Universidad Austral de Chile
Facultad de Ciencias de la Ingeniería
Escuela de Electricidad y Electrónica

VOZ SOBRE IP
"Creación de una central telefónica a través del modulo Asterisk-UBUNTU"

Trabajo de Titulación para optar al
Título de Ingeniero en Electrónica

PROFESOR PATROCINANTE:
Sr. Néstor Fierro Morineaud

JOEL URTUBIA UGARTE
VALDIVIA – CHILE
2007

Agradecimientos

Mis agradecimientos es para todos lo que me ayudaron a realizarme como ingeniero, a mi madre, Guillermo y a mi padre que me apoyaron es todo momento de mi carrera, a mi novia Ingrid que me acompaño en gran parte de mi carrera y fue un gran pilar en esta etapa; a mi hermano Jonatan por todo el esfuerzo que representa un hombre con sueños, a los profesores de la universidad, a mis amigos de universidad que son muchos , a los funcionarios que atienden el gimnasio, Sr. Abraham Vera y Sr. Domingo y a mis amigos y compañeros de trabajo de la casona verde con los cuales tengo un lazo afectivo fuerte.

Nadie sabe lo que cuestan las cosas hasta que se cobra una deuda

Resumen

La presente tesis esta enfocada principalmente a descubrir el cambio que se realizara en las telecomunicaciones en el futuro, con una visión practica de cómo es la transmisión de telefonía que esta emergiendo y desplazara a la telefonía actual, en la parte practica consiste en la instalación de una central de telefonía y analizar como se transmite la información de voz a través de paquetes IP.

Este proyecto esta enfocado a Ingenieros electrónicos e ingenieros informáticos, que quieran aprender a desarrollar esta tecnología e implementarla en forma practica en cualquier parte que se desee, este proyecto tiene una enorme importancia en conectividad ya que se une a través de Internet redes de telefonía, por lo que podemos llegar a cualquier parte que se desee y este bien implementada una red ya sea alambica e inalámbrica.

Summary

They summarize the present thesis this focused mainly to discover the change that was made in the telecommunications in the future, with a vision practices of how it is the telephony transmission that this emerging and moved to the present telephony, in the part it practices consists of the installation of a telephony power station and to analyze as the information of voice through packages IP is transmitted.

This project this focused computer science Electronics engineers and engineer, whom they love to learn to develop this technology and to implement it in form practices anywhere that it is desired, this project has an enormous importance in connectivity since it is united through Internet telephony networks, reason why we can arrive at any part that are desired and this implemented good a network or distills and wireless.

ÍNDICE

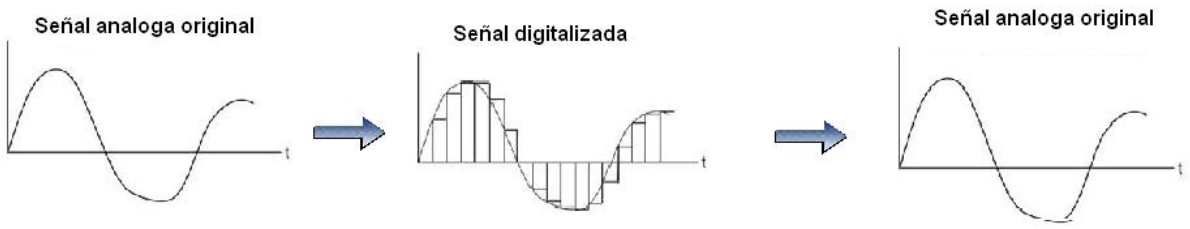
Capitulo I Marco Teórico

1.1 Necesidad de la telefonía IP

La utilización de una red ya existente da pie a la maximización de los recursos de esta red, la red IP, por esto nace la implementación de esta telefonía y con esto se abaratan costos y se otorgan mayores prestaciones a la telefonía convencional

1.2 Concepto de la voz sobre IP

La voz sobre IP se trasmite digitalizando la señal analógica, que en este caso es la voz, y transmitiéndola sobre Internet como paquetes IP, cuando este paquete llega a su destino, receptor, es decodificada de nuevo a señal análoga.



(Figura 1-0)

Este es el principio básico de la transmisión de voz sobre Internet, en el intermedio de la conversación entre dos personas en voz IP se aprecia distintos actores que participan tácitamente de esta conversación, como son los protocolos, codecs, tipos de servidores, softphone y ATA, los cuales explicare mas adelante cuales son las funciones y sus principales características para ser utilizados

Factores que proporcionan la transmisión de la telefonía IP

Este tipo de transmisión de voz necesita de codecs, los codecs son capaces de transformar flujos de datos, en este caso la voz, para ser codificada y enviada a través de una red IP, la elección del tipo de codec es importante para saber el ancho de banda que utilizara y con esto evaluar el retardo en la conversación que puede haber.
Para transmitir estos datos codificados debemos contar con protocolos de transmisión, que son en realidad un conjunto de reglas que se utilizan para que la información viaje ordenada y la parte transmisora y receptora puedan establecer una comunicación

La telefonía IP ocupa protocolos de comunicación, los cuales se dividen en 2 tipos:

- El primer tipo es para el inicio de sesión de la llamada (SIP), este protocolo es para establecer todos lo parámetros con que se trabajara entre el emisor y el receptor, como son ,el codec se trabajara en la transmisión, el ancho del paquete a trasmitir, si se aplicara Nateo, y otras opciones que se explicaran a continuación.

- Protocolo de tiempo real (RTP) es el protocolo que lleva la información de la conversación establecida.

1.3 Protocolos de Voz sobre IP

Hoy en día, los protocolos mas conocidos para transmitir voz sobre IP ,son H.323 y SIP, ambos definen la manera en que los dispositivos de este tipo deben establecer comunicación entre sí.

1.3.1 H.323

H.323 es el estándar creado por la Unión Internacional de Telecomunicaciones (ITU) que se compone por un protocolo sumamente complejo y extenso, el cual además de incluir la voz sobre IP, ofrece especificaciones para vídeo-conferencias y aplicaciones en tiempo real, entre otras variantes.

1.3.2 Session Initiation Protocol (SIP)

Session Initiation Protocol (SIP) fue desarrollado por la IETF (Internet Engineering Task Force) específicamente para telefonía IP, que a su vez toma ventaja de otros protocolos existentes para manejar parte del proceso de conversión, situación que no se aplica en H.323 ya que define sus propios protocolos bases.

1.4 SIP

Se enfocara este proyecto de tesis al protocolo SIP porque es el que se utiliza masivamente y desplazo al protocolo H.323

“Session Initiation Protocol” o SIP (Protocolo de Iniciación de Sesión), es un protocolo de señalización .Este protocolo hereda de ciertas funcionalidades de los protocolos “Hyper Text Transport Protocol” o “http”, utilizados para navegar sobre el WEB y “Simple Mail Transport Protocol” o “SMTP”, utilizados para transmitir mensajes electrónicos (e-mails). SIP se apoya sobre un modelo transaccional cliente / servidor como http. El direccionamiento utiliza el concepto “Uniform Resource Locator” o “URL SIP” parecido a una dirección E-mail. Cada participante en una red SIP es entonces alcanzable vía una dirección, por medio de una URL SIP. Por otra parte, los requerimientos SIP son satisfechos por respuestas identificadas por un código digital. De hecho, la mayor parte de los códigos de respuesta SIP han sido tomados del protocolo http. Por ejemplo, cuando el destinatario no esta ubicado, un código de respuesta «404 Not Found» esta devuelto. Un requerimiento SIP esta constituido de “headers” o encabezamientos, al igual que un mando SMTP. Por fin, SIP, al igual de SMPT es un protocolo textual.

1.4.1 Entidades SIP

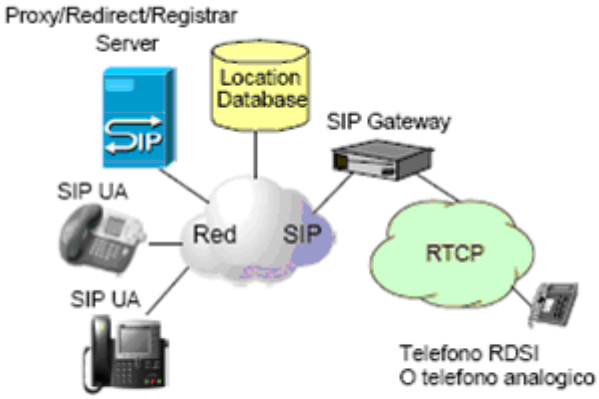
SIP define dos tipos de entidades: los clientes y los servidores. De manera más precisa, las entidades definidas por SIP son (figura 1-1):

1.4.1.1 El Servidor Proxy (Proxy Server): el recibe solicitudes de clientes que el mismo trata o encamina hacia otros servidores después de haber eventualmente, realizado ciertas modificaciones sobre estas solicitudes.

1.4.1.2 El Servidor de Redireccionamiento (Redirect Server) : se trata de un servidor quien acepta solicitudes SIP, traduce la dirección SIP de destino en una o varias direcciones de red y las devuelve al cliente. De manera contraria al Proxy Server, el Redirect Server no encamina las solicitudes SIP. En el caso de la devolución de una llamada, el Proxy Server tiene la capacidad de traducir el numero del destinatario en el mensaje SIP recibido, en un numero de reenvió de llamada y encaminar la llamada a este nuevo destino, y eso de manera transparente para el cliente de origen; para el mismo servicio, el Redirect Server devuelve el nuevo numero (numero de reenvió) al cliente de origen quien se encarga de establecer una llamada hacia este nuevo destino.

1.4.1.3 El Agente Usuario (User Agent) o "UA" : se trata de una aplicación sobre un equipo de usuario que emite y recibe solicitudes SIP. Se materializa por un software instalado sobre un « User Equipment » o UE : una PC, un teléfono IP o una estación móvil UMTS.

1.4.1.4 El Registrador (Registrar) : se trata de un servidor quien acepta las solicitudes SIP .REGISTER. SIP dispone de la función de registro de los usuarios. El usuario indica por un mensaje REGISTER emitido al Registrar, la dirección donde es localizable (dirección IP). El "Registrar" actualiza entonces una base de dato de localización. El registrador es una función asociada a un Proxy Server o a un Redirect Server. Un mismo usuario puede registrarse sobre distintas UAs SIP, en este caso, la llamada le será entregada sobre el conjunto de estas UAs.


Proxy/Redirect/Registrar
Server
Location
Database
SIP
SIP Gateway
SIP UA
Red
SIP
RTCP
SIP UA
Telefono RDSI
O telefono analogico

(Figura 1-1)

1.4.2 Métodos SIP

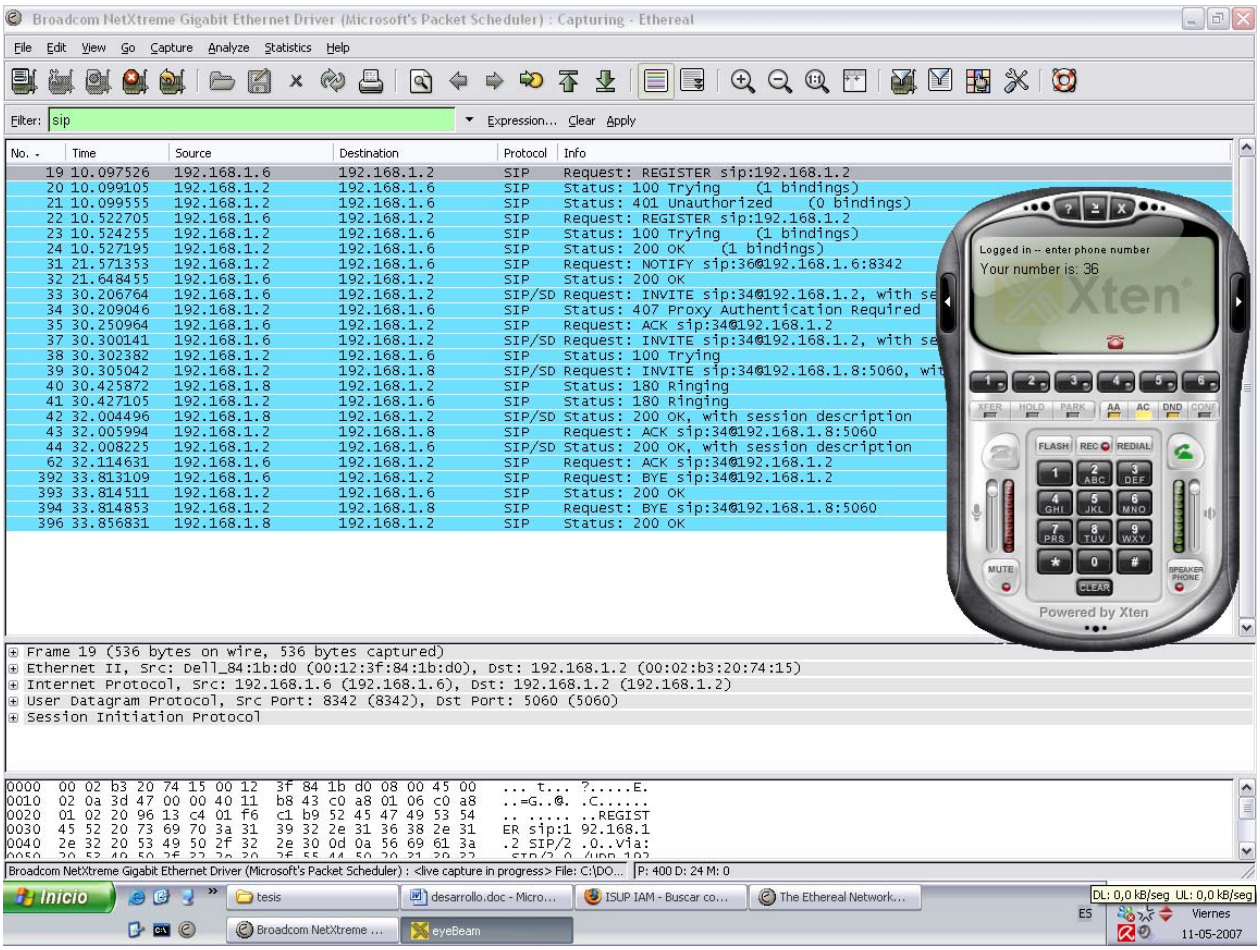
Los métodos SIP son requerimientos con los cuales se puede establecer o liberar una llamada, estas definen 6 posibles requerimientos las cuales se plantean a continuación:

El método “REGISTER” es usado por una UA , usuario, con el fin de indicar al Registrar la Correspondencia entre su Dirección SIP y su dirección de contacto (ejemplo: dirección IP).

