1	SIP	Status: 100 Trying (1 bindings)
156	71.299643	172.31.6.239	172.31.7.1	SIP	Status: 200 OK (1 bindings)
157	71.304660	172.31.6.239	172.31.7.1	SIP	Request: NOTIFY sip:6005@172.31.7.1:52956;rinstance=575f6b9e50c896a6
159	71.427209	172.31.7.1	172.31.6.239	SIP	Request: SUBSCRIBE sip:6005@172.31.6.239
160	71.427502	172.31.7.1	172.31.6.239	SIP	Status: 200 OK

Figura 4-27 Proceso del registro de una extensión

Como se indicó anteriormente, el servidor Asterisk tiene la dirección local 172.31.46.20 y, de acuerdo a las seguridades de la Polired, para que un Host remoto tenga conectividad con un PC en la Polired, el PC debe tener una dirección en la subred en la red 172.31.6.0, por lo que el servidor Asterisk se traduce con la dirección 172.31.6.239. Para otra empresa, como SONDA, la traducción de dirección, no es necesaria, ya que se puede comunicar el host remoto con cualquier PC o servidor en la Intranet.

Con esta aclaración se demuestra que el proceso de registro de una llamada es igual al que se describió en el segmento 4.4.1.1

4.5.3 MONITOREO DEL ESTABLECIMIENTO DE UNA LLAMADA

Una vez que el usuario remoto se encuentra registrado en el servidor Asterisk, el proceso para realizar llamadas es igual entre cualquier extensión debidamente autorizada.

En la Figura 4-26 se indica de manera detallada el intercambio de paquetes que se realizan para establecer una llamada entre dos extensiones, como se describió en el segmento 4.4.1.2.

No.	Time	Source	Destination	Protocol	Info
208	90.952789	172.31.7.1	172.31.6.239	SIP/SD	Request: INVITE sip:6001@172.31.6.239, with session description
209	91.091009	172.31.6.239	172.31.7.1	SIP	Status: 100 Trying
212	91.223022	172.31.6.239	172.31.7.1	SIP	Status: 180 Ringing
214	91.819023	172.31.6.239	172.31.7.1	SIP/SD	Status: 183 Session Progress, with session description
217	91.824868	172.31.6.239	172.31.7.1	SIP/SD	Status: 200 OK, with session description
232	91.970778	172.31.7.1	172.31.46.20	SIP	Request: ACK sip:6001@172.31.46.20
20668	292.561919	172.31.6.239	172.31.7.1	SIP	Request: NOTIFY sip:6005@172.31.7.1:52956
20681	292.677067	172.31.7.1	172.31.6.239	SIP	Status: 200 OK
20741	293.256699	172.31.6.239	172.31.7.1	SIP	Request: NOTIFY sip:6005@172.31.7.1:52956
20742	293.257356	172.31.7.1	172.31.6.239	SIP	Status: 200 OK
20814	293.967883	172.31.6.239	172.31.7.1	SIP	Request: NOTIFY sip:6005@172.31.7.1:52956
20815	293.968171	172.31.7.1	172.31.6.239	SIP	Status: 200 OK
20969	295.438723	172.31.6.239	172.31.7.1	SIP	Request: NOTIFY sip:6005@172.31.7.1:52956
20970	295.439011	172.31.7.1	172.31.6.239	SIP	Status: 200 OK
27224	356.828305	172.31.6.239	172.31.7.1	SIP	Status: 200 OK
27283	357.393032	172.31.6.239	172.31.7.1	SIP	Status: 200 OK
27389	358.411488	172.31.6.239	172.31.7.1	SIP	Status: 200 OK
30884	392.623597	172.31.6.239	172.31.7.1	SIP	Request: BYE sip:6005@172.31.7.1:52956
30886	392.735433	172.31.7.1	172.31.6.239	SIP	Status: 200 OK

Figura 4-28 Proceso de una llamada entre el Host remoto y una extensión en la Polired

En este capítulo se realizaron pruebas, y de acuerdo a los resultados obtenidos, se demuestra el establecimiento del túnel, y la seguridad que se brinda a las llamadas entre un usuario remoto y usuarios en la LAN, de acuerdo al monitoreo realizado y la comprobación de que los paquetes se encriptan.

La calidad de la voz en las llamadas, es muy buena a pesar del retardo, ya que las llamadas se realizan a través de Internet y sobre un túnel VPN.

Con estas referencias, se prosigue al Capítulo 5 donde se realiza el estudio de costos para una futura implementación del presente proyecto.

CAPÍTULO 5

5 ESTUDIO DE COSTOS DEL PROYECTO

Luego de culminado el proceso de pruebas, y con un panorama completo del alcance del presente proyecto, es posible establecer que equipos y elementos intervienen; o pueden intervenir, en la implementación y puesta en marcha de la red diseñada.

Es importante destacar que para la realización del presente proyecto se utilizan recursos de software libre que, además de ser de fácil acceso, permiten una distribución libre entre los usuarios de la red. Se destaca también la posibilidad, en el caso de Asterisk, de manipular el código fuente permitiendo, en caso de requerir, la creación de nuevos servicios o herramientas administrativas que se acoplen mejor a las necesidades particulares de cada empresa.

En este capítulo se realizará el estudio de costos, además se detallan los equipos necesarios para una futura implementación real del proyecto.

Habiendo elegido elementos gratuitos y tratando de mantener un enfoque objetivo y de menor impacto económico, se presenta como un proyecto de bajo presupuesto y de grandes alcances tanto a nivel administrativo como económico.

5.1 EQUIPOS NECESARIOS PARA LA IMPLEMENTACIÓN

Considerando una empresa que cuenta con una red de cableado estructurado e infraestructura LAN previa, no es pertinente al presente proyecto el aspecto de cableado interno de la empresa y no se requiere de cambios tanto en la arquitectura física como en la arquitectura lógica de la red. Teniendo en cuenta este aspecto, se procede a detallar los equipos y elementos de software que se

utilizan para este proyecto.

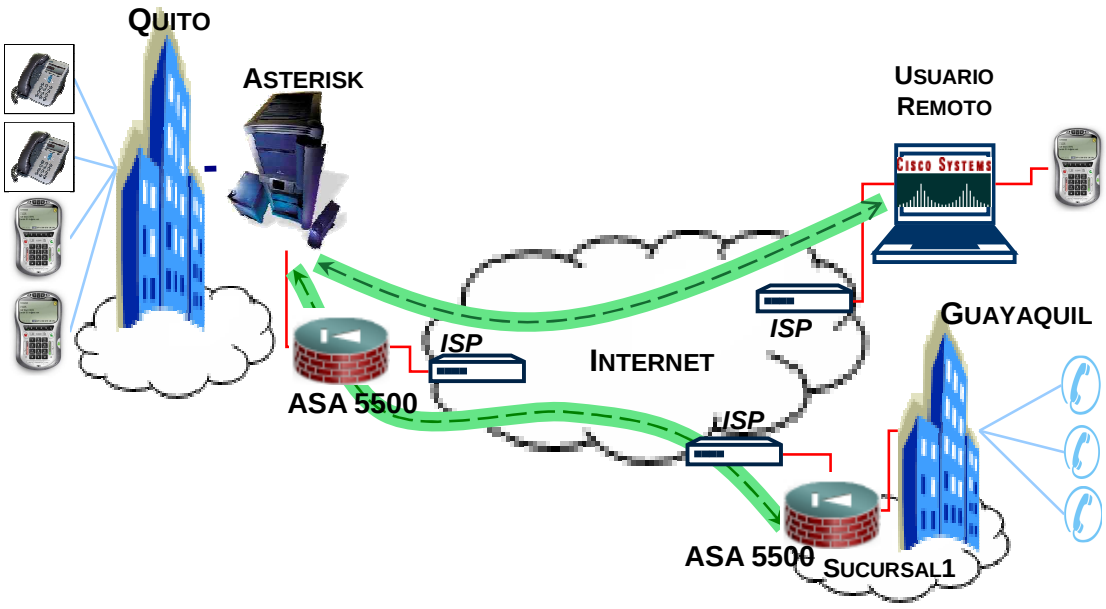


Figura 5-1 Elementos de Red Telefónica-VPN

De acuerdo con el esquema propuesto en la Figura 5-1, se pueden observar 2 escenarios VPN. El primero del tipo Intranet y el segundo del tipo acceso remoto.

Para formar un escenario Intranet VPN se requiere de 2 equipos que soporten túneles IPSec VPN y una conexión a Internet con un ancho de banda de 1024 Kbps, en la Oficina Matriz y en la Sucursal, como se indicó en el Capítulo 2.

Para una conexión de Acceso Remoto VPN se requiere un equipo que soporte conexiones remotas a través de un túnel IPSec VPN, que puede ser cualquiera de los equipos utilizados para la Intranet VPN. Este equipo controlará el acceso de usuarios remotos. El usuario remoto requiere de una conexión a Internet que puede ser de 128 Kbps como mínimo y el software Cliente VPN de Cisco.

En ambos escenarios, Intranet VPN y Acceso Remoto, se configura la red para que los usuarios en los 2 escenarios estén asociados a una central telefónica Asterisk, Para ello se requiere un PC que pueda soportar el sistema operativo Asterisk Now.

5.2 COSTOS

Considerando los equipos y otros elementos que interviene para la realización del presente proyecto, se diferencian 3 tipos de gastos, que se reflejan en costos de:

5.2.1 COSTOS DE LOS EQUIPOS

Los rubros más importantes respecto a los equipos utilizados, son los relacionados a los equipos de borde, Firewall ASA 5520, que por las características que presta, fácilmente permite reemplazar a cualquier equipo destinado a la administración de la red, y en especial a equipos destinados a la prestación de servicios de seguridad, en cuyo caso es una inversión muy acertada. En la Tabla 5-1 se indican los parámetros básicos que debe tener el equipo VPN.

Usuarios / Nodos	**200**	**Ilimitado**
Throughput VPN 3DES/ AES	**50 Mbps**	**Sobre los 225 Mbps**
Pares VPN IPsec	**50**	**750**
Puertos de Red Integrados	**1 Gigabit Ethernet, 2 Fast Ethernet**	**4 Gigabit Ethernet, 1 Fast Ethernet**
Protocolos VPN Soportados	**IPSec**	**IPSec, PPTP, SSL**
Algoritmos de Encripción	**AES (128 bits)**	**DES, 3DES, AES (128, 192, 256 bits)**
Algoritmos de Autenticación	**MD5**	**MD5, SHA, rsa, dsa**
Protocolos de Encapsulamiento	**ESP**	**ESP**
Protocolo de establecimiento de sesión	**IKE, ISAKMP**	**IKE, ISAKMP**
Protocolo de llaves públicas	**Diffie-Hellman Grupo 1 (768 bits)**	**Diffie-Hellman Grupo 1 (768 bits) Grupo 2 (1024 bits) Grupo 5 (1536 bits) Grupo 7 (mayor 1536**

		bits)

Tabla 5-1 Características necesarias del equipo VPN

Por otra parte, si la empresa que requiere el servicio VPN no dispone del capital necesario que se detalla en la Tabla 5-3 para la compra de equipos ASA 5520, puede recurrir a una opción mas económica, como por ejemplo un equipo de la serie Cisco Routers 2600 cargado con un IOS versión 12.2 o superior, que cumple con el requerimiento de administración de túneles VPN, tanto para escenarios Sitio a Sitio como para escenarios de Acceso Remoto.

La principal ventaja de los sistemas Linux es que requieren un mínimo de recursos de hardware concentrando su rendimiento sobre aplicaciones específicas. En este caso Asterisk está direccionado a la administración de centrales telefónicas y para ello se requiere de un equipo con las características indicadas en la Tabla 5-2.

Disco Duro	**80 GB**	**180 GB**
Procesador	**Pentium 4 3,5 GHz**	**Doble Núcleo 2 GHZ**
Memoria RAM	**512 MB**	**1 GB**

Tabla 5-2 Características necesarias del equipo VPN

La Tabla 5-3 muestra también otros rubros como son el equipo necesario para soportar el servidor Asterisk, caracterizado en la Tabla 5-2.

Se requiere además una cantidad de 10 teléfonos IP 3COM 3101 que cumplen con el requisito necesario de soportar protocolo SIP.

En cuanto al número de teléfonos IP que se requieren en un principio, no es necesario facilitar un equipo de comunicación para cada punto de red en que se requiera de una extensión. En este sentido se puede fácilmente permitir el uso del

software X-lite, que es fácil de utilizar y no interfiere en el desempeño del host sobre el que se instala.

1	**Cisco ASA 5520**	**Para administrar conexiones VPN LAN a LAN y usuarios remotos.**	**Edificio Matriz**	**6000**	**6000**
1	**Cisco ASA 5520**	**Para administrar conexiones VPN LAN a LAN.**	**Edificio Sucursal**	**6000**	**6000**
1	**Computador-Servidor Asterisk**	**Para soportar sistema operativo Asterisk.**	**Edificio Matriz**	**700**	**700**
10	**Teléfonos IP**	**Extensión telefónica**	**Edificio Matriz, Sucursal**	**30**	**300**
TOTAL SIN IMPUESTOS					**13000**

Tabla 5-3 Costos de Equipos y Hardware

5.2.2 COSTOS DE SOFTWARE

El software Cliente VPN Cisco es el único software propietario que se requiere para la realización de este proyecto, los elementos adicionales se encuentran disponibles en diferentes sitios de Internet en forma gratuita. El servidor Asterisk se puede obtener de la dirección www.asterisknow.org:, mientras que X-lite del

sitio www.counterpath.com. El detalle de los costos de software se detalla en la Tabla 5-4.

1	**Software Cliente VPN Cisco**	**Realiza una conexión segura entre un host y un equipo de frontera.**	**Equipos remotos**	**200**	**200**
1	**Software Asterisk Now**	**Administra extensiones telefónicas.**	**Servidor ubicado en el Edificio Matriz.**	**0**	**0**
1	**Softphone X-Lite**	**Emula un teléfono físico IP y se carga sobre PCs**	**En equipos dentro de la Matriz, Sucursal y usuarios remotos.**	**0**	**0**
TOTAL SIN IMPUESTOS					**200**

Tabla 5-4 Costos de Elementos De Software

El gasto mensual que se requiere para una conexión a Internet se describe en la Tabla 5-5, y como ya se explicó en el Capítulo 2 se requiere el mismo ancho de banda tanto en el lado de la oficina Matriz como del lado de la oficina Sucursal.

2	**Conexión 1024 Kbps**	**200**	**400**
1	**Conexión residencial 128 Kbps**	**21**	**21**

TOTAL MENSUAL SIN IMPUESTOS	**421**

Tabla 5-5 Rubros Mensuales

5.2.3 COSTOS DE INSTALACIÓN

Los costos de configuración incluyen el periodo de pruebas que se lleve a cabo, una vez configurados los equipos, los cuáles se muestran en la Tabla 5-6.

5	**Router ASA 5520, oficina matriz**	**100**	500
3	**Router ASA 5520, oficina sucursal**	**100**	300
6	**Central Telefónica Asterisk**	**60**	360
10	**Teléfono IP y Softphone**	**30**	300
1	**Cliente VPN Asterisk**	**40**	40
VALOR TOTAL SIN IMPÙESTOS			1500

Tabla 5-6 Costos de Configuración

En el caso del equipo ASA 5520 ubicado en la oficina matriz se toma en cuenta un número adicional de horas debido a que ese equipo contendrá la configuración para usuarios remotos, además del respectivo periodo de pruebas. En el caso de la configuración de la Central telefónica Asterisk, se considera un largo tiempo debido al número de extensiones que se requiere. En el caso de la empresa que se tomó como referencia, SONDA, son 93 extensiones sin tomar en cuenta el número adicional de extensiones para empleados remotos.

Para el caso de los Teléfonos IP y Softphone, se estima un tiempo aproximado de 5 minutos por extensión, y el tiempo se justifica debido al número de extensiones que se requiera configurar.

El software Cliente VPN Cisco se instala en los PC remotos, y el costo dependerá del número de usuarios remotos que se puedan tener.

5.2.4 COSTOS FINALES

Finalmente el costo total para la implementación del presente proyecto se muestra en la Tabla 5-7. Se toman en cuenta todas las consideraciones hechas anteriormente y no se incluyen los costos mensuales por concepto de Internet.

Total Equipos Hardware	**13000**
Total Elementos Software	**200**
Total Configuración	**1500**
TOTAL SIN IMPUESTOS	**14700**

Tabla 5-7 Costos Total Del Proyecto

Con los cálculos realizados anteriormente se da una visión general del costo de implementar el presente proyecto con los equipos propuestos. Cabe recalcar que para la implementación del túnel se pueden utilizar otros equipos más económicos, pero que no cuentan con todas las funcionalidades del equipo propuesto.

6 CAPÍTULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- ✓ Las redes VPN disminuyen significativamente costos adicionales por comunicación y/o compartición de recursos entre dependencias de una misma empresa que se encuentran geográficamente distantes; a diferencia de enlaces WAN que representan altos costos mensuales. Por lo tanto se puede concluir que el uso de VPNs es conveniente para una empresa.

- ✓ Se utiliza una conexión VPN de acceso remoto para facilitar la comunicación entre un empleado fuera de la empresa con los servicios y usuarios de la red LAN interna. Se puede concluir, con las pruebas realizadas, que mientras un usuario remoto se encuentre conectado a la red VPN de la empresa, únicamente podrá acceder a los servicios y sitios dentro de la Intranet, restringiendo el acceso del usuario remoto hacia Internet.

- ✓ Para telefonía IP se aplicaron los mismos conceptos de tráfico que se usan para telefonía analógica. Se pudo comprobar durante el proceso de pruebas que el ancho de banda estimado para cada canal telefónico, permitió una comunicación legible y libre de interferencias.

- ✓ Otra manera de brindar seguridad en las llamadas telefónicas, es a través del registro y autorización por parte del administrador de la Central Telefónica. Esto se puede comprobar al momento que se inicia una sesión X-lite en que el primer proceso que se realiza, es la verificación del registro de cada extensión. Con lo que se concluye que sólo se podrán realizar

llamadas entre usuarios debidamente registrados, incluyendo usuarios remotos.

- ✓ Un proceso de doble NAT permite limitar el acceso a los equipos y recursos de red, permitiendo únicamente el acceso a los servidores requeridos. En el presente proyecto se comprobó que el usuario remoto puede acceder únicamente al servidor Asterisk, y a través de éste a los usuarios registrados en el servidor, pero no a los usuarios directamente; es decir, para aplicaciones de voz el usuario remoto puede contactar con los usuarios dentro del servidor Asterisk, pero para otro tipo de aplicaciones los mismos usuarios registrados en Asterisk no están al alcance del usuario remoto. Luego del período de pruebas se concluye que cualquier host dentro de la LAN puede tener conexión directa con el usuario remoto, sin la mediación del servidor Asterisk.

- ✓ Una vez revisada la ley que regula el servicio de VoIP se concluye que una llamada por VoIP a través de una VPN, no infringe las leyes que regulan este servicio, ya que las llamadas se realizan únicamente en la red privada de una misma empresa, ya sea localmente o virtualmente.

- ✓ Durante el proceso de pruebas, en un escenario VPN de Acceso Remoto, se determinó que cuando más de un usuario está asociado a una única conexión a Internet; por ejemplo, en un Cybercafe, solo se podrá conectar un usuario remoto a la vez, debido a que el servidor VPN, registra la dirección IP pública con la que se está accediendo al túnel, por lo que no se podrán tener más de una conexión con la misma dirección pública.

- ✓ El tráfico monitoreado por el software Wireshark, permite distinguir los protocolos utilizados por el usuario remoto dentro del túnel VPN, como TCP, UDP, SIP, etc. Pero cuando se monitorea desde un PC externo, conectado al mismo dominio que el usuario remoto, el tráfico se identifica

como ESP. De esta manera se demuestra que el tráfico que sale del usuario remoto se transmite de forma encriptada.

6.2 RECOMENDACIONES

- ✓ Una vez implementada la VPN, se recomienda brindar servicios adicionales aprovechando el túnel establecido, por lo que el presente proyecto se limita a brindar el servicio de VoIP. Entre los servicios que se pueden brindar a través del túnel se encuentra el servicio de escritorio remoto, teletrabajadores, video conferencia, compartición de recursos como documentos e impresoras, etc.

- ✓ Se recomienda que las contraseñas tengan un periodo corto de duración y el administrador del túnel las cambie periódicamente, de esta manera se evita que algún usuario no autorizado acceda al túnel.

- ✓ Se recomienda mantener una base de datos en donde se almacenen las extensiones telefónicas con sus respectivas identificaciones, usuarios, número de extensión y contraseñas. En caso de que se llegue a tener un gran número de usuarios y de extensiones en la central.

- ✓ Se recomienda que el servicio de VoIP sea política de la empresa, brindando prioridad al tráfico telefónico al necesitar ser transmitido en tiempo real.

- ✓ Previo a la implementación de la central telefónica se debe tener un monitoreo de la red, de tal manera que se conozca el ancho de banda adicional que se requiere al aumentar el servicio de VoIP a través de Internet.

- ✓ Este proyecto se puede implementar en medianas y grandes empresas, Instituciones gubernamentales, militares, campus universitarios y toda empresa donde se requiera seguridad y confidencialidad de las llamadas telefónicas dentro o hacia fuera de la Institución.

- ✓ Para empresas que no cuenten con una central analógica PBX, pero que cuenten con una red LAN estructurada, se puede implementar una central telefónica digital mediante Asterisk Now, optimizando la red existente.

- ✓ Es recomendable realizar llamadas por VoIP cuando se tienen trabajadores que viajen constantemente dentro y fuera del país, abaratando notablemente el costo de las llamadas y permitiendo una comunicación continua con la empresa.

BIBLIOGRAFÍA

[1] RFC 2764, A framework for IP Based Virtual Private Networks, B. Gleeson A. Lin, J. Heinanen, Telia Finland, G. Armitage, A. Malis; Febrero 2000

[2] MURHAMMER Martin W, “A guide to virtual Private Networks”, Editorial Prentice Hall PTR, 1998.

[3] OLIVIER Victor, Different Flavours of VPN: Technology and Applications, http://www.ja.net/documents/services/mcas/different-flavours-of-vpn-web.pdf

[4] URL: http://www.textoscientificos.com/criptografia/privada

[5] URL: http://www.kriptopolis.org/

[6] URL: http://es.wikipedia.org/wiki/Data_Encryption_Standard

[7] ANGEL José de Jesús, Advanced Encription Standard, http://computacion.cs.cinvestav.mx/~jjangel/aes/AES_v2005_jjaa.pdf

[8] URL: http://tools.ietf.org/html/rfc4309 Using Advanced Encryption Standard (AES) CCM

[9] RFC 4301, Security Architecture for the Internet Protocol, S. Kent, K. Seo; Diciembre 2005

[10] URL: http://seguridad.internet2.ulsa.mx/congresos/2001/cudi2/tutorial_ipsec.pdf

[11] RFC 4302, IP Authentication Header**,** S. Kent, Diciembre 2005

[12] RFC 4303, IP Encapsulating Security Payload (ESP)**,** S. Kent, December 2005

[13] RFC 4306, **Internet Key Exchange (IKEv2) Protocol,** C. Kaufman, Diciembre 2005

[14] URL: http://es.wikipedia.org/wiki/Diffie-Hellman

[15] URL: www.voipforo.com

[16] VoIP no es Telefonía IP (iptel), http://www.uberbin.net/archivos/rants/voip-no-es-telefonia-ip.php

[17] FLANNAGAN Michael, CCNA, CCDA, CISCO QoS Administering IP networks, Syngpress Publishing, 2001.

[18] ITU T H.323, Sistemas de comunicación multimedios basados en paquetes, Febrero 1998.

[19] Huidobro José Manuel, H.323 Multimedia sobre redes IP, http://www.coit.es/publicac/publbit/bit109/quees.htm

[20] RFC 3261, *Session Initiation Protocol (SIP)*, J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler; Junio 2002.

[21] Nuevas Tecnologías De Conmutación De Voz Sobre Datos, Valero Dario, Universidad Bicentenaria de Aragua, Diciembre 1998, Maracay – Venezuela

[22] Voz sobre Frame Relay, Gustavo Salvuci, http://www.monografias.com/trabajos12/framerelay/framerelay.shtml

[23] URL: http://isis.faces.ula.ve/COMPUTACION/Internet/VoIP/atm.htm

[24] Knowledgenet.Cisco.Securing.Networks.with.PIX.and.ASA.SNPA.Student. Guide.V4.0.eBook-DDU.pdf

[25] Curriculum Académico, ***Cisco*** Certified ***Network*** Associate, Modulo 3

[26] Curriculum Académico, ***Cisco*** Certified ***Network*** Associate, Modulo 4

[27] URL: http://seguridad.internet2.ulsa.mx/congresos/2001/cudi2/tutorial_ipsec.pdf

[28] URL: http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625, sid14_gci1218461,00.html

[29] CARRION Hugo, Ingeniería de tráfico de telecomunicaciones, Carrión & Carrión Consultores, Julio 2005.

[30] Tecnologías de Banda Ancha Tráfico, Universidad Nacional de rosario, Facultad de Ciencias Exactas y Agrimensura,

[31] URL: http://www.teldat.es/docs/products/pdf/ancho_banda.pdf

[32] URL: http://www.supertel.gov.ec

[33] URL: http://linux.pucp.edu.pe/downloads/linuxweek2006/lwp-asterisk.pdf Handbook.- http://www.digium.com/handbook-draft.pdf

[34] URL: http://www.investigacion.frc.utn.edu.ar/labsis/Publicaciones/QueEsLinux/QueEsLinux.html

[36] URL: http://www.balearsinnovacio.com/blog/wpcontent/uploads/2007/07/ManualAsterisk_innova.pdf

[37] URL: http://garvanet.com/xten/

[38] URL: http://www.sistemasyenlaces.com.ar/Cisco7960_7940_IPPhone.html

ANEXOS

ANEXO A

CARACTERÍSTICAS EQUIPO ASA 5500

(Adaptive Security Appliance)

Cisco ASA 5500 Series SSL/IPsec VPN Edition

The Cisco® ASA 5500 Series Adaptive Security Appliance is a purpose-built platform that combines best-in-class security and VPN services for small and medium-sized business (SMB) and enterprise applications. The Cisco ASA 5500 Series enables customization for specific deployment environments and options, with special product editions for SSL/IPsec VPN, Firewall, Anti-X, and Intrusion Prevention.