El método “CANCEL” es utilizado para pedir el abandono de la llamada en curso pero no tiene ningún efecto sobre una llamada ya aceptada. De hecho, solo el método “BYE” puede terminar una llamada establecida.

El método “OPTIONS” es utilizado para interrogar las capacidades y el estado de un User Agent o de un servidor. La respuesta contiene sus capacidades (ejemplo: tipo de media siendo soportado, idioma soportado) o el hecho de que el UA sea indisponible.

Podemos apreciar un ejemplo en la siguiente figura de los métodos SIP analizando con el sniffer ethereal y registrándose el teléfono 36 con la central de dirección IP 192.168.1.2


Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler) : Capturing - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: sip
Expression... Clear Apply
No. Time Source Destination Protocol Info
19 10.097526 192.168.1.6 192.168.1.2 SIP Request: REGISTER sip:192.168.1.2
20 10.099105 192.168.1.2 192.168.1.6 SIP Status: 100 Trying (1 bindings)
21 10.099555 192.168.1.2 192.168.1.6 SIP Status: 401 Unauthorized (0 bindings)
22 10.522705 192.168.1.6 192.168.1.2 SIP Request: REGISTER sip:192.168.1.2
23 10.524255 192.168.1.2 192.168.1.6 SIP Status: 100 Trying (1 bindings)
24 10.527195 192.168.1.2 192.168.1.6 SIP Status: 200 OK (1 bindings)
31 21.571353 192.168.1.2 192.168.1.6 SIP Request: NOTIFY sip:36@192.168.1.6:8342
32 21.648455 192.168.1.6 192.168.1.2 SIP Status: 200 OK
33 30.206764 192.168.1.6 192.168.1.2 SIP/SD Request: INVITE sip:34@192.168.1.2, with se
34 30.209046 192.168.1.2 192.168.1.6 SIP Status: 407 Proxy Authentication Required
35 30.250964 192.168.1.6 192.168.1.2 SIP Request: ACK sip:34@192.168.1.2
37 30.300141 192.168.1.6 192.168.1.2 SIP/SD Request: INVITE sip:34@192.168.1.2, with se
38 30.302382 192.168.1.2 192.168.1.6 SIP Status: 100 Trying
39 30.305042 192.168.1.2 192.168.1.8 SIP/SD Request: INVITE sip:34@192.168.1.8:5060, wit
40 30.425872 192.168.1.8 192.168.1.2 SIP Status: 180 Ringing
41 30.427105 192.168.1.2 192.168.1.6 SIP Status: 180 Ringing
42 32.004496 192.168.1.8 192.168.1.2 SIP/SD Status: 200 OK, with session description
43 32.005994 192.168.1.2 192.168.1.8 SIP Request: ACK sip:34@192.168.1.8:5060
44 32.008225 192.168.1.2 192.168.1.6 SIP/SD Status: 200 OK, with session description
62 32.114631 192.168.1.6 192.168.1.2 SIP Request: ACK sip:34@192.168.1.2
392 33.813109 192.168.1.6 192.168.1.2 SIP Request: BYE sip:34@192.168.1.2
393 33.814511 192.168.1.2 192.168.1.6 SIP Status: 200 OK
394 33.814853 192.168.1.2 192.168.1.8 SIP Request: BYE sip:34@192.168.1.8:5060
396 33.856831 192.168.1.8 192.168.1.2 SIP Status: 200 OK
Logged in -- enter phone number
Your number is: 36
Xten
Powered by Xten
Frame 19 (536 bytes on wire, 536 bytes captured)
Ethernet II, Src: Dell_84:1b:d0 (00:12:3f:84:1b:d0), Dst: 192.168.1.2 (00:02:b3:20:74:15)
Internet Protocol, Src: 192.168.1.6 (192.168.1.6), Dst: 192.168.1.2 (192.168.1.2)
User Datagram Protocol, Src Port: 8342 (8342), Dst Port: 5060 (5060)
Session Initiation Protocol
0000 00 02 b3 20 74 15 00 12 3f 84 1b d0 08 00 45 00 ... t... ?.....E.
0010 02 0a 3d 47 00 00 40 11 b8 43 c0 a8 01 06 c0 a8 ..=G..@. .C......
0020 01 02 20 96 13 c4 01 f6 c1 b9 52 45 47 49 53 54 .. ..REGIST
0030 45 52 20 73 69 70 3a 31 39 32 2e 31 36 38 2e 31 ER sip:1 92.168.1
0040 2e 32 20 53 49 50 2f 32 2e 30 0d 0a 56 69 61 3a .2 SIP/2 .0..Via:
Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler) : <live capture in progress> File: C:\DO...
P: 400 D: 24 M: 0
Inicio
tesis
desarrollo.doc - Micro...
ISUP IAM - Buscar co...
The Ethereal Network...
Broadcom NetXtreme ...
eyeBeam
DL: 0,0 kB/seg UL: 0,0 kB/seg
ES
Viernes
11-05-2007

(Figura 1-2)

1.4.3 Respuestas SIP

Después de haber recibido y interpretado un requerimiento SIP, el destinatario de este requerimiento devuelve una respuesta SIP. Existen seis clases de respuestas:

Clase 1xx : Información, el requerimiento ha sido recibido y esta en curso de tratamiento

Clase 2xx: Éxito, el requerimiento ha sido recibido, entendido y aceptado.

Clase 3xx: Reenrutamiento, la llamada requiere otros procesamientos antes de poder determinar si puede ser realizada.

Clase 4xx: Error requerimiento cliente, el requerimiento no puede ser interpretado o servido por el servidor. El requerimiento tiene que ser modificado antes de ser reenviado.

Clase 5xx: Error servidor, el servidor fracasa en el procesamiento de un requerimiento aparentemente valido.

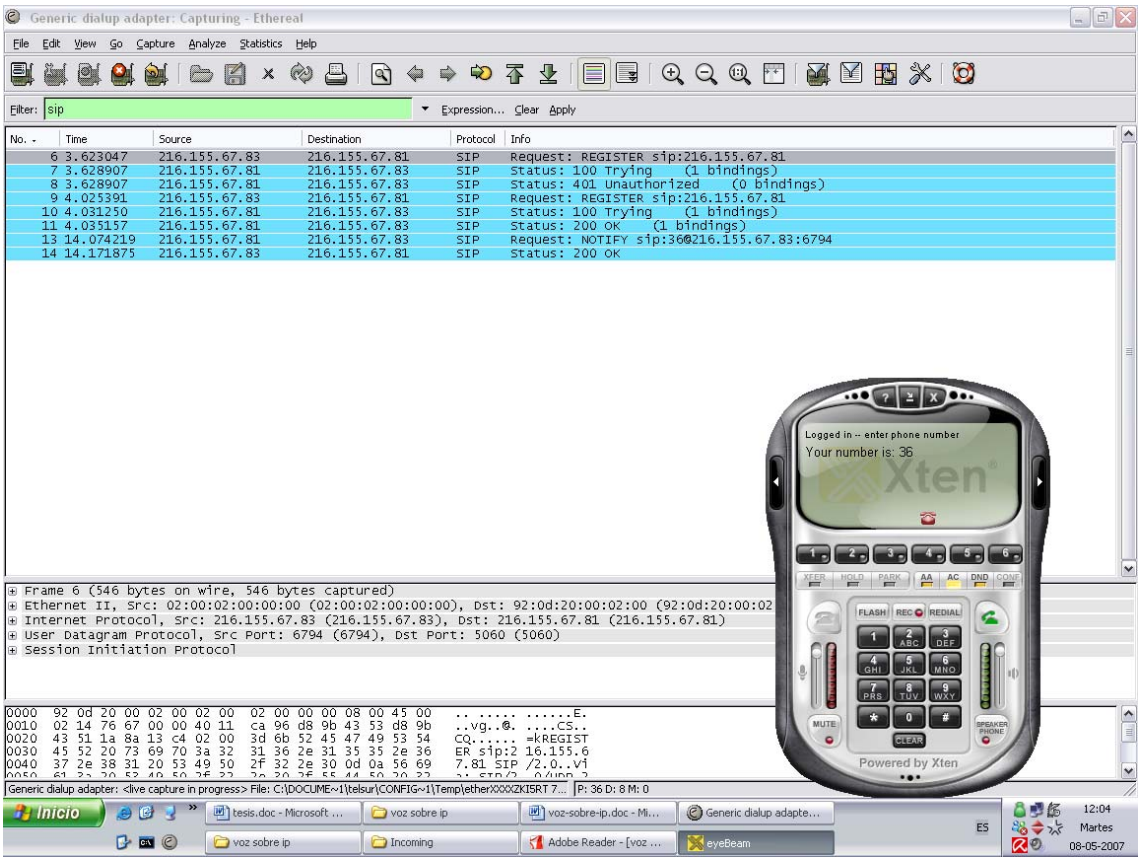
Clase 6xx: Fracaso global, el requerimiento no puede ser procesado por ningún servidor.

1.4.4 Inscripción a la red SIP

El proceso de registro contra un servidor es relativamente simple el usario envia un requerimiento para registrarse, primero le envia los datos de la ubicación del servidor al que se quiere conectar, en este paquete de información viaja un Hash MD5 que es una encriptación de datos, para que la información no se pueda descifrar fácilmente, después que el servidor verifica correspondencia entre sus datos y los del usuario envia una segunda petición (401 Unauthorized), para que envie su contraseña y su nombre de usuario, el usuario lo envia nuevamente, y el servidor responde con 200 Ack que significa que ya esta logeado contra el servidor.

(Figura 1-3)

Ejemplo de registro con la central asterisk 216.155.67.81

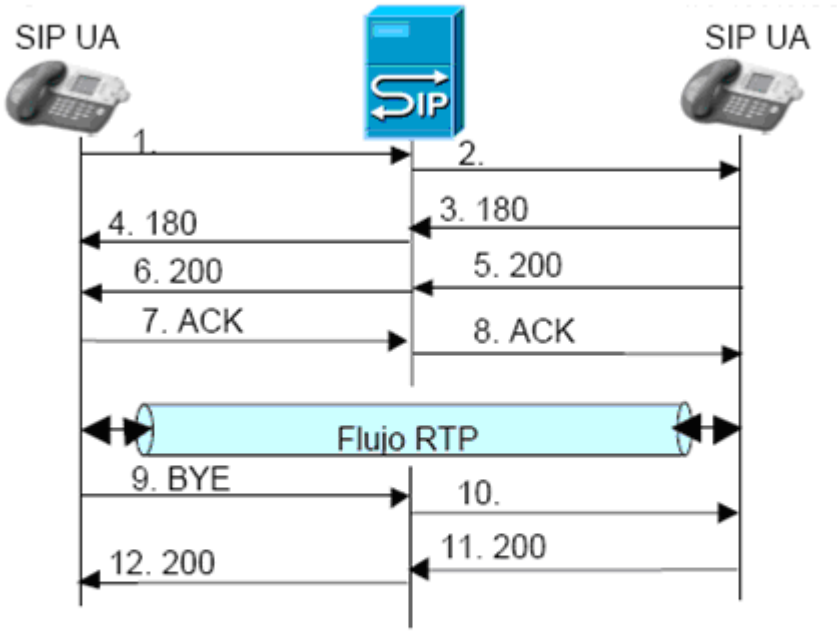


(Figura 1-4)

Ejemplo de establecimiento y liberación de sesión SIP

En el ejemplo siguiente, el que llama tiene como URL SIP sip : 36@192.168.1.6, mientras la URL SIP del destinatario de la llamada es sip: 34@192.168.1.8 (Figura 2)
Un mensaje de establecimiento de llamada SIP INVITE esta emitido por parte de la UA SIP del que llama al Proxy Server. Este ultimo interroga la base de datos de localización para identificar la localización del que esta llamado (dirección IP) y encamina la llamada a su destino que en este caso es la direccion 34@192.168.1.8. El mensaje INVITE contiene distintos “headers” o encabezamientos obligatorios, entre los cuales la dirección SIP de la persona que llama “From”, la dirección SIP de la persona que recibe la llamada “To”, una identificación de la llamada “Call-ID”, un numero de secuencia “Cseq”, un numero máximo de saltos “max-forwards”. El encabezamiento “Via” esta actualizado por todas las entidades que participaron al enrutamiento del requerimiento INVITE. Eso asegura que la respuesta seguirá el mismo camino que el requerimiento.