The Cisco ASA 5500 Series SSL/IPsec VPN Edition enables organizations to gain the connectivity and cost benefits of Internet transport without compromising the integrity of corporate security policies. By converging Secure Sockets Layer (SSL) and IP Security (IPsec) VPN services with comprehensive threat defense technologies, the Cisco ASA 5500 Series delivers highly customizable network access tailored to the requirements of diverse deployment environments while providing advanced endpoint and network-level security (Figure 1).

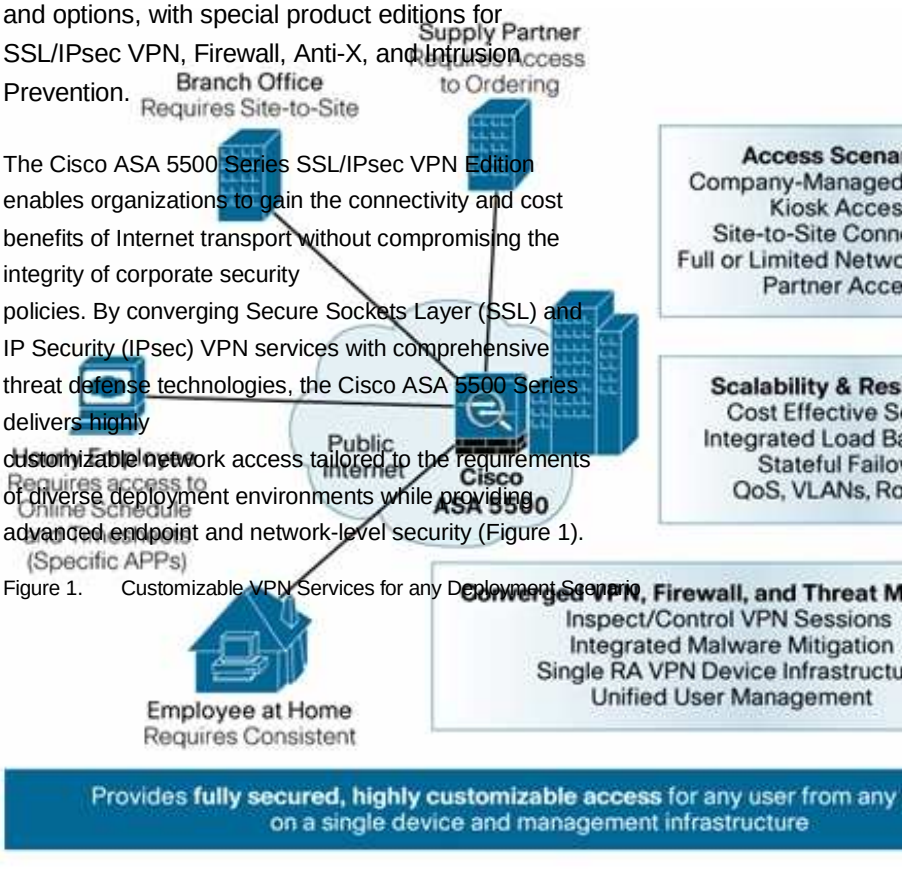


Figure 1. Customizable VPN Services for any Deployment Scenario

Cisco ASA 5500 Series SSL/IPSEC VPN Edition

The Cisco ASA 5500 Series SSL/IPsec VPN Edition offers flexible VPN technologies for any connectivity scenario, with scalability up to 10,000 concurrent users per device. It provides easy-to-manage, full-tunnel network access through SSL, Datagram Transport Layer Security (DTLS), IPsec VPN client technologies, advanced clientless SSL VPN capabilities, and network-aware site-to-site VPN connectivity, enabling secure connections across public networks to mobile users, remote sites, contractors, and business partners. Costs associated with VPN deployment and operations are reduced by eliminating ancillary equipment required to scale and secure a VPN.

Benefits of the Cisco ASA 5500 Series SSL/IPsec VPN Edition include:

- SSL, DTLS, and IPsec-based full network remote access—Full network access provides network-layer remote-user connectivity to virtually any application or network resource and is often used to extend access to managed computers such as company-owned laptops. Connectivity is available through the automatically downloaded Cisco AnyConnect VPN Client, the Cisco IPsec VPN Client, and the Microsoft and Mac OS X Layer 2 Tunneling Protocol (L2TP)/IPsec VPN clients. The Cisco AnyConnect VPN Client will automatically adapt its tunneling protocol to the most efficient method based on network constraints and is the first VPN product to use the DTLS protocol to provide an optimized connection for latency-sensitive traffic, such as voice over IP (VoIP) traffic or TCP-based application access. By supporting SSL, DTLS, and IPsec-based remote-access VPN technologies, the Cisco ASA 5500 Series delivers unsurpassed flexibility to meet the needs of the most diverse deployment scenarios.
- Superior clientless network access—Clientless remote access provides access to network applications and resources, regardless of location, without the need for desktop VPN client software. Using the ubiquity of SSL encryption available in Internet browsers, the Cisco ASA 5500 Series delivers clientless access to any Web-based application or resource, terminal services applications such as Citrix, and optimized Microsoft Outlook Web access and Lotus iNotes, as well as access to common thick-client applications like e-mail and calendering, instant messaging, FTP, Telnet, and SSH. Additionally, the superior content rewriting capabilities of the Cisco ASA 5500 Series help ensure reliable rendering of complex Web pages with Java, JavaScript, ActiveX, Flash, and other sophisticated content.
- Network-aware Site-to-Site VPNs—Secure, high-speed communications are possible between multiple office locations. Support for quality of service (QoS) and routing across the VPN helps ensure reliable, business-quality delivery of latency-sensitive applications like voice, video, and terminal services.
- Threat-protected VPN—VPNs are a primary source of malware infiltration into networks. Malware includes worms, viruses, spyware, keyloggers, Trojan horses, and rootkits. The depth and breadth of intrusion prevention, antivirus, application-aware firewall, and VPN endpoint security capabilities in the Cisco ASA 5500 Series minimizes the risk that the VPN connection will become a conduit for security threats.
- More cost-effective VPN deployment and operations—Scaling and securing VPNs often requires additional load balancing and security equipment, which increases both equipment and operational costs. The Cisco ASA 5500 Series integrates these functions, delivering an unprecedented level of network and security integration among the VPN products available today. And by offering support for flexible tunneling options on a single platform, the Cisco ASA 5500 Series provides customers with cost-effective alternatives to deploying parallel VPN infrastructures.

- Scalability and resiliency—The Cisco ASA 5500 Series can support up to 10,000 simultaneous user sessions per device, with the ability to scale to tens of thousands of simultaneous user sessions through integrated clustering and load-balancing capabilities. Stateful failover features deliver high-availability services for unsurpassed uptime.
- OpenSSL Technology—This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org)

Customizable Remote-Access VPN Features

Full Network Access

The Cisco ASA 5500 Series SSL/IPsec VPN Edition provides broad application and network resource access through network tunneling features available in either the Cisco AnyConnect VPN Client, as shown in Table 1, or the Cisco IPsec VPN Client.

Table 1. Cisco AnyConnect VPN Client Features

Feature	Description
Optimized Network Access	● The Cisco AnyConnect VPN Client automatically adapts its tunneling to the most efficient method possible based on network constraints. The DTLS protocol is automatically used to provide an optimized connection for latency-sensitive traffic, such as VoIP traffic or TCP-based application access. HTTP over SSL is used to ensure availability of network connectivity through locked-down environments, including those using Web proxy servers. ● Data compression may be used to reduce the amount of data transmitted. ●
Broad Operating System Support	Windows 2000 ● XP 32-bit (x86) and 64-bit (x64) ● Windows Vista 32-bit (x86) and 64-bit (x64), including Service Pack 1 (SP1) ● Mac OS X Power PC and Intel 10.4 and 10.5 ● Linux Intel (2.6.x kernel)
Wide Range 0f Deployment and Connection Options	Deployment options: ● Pre-deployment, including Microsoft Installer ● Automatic headend deployment (administrative rights are required for initial installation) via ActiveX (Windows only) and Java Connection modes: ● Standalone via system icon ● Browser initiated (Weblaunch) ● Clientless portal initiated ● Command line interface (CLI) initiated
Ease of Client Administration	● The Cisco AnyConnect VPN Client allows an administrator to automatically distribute software and policy updates from the headend security appliance, thereby eliminating administration associated with VPN client software updates
Consistent User Experience	● Full tunnel client mode supports remote-access users requiring a consistent LAN-like user experience ● Multiple delivery methods and small download size help ensure broad compatibility and rapid download of the Cisco AnyConnect VPN Client
Advanced IP Network Connectivity	● Access to internal IPv4 and IPv6 network resources ● Centralized split tunneling control for optimized network access IP address assignment mechanisms: ● Static ● Internal pool ● Dynamic Host Configuration Protocol (DHCP) ● RADIUS/Lightweight Directory Access Protocol (LDAP)

Clientless Network Access

Clientless SSL VPN access, with features shown in Table 2, allows precisely controlled Web-based access to specific network resources and applications from Internet kiosks, shared computers, extranet partners, employee-owned desktops, and company-owned employee desktops.

Table 2. Cisco ASA 5500 Series Web-Based Clientless Access

Feature	Description
Broad, Reliable Compatibility	An advanced transformation capability helps ensure compatibility with Web pages containing complex content, including HTML, Java, ActiveX, JavaScript, and Flash.
Integrated Clientless Application Optimization	Integrated performance optimization for resource-intensive applications, such as Microsoft Outlook Web Access and Lotus iNotes, delivers exceptional response times and low latency to provide a high-quality SSL VPN end-user experience.
Customizable User Experience	The enhanced clientless portal features group-based customization features for detailed access, ease of use, and a customizable user experience: ● Support for multilanguage clientless user portals ● User-customizable resource bookmarks ● Publishing of Really Simple Syndication (RSS)-based information resources for automatic updating of important real-time content
Fully Clientless Citrix Access	No extraneous helper applications are required for Citrix access over clientless SSL VPN, which helps ensure fast application initiation time and reduces the risk of desktop software conflicts.
Integrated Client/Server Application Support	Provides access to common client/server applications without the need for pre-deployed remote clients, granting rapid access to Telnet, SSH, Remote Desktop Protocol (RDP), and Virtual Network Computing (VNC) resources.
Support for Common Thick-Client Applications	Port forwarding enables clientless access to popular thick client applications like Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), e-mail, online calendars, instant messaging, Telnet, SSH, and other client-initiated TCP applications via a small Java applet. Smart tunneling allows Microsoft Windows users access to TCP applications without the prerequisite of administrative rights and allows VPN administrators to grant only approved applications access to internal resources.
Broad Browser Support	Multiple browser support, including Microsoft Internet Explorer, Firefox, Opera, Safari, and Pocket Internet Explorer (PIE) helps ensure broad connection compatibility from any location.
Advanced IP Network Connectivity	Access to internal IPv4 and IPv6 network resources.

Comprehensive Authentication and Authorization Choices

The Cisco ASA 5500 Series provides a comprehensive set of options for authentication and authorization of users, as shown in Table 3.