Por otra parte, el requerimiento SIP INVITE contiene una sintaxis “Session Description Protocol” o SDP. Esta estructura consiste en varias líneas que describen las características del media que el que llama “36” necesita para la llamada, a continuación podemos apreciar el la siguiente figura el encaminamiento de la llamada entre el teléfono SIP 36@192.168.1.6 y el teléfono SIP 36@192.168.1.6



Establecimiento y liberación de sesión SIP

(Figura 1-5)

(Untitled) - Ethereal

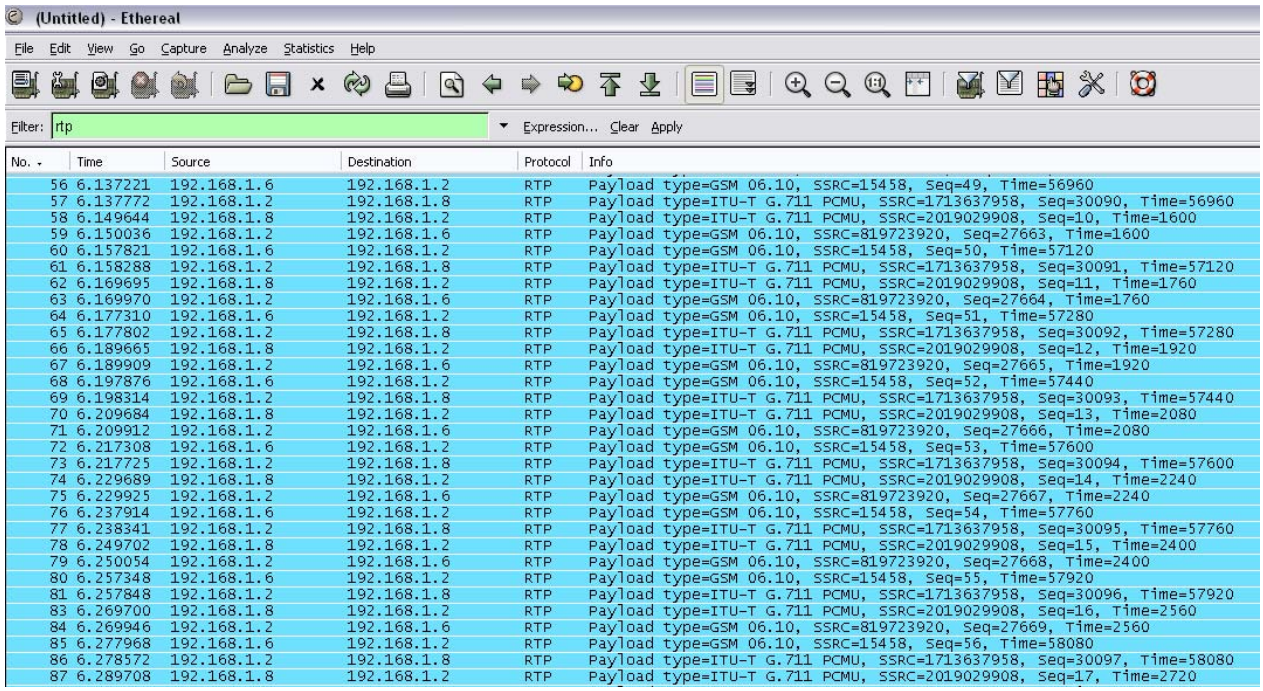
File Edit View Go Capture Analyze Statistics Help

Filter: sip Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.6	192.168.1.2	SIP/SD	Request: INVITE sip:34@192.168.1.2, with session description
2	0.002338	192.168.1.2	192.168.1.6	SIP	Status: 407 Proxy Authentication Required
3	0.008903	192.168.1.6	192.168.1.2	SIP	Request: ACK sip:34@192.168.1.2
4	0.019063	192.168.1.6	192.168.1.2	SIP/SD	Request: INVITE sip:34@192.168.1.2, with session description
5	0.021211	192.168.1.2	192.168.1.6	SIP	Status: 100 Trying
6	0.023616	192.168.1.2	192.168.1.8	SIP/SD	Request: INVITE sip:34@192.168.1.8:5060, with session description
7	0.142727	192.168.1.8	192.168.1.2	SIP	Status: 180 Ringing
8	0.143751	192.168.1.2	192.168.1.6	SIP	Status: 180 Ringing
9	2.639553	192.168.1.2	192.168.1.8	SIP	Request: OPTIONS sip:33@192.168.1.8:5060
10	2.663767	192.168.1.8	192.168.1.2	SIP	Status: 501 Not Implemented
13	5.943513	192.168.1.8	192.168.1.2	SIP/SD	Status: 200 OK, with session description
14	5.945017	192.168.1.2	192.168.1.8	SIP	Request: ACK sip:34@192.168.1.8:5060
15	5.946837	192.168.1.2	192.168.1.6	SIP/SD	Status: 200 OK, with session description
34	6.034677	192.168.1.6	192.168.1.2	SIP	Request: ACK sip:34@192.168.1.2
408	7.890959	192.168.1.8	192.168.1.2	SIP	Request: BYE sip:36@192.168.1.2
410	7.891871	192.168.1.2	192.168.1.8	SIP	Status: 200 OK
411	7.892956	192.168.1.2	192.168.1.6	SIP	Request: BYE sip:36@192.168.1.6:8342
415	7.975107	192.168.1.6	192.168.1.2	SIP	Status: 200 OK
429	62.673411	192.168.1.2	192.168.1.8	SIP	Request: OPTIONS sip:33@192.168.1.8:5060
430	62.701927	192.168.1.8	192.168.1.2	SIP	Status: 501 Not Implemented
444	122.71160	192.168.1.2	192.168.1.8	SIP	Request: OPTIONS sip:33@192.168.1.8:5060
445	122.74019	192.168.1.8	192.168.1.2	SIP	Status: 501 Not Implemented
471	182.74978	192.168.1.2	192.168.1.8	SIP	Request: OPTIONS sip:33@192.168.1.8:5060
472	182.77403	192.168.1.8	192.168.1.2	SIP	Status: 501 Not Implemented
500	242.78400	192.168.1.2	192.168.1.8	SIP	Request: OPTIONS sip:33@192.168.1.8:5060
501	242.81936	192.168.1.8	192.168.1.2	SIP	Status: 501 Not Implemented

(Figura 1-6)

En la figura que se mostrara a continuación podemos observar que cada conversación que se establece pasa necesariamente por el servidor asterisk que tiene IP 192.168.1.2 y después va hacia el teléfono de destino, indicando en el transpaso de informacion la versión 0 del protocolo, que se trata de una sesión telefónica (m = audio), que la voz constituida en paquetes le debe ser entregada a la dirección de transporte (puerto UDP = 12270, dirección IP =192.168.1.8) con el protocolo RTP y utilizando el codec G. 711.



(Figura 1-7)

1.4.5 Interfuncionamiento entre SIP y RTC

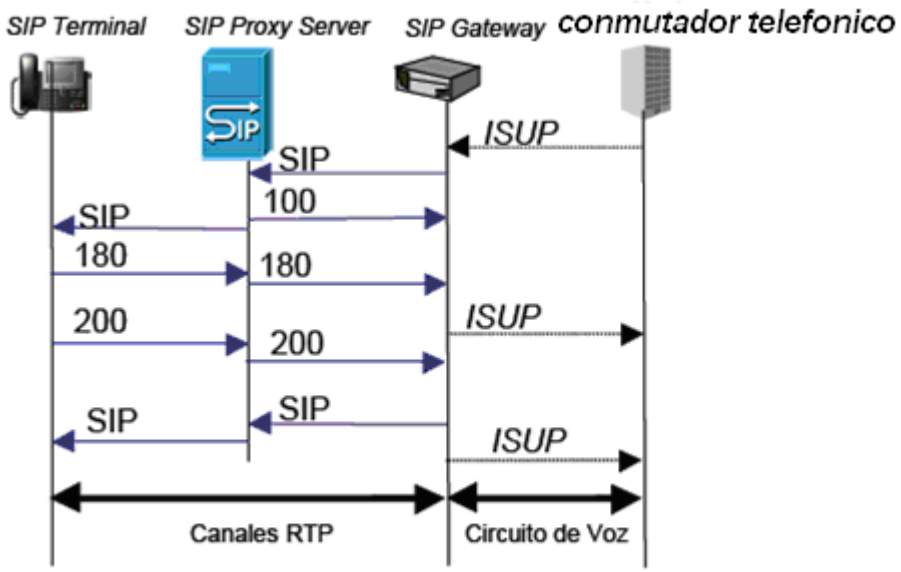
Para el interfuncionamiento entre la Red Telefónica Conmutada RTC y SIP, es necesario introducir una pasarela o Gateway RTC/SIP (tarjeta E1 PRI) que se interfase por una parte al RTC y por otra parte a una red SIP. Este Gateway cumple con dos funciones:

Traducción de la señalización ISDN User Part o ISUP en señalización SIP y recíprocamente, conversión de señales audio en paquetes RTP y recíprocamente; en efecto, este Gateway establece canales lógicos RTP con la terminal SIP y establece circuitos de palabras con un conmutador telefonico.

En el ejemplo contemplado en la figura 3, un terminal conectado a la RTC llama un UA SIP. El conmutador telefonico al cual esta conectado el que genera la llamada, emite un mensaje ISUP IAM al Gateway RTC/SIP. Este mensaje contiene el numero del destinatario, el identificador del circuito elegido por el conmutador telefonico para la llamada (Circuit Identification Code o CIC) así como informaciones indicando la naturaleza de la llamada (palabras, fax, datos, etc...). El Gateway RTC/SIP traduce este mensaje en un requerimiento SIP INVITE que contiene una dirección de destino SIP de la cual el campo “user” es un numero telefónico. Pasa el mensaje al SIP Proxy Server que obtiene la dirección IP del destinatario con la dirección SIP por medio de la interrogación de una base de datos o de un servidor de localización. El mensaje INVITE esta relevado a la UA SIP. En paralelo, el Proxy Server notifica al Gateway la recepción del requerimiento INVITE por medio de la respuesta 100 Trying. El terminal SIP devuelve al Proxy Server una respuesta 180 Ringing para informar el que llama de la alerta del que esta llamado, mensaje relevado por el Proxy Server al Gateway. El Gateway traduce esta respuesta en un mensaje ISUP “Address Complete Message” o ISUP ACM enviado al conmutador telefónico. Este mensaje esta traducido por el conmutador telefónico en un mensaje “Alerting” si el terminal que origina la llamada es una terminal RDSI o en una señal “Ringing Tone” en el caso de una Terminal analógica.

Cuando el destinatario descuelga, una respuesta 200 OK esta devuelta al Proxy Server quien la releva al Gateway. El Gateway pone el recibí de esta respuesta por un requerimiento ACK encaminado por el Proxy Server al destinatario. En paralelo, el Gateway genera un mensaje ISUP Answer Message o ISUP ANM emitido al conmutador telefonico.

Este intercambio de señalización a permitido el establecimiento de canales RTP entre el terminal SIP y el Gateway así como la colocación de un circuito de voz entre el Gateway y el conmutador telefónico.



Interfuncionamiento RTC/SIP

(Figura 1-8)

Servidor Media SIP

El servidor media corresponde a las prestaciones que podemos obtener con la telefonía IP, como son por ejemplo, la lectura de correo electronico, llamadas entre mas de 2 personas, menú IVR, operadora digital, llamada con cámara digital, entre muchas otras que se explican a continuación.

Funcionalidades del servidor de media

Las funcionalidades del servidor de media SIP incluyen las funciones de control del media y de recursos media:

Anuncios: la mayor parte de los servicios evolucionados utiliza formas de anuncios, bien sea un mensaje de bienvenida durante el acceso a su buzón de mensajes unificado o de un mensaje de introducción a un portal local.

Automated Speech Recognition (ASR): el reconocimiento de la palabra es un componente de la mayor parte de los servicios al usuario tales como mensajeria vocal (voicemail), la mensajeria unificada, juegos interactivos y portales vocales.

Generación de información de tasación: una tasación precisa y justa es una exigencia por los operadores de servicio con el fin de ofrecer servicios de voz y datos con fuerte valor agregado. El servidor de media SIP genera informaciones de tasación.

Interactive Voice Response (IVR) : el servidor de media SIP debe soportar la detección de tonalidades DTMF enviadas en la banda así como los dígitos recibidos vía SIP INFO
.

Grabación : el servidor de media SIP tiene capacidades de grabación y de restitución (playback). Numerosas aplicaciones tales como la mensajeria vocal, la mensajeria unificada, el pushto- talk y la conferencia utilizan esta función de grabación de la llamada para que sea restituida posteriormente. El servidor de media SIP utiliza servidores de almacenamiento que existen donde el operador de servicios.

Text-To-Speech : la tecnología “text-to-speech” es estrechamente asociada a la funcionalidad IVR. El “text-to-speech” es utilizado en aplicaciones tales como la mensajeria unificada a fin de leer E-mail o fax a través del teléfono. La traducción puede ser realizada en varios idiomas.

Gestión del multipartes : el servidor de media SIP debe ser capaz de proveer todos los mecanismos de control de las llamadas con varios participantes.

Interfaces estándares abiertas : el servidor de media SIP debe poder ser controlado a través del protocolo SIP y debe poder ejecutar escritos Voice XML.

1.5 RTP PROTOCOLO PARA APLICACIONES MULTIMEDIALES

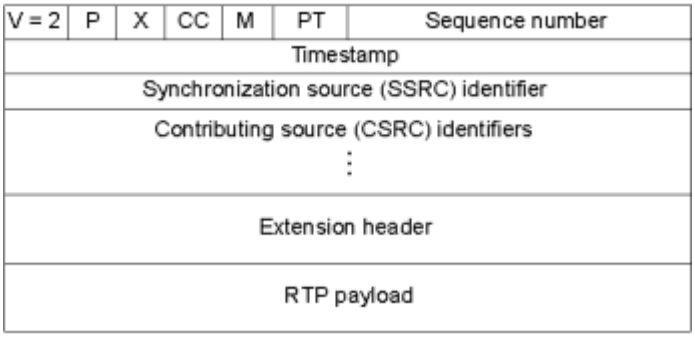
Después que se analizo el protocolo SIP que es el protocolo de inicio de sesión, analizaremos el transporte, el transporte se hace a traves de datagramas UDP, este tipo de protocolos no da confiabilidad en la llegada de paquetes de extremo a extremo, ni tampoco confiabilidad en el envío de paquetes, ya que no hay un orden de llegada de estos, para esto se plantea el protocolo RTP real time protocolo, que se transporta sobre UDP, este protocolo transporta en orden paquetes enviados en tiempo real y se ocupa tanto para voz IP y Streaming de video.

ASPECTOS TECNICOS DE RTP

RTP soporta una amplia variedad de aplicaciones multimedia y está diseñado para adicionarle más aplicaciones sin cambiar el protocolo. Para cada clase de aplicación (por ejemplo, audio), RTP define un perfil (profile) y uno o más formatos (formats). El profile proporciona información para asegurar el entendimiento de los campos del header de RTP para dicho tipo de aplicación. El formato especifica cómo los datos que siguen al header deben ser interpretados.