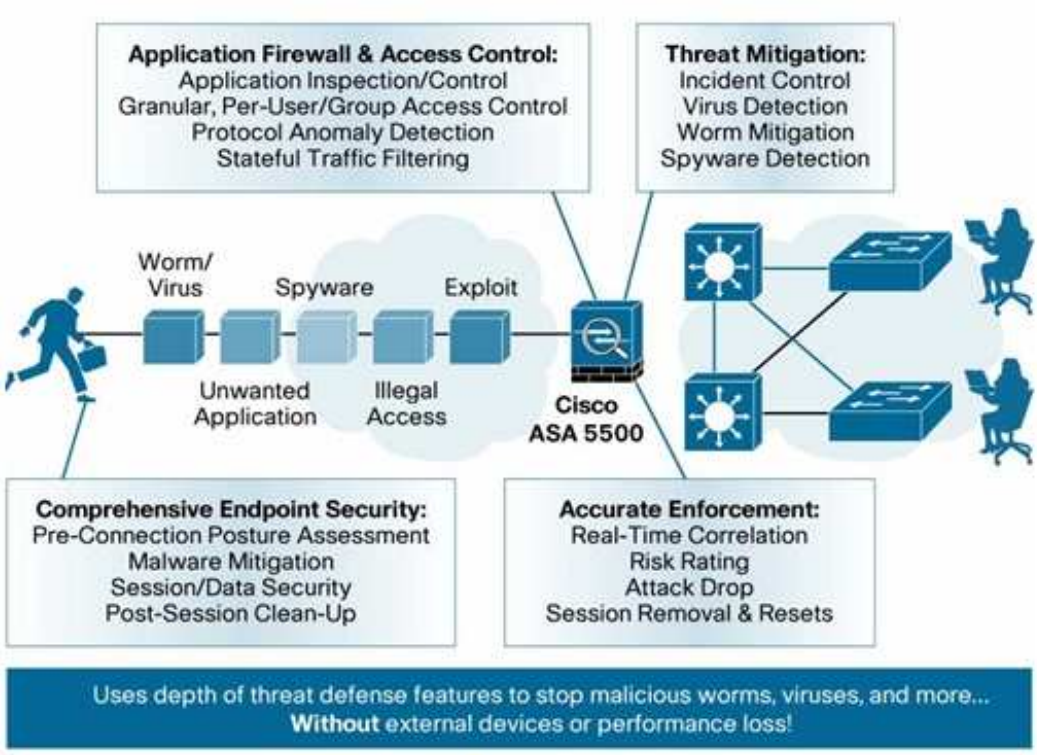
Table 3. Cisco ASA 5500 Series Authentication and Authorization Options

Feature	Description
Authentication Options	● RADIUS ● RADIUS with Password Expiry (MSCHAPv2) to NT LAN Manager (NTLM) ● RADIUS OTP Support (state/reply message attributes) ● RSA SecurID ● Active Directory/Kerberos ● Embedded Certificate Authority (CA) ● Digital Certificate / Smartcard ● LDAP with Password Expiry and Aging ● Generic LDAP Support ● Combined certificate and username/password multifactor authentication ● Internal domain password prompting for simplified Single Sign On (SSO) ● SSL VPN virtual keyboard authentication for additional protection against keystroke loggers
Sophisticated Authorization	● Policy mapping from RADIUS and LDAP ● Dynamic access policies directly leverage domain membership and posture status for creation of user policy
Single Sign On (SSO) for Clientless SSL VPN Users	● Computer Associates Siteminder (Netegrity) ● RSA Access Manager (ClearTrust) ● Security Assertion Markup Language (SAML) ● Basic/NTLM authentication pass-through ● Forms-based authentication pass-through

Threat-Protected VPN Features

The Cisco ASA 5500 Series SSL/IPsec VPN Edition provides advanced security for VPN deployments through its integrated network and endpoint security technologies. Securing the VPN is necessary to ensure it prevents network attacks such as worms, viruses, spyware, keyloggers, Trojan horses, rootkits, or hacking. Detailed application and access control policy helps ensure that individuals and groups of users have access only to the applications and network services to which they are entitled (Figure 2).

Figure 2. Threat-Protected VPN Services Use Onboard Security to Protect Against VPN Threats



Network Security at the VPN Gateway

Worms, viruses, application-embedded attacks, and application abuse are among the greatest security challenges in today's networks. Remote access and remote-office VPN connectivity are common points of entry for such threats due to limited security capabilities on VPN devices. VPNs are often deployed without proper inspection and threat mitigation applied at the tunnel termination point at the headquarters location, which allows malware from remote offices or users to infiltrate the network and spread. With the converged threat mitigation capabilities of the Cisco ASA 5500 Series, customers can detect malware and stop it before it enters the network interior. For application-embedded attacks, such as spyware or adware spread through file-sharing peer-to-peer networks, the Cisco ASA 5500 Series deeply examines application traffic to identify a dangerous payload and drops its contents before it reaches its target and causes damage. Table 4 lists some VPN gateway security features provided by the Cisco ASA 5500 Series.

Table 4. Network Security at the VPN Gateway

Feature	Description
Extensive Malware Mitigation	Worms, viruses, spyware, keyloggers, Trojan horses, and rootkits are thwarted at the Cisco ASA 5500 Series VPN gateway, thereby eliminating threats before they spread throughout the network.
Application-Aware Firewall and Access Control	Application-aware traffic inspection enables thorough user access control and helps prevent abuse of unwanted applications, such as peer-to-peer file sharing across the VPN connection.
Intrusion Prevention	The Cisco ASA 5500 Series guards against a multitude of network exploits.
Access Restrictions	The permission or denial of access to confidential resources is based on flexible configuration policies and current posture status.
Virtual LAN (VLAN) Mapping	Enforcement of user and group-based traffic access restrictions are based on a configured VLAN.

Comprehensive Endpoint Security for SSL VPN

SSL VPN deployments enable universal access from both secure and non-corporate-managed endpoints, and provide the ability to extend network resources to diverse user communities. With this extension of the network, the points for potential network security attacks also increase. Whether users are accessing the network from a corporate-managed PC, personal network-accessible device, or public terminal, Cisco Secure Desktop minimizes data such as cookies, browser history, temporary files, and downloaded content left behind after an SSL VPN session terminates. Endpoint posture checking for full network access users is also available through integration with the Cisco NAC Appliance and Cisco NAC Framework. Table 5 highlights Cisco Secure Desktop features.

Table 5. Cisco Secure Desktop Provides Comprehensive Security of Information from the Network to the Endpoint

Feature	Description
Pre-Connection Posture Assessment	Host integrity verification checking seeks to detect the presence of antivirus software, personal firewall software, and Windows service packs on the endpoint system prior to granting network access. A significantly expanded list of applications and versions are now supported through this mechanism. Frequent updates are available to support new product releases. Administrators also have the option of defining custom posture checks based on the presence of running processes.
Pre-Connection Asset Assessment	Cisco Secure Desktop can detect the presence of a watermark on a remote system. The watermark can be used to identify assets that are corporate-owned and provide differentiated access as a result. The watermark checking capability includes system registry values, file existence matching a required CRC32 checksum, IP address range matching, and certificate issued by/to matching.
Comprehensive Session Protection	Additional protection is provided for all data associated with the session, including passwords, file downloads, history, cookies, and cache files. Session data is encrypted to the secure vault of Cisco Secure Desktop.
End-of-Session Data Cleanup	Data in the secure vault is overwritten at the end of the session.
Keystroke Logger Detection	Cisco Secure Desktop performs an initial check for certain software-based keystroke logging software at the start of the session. If an anomalous program begins running inside the secure vault, after session initiation, the user is prompted to stop the suspicious activity.
Available with Guest Permissions	Users accessing the network from remote machines may not have administrator privileges on all systems. Cisco Secure Desktop can often be installed with only guest permissions. This helps to ensure delivery and installation on all systems.
Advanced Endpoint Assessment License	An advanced endpoint assessment option is available to automate the process of repairing out-of-compliance applications.

Network-Aware Site-to-Site VPN Features

Using the network-aware IPsec site-to-site VPN capabilities provided by the Cisco ASA 5500 Series SSL/IPsec VPN Edition, businesses can securely extend their networks across low-cost Internet connections to business partners and remote and satellite offices worldwide (Table 6).

Table 6. Cisco ASA 5500 Series SSL/IPsec VPN Edition Site-to-Site VPN Connectivity

Feature	Description
QoS-Enabled	Supports latency-sensitive applications like voice, video, and terminal services.
Network-Aware Routing	Open Shortest Path First (OSPF) support across tunneling neighbors enables network topology awareness for ease of network integration.

VPN Cost-Effectiveness through Platform Integration

The Cisco ASA 5500 Series integrates numerous functions—such as security and load balancing—that can reduce the number of devices required to scale and secure the VPN, thereby decreasing equipment costs, architectural complexity, and operational costs (Table 7).

Table 7. Integrated Functions that Complement VPN Deployment

Feature	Description
Network and Endpoint Security	Onboard malware mitigation, IPS, and firewall capabilities increase VPN security while decreasing the amount of equipment that needs to be deployed.
Load Balancing	Integrated load-balancing features enable multichassis clusters without expensive external load balancing equipment.

Cisco ASA 5500 Series Platform Overview

The Cisco ASA 5500 Series delivers site-specific scalability, from small offices to enterprise headquarter locations, through its seven models: 5505, 5510, 5520, 5540, 5550, 5580-20 and 5580-40 (Figure 3). Models 5510 through 5550 share a common chassis, built with a foundation of concurrent services scalability, investment protection, and future technology extensibility. Table 8 lists the specifications of the Cisco ASA 5500 Series models.

Figure 3. The Cisco ASA 5500 Series Portfolio

Table 8. Specifications of Cisco ASA 5500 Series Adaptive Security Appliances

Platform	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580-20	Cisco ASA 5580-40
Maximum VPN Throughput	100 Mbps	170 Mbps	225 Mbps	325 Mbps	425 Mbps	1Gbps	1Gbps
Maximum Concurrent SSL [1] VPN Sessions	25	250	750	2500	5000	10,000	10,000
Maximum Concurrent IPsec VPN Sessions[1]	25	250	750	5000	5000	10,000	10,000
Interfaces	Eight 10/100 copper Ethernet ports with dynamic port grouping. Includes two Power over Ethernet (PoE) ports, three USB ports	Three 10/100/1000 copper Ethernet ports, one out-of-band management port, two USB ports	Four 10/100/1000 copper Ethernet ports, one out-of-band management port, two USB ports	Four 10/100/1000 copper Ethernet ports, one out-of-band management port, two USB ports	Eight Gigabit Ethernet ports, four small form factor-pluggable (SFP) fiber ports, one Fast Ethernet port	Two USB ports, Two RJ-45 Management ports, Two Gigabit Ethernet Management ports With Interface Expansion Cards: • Up to Twelve 10Gigabit Ethernet (10GE) ports • Up to Twenty-Four Gigabit Ethernet ports • Up to Twenty-Four 10/100/1000 Ethernet ports	Two USB ports, Two RJ-45 Management ports, Two Gigabit Ethernet Management ports With Interface Expansion Cards: • Up to Twelve 10Gigabit Ethernet (10GE) ports • Up to Twenty-Four Gigabit Ethernet ports • Up to Twenty-Four 10/100/1000 Ethernet ports
Profile	Desktop	1-RU	1-RU	1-RU	1-RU	4-RU	4-RU
Stateful Failover	No	Licensed [2] feature	Yes	Yes	Yes	Yes	Yes
VPN load Balancing	No	Licensed feature[2]	Yes	Yes	Yes	Yes	Yes

Cisco Services

Cisco and its partners provide services that can help you deploy and manage security solutions. Cisco has adopted a lifecycle approach to services that addresses the necessary set of requirements for deploying and operating Cisco adaptive security appliances and other Cisco security technologies. This approach can help you improve your network security posture to achieve a more available and reliable network, prepare for new applications, lower your network costs, and maintain network health through day-to-day operations. For more information about Cisco Security Services, visit http://www.cisco.com/go/services/security.

For More Information

- Cisco ASA 5500 Series: http://www.cisco.com/go/asa
- Cisco Adaptive Security Device Manager: http://www.cisco.com/go/asdm
- Cisco Product Certifications: http://www.cisco.com/go/securitycert
- Cisco Security Services: http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html

[1] Devices include a license for two SSL VPN users for evaluation and remote management purposes. The total concurrent IPsec and SSL (clientless and tunnel-based) VPN sessions may not exceed the maximum concurrent IPsec session count shown in the chart. The SSL VPN session number may also not exceed the number of licensed sessions on the device. The ASA 5580 Series supports greater simultaneous users than the ASA 5550 Series at comparable overall SSL VPN throughput as the ASA 5550 Series. These items should be taken in to consideration as part of your capacity planning.

[2] Upgrade is available with Cisco ASA 5510 Security Plus license.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

ANEXO B

REGULACIÓN VoIP

RESOLUCIÓN 491-21-CONATEL-2006

CONSEJO NACIONAL DE TELECOMUNICACIONES
CONATEL

CONSIDERANDO:

Que de conformidad a la Ley Especial de Telecomunicaciones y sus reformas y al Reglamento General a la Ley Especial de Telecomunicaciones Reformada, el CONATEL es el ente público encargado de establecer, en representación del Estado, las políticas y normas de regulación de las telecomunicaciones en el Ecuador.

Que el avance tecnológico ha impulsado la introducción de programas y aplicaciones sobre la red Internet, que facilitan la transmisión y recepción de voz, video y datos.

Que es política del Estado impulsar la masificación del uso de Internet como herramienta para el desarrollo económico, cultural, social y político del Ecuador y reducir la brecha digital, que afecta a los sectores más vulnerables de la sociedad, limitando su acceso por su condición económica, social, cultural, étnica o localización.

Que los proveedores de Servicios de Valor Agregado de Internet están facultados legalmente por el CONATEL para la provisión de acceso a Internet.

Que los Centros de Acceso a Internet y Ciber Cafés están regulados mediante la Resolución 073-02-CONATEL-2005, demás normas y regulación vigente.

Que Internet, por su naturaleza de red global, opera sobre una infraestructura distinta de las redes públicas de telecomunicaciones que se han desplegado dentro de territorio ecuatoriano, de conformidad con la legislación y normativa vigente.

Que la denominada Voz sobre IP, identificada con las siglas VoIP, es un término genérico que incluye varias modalidades de uso que requieren ser diferenciadas para determinar la aplicación de normas de regulación y control vigentes dentro del territorio del Ecuador.

Que el denominado Protocolo de Internet, identificado por las siglas IP, es un lenguaje de transmisión de información caracterizado por el envío de datos en formato de paquetes.