Formato del header

La siguiente figura muestra el header utilizado por el protocolo RTP.



(Figura 1-9)

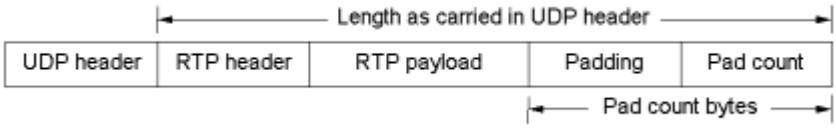
Los primeros 12 octetos (es decir, los campos V, P, X, CC, M, PT, sequence number, timestamp y SSRC) siempre están presentes, en tanto que los identificadores de "fuentes contribuyentes" (nodos que generan información al mismo tiempo para, supongamos, una videoconferencia) son utilizados sólo en ciertas circunstancias. Después del header "básico" puede tenerse extensiones opcionales para el header (Extensión header).

Finalmente el header es seguido por los datos (payload) que transporta RTP y su formato es definido por la aplicación.

El diseño del header de RTP busca llevar sólo aquellos campos que son necesarios para diversos tipos de aplicaciones.

* V (versión), 2 bits: Los primeros dos bits identifican la versión del protocolo.

* P (padding), 1 bit: El siguiente bit identifica el padding. Informa que los datos de RTP llevan un "relleno" para completar un bloque de cierto tamaño. El último byte en el mensaje UDP dice de qué tamaño es el padding



Con esto se cumple el objetivo de tener un header RTP pequeño. La longitud de los datos se calcula a partir de la información del header del protocolo de la capa inferior (UDP en este caso).

* X (extension), 1 bit: El bit de extensión es utilizado para indicar la presencia de un header de extensión que puede ser definido para una aplicación específica y sigue al header principal. Ese tipo de headers son utilizados en raras ocasiones ya que es posible definir un header dentro de los datos (payload) como parte de la definición del formato de los datos para una aplicación en particular.

* CC (CSRC count), 4 bits: El bit X es seguido por 4 bits (CC) que cuentan el número de "fuentes contribuyentes" incluidas en el header de RTP (en caso de que existan dichas fuentes).

* M (marker), 1 bit: Este bit es utilizado para indicar el frame. Por ejemplo, puede indicar el inicio de una conversación en RTP: el primer frame.

* PT (payload type), 7 bits: Los siguientes 7 bits indican qué tipo de dato multimedial se está transportando (payload type). Un posible uso de este campo es permitir a una aplicación pasar de un esquema de codificación a otro basado en la información sobre la disponibilidad de recursos en la red. El uso exacto del bit "marker" (M) y del "payload type" (PT) dependen del perfil (profile) de la aplicación. El payload type NO se usa como llave de demultiplexamiento para dirigir los datos a una aplicación diferente; ese demultiplexamiento lo realiza el protocolo de la capa inferior: UDP. Dos streams de datos multimediales diferentes utilizan números de puerto diferente.

* Sequence number, 16 bits: El número de secuencia es utilizado para permitir al receptor de un stream RTP detectar paquetes perdidos o que lleguen en desorden. Observe que RTP no indica qué hacer cuando se pierde un paquete (muy diferente a TCP que corrige la perdida -por retransmisión- e interpreta la perdida como un indicador de congestión -que puede llevar a reducir el tamaño de la ventana en TCP-). Por el contrario, RTP deja que la aplicación decida qué es lo mejor que puede hacer cuando el paquete se pierde.

* Timestamp, 32 bits: El campo de timestamp permite al receptor reproducir (playback) las muestras en los intervalos de tiempo apropiados y permite que diferentes media streams se puedan sincronizar. RTP no especifica en que unidades se debe enviar este timestamp -las aplicaciones y sus formatos requieren diferentes granularidades en tiempo-. El timestamp viene a ser un contador de "ticks" donde el tiempo entre "ticks" depende del formato de codificación de la aplicación (la granularidad del reloj es uno de los detalles que se especifica en el profile de RTP o en los datos -payload- de la aplicación).

* SSRC, 32 bits: El identificador de fuente de sincronización (SSRC) es un número de 32 bits que identifica de manera única una sola fuente en un stream RTP. En una conferencia multimedial, cada emisor escoge un SSRC aleatorio. El identificador de fuente es diferente de la dirección IP o del número de puerto, que permite, por ejemplo, que un nodo con múltiples fuentes (un equipo con varias cámaras) distinga cada una de las fuentes. Cuando un sólo nodo genera diferentes media streams (por ejemplo, audio y video al mismo tiempo), no es necesario que utilice el mismo SSRC en cada stream ya que RTCP tiene un mecanismo para hacer sincronización intermedia.

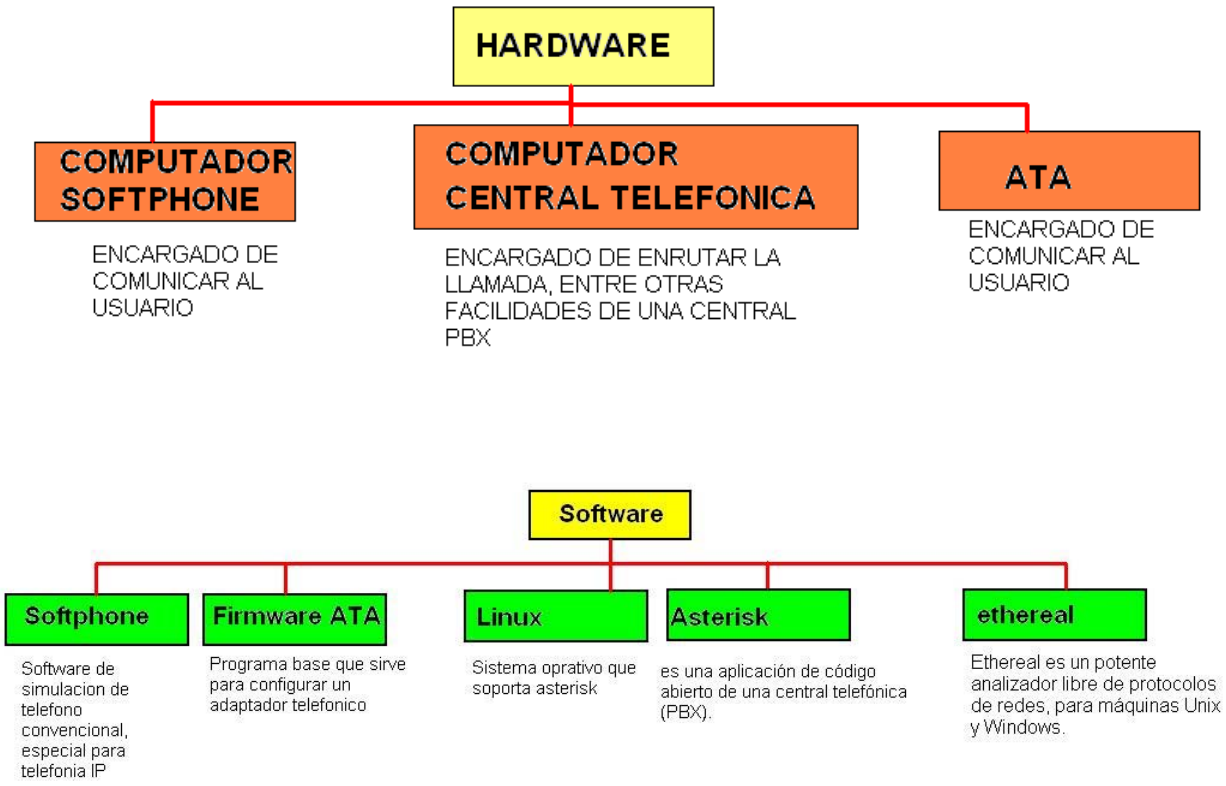
* Lista CSRC, de 0 a 15 elementos, cada uno de 32 bits: El identificador de fuente contribuyente (CSRC) es utilizado sólo cuando varios streams RTP pasan a través de un mezclador (mixer). Un mezclador puede ser utilizado para reducir los requerimientos de ancho de banda para una conferencia recibiendo datos de muchas fuentes y enviando estas como un sólo stream. El número de identificadores incluidos en el header RTP viene colocado en el campo CC (CSRC count). Si hay más de 15 fuentes contribuyentes, sólo 15 pueden ser identificadas.

CAPITULO II: “IMPLEMENTACION”

En este capitulo se explicara cada parte de software a utilizar en el proyecto de tesis

(Figura 2-1)

Para comprensión del marco teórico, será necesario apreciar el siguiente esquema, en donde es posible observar los distintos dispositivos asociados al hardware y software (Fig.2-2):



(Figura 2-2)

2.1 Programas Utilizados.

Debido a que la implementación en forma practica de la telefonía IP, será necesario instalar en el sistema operativo Linux, mas específicamente su versión UBUNTU, después instalaremos el modulo asterisk para que actúe como central telefónica, este modulo es el cerebro de la central de telefonia IP y es indispensable tanto para el control de flujo de llamadas, creación de números telefónicos, menú de inicio ,en el fondo da todas las prestaciones necesarias de una central telefónica.

Para que dos usuarios puedan tener conexión punto a punto, se requiere de teléfonos IP , los cuales pueden ser softphone o ATAS para que puedan establecer llamadas los usuarios, la particularidad de estos elementos es que sirven para autentificarse directamente con la central de telefonía IP, y después de autentificarse establecer llamadas.

Para observar como funciona a través de protocolos y envió de paquetes la telefonía IP se requiere de servicio de un sniffer así se puede capturar la información de la comunicación que se establezca en la practica.

Todo lo anterior permite la implementación de la telefonía IP, a continuación se describen detalladamente los programas utilizados:

2.1.1 Ubuntu

Este es un sistema operativo llamado Linux, la versión es Ubuntu, se instala para ser utilizado como plataforma para albergar al modulo asterisk , para crear nuestra central PBX

(Figura 2-3)

2.1.2 Asterisk

Es un modulo o software el cual permite crear una central de telefonía IP, Asterisk incluye muchas características anteriormente sólo disponibles en caros sistemas propietarios PBX: buzón de voz, conferencias, IVR, distribución automática de llamadas, y otras muchas más. Los usuarios pueden crear nuevas funcionalidades escribiendo un *dialplan* (se refiere a la creación de numeros telefonicos agregando funcionalidades a cada usuario) en el lenguaje de script de Asterisk.

Instalacion de asterisk
Para la correcta instalacion de asterisk se debe instalar las siguientes librerias en linux ubuntu:
Desde el Terminal
Debemos instalar

 Actualizar repositorios
sudo apt-get update

 Instalar librerias para acceso via SSH
sudo apt-get install openssl libssl-dev ssh

 librerías de compilación de software, sirve para compilar Asterisk
sudo apt-get install gcc make g++

 verificar que versiones de kernel tengo instalado en el servidor
uname -a

 me regresa algo como esto
Linux AsteriskServer 2.6.15-23-386

 buscar las fuentes del kernel con las versiones instaladas en el server
apt-cache search 2.6.15

 instalamos los encabezados para 2.6.15 espec?ficos para el procesador (linux-headers-2.6.15-23-386 , linux-source-2.6.15 , linux-image-2.6.15-23-386)
sudo apt-get install linux-headers-2.6.15-23-server linux-image-2.6.15-23-server linux-source-2.6.15

 sinstalamos algunas utilerias de linux, Linux es un navegador web de texto, nmap es sniffer depuertos, emacs es un editor de textos potente aunque puedes usar editor instalado ya en Ubuntu y sencillo de usar
sudo apt-get install nmap lynx emacs21

 festival son paquetes para el manejo de voz
sudo apt-get install festival festival-dev

 para poder usar la consola de asterisk
sudo apt-get install ncurses-base ncurses-bin ncurses-term libncurses5 libncursesw5 libncurses5-dev libncursesw5-dev

 librerias de compresion
sudo apt-get install zlib1g zlib1g-dev

 librerias requeridas por el servicio web de FreePBX
sudo apt-get install bison bison-doc

 cd /usr/src/asterisk-1.2.9.1

 make clean

 make

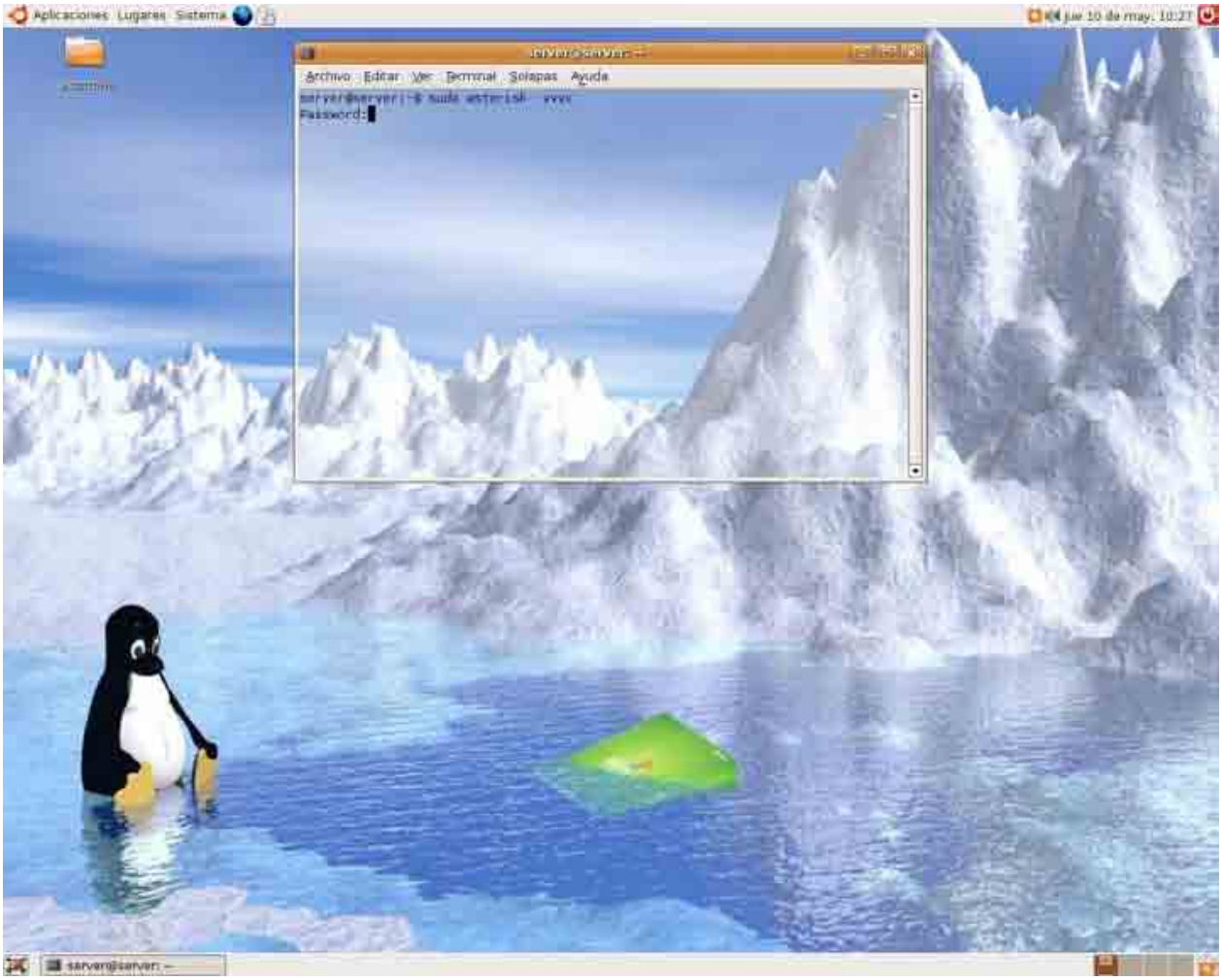
 make install

 make samples

Con esto queda instalado asterisk en UBUNTU, para empezar a utilizar el asterisk, se ingresa en el Terminal