En ejercicio de sus facultades,

RESUELVE:

ARTÍCULO UNO. La Voz sobre Internet, cursada a través de la red Internet, permite a sus usuarios comunicarse entre sí o entre un usuario conectado a la red Internet con un usuario conectado a una Red Pública de Telecomunicaciones. La Voz sobre Internet es reconocida como una aplicación tecnológica disponible en Internet. El video, los datos y multimedios cursados a través de la red Internet, son igualmente reconocidos como aplicaciones tecnológicas disponibles en Internet.

ARTÍCULO DOS. Cuando un operador de telecomunicaciones preste el servicio de telefonía utilizando Protocolo IP, el operador está sujeto al marco legal, las normas de regulación y control aplicables.

RESOLUCIÓN 491-21-CONATEL-2006

ARTÍCULO TRES. Los proveedores de Servicio de Valor Agregado de Internet no restringirán a sus usuarios el acceso a las aplicaciones detalladas en el Artículo 1 de la presente Resolución, incluido su uso, sin perjuicio de origen, marca o proveedor de tales aplicaciones.

ARTICULO CUATRO. Cualquier persona natural o jurídica, incluyendo a los proveedores de Servicio de Valor Agregado de Internet dentro de los servicios que prestan a sus usuarios, podrán comercializar dispositivos y planes para el uso de las aplicaciones detalladas en el Artículo 1 de la presente Resolución.

ARTICULO CINCO. Ninguna persona natural o jurídica, incluyendo a los Proveedores de Servicio de Valor Agregado de Internet, podrán usar, dentro del territorio nacional, dispositivos de conmutación, tales como interfaces o compuertas (gateways) o similares, que permitan conectar las comunicaciones de Voz sobre Internet o las llamadas sobre Internet a las Redes Públicas de Telecomunicaciones del Ecuador.

Se exceptúan de esta limitación a los operadores de telecomunicaciones debidamente autorizados.

ARTICULO SEIS. El CONATEL, a través de la SENATEL, no concederá recurso de numeración telefónica, de conformidad al Plan Técnico Fundamental de Numeración, para las aplicaciones detalladas en el Artículo 1 de la presente Resolución.

ARTÍCULO SIETE. Deróguese los literales b) y c) del Artículo tres (3) de la Resolución 073-02-CONATEL-2005 de 25 de enero de 2005.

ARTÍCULO OCHO. Sustitúyase el literal d) del Artículo tres (3) de la Resolución 073-02-CONATEL-2005 por el siguiente: literal “d) Los “Centros de información y acceso a la red de Internet” o “Ciber Cafés” que ofrezcan voz sobre Internet, de conformidad con lo señalado en el literal a) del presente artículo requerirán únicamente de un certificado de registro, de conformidad con el artículo 7 de la presente resolución;”.

ARTÍCULO NUEVE. Encárguese a la SENATEL que, en el término de noventa días, elabore los parámetros de calidad, las consideraciones de numeración, interconexión y otros aspectos necesarios para los operadores legalmente autorizados que brinden Telefonía sobre Protocolo IP.

La presente Resolución es de ejecución inmediata y entrará en vigencia a partir de la presente fecha, sin perjuicio de su publicación en el Registro Oficial.

Dado en Quito, 8 de septiembre de 2006.

DR. JUAN CARLOS SOLINES MORENO
PRESIDENTE DEL CONATEL

AB. ANA MARÍA HIDALGO CONCHA
SECRETARIA DEL CONATEL

ANEXO C

INSTALACIÓN DEL SERVIDOR ASTERISK

Instalación de Asterisk Now

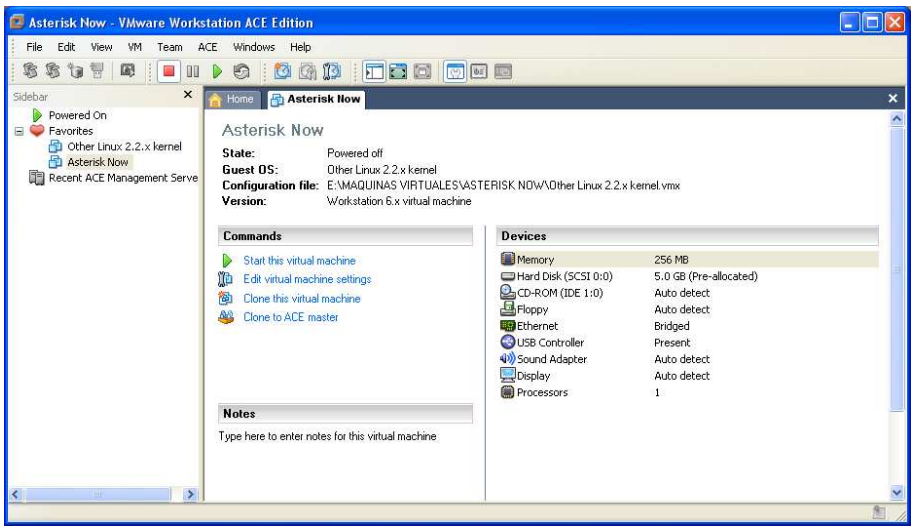
Existen algunas versiones de Asterisk que se instalan como aplicaciones o programas para sistemas operativos Linux y Windows. La versión utilizada en este proyecto es un sistema operativo basado en Linux.

Lo primero que se debe hacer es obtener una versión de Asterisk Now, que se puede descargar de http://www.asterisknow.org/, que es un software desarrollado por Digium, se trata de una distribución de Linux especialmente adaptada para hacer funcionar Asterisk en cuestión de minutos ya que viene con todos los requerimientos y dependencias de software preconfigurados y permite la administración y mantenimiento del servidor de una manera realmente sencilla.

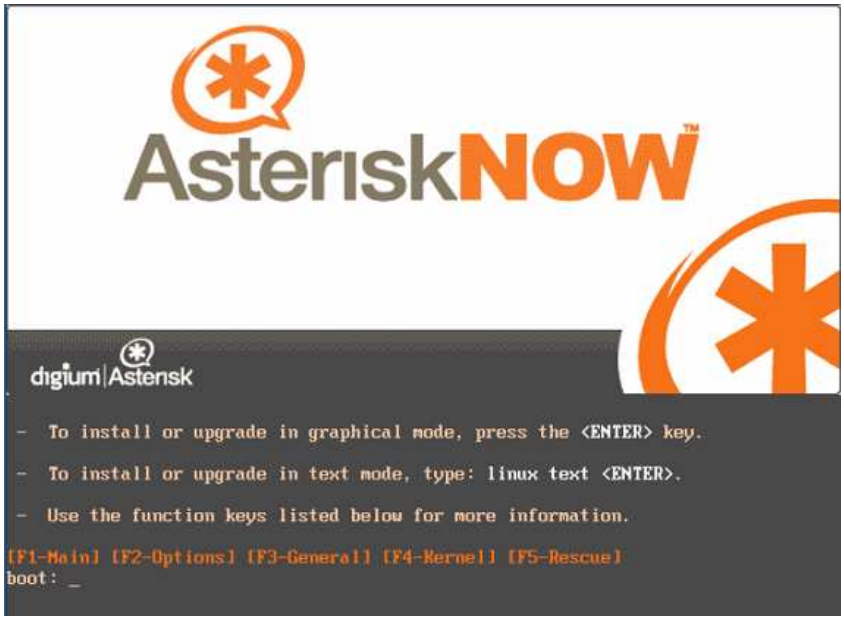
En esta página se descarga una imagen ISO de la versión de Asterisk y luego se graba la imagen en un CD.

En nuestro caso al no contar con una PC dedicada a ser el servidor Asterisk hemos utilizado una portátil en la que hemos instalado el software VMware Workstation que sirve para crear máquinas virtuales.
La máquina virtual en la que hemos instalado tiene las siguientes características:

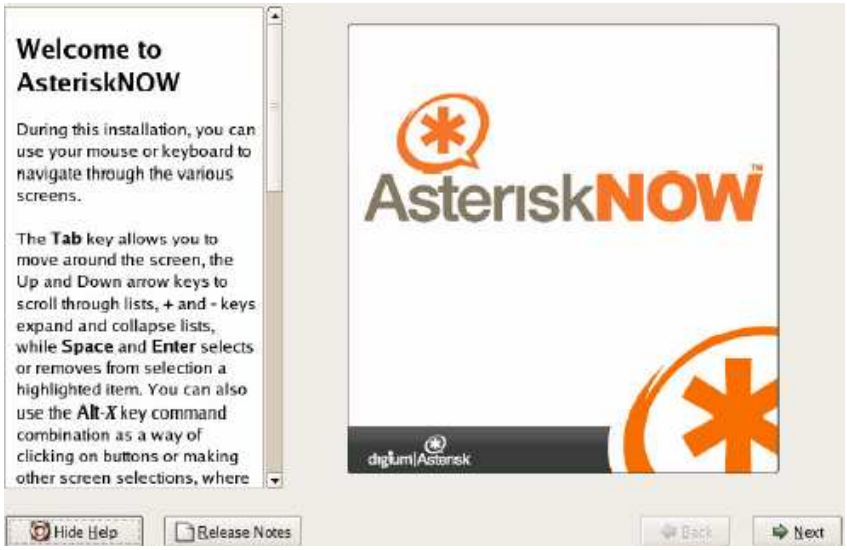
- ✓ Memoria 256 MB
- ✓ Disco Duro 5 GB
- ✓ Procesador AMD Turion 64x2



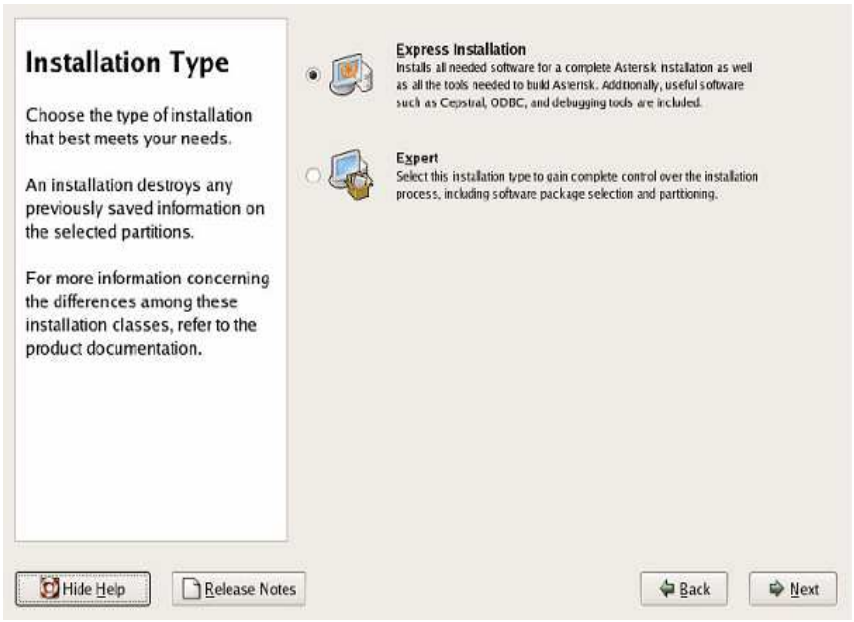
Se arranca el PC, con el CD introducido y nos aparecerá la siguiente pantalla



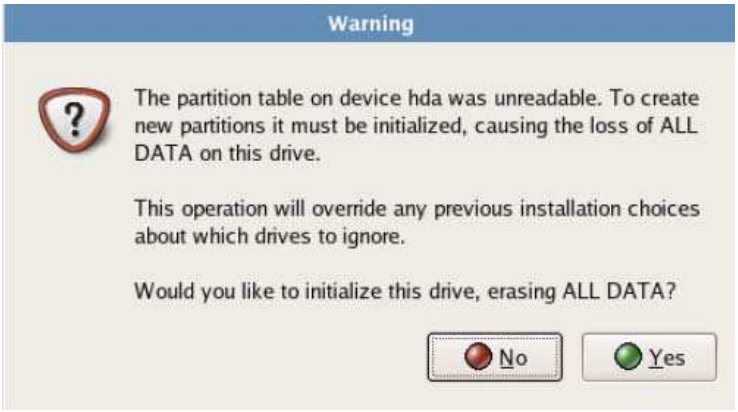
Donde se pulsa ENTER para hacer la instalación en modo grafico. Luego saldrá una pantalla que da la bienvenida a la instalación.



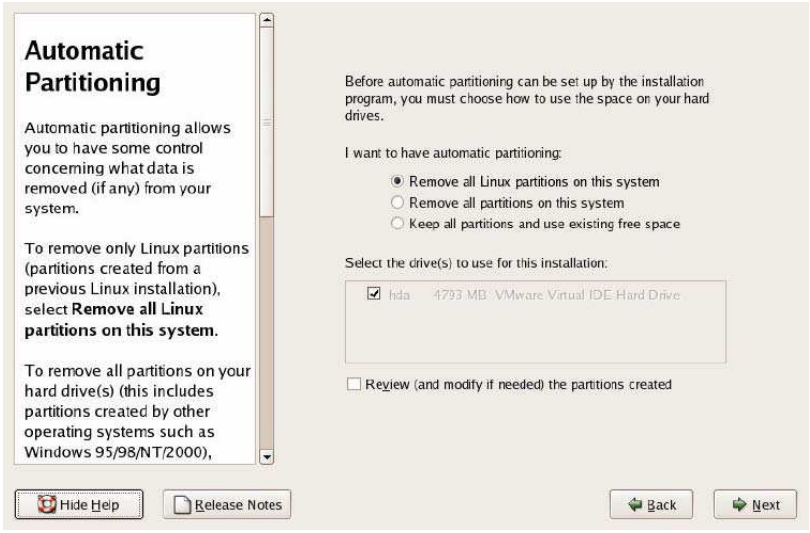
Se pulsa el botón Next y se muestra la siguiente pantalla, donde se selecciona la opción de Express installation y se pulsa Next.



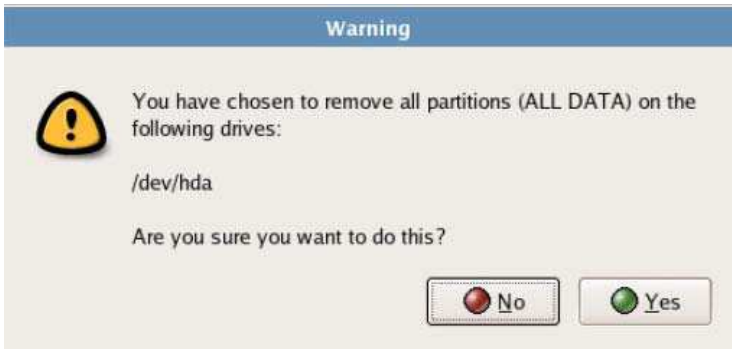
La siguiente pantalla puede variar. Si en el PC donde se va a realizar la instalación de Asterisk Now, existe previamente una instalación de Windows o Linux, saldrá un mensaje indicando que se borraran todos lo datos. Donde se debe pulsar yes. Es por este motivo que en la máquina donde se instale el servidor Asterisk deberá ser dedicada solo para este servicio y no se podrá tener más de un Sistema operativo.



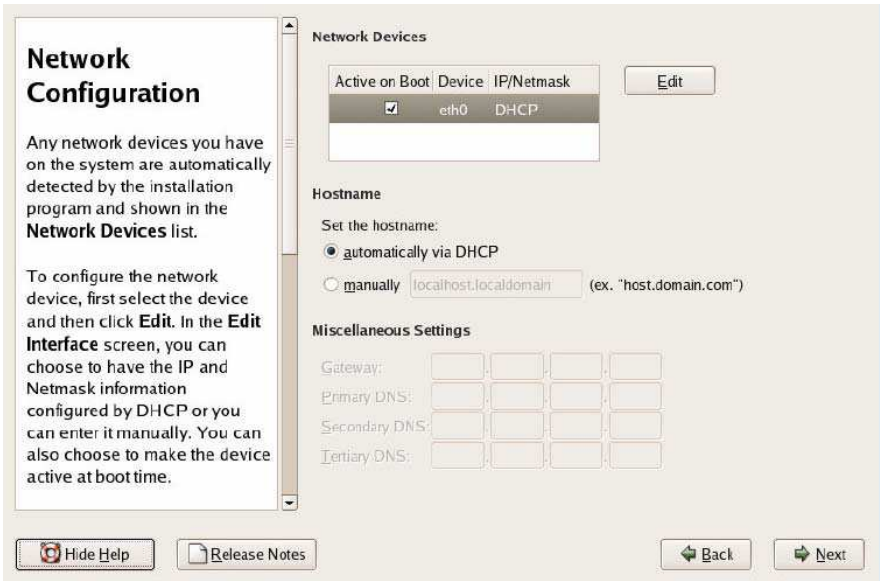
Empieza el proceso de partición automático. Donde dependiendo del caso se debe seleccionar la primera o segunda opción, y pulsar next.



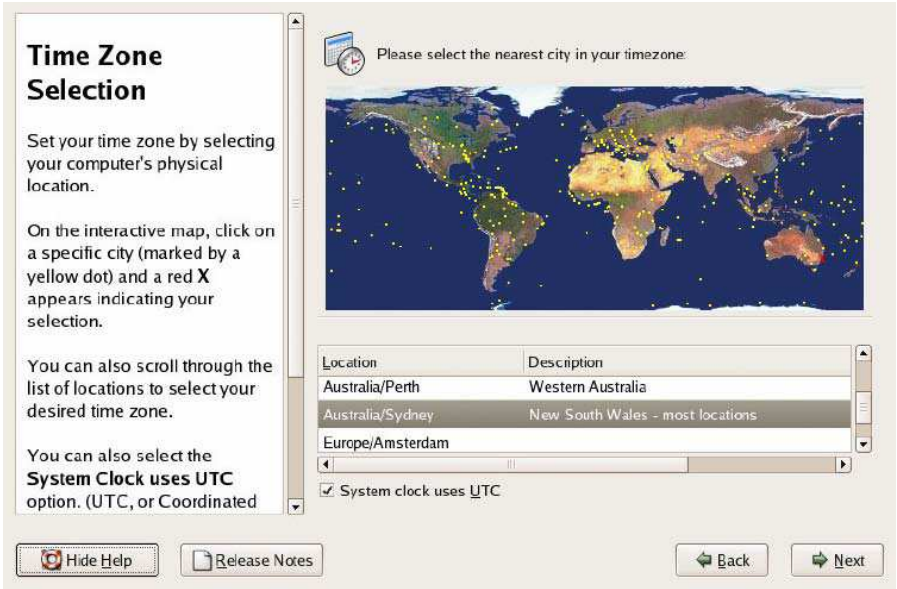
Antes de empezar el proceso de instalación, saldrá un mensaje indicando que si se está seguro de eliminar las particiones. Donde se deberá pulsar yes.



La siguiente pantalla es para configurar la red en el servidor Asterisk. Donde se puede configurar mediante DHCP (obtención automática de dirección) o manualmente. Y se le aplicó la opción de DHCP debido a que se cuenta con un servidor DHCP en el campus de la Politécnica cuya dirección es la 172.31.4.3 / 24, una vez instalado Asterix se puede cambiar la dirección IP para asignar una dirección fija.

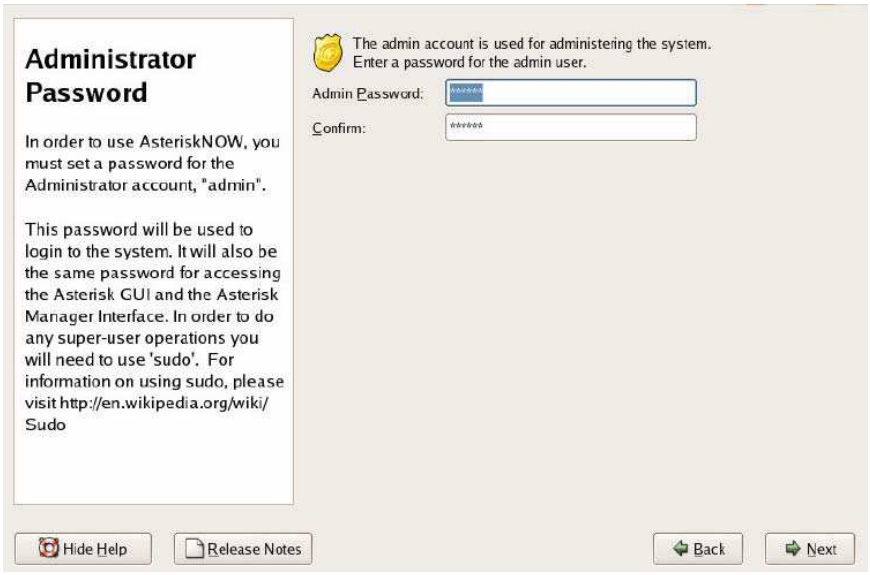


La siguiente pantalla es para configurar la zona de tiempo. En este caso se toma la opción de Bogotá, Guayaquil, Lima que es el uso horario de -5, y se continúa con el proceso de instalación.

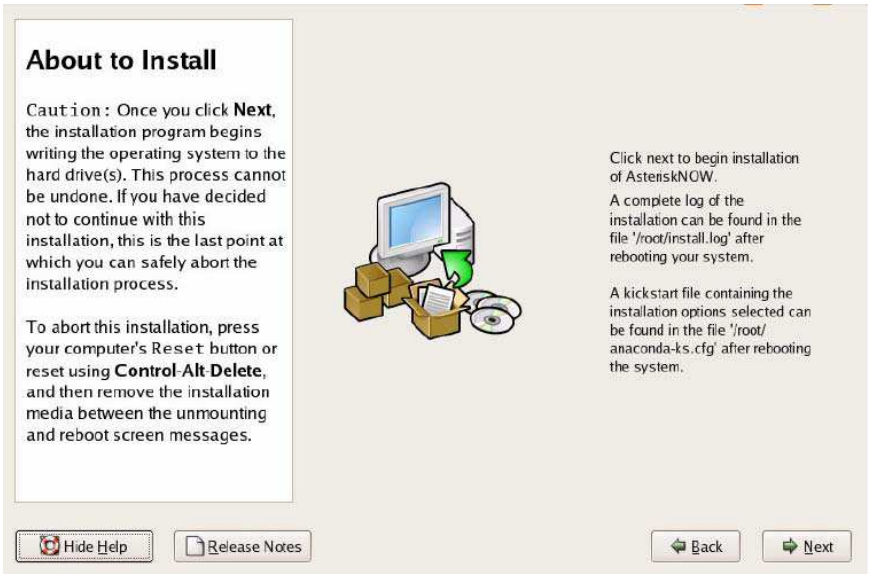


Por defecto se crea un usuario ADMIN, donde en la siguiente pantalla se solicita el ingreso y confirmación de una contraseña. Este usuario admin, será un usuario limitado, también existe el usuario ROOT que es el usuario administrador. Luego se pulsa next.

La contraseña que se configuró para el usuario *admin* es "*asterix*".

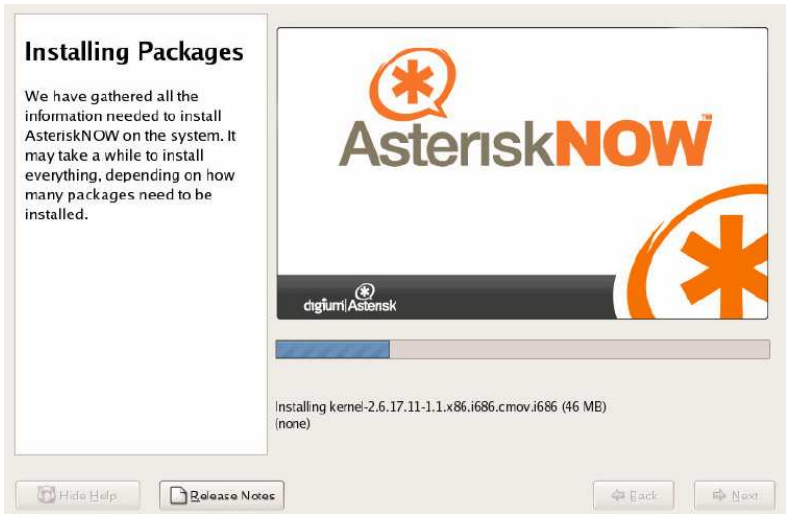


Antes de continuar con la instalación, se muestra una pantalla que indica los procesos que se llevan a cabo en la instalación y se pulsa next para instalar todos los paquetes seleccionados.

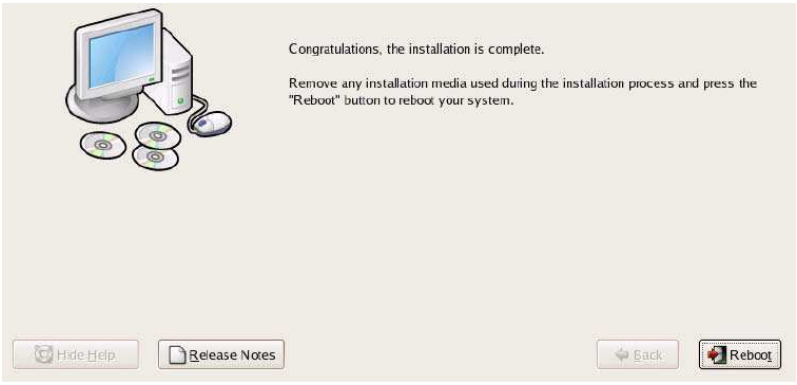


Antes de realizar la instalación, se debe realizar el formateo del sistema.

Luego comienza el proceso de instalación, que nos saldrán las siguientes pantallas.