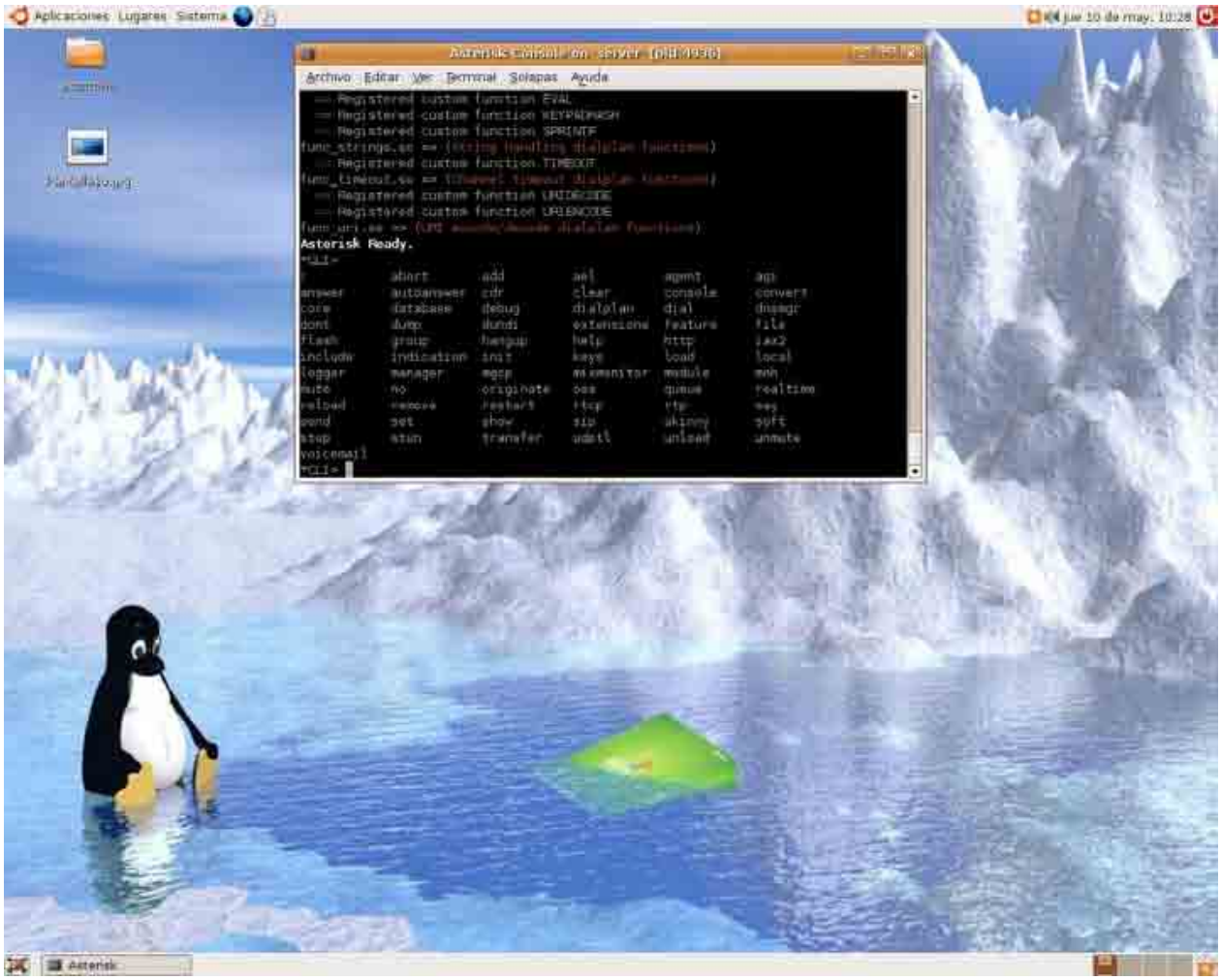
 sudo asterisk –vvvc

Nos pedirá un password de root, después de ingresarlo se presiona enter y ya esta creada la central telefonica lista para la configurarla de acuerdo a las prestaciones que se requiera.



(Figura 2-4)

Este programa se puede configurar directamente desde su base de datos o desde el Terminal, mas adelante entregare un ejemplo de cómo configurar una central PBX.

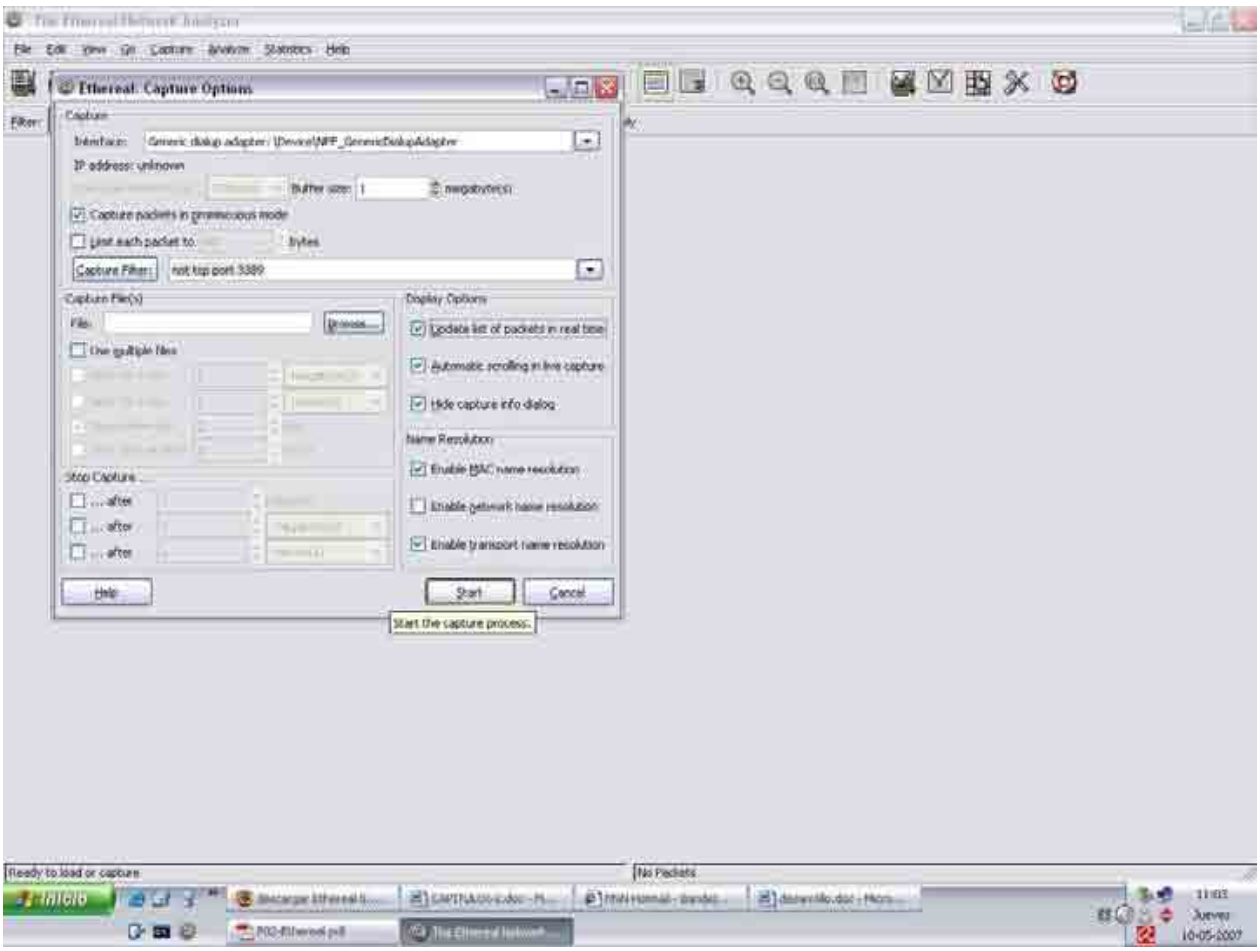


(Figura 2-5)

2.1.3 Ethereal

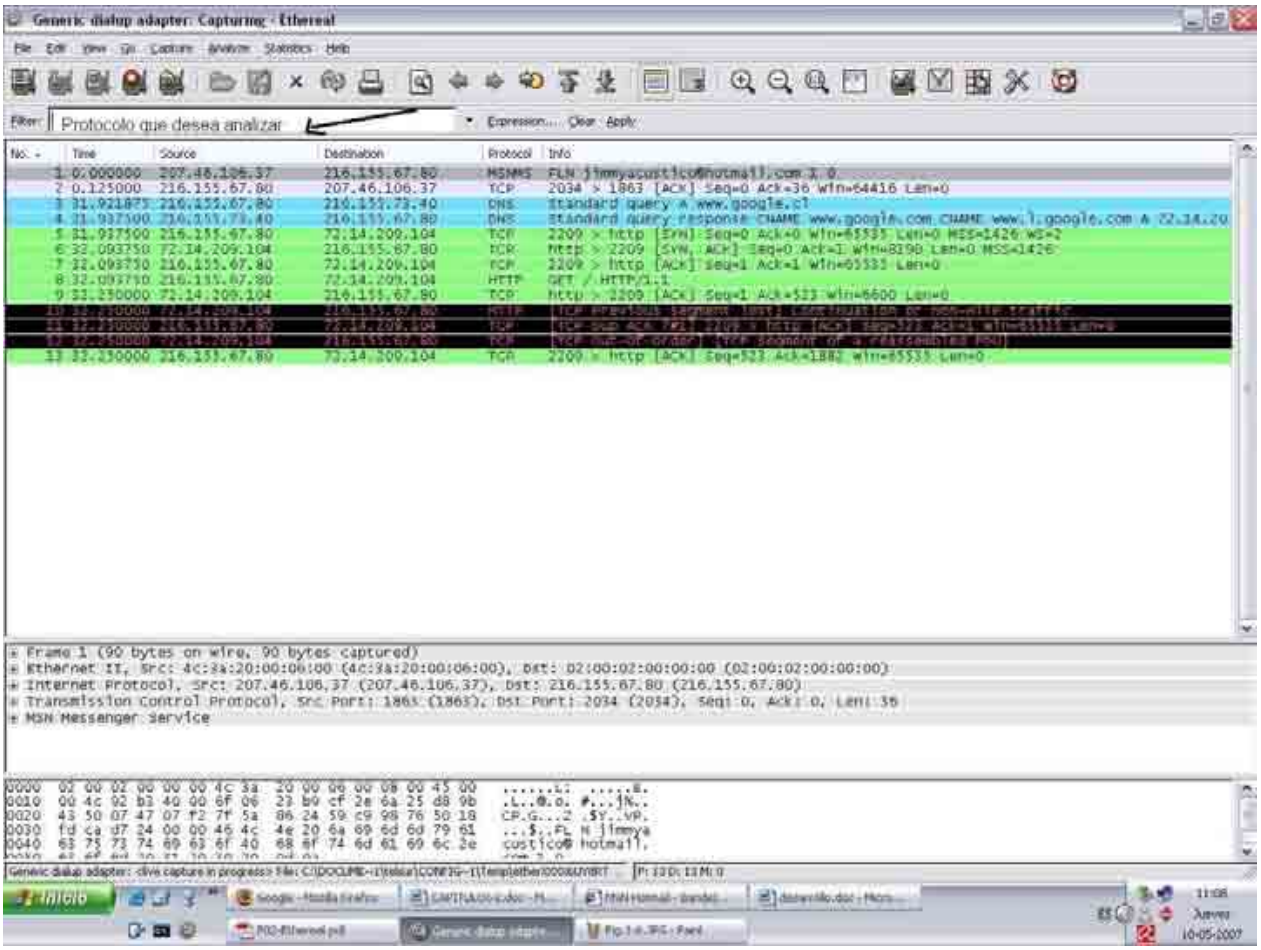
Ethereal es un sniffer, una aplicación capaz de capturar todos los paquetes de información que se difunden a través de la red para posteriormente interpretarlos y así conocer que tareas se llevan a cabe en la red.

Para llevar a cabo la captura de paquetes debemos configurar el ethereal para que nos entregue los protocolos en tiempo real, en Capture>Options…>Display Options



(Figura 2-6)

Al iniciar la captura de paquetes con Satrt, inicia el sniffer su trabajo, en el espacio en blanco se coloca el protocolo que desea analizar, proporcionando el tiempo, la partida y el destino del paquete enviado, el protocolo utilizado y la información del estado en que se encuentra el paquete.



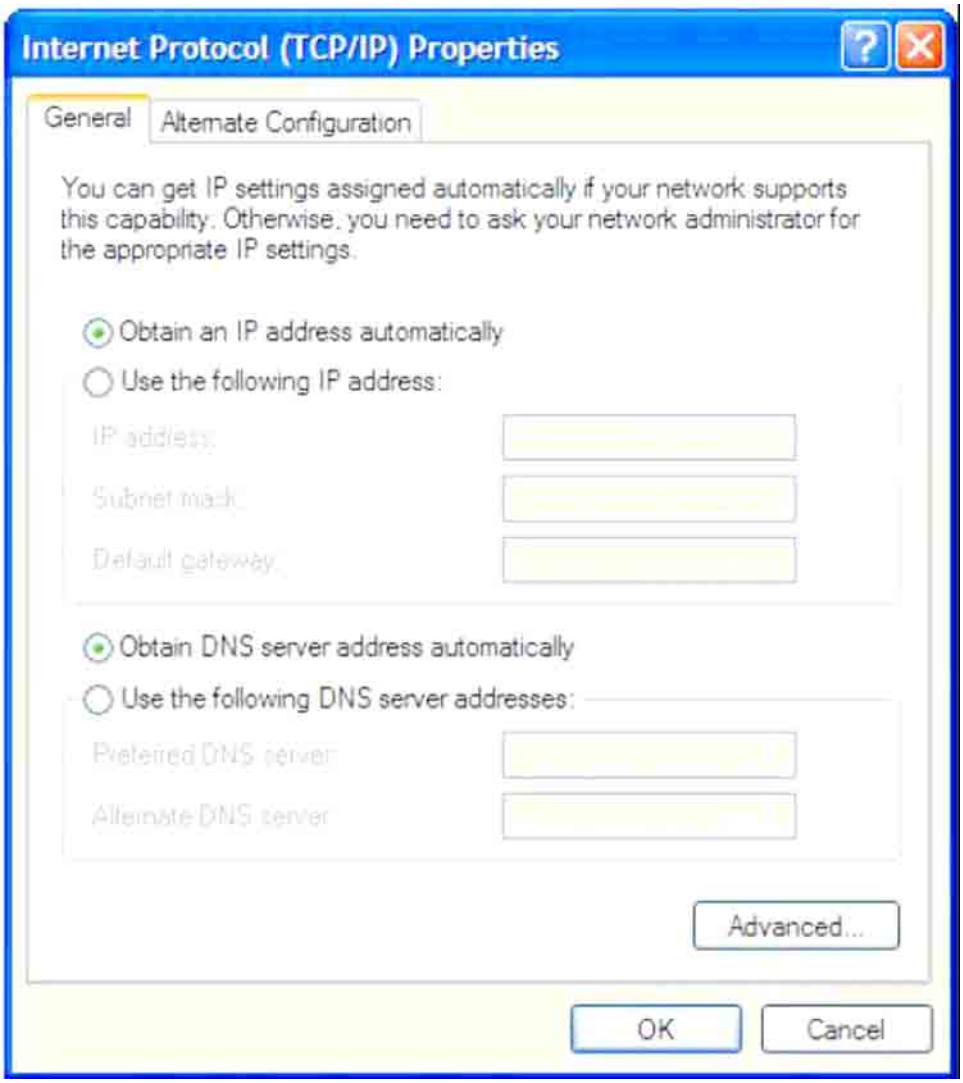
(Figura 2-7)

2.1.4 Firmware ATA

Es un bloque de instrucciones de programa para propósitos específicos, grabado en una memoria tipo ROM, que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo. Al estar integrado en la electrónica del dispositivo es en parte hardware, pero también es software, ya que proporciona lógica y se dispone en algún tipo de lenguaje de programación. Funcionalmente, el firmware es el intermediario (interfaz) entre las órdenes externas que recibe el dispositivo y su electrónica, ya que es el encargado de controlar a ésta última para ejecutar correctamente dichas órdenes externas.

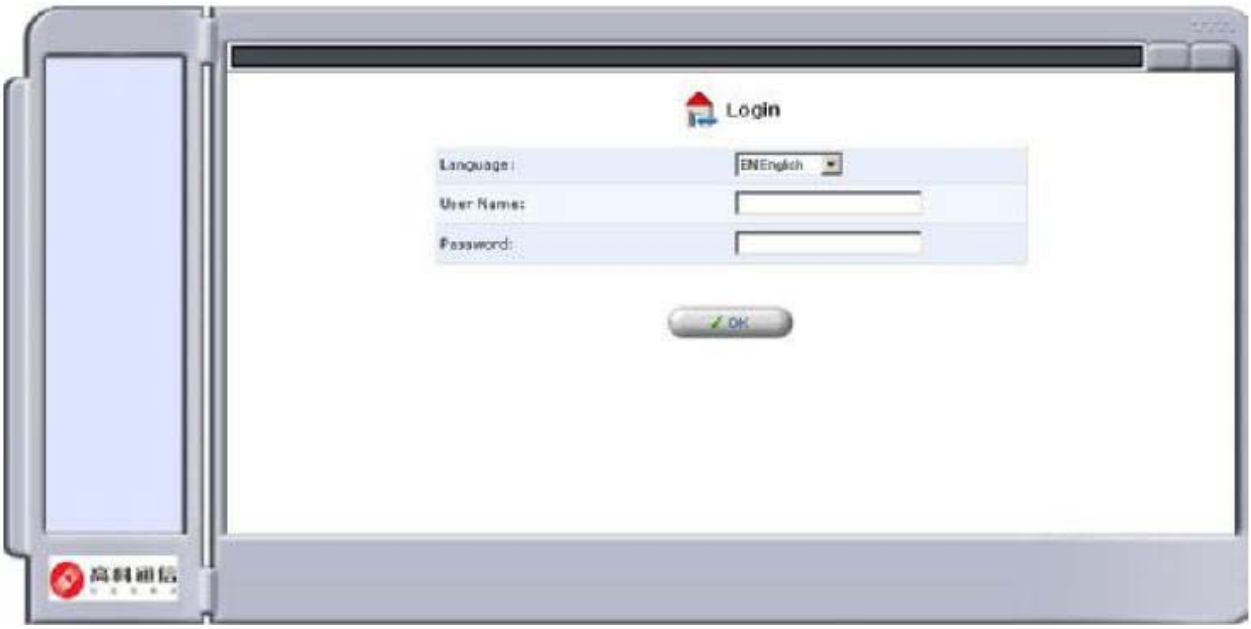
Para el caso de nuestro el ATA gaoke, debemos configurar su servidor Proxy SIP y también debemos configurar el puerto por el cual va a salir los paquetes RTP, nombre de usuario y contraseña la cual nos entregara nuestro proveedor SIP, su configuración es la siguiente:

En Windows XP, con el ATA gaoke conectado por la puerta LAN al computador, se debe ir al menú de conexiones de red y en la configuración TCP/IP asignar la obtención de una IP automática, la cual la entrega el equipo, como se muestra en la figura


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

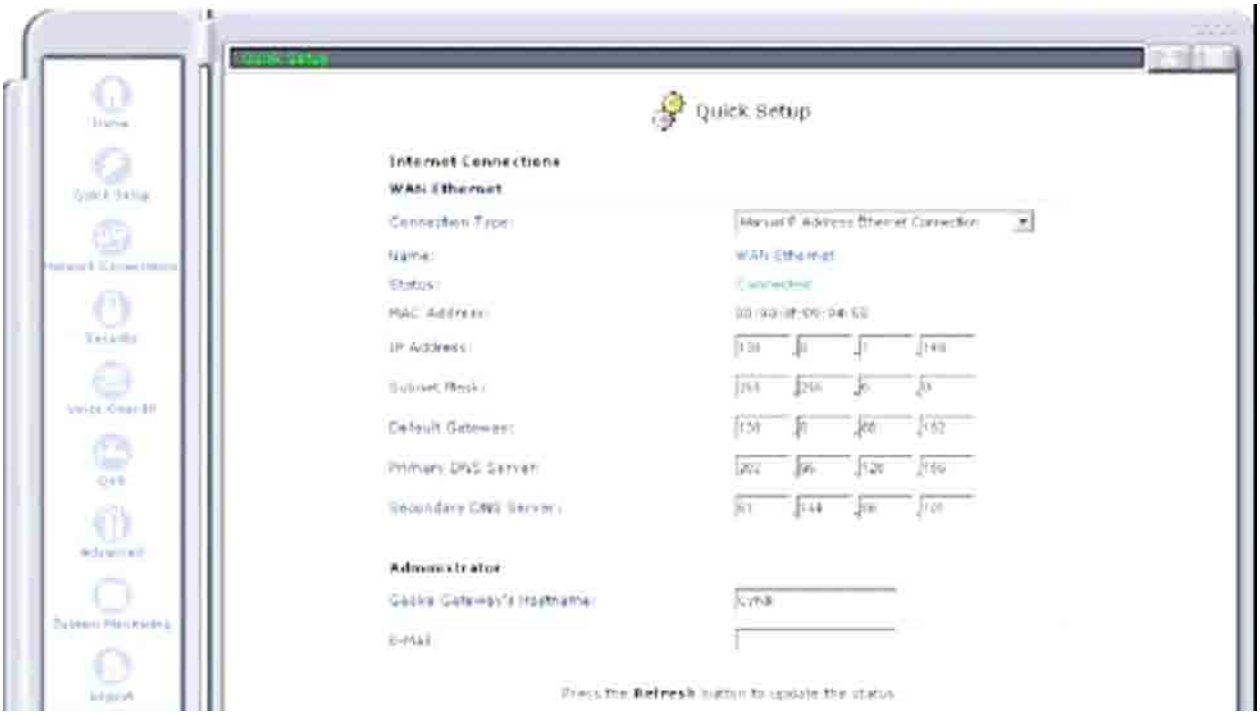
(Figura 2-8)

Mas adelante en Internet Explorer, en la barra de direcciones se ingresa la siguiente dirección IP 192.168.2.1, que es la dirección del ATA e ingresamos a su menú como lo muestra la figura (Fig.1-9)



(Figura 2-9)

El nombre de usuario y la contraseña es admin. Después que se ingresa se debe tener en cuenta que la conexión que se requiere modificar debe ser Lan o Wan para este caso elegimos una conexión LAN, **Manual IP Address Ethernet Connection**, ya que lo vamos a implementar una pequeña red LAN.



(Figura 2-10)

En el capitulo practico entregare una configuración detallada de un ATA

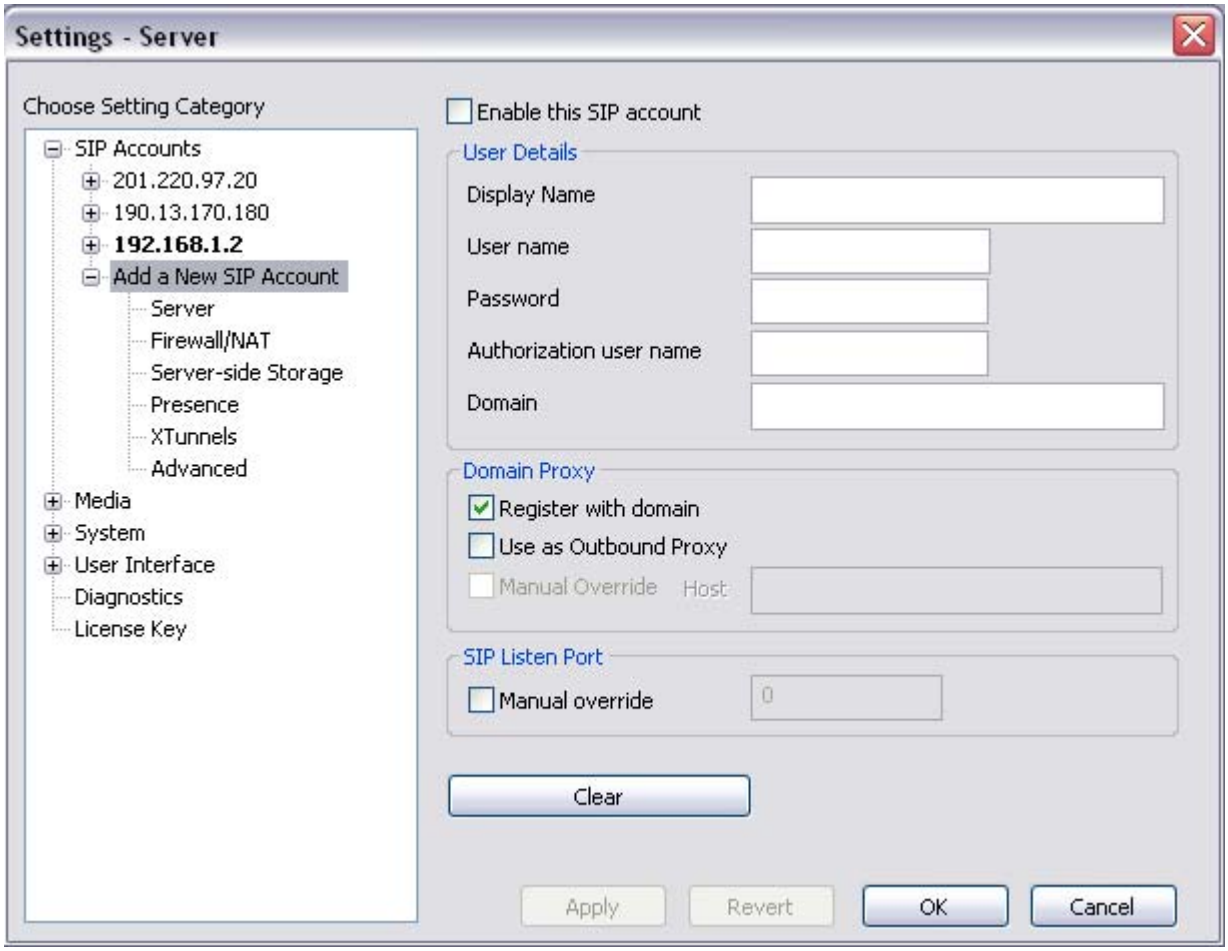
2.1.5 Softphone

Un Softphone (en inglés combinación de Software y de Telephone) es un software que hace una simulación de teléfono convencional por computadora. O sea permite usar la computadora para hacer llamadas a otros softphones o a otros teléfonos convencionales usando un proveedor de Telefonía IP.