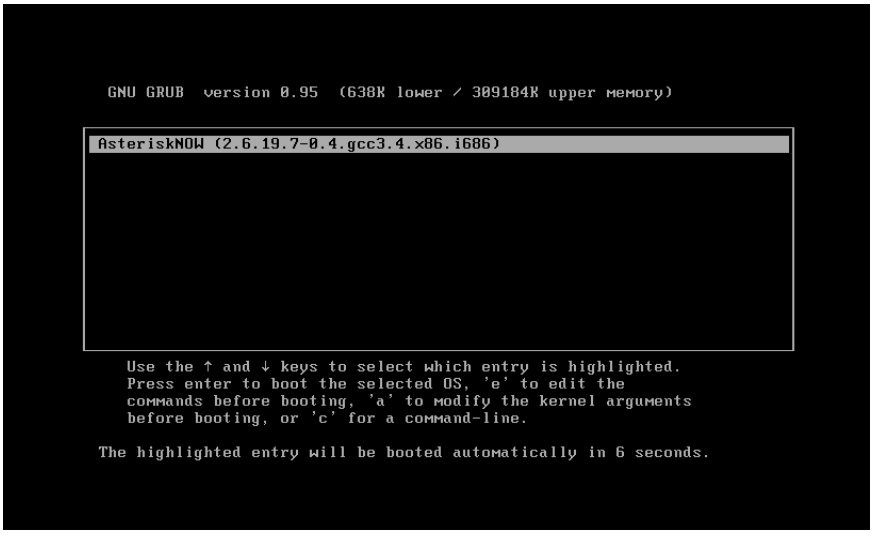


Una vez finalizada la instalación, nos solicitara el reinicio del sistema



Primer arranque de Asterisk Now

Una vez finalizada la instalación, se ha reiniciado el PC, donde se muestra una pantalla que solicita el núcleo de arranque.



La pantalla siguiente saldrá en el primer arranque de Asterisk Now, donde nos indica que existe un usuario llamado admin, y que su contraseña la hemos introducido durante el proceso de instalación.

Por ultimo, el PC se quedara con la consola de Asterisk Now y se prosigue con la administración y configuración del servidor Asterisk ya sea en forma gráfica (vía Web) o a través de comandos (vía SSH).

ANEXO D

INSTALACIÓN Y FUNCIONES DE WIRESHARK

ETHEREAL es una herramienta gráfica utilizada por los profesionales y/o administradores de la red para identificar y analizar el tipo tráfico en un momento determinado. En el argo IT se denominan analizadores de protocolos de red, analizadores de paquetes, packet sniffer o sniffer. Ethereal permite analizar los paquetes de datos en una red activa como también desde un archivo de lectura previamente generado, un caso particular es generar un archivo con TCPDUMP y luego analizarlo con Ethereal.

A partir del año 2006 Ethereal es conocido como **WireShark**[25] y hoy en día está categorizado como uno de los TOP 10 como *sniffer* junto a Nessus y Snort ocupando el segundo lugar entre estos.

Algunas de las características de WireShark son las siguientes:

- Disponible para UNIX, LINUX, Windows y Mac OS.
- Captura los paquetes directamente desde una interfaz de red.
- Permite obtener detalladamente la información del protocolo utilizado en el paquete capturado.
- Cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas.
- Filtra los paquetes que cumplan con un criterio definido previamente.
- Realiza la búsqueda de los paquetes que cumplan con un criterio definido previamente.
- Permite obtener estadísticas.
- Sus funciones gráficas son muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos.

Es importante tener presente que WireShark no es un IDS (*Instrusion Detection System*) ya que no es capaz de generar una alerta cuando se presentan casos anómalos en la red. Sin embargo, permite a los profesionales de IT analizar y solventar comportamientos anómalos en el tráfico de la red.

[25] A partir de esta nota nos referiremos a Ethereal como WireShark.

INSTALACIÓN DE WIRESHARK

El instalador y los archivos binarios de Ethereal pueden ser descargados en http://www.ethereal.com/download.html y sus últimas versiones en http://www.wireshark.org/download.html. Adicional a esto en http://wiki.ethereal.com y http://wiki.wireshark.org se podrá obtener una amplia cantidad de información relacionada con la aplicación, listas de correo tanto para usuarios finales como desarrolladores.

WireShark soporta múltiples plataforma entre ellas UNIX, LINUX y Windows, a continuación se describe la instalación para cada uno de estos sistemas operativos.

Instalación UNIX

Para iniciar la instalación debemos contar con las siguientes utilidades instaladas:

- GTK+, GIMP Tool Kit y Glib (puede obtener en el siguiente site: www.gtk.org)
- libpcap (puede obtener en el siguiente site: www.tcpdump.org)

Si es el caso de obtener los archivos fuentes los siguientes pasos describen el proceso para descomprimir los archivos y generar el ejecutable:

1. Según la distribución de UNIX, se aplica el comando correspondiente para descomprimir el archivo obtenido.

   - En versiones de UNIX con GNU tar

     ```
     tar zxvf wireshark-1.0.0-tar.gz
     ```

   - En caso contrario se deberá ejecutar los siguientes comandos

```
gzip –d wireshark-1.0.0-tar.gz
tar xvf wireshark-1.0.0-tar
```

2. Cambiar al directorio raíz de WireShark.

```
cd <ruta_directorio_wireshark>
```

3. Configuración de los archivos fuentes con el objetivo de asegurar su buen funcionamiento en la versión de UNIX correspondiente.

```
./configure
```

4. Para generar el archivo ejecutable se debe aplicar el siguiente comando.

```
make
```

5. Finalmente para culminar la instalación de la aplicación se ejecuta el comando:

```
make install
```

Otros métodos son aplicados para la instalación según las distribuciones de UNIX todos estos disponibles en el siguiente link http://www.wireshark.org/docs/wsug_html_chunked/ChBuildInstallUnixInstallBins.html, particularmente para el caso de DEBIAN se aplica el siguiente comando para hacer uso de la interfaz gráfica para APT:

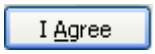
```
aptitude install wireshark
```

Instalación Windows

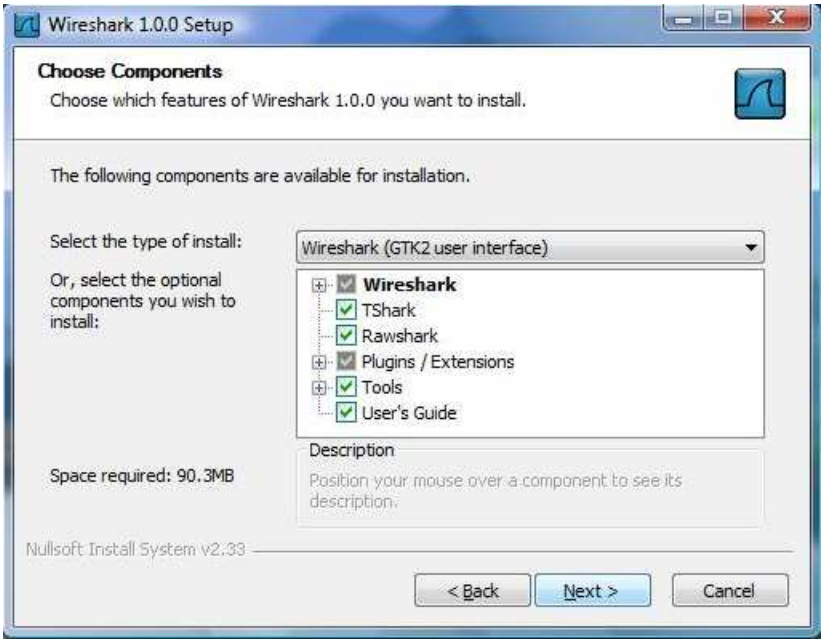
1. Una vez que se obtiene el instalador desde http://www.wireshark.org/download.html se ejecuta el archivo wireshark-setup-1.0.0.exe (en este caso la versión es 1.0.0) para iniciar la instalación. Es importante mencionar que las librerías necesarias como WinPcap están incluidas en el instalador.

   Se muestra la siguiente pantalla del asistente:

2. Presionando el botón 

se despliega la especificación de la licencia y al presionar el botón 

se despliega la siguiente ventana para seleccionar los componentes que se desean instalar.



Para esta instalación se seleccionarán los siguientes:

- Wireshark, GUI del analizador de protocolos.
- TShark, línea de comando del analizador de protocolos. Plugins/Extensions, especificar plugins y extensiones para TShark y Wireshark en este punto deberá seleccionar todos los ítems listados.
- Tool, ofrece herramientas adicionales aplicar a los archivos que contienen los paquetes para su análisis seleccionar todas las ofrecidas durante la instalación.

  Editcap, para manipular los archivos.

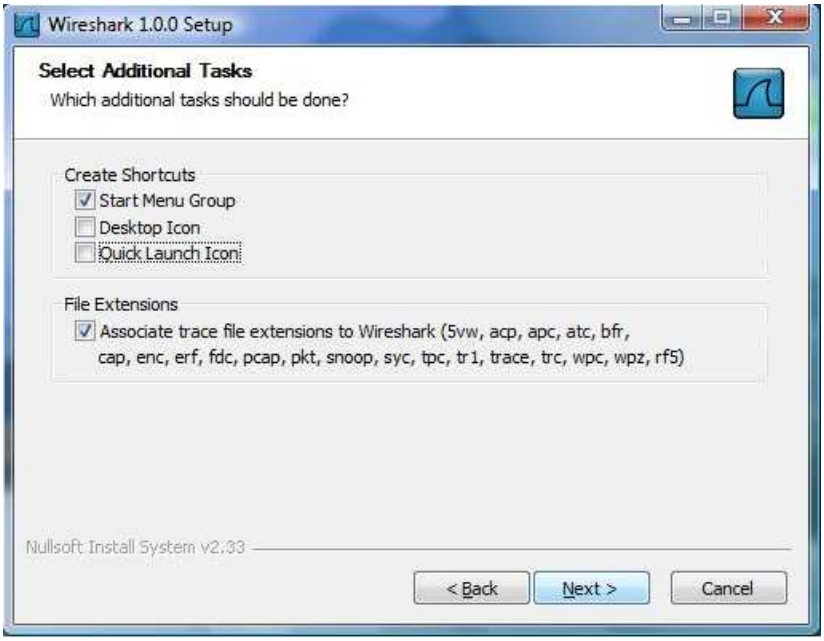
  Text2Pcap, convierte un archivo ASCII en formato libpcap.

  Mergecap, permite obtener un archivo desde la combinación de 2 o más archivos de paquetes capturados.

  Capinfos, es un programa que proporciona información de los paquetes capturados.

3. La siguiente pantalla permite seleccionar si se desea crear un acceso directo a la aplicación en el escritorio, crear un menú de inicio y visualizar el icono en la barra de tareas. Adicionalmente se tiene la posibilidad de

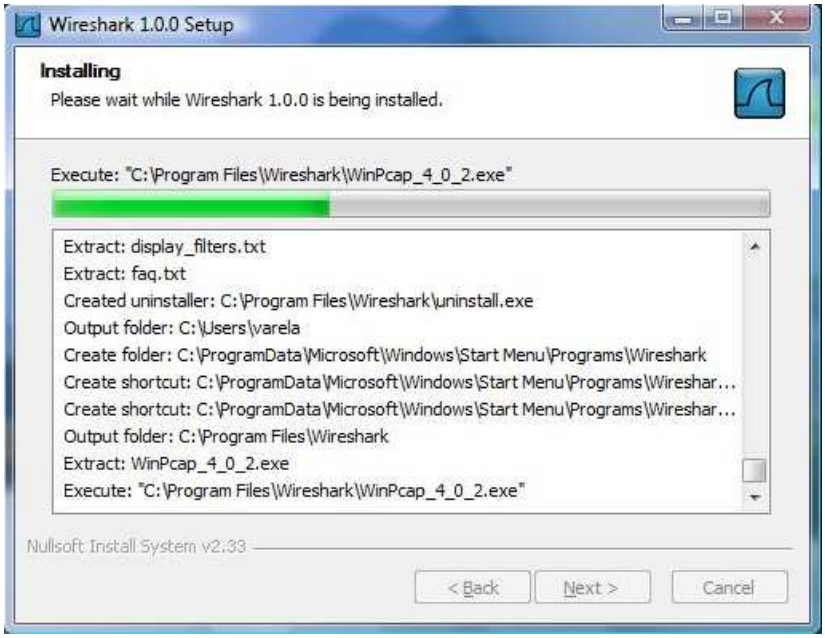
permitir, que los archivos generados por otros analizadores de tráfico puedan ser visualizados con Wireshark (opción que debemos seleccionar).



4. A continuación se deberá seleccionar el directorio donde se instalará la aplicación, en este punto se acepta el indicado por defecto en el instalador.