En la siguiente figura especifico las funciones que posee un softphone, en este caso de el trabajo de titulacion se ocupara el softphone X-lite, posee control de codec y esta hecho para el protocolo SIP que es el que se utilizara en el trabajo de titulacion.

(Figura 2-11)

Para su configuración se presionael botton derecho del Mouse ye ingresamos Settings… y aparece un menú con la configuración del Softphone



(Figura 2-12)

Se puede habilitar una cuenta SIP, las opciones que entrega son el nombre de usuario ,el pasword, el dominio al cual se va a registrar el Softphone SIP, en la parte de media se habilitar el tipo de codec que se requiere, de acuerdo a los recursos que se tiene, y los tonos DTMF, etcétera. Se puede obtener diferentes funciones en este softphone

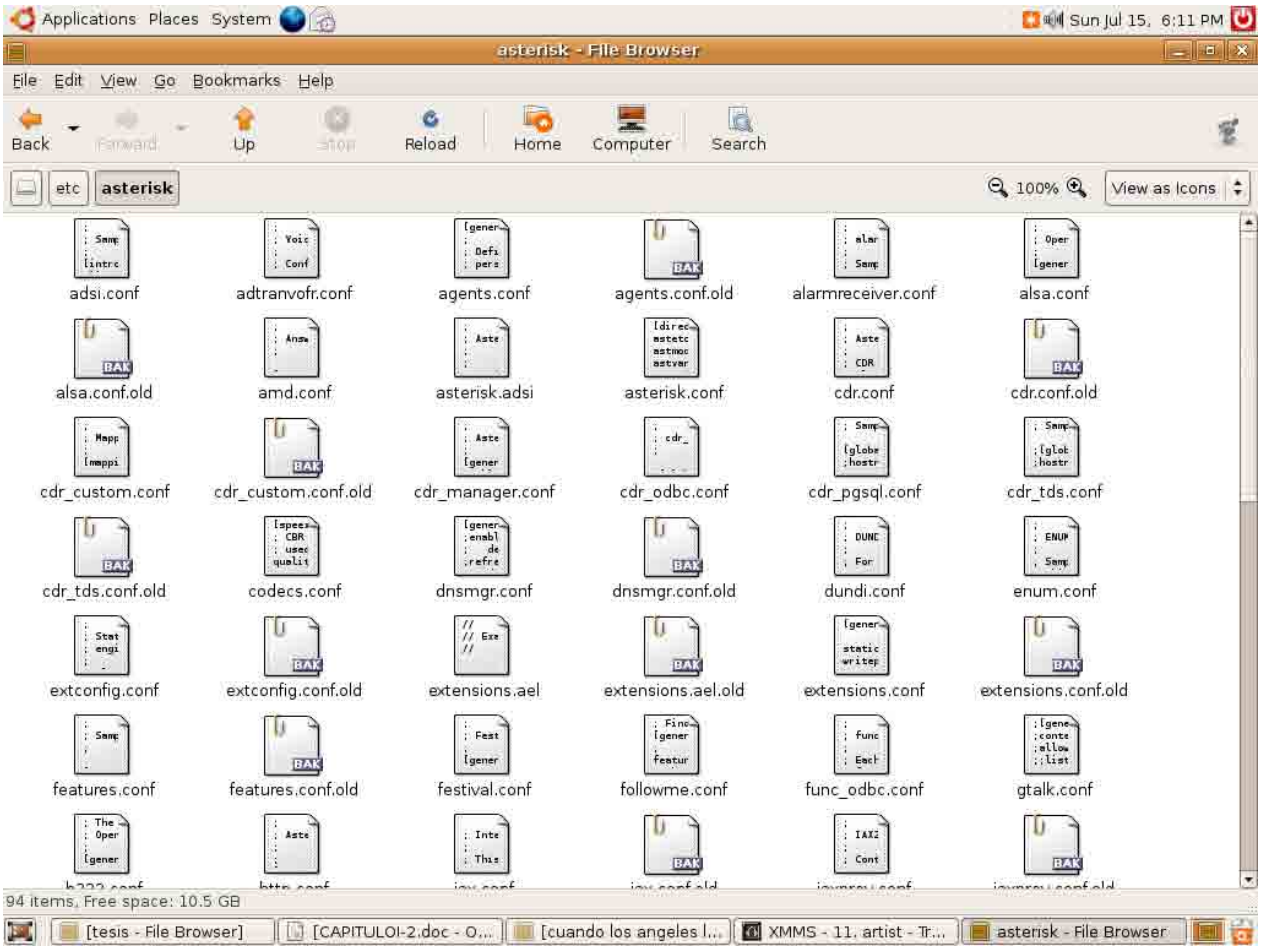
2.2 Implementación de una central telefónica IP

Al implementar la central de telefonía IP se debe tener en cuenta que esta se compone de 2 partes que son la interconexión en el mundo IP, y la salida de la llamada hacia la RTC (red telefónica conmutada), la implementación que se realiza en este trabajo de titulacion se refiere a solamente el mundo IP, ya que por costos no es viable la implementación de la salida a la red de telefonía actual, a cambio de esto la central tendrá un análisis de una verdadera central, no solamente como un conmutador de llamadas, ya que se implementara un IVR, cada teléfono tendrá un buzón de voz , el cual se podrá revisar, llamada en espera y otras aplicaciones que hacen a este proyecto mas robusto. Para poder analizar en forma practica ese ejemplo se va a recurrir al apoyo de la empresa Telefónica del Sur, la cual tiene implementada un Asterisk con salida a la red telefónica conmutada, en su sucursal de Camilo Henríquez. Teniendo esto claro se procede a la explicación de la implementación de la central de telefonía IP.

2.2.1 Pasos a seguir:

Después de instalar y compilar el asterisk , que es la espina dorsal del proyecto, se procede a configurar el asterisk para su uso.

Los archivos de configuración de los módulos de asterisk por defecto están guardados en la ruta /etc/asterisk/ se procede a ingresar a esa dirección con el explorador en el sistema operativo ubuntu linux.


Applications Places System
Sun Jul 15, 6:11 PM
asterisk - File Browser
File Edit View Go Bookmarks Help
Back Forward Up Stop Reload Home Computer Search
etc asterisk
100% View as Icons
adsi.conf
adtranvofr.conf
agents.conf
agents.conf.old
alarmreceiver.conf
alsa.conf
alsa.conf.old
amd.conf
asterisk.adsi
asterisk.conf
cdr.conf
cdr.conf.old
cdr_custom.conf
cdr_custom.conf.old
cdr_manager.conf
cdr_odbc.conf
cdr_pgsql.conf
cdr_tds.conf
cdr_tds.conf.old
codecs.conf
dnsmgr.conf
dnsmgr.conf.old
dundi.conf
enum.conf
extconfig.conf
extconfig.conf.old
extensions.ael
extensions.ael.old
extensions.conf
extensions.conf.old
features.conf
features.conf.old
festival.conf
followme.conf
func_odbc.conf
gtalk.conf
94 items, Free space: 10.5 GB
[tesis - File Browser]
[CAPITULOI-2.doc - O...
[cuando los angeles l...
XMMS - 11. artist - Tr...
asterisk - File Browser

(Figura 2-13)

Como se aprecia existen bastantes archivos lo que podemos configurar, para la central, pero los que se modificaran son los siguientes:

Sip.conf
extensions .conf
voicemail.conf
Estos archivos constituyen una cadena para enrutar la llamada hacia su destino:

El Modulo Sip.conf es para el registro de los usuarios, la central de telefonía IP, en este modulo compara nombre de usuario, pasword, lenguaje de la comunicación, la calidad de la conversación, etc. a continuación se muestra un ejemplo de configuración de 1 usuario:
videosupport:
Este usuario, esta configuración se observa que el usuario puede soportar video en su conversación, por ejemplo para implementar una cámara web en su llamada, el puerto es el 5060 que es el puerto utilizado para las llamadas de Voz sobre IP
bindaddr acepta cualquier Ip entrante para logearse contra este servidor.

allow se refiere a los codecs con que trabaja, en este caso esta con el codec G.711 que es el mas utilizado en redes LAN porque no utiliza técnicas de compresión muy altas, ya que el ancho de banda que utiliza es de 64 Kbps, comparado con otros codec, la ventaja es que la calidad de la conversación es alta y no necesita demasiado procesamiento para su envió,

[general]
videosupport=yes
port=5060
bindaddr = 0.0.0.0
allow=ulaw
nat=no

El numero 33 se refiere al nombre de usuario,

El tipo (type) "user" se usa para autenticar llamadas entrantes, "peer" para llamadas salientes y "friend" para ambas. En nuestro caso hemos definido una extensión pedro como "friend". Puede realizar y recibir llamadas.
languaje es el lenguaje de la comunicación, es en español, esto es utilizado en el buzón de voz y en el menú IVR para que la operadora pueda establecer la llamada en español, el tipo de host se refiere a si la IP del usuario es dinámica o fija
nat es si la central PBX realiza nateo o no

dtmfmode son los tonos del teclado del fax y el telefono que son para el establecimiento de la llamada.
canreinvite =no ; Asterisk por defecto trata de redirigir
context=cero ; El contexto que controla todo esto
Mailbox se refiere a que contexto debe ir el usuario con su buzon de voz

```
[33]
type=friend
language=es
username=33
secret=1234
host=dynamic
nat=no
dtmfmode=rfc2833
qualify=yes
canreinvite=no
context=cero
allow=h263
```

allow=h263p
mailbox=77@mb_tutorial

El archivo extensions.conf es el más importante del Asterisk y tiene como misión principal definir el dialplan o plan de numeración que seguirá la centralita para cada contexto y por tanto para cada usuario.

Contexto [general]
El contexto [general] configura unas pocas opciones generales como son:

- static : Indica si se ha de hacer caso a un comando "save dialplan" desde la consola. Por defecto es "yes". Funciona en conjunto con "writeprotect"
- writeprotect : Si writeprotect=no *y* static=yes se permite ejecutar un comando "save dialplan" desde la consola. El valor por defecto es " *no"* .
- autofallthrough : Si está activado y una extensión se queda sin cosas que hacer termina la llamada con BUSY, CONGESTION o HANGUP Si no está activada se queda esperando otra extensión. Nunca debería suceder que una extensión se quede sin cosas que hacer como explicaremos posteriormente.

En general estas opciones no son muy importantes y se pueden dejar tal y como aparecen por defecto.

Resto de Contextos :

Esto es lo más importante de este fichero. Vamos a indicar ahora como crear un contexto especifico y asignar un plan de numeración. Todas las líneas de un determinado contexto tienen el mismo formato:

exten => *extension* , *prioridad*, *Comando(parametros)*

La extensión hace referencia al numero marcado
La prioridad al orden en que se ejecutan las instrucciones. Primero se ejecuta la de prioridad 1, luego la 2 y sucesivamente
El Comando hace referencia a la acción a ejecutar

Vamos a ir viendo unos ejemplos para ir aprendiendo los comandos

Ejemplo 1: Colgar la linea
exten => 333,1,Hangup ; indica que cuando alguien llame al 333 saltará la prioridad 1 y el sistema colgará la llamada

Ejemplo 2 : Llamar a el usuario SIP 3000 y que salte el contestador si no contesta
exten => 3000,1,Dial(SIP/3000,30,Ttm) ; intenta llamar al usuario 3000 de sip que tiene que estar definido en sip.conf con ese contexto
exten => 3000,2,Hangup ; cuando acaba la llamada cuelga
exten => 3000,102,Voicemail(3000) ; La prioridad 102 significa que el usuario no estaba conectado y salta el contestador al buzon 3000
exten => 3000,103,Hangup ; se cuelga después de dejar el mensaje

En este caso al llamar a la extension 3000 usuamos el comando *Dial (destino, tiempo de timeout, opciones)*
El destino es el usuario 3000 del archivo sip.conf, 30 segundos de timeout. El usuario 3000 deberia existir en sip.conf

las opciones hacen referencia a opciones del comando dial:
la "T" permite al usuario llamante transferir la llamada pulsando #
la "t" permite al usuario llamado transferir la llamada pulsando #
la "m" indica que vamos a oir una musica especial mientras esperamos a que el otro conteste
Si el usuario 3000 no está conectado salta a la prioridad +101 (en nuestro caso a la 102=1+101 ya que estabamos en la prioridad 1) y hacemos que salte el contestador para dejar un mensaje.

Es importante que por cada rama siempre se cierre el camino y se cuelgue la llamada con un Hangup

Configuración del archivo voicemail.conf (Contestador automatico)

El archivo voicemail.conf sirve para configurar el contestador automatico y gestionar los buzones de los usuarios

El fichero extensions.conf se compone también de secciones o contextos entre corchetes
Hay dos contextos especiales llamados [general] y [zonemessages] que siempre están presentes.