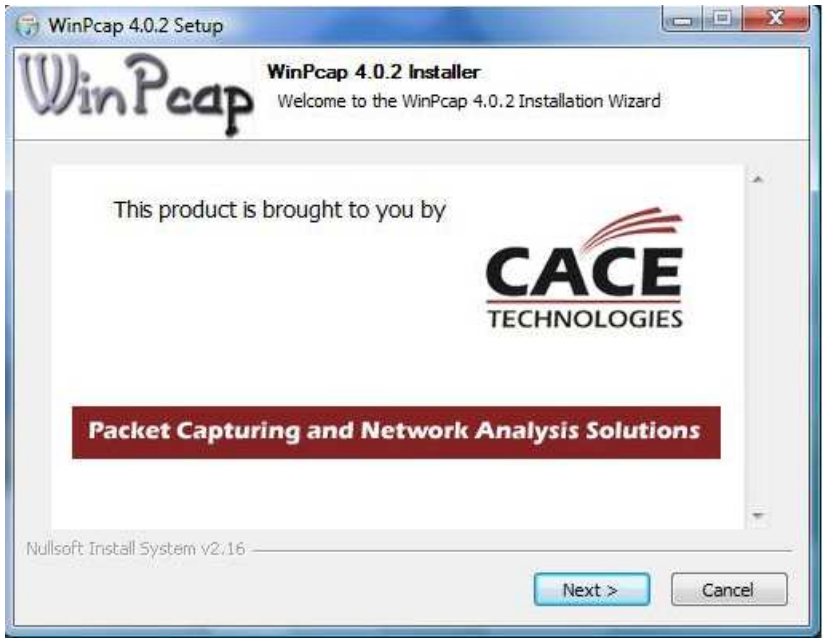
   El instalador de WireShark contiene una versión de WinPcap se verifica si se debe actualizar versión en el PC donde se está realizado la instalación y ofrece la opción de agregar un servicio para que usuarios que no tiene privilegios de administrador pueda capturar paquetes. En este punto se seleccionan ambos ítems.

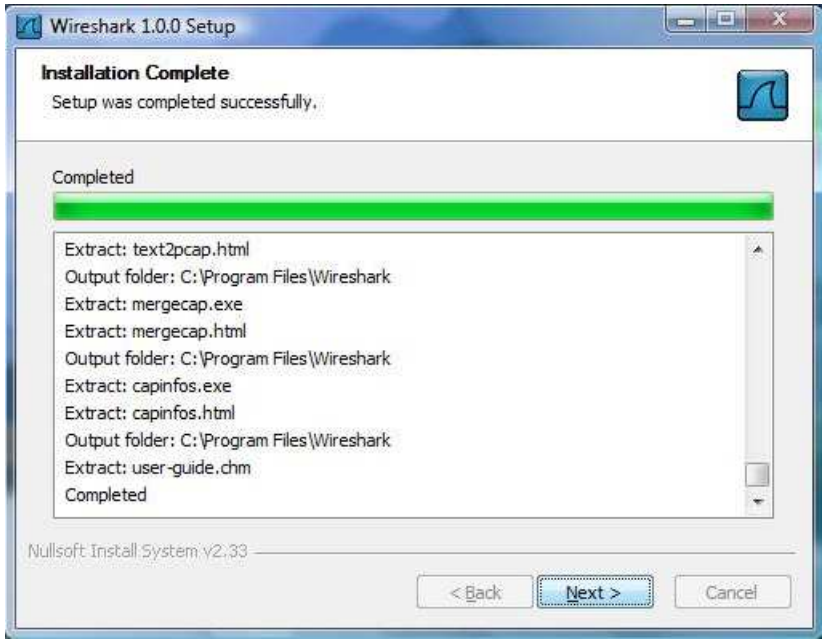
Se presiona el botón  para iniciar el proceso de instalación.



5. Como se mencionó anteriormente el instalador de WireShark para Windows permite hacer la instalación de las librerías, plugins, servicios, etc. Particularmente para el caso de WinPcap se interrumpe la instalación en el punto que muestra la pantalla arriba e inicia el asistente para la

instalación de WinPcap. Se debe seleccionar Next > hasta finalizar la instalación.





La siguiente pantalla indica que la instalación ha finalizado exitosamente.

Para la actualización de WireShark se debe realizar el proceso descrito anteriormente. Se descarga la nueva versión y se ejecuta el instalador, una buena manera de estar actualizados en el mundo de Wireshark es a través de las lista de correo ofrecidas.

Interfaz de Usuario

A continuación se muestra y detalla la interfaz de usuario y como se aplican las principales funciones de WireShark (Capturar, Desplegar y Filtrar paquetes).

Existen dos maneras de iniciar la aplicación una es desde la línea de comando (*shell*) y otra desde el entorno gráfico. Cuando se inicia desde la línea de comando se tiene la posibilidad de especificar opciones adicionales que depende de las funciones que se quieran aprovechar.

La interfaz principal de WireShark cuenta con varias secciones:

- El Menú principal es utilizado para iniciar las acciones y/o funciones de la aplicación.

File, similar a otras aplicaciones GUI este contiene los ítems para manipular archivos y para cerrar la aplicación Wireshark.

Edit, este menú contiene ítems para aplicar funciones a los paquetes, por ejemplo, buscar un paquetes especifico, aplicar una marca al paquete y configurar la interfaz de usuario.

View, permite configurar el despliegue de la data capturada.

Go, contiene ítems que permiten el desplazamiento entre los paquetes.

Capture, para iniciar y detener la captura de paquetes.

Analyze, contiene ítems que permite manipular los filtros, habilitar o deshabilitar protocolos, flujos de paquetes, etc.

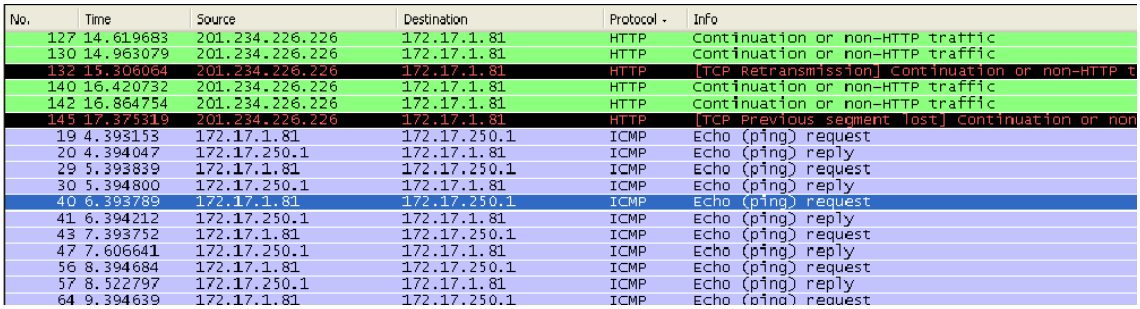
Statistics, contiene ítems que permiten definir u obtener las estadísticas de la data capturada.

Help, menú de ayuda.

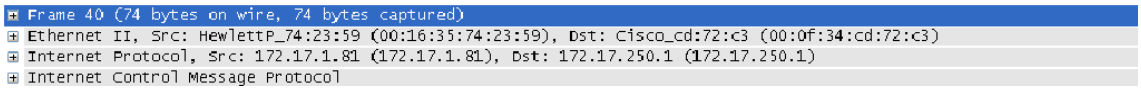
- Barra de herramientas principal, permite el acceso rápido a las funciones más utilizadas.

- Barra de herramientas para filtros, aquí se especifica el filtro que se desea aplicar a los paquetes que están siendo capturados.

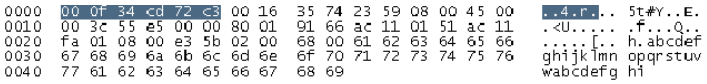
- Panel de paquetes capturados, en este panel se despliega la lista de paquetes capturados. Al hacer clic sobre algunos de estos se despliega cierta información en los otros paneles.



- Panel para detalles del paquete, aquí se despliega información detallada del paquete seleccionado en el panel de paquetes.



- Panel de paquetes capturados en bytes, despliega en bytes la información contenida en el campo seleccionado desde el panel de detalles del paquete seleccionado en el panel de paquetes.



- La barra de estado, muestra información acerca del estado actual del programa y de la data capturada.

La interfaz de usuario puede ser cambiada desde el menú principal en la opción de *Preferences* en el menú *Edit*, según sea las necesidades.

Panel de paquetes capturados

Cada línea corresponde a un paquete capturado al seleccionar una de estas, ciertos detalles son desplegados en el resto de los paneles (Detalles y bytes). Y las columnas muestran datos del paquete capturado, Wireshark dispone de una

gran cantidad de detalles que pueden agregarse en estas columnas desde el menú *Edit->Preferences*, por defecto se tienen:

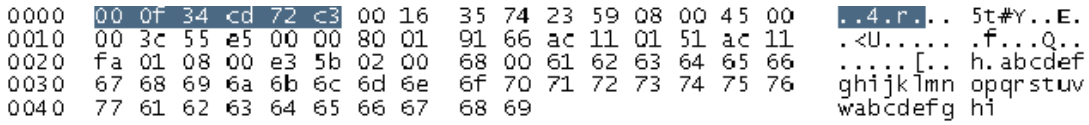
- No.: posición del paquete en la captura.
- *Time*: muestra el *Timestamp* del paquete. Su formato puede se modificado desde el menú *View->Time Display Format*.
- *Source*: dirección origen del paquete.
- *Destination*: dirección destino del paquete.
- *Protocol*: nombre del protocolo del paquete.
- Info: información adicional del contenido del paquete.

Panel para detalles de paquetes capturados

Contiene el protocolo y los campos correspondientes del paquete previamente seleccionado en el panel de paquetes capturados. Seleccionando una de estas líneas con el botón secundario del Mouse se tiene opciones para ser aplicadas según las necesidades.

Panel de paquetes capturados en Bytes

En este panel se despliega el contenido del paquete en formato hexadecimal.



De izquierda a derecha se muestra el *offset* del paquete seguidamente se muestra la data del paquete y finalmente se muestra la información en caracteres ASCII si aplica o "." (Sin comillas) en caso contrario.

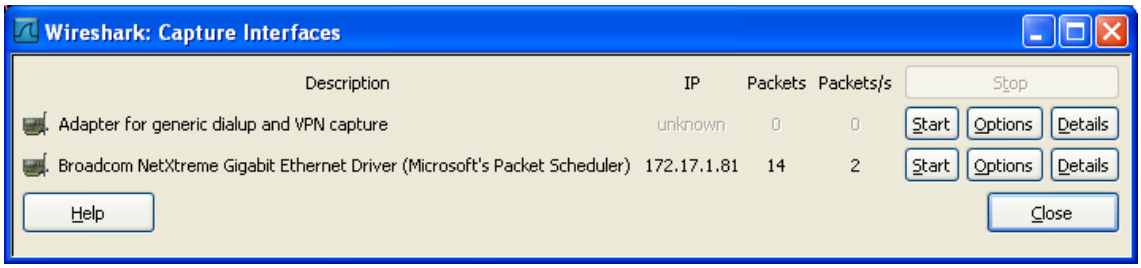
Captura de Paquetes

Una de las principales funciones de WireShark es capturar paquetes con la finalidad de que los administradores y/o ingenieros de redes puedan hacer uso de

estos realizar el análisis necesario para tener una red segura y estable. Como requisito para el proceso de capturar datos es ser administrador y/o contar con estos privilegios y es necesario identificar exactamente la interfaz que se quiere analizar.

WireShark cuenta con cuatro maneras para iniciar la captura de los paquetes:

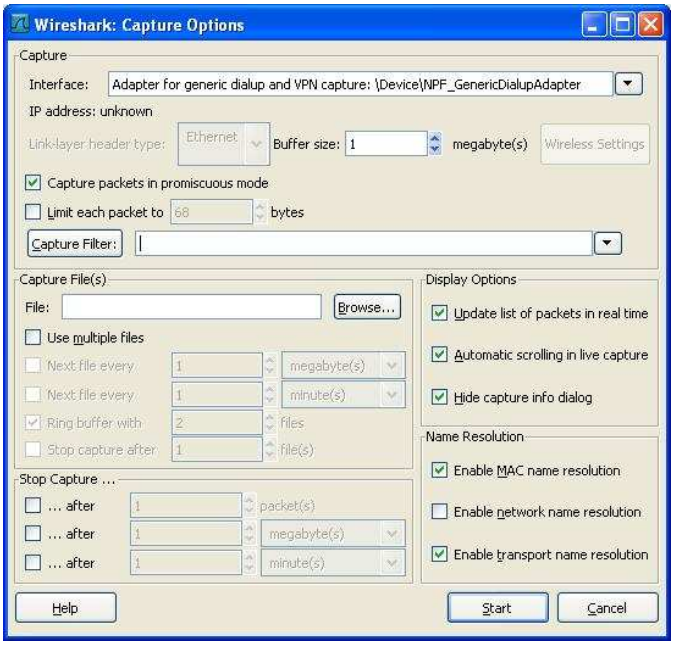
1. Haciendo doble clic en  se despliega una ventana donde se listan las interfaces locales disponibles para iniciar la captura de paquetes.



Tres botones se visualizan por cada interfaz

- Start, para iniciar
- Options, para configurar
- Details, proporciona información adicional de la interfaz como su descripción, estadísticas, etc.

2. Otra opción es seleccionar con el Mouse el icono  en la barra de herramientas, se despliega la siguiente ventana donde se muestra opciones de configuración para la interfaz.



3. Si es el caso donde se ha predefinido las opciones de la interfaz, haciendo clic en  se inicia la captura de paquetes inmediatamente.

4. Otra manera de iniciar la captura de paquetes es desde la línea de comandos ejecutando lo siguiente:

```
wireshark –i eth0 -k
```

Donde eth0 corresponde a la interfaz por la cual se desea iniciar la captura de paquetes.