Contexto [general]
El contexto [general] configura las opciones generales del buzón de voz:

Un ejemplo básico podría ser:

[general]
; Enviar archivos en las notificaciones de e-mail
attach=yes

; Usar el formato wav para los mensajes de voz
format=wav
; Limitar el tiempo máximo del mensaje de voz a 180 segundos
maxmessage=180
; Limitar el tiempo minimo del mensaje a 3 segundos
minmessage=3
; Anunciar el numero que llamó antes de repetir el mensaje
saycid=yes
; Limitar el numero de intentos de registro a 3
maxlogins=3
; Define los contextos internos para especificar que vienen de una extensión interna
cidinternalcontexts=house_local,house_toll,house_admin

Contexto [zonemessages]
Este contexto define zonas horarias. La hora para distintos usuarios no es la misma y para poder informarle sobre la hora en que recibió el mensaje es necesario fijar diferentes zonas horarias:

Un ejemplo podría ser

[zonemessages]
madrid=Europe/Paris|'vm-received' Q 'digits/at' R
paris=Europe/Paris|'vm-received' Q 'digits/at' R
sthlm=Europe/Stockholm|'vm-recieved' Q 'digits/at' R
europa=Europe/Berlin|'vm-received' Q 'digits/at' kM
italia=Europe/Rome|'vm-received' Q 'digit/at' HMP

El formato de las líneas es el siguiente:

zona=Pais/Ciudad|Opciones --> El Pais y la ciudad deben ser válidos y son los del archivo /usr/share/zoneinfo de la instalación de Linux

Resto de Contextos

En el resto de contextos definen los buzones de los usuarios. Podemos tener todos los usuarios en un solo contexto por ejemplo [default] o tener más de un contexto.

El formato básico es el siguiente:

[default]
extension => contraseña, nombre de usuario, email de usuario, email de notificación,opciones

La extensión hace referencia al numero de telefono llamado.

- La contraseña hacer referencia a la contraseña para ese usuario de su buzón de voz.
- El nombre de usuario es el nombre del cliente de la extensión
- El email del usuario es el correo al que serán enviados los mensajes
- El email de notificacion es un email alternativo donde pueden ser enviadas las notificaciones para administración o control
- Las opciones sirven para sobreescribir las del contexto [general] o especificar una zona horaria para el usuario.Hay 9 especificas: **attach, serveremail, tz, saycid, review, operator, callback, dialout** and **exitcontext.** Son las mismas que las contexto [general] salvo tz.La opción **tz** se usa para sobrescribir la zona por defecto y debe estar presente en el contexto [zonemessages]

Ejemplos:

[default]
1234 => 3456,Ejemplo1,mail@dominio.com
4200 => 9855,Pedro
Perez,pedro@dominio.com,admin@dominio.com,attach=no|serveremail=info@dominio.com|tz=madrid

Configurando estos 3 módulos podemos tener una configuración básica de la central telefónica, conectarla a Internet para subir el Server y establecer llamadas desde cualquier parte del mundo con una buena calidad de audio.

2.2.2 Diagrama de flujo de una comunicación

(Figura 2-14)

2.2.3 Configuración para proyecto tesis

A continuación se entregara la configuración para las pruebas que se realizaran en esta tesis, esta configuración esta hecha por Joel Urtubia Ugarte. Es para 4 teléfonos con su respectivo buzón de voz cada uno, menú IVR para la comunicación de anexos, música en espera con mp3, grabación de voz para contestar en buzón de voz y bloqueo de llamadas y desvío de llamadas a todos los números menos el numero 36, al llamar al numero 120, es un ejemplo de lo que se puede implementar en una central IP PBX

Ver Anexo 1

CAPITULO III Factores que afectan la telefonia IP

3.1 Retrasos en la red (Factores)

Los factores que afectan la telefonia IP es la calidad de la llamada que se establece sea aceptable para los usuarios

Los principales problemas en cuanto a la calidad del servicio (QoS) de una una red de VoIP, son la Latencia, el Jitter la pérdida de paquetes y el Eco. En VoIP estos problemas pueden ser resueltos mediante diversas técnicas que se explican en los siguientes apartados.

Los problemas de la calidad del servicio en VoIP vienen derivados de dos factores principalmente:

a) Internet es un sistema basado en conmutación de paquetes y por tanto la información no viaja siempre por el mismo camino. Esto produce efectos como la pérdida de paquetes o el jitter.

b) Las comunicaciones VoIP son en tiempo real lo que produce que efectos como el eco, la pérdida de paquetes y el retardo o latencia sean muy molestos y perjudiciales y deban ser evitados.

Jitter

CAUSAS:

El jitter es un efecto de las redes de datos no orientadas a conexión y basadas en conmutación de paquetes. Como la información se discretiza en paquetes cada uno de los paquetes puede seguir una ruta distinta para llegar al destino.

El jitter se define técnicamente como **la variación en el tiempo en la llegada de los paquetes, causada por congestión de red, perdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino**.

Las comunicaciones en tiempo real (como VoIP) son especialmente sensibles a este efecto. En general, es un problema frecuente en enlaces lentos o congestionados. Se espera que el aumento de mecanismos de QoS (calidad del servicio) como prioridad en las colas, reserva de ancho de banda o enlaces de mayor velocidad (100Mb Ethernet, E3/T3, SDH) puedan reducir los problemas del jitter en el futuro aumque seguirá siendo un problema por bastante tiempo.

VALORES RECOMENDADOS:

El jitter entre el punto inicial y final de la comunicación **debiera ser ser inferior a 100 ms**. Si el valor es menor a 100 ms el jitter puede ser compensado de manera apropiada. En caso contrario debiera ser minimizado.

POSIBLES SOLUCIONES:

- La solución más ampliamente adoptada es la utilización del **jitter buffer**. El jitter buffer consiste básicamente en asignar una pequeña cola o almacen para ir recibiendo los paquetes y sirviendolos con un pequeño retraso. Si alguno paquete no está en el buffer (se perdió o no ha llegado todavía) cuando sea necesario se descarta. Normalmente en

los telefonos IP (hardware y software) se pueden modificar los buffers. Un aumento del buffer implica menos perdida de paquetes pero más retraso. Una disminución implica menos retardo pero más perdida de paquetes.

Latencia

CAUSAS:

A la latencia también se la llama retardo. No es un problema específico de las redes no orientadas a conexión y por tanto de la VoIP. Es un problema general de las redes de telecomunicación. Por ejemplo, la latencia en los enlaces via satelite es muy elevada por las distancias que debe recorrer la información.

La latencia se define técnicamente en VoIP como el tiempo que tarda un paquete en llegar desde la fuente al destino.

Las comunicaciones en tiempo real (como VoIP) y full-duplex son sensibles a este efecto. Es el problema de "pisarnos". Al igual que el jitter, es un problema frecuente en enlaces lentos o congestionados.

VALORES RECOMENDADOS:

La latencia o retardo entre el punto inicial y final de la comunicación debiera ser ser inferior a 150 ms. El oído humano es capaz de detectar latencias de unos 250 ms, 200 ms en el caso de personas bastante sensibles. Si se supera ese umbral la comunicación se vuelve molesta.

POSIBLES SOLUCIONES:

No hay una solución que se pueda implementar de manera sencilla. Muchas veces depende de los equipos por los que pasan los paquetes, es decir, de la red misma. Se puede intentar reservar un ancho de banda de origen a destino o señalizar los paquetes con valores de TOS para intentar que los equipos sepan que se trata de tráfico en tiempo real y lo traten con mayor prioridad pero actualmente no suelen ser medidas muy eficaces ya que no disponemos del control de la red.

Si el problema de la latencia está en nuestra propia red interna podemos aumentar el ancho de banda o velocidad del enlace o priorizar esos paquetes dentro de nuestra red

Eco

CAUSAS:

El eco se produce por un fenomeno técnico que es la conversión de 2 a 4 hilos de los sistemas telefónicos o por un retorno de la señal que se escucha por los altavoces y se cuela de nuevo por el microfono. El eco también se suele conocer como reverberación.

El eco se define como una reflexión retardada de la señal acustica original.

El eco es especialmente molesto cuanto mayor es el retardo y cuanto mayor es su intensidad con lo cual se convierte en un problema en VoIP puesto que los retardos suelen ser mayores que en la red de telefonía tradicional.

VALORES RECOMENDADOS:

El oído humano es capaz de detectar el eco cuando su retardo con la señal original es igual o superior a 10 ms. Pero otro factor importante es la intensidad del eco ya que normalmente la señal de vuelta tiene menor potencia que la original. Es tolerable que llegue a 65 ms y una atenuación de 25 a 30 dB.

POSIBLES SOLUCIONES:

En este caso hay dos posibles soluciones para evitar este efecto tan molesto.

- Supresores de eco - Consiste en evitar que la señal emitida sea devuelta convirtiendo por momentos la linea full-duplex en una linea half-duplex de tal manera que si se detecta comunicación en un sentido se impide la comunicación en sentido contrario. El tiempo de conmutación de los supresores de eco es muy pequeño. Impide una comunicación full-duplex plena.

- Canceladores de eco - Es el sistema por el cual el dispostivo emisor guarda la información que envía en memoria y es capaz de detectar en la señal de vuelta la misma información (tal vez atenuada y con ruido). El dispostivo filtra esa información y cancela esas componentes de la voz. Requiere mayor tiempo de procesamiento.

Perdida de paquetes

CAUSAS:

Las comunicaciones en tiempo real están basadas en el protocolo UDP. Este protocolo no está orientado a conexión y si se produce una pérdida de paquetes no se reenvian. Además la perdida de paquetes también se produce por descartes de paquetes que no llegan a tiempo al receptor.

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.

VALORES RECOMENDADOS:

La perdida de paquetes máxima admitida para que no se degrade la comunicación deber ser inferior al 1%. Pero es bastante dependiente del códec que se utiliza. Cuanto mayor sea la compresión del codec más pernicioso es el efecto de la pérdida de paquetes. Una pérdida del 1% degrada más la comunicación si se usa el códec G.729 en vez del G.711.

POSIBLES SOLUCIONES:

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

De todos modos este fenomeno puede estar también bastante relacionado con el jitter y el jitter buffer.

3.2 Ataques posibles a la telefonía IP

3.2.1 Seguridad en el protocolo VoIP

Consideremos las limitaciones de seguridad en un sistema de Voz sobre IP. En el proceso de ahorrar dinero (factor necesario) e incrementar la eficacia, dos porciones cruciales de cualquier infraestructura, voz y datos, fueron combinadas. Los servidores de VoIP actúan como puertas de enlace; así, routers especiales, teléfonos, nuevos protocolos y sistemas operativos están ahora entremezclándose con esta nueva tecnología.

3.2.2 Amenazas

Desafortunadamente existen numerosas amenazas que conciernen a las redes VoIP; muchas de las cuales no resultan obvias para la mayoría de los usuarios. Los dispositivos de redes, los servidores y sus sistemas operativos, los protocolos, los teléfonos y su software, todos son vulnerables.

La información sobre una llamada es tan valiosa como el contenido de la voz. Por ejemplo, una señal comprometida en un servidor puede ser usada para configurar y

dirigir llamadas, del siguiente modo: una lista de entradas y salidas de llamadas, su duración y sus parámetros. Usando esta información, un atacante puede obtener un mapa detallado de todas las llamadas realizadas en la red, creando grabaciones completas de conversaciones y datos de usuario.

La conversación es en sí misma un riesgo y el objetivo más obvio de una red VoIP. Consiguiendo una entrada en una parte clave de la infraestructura, como una puerta de enlace de VoIP, un atacante puede capturar y volver a montar paquetes con el objetivo de escuchar la conversación. O incluso peor aún, grabarlo absolutamente todo, y poder retransmitir todas las conversaciones sucedidas en la red.

Las llamadas son también vulnerables al “secuestro”. En este escenario, un atacante puede interceptar una conexión y modificar los parámetros de la llamada. Se trata de un ataque que puede causar bastante pavor, ya que las víctimas no notan ningún tipo de cambio. Las posibilidades incluyen la técnica de spoofing o robo de identidad, y redireccionamiento de llamada, haciendo que la integridad de los datos estén bajo un gran riesgo.

La enorme disponibilidad de las redes VoIP es otro punto sensible. En el PSTN, la disponibilidad era raramente un problema. Pero es mucho más sencillo hackear una red VoIP. Todos estamos familiarizados con los efectos demoledores de los ataques de denegación de servicio. Si se dirigen a puntos clave de la red, podrían incluso destruir la posibilidad de comunicarte vía voz o datos.

Los teléfonos y servidores son blancos por sí mismos. Aunque sean de menor tamaño o nos sigan pareciendo simples teléfonos, son en base, computadores con software. Obviamente, este software es vulnerable con los mismos tipos de bugs o agujeros de seguridad que pueden hacer que un sistema operativo pueda estar a plena disposición

del intruso. El código puede ser insertado para configurar cualquier tipo de acción maliciosa.

(Figura 3-1)

3.2.3 Clasificación de los ataques

Durante los siguientes apartados se va a intentar detallar cuales son las amenazas más significativas que afectan a la telefonía sobre redes IP. Como ya se ha comentado la mayoría los riesgos son inherentes de las capas sobre las que se apoya la tecnología VoIP por lo que muchos de los ataques se basarán en técnicas bien conocidas. Se mostraran, también, ciertas vulnerabilidades que afecta específicamente a las redes VoIP y a sus protocolos.

Las amenazas de las redes de telefonía IP las podemos clasificar en las siguientes categorías:

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

3.2.3.1 Accesos desautorizados y Fraudes

Una de las mas importantes amenazas de las redes VoIP, son los fraudes consecuencia de un acceso desautorizado a una red legal VoIP (por ejemplo haber obtenido anteriormente obtener datos de cuentas). Una vez se ha obtenido el acceso, usuario desautorizados realizan llamadas de larga distancia, en muchos casos dependiendo del perfil creado en la central, internacionales. Principalmente ocurren en entornos empresariales. El control y el registro estricto de las llamadas puede paliar el problema

3.2.3.2 Explotando la red subyacente

Uno de los mayores problemas sea quizás la interceptación o eavesdropping.. Traducido literalmente como “escuchar secretamente”, es el término con el que se conoce a la captura de información (cifrada o no) por parte de un intruso al que no iba dirigida dicha información. En términos de telefonía IP, estamos hablando de la

interceptación de las conversaciones VoIP por parte de individuos que no participan en la conversación.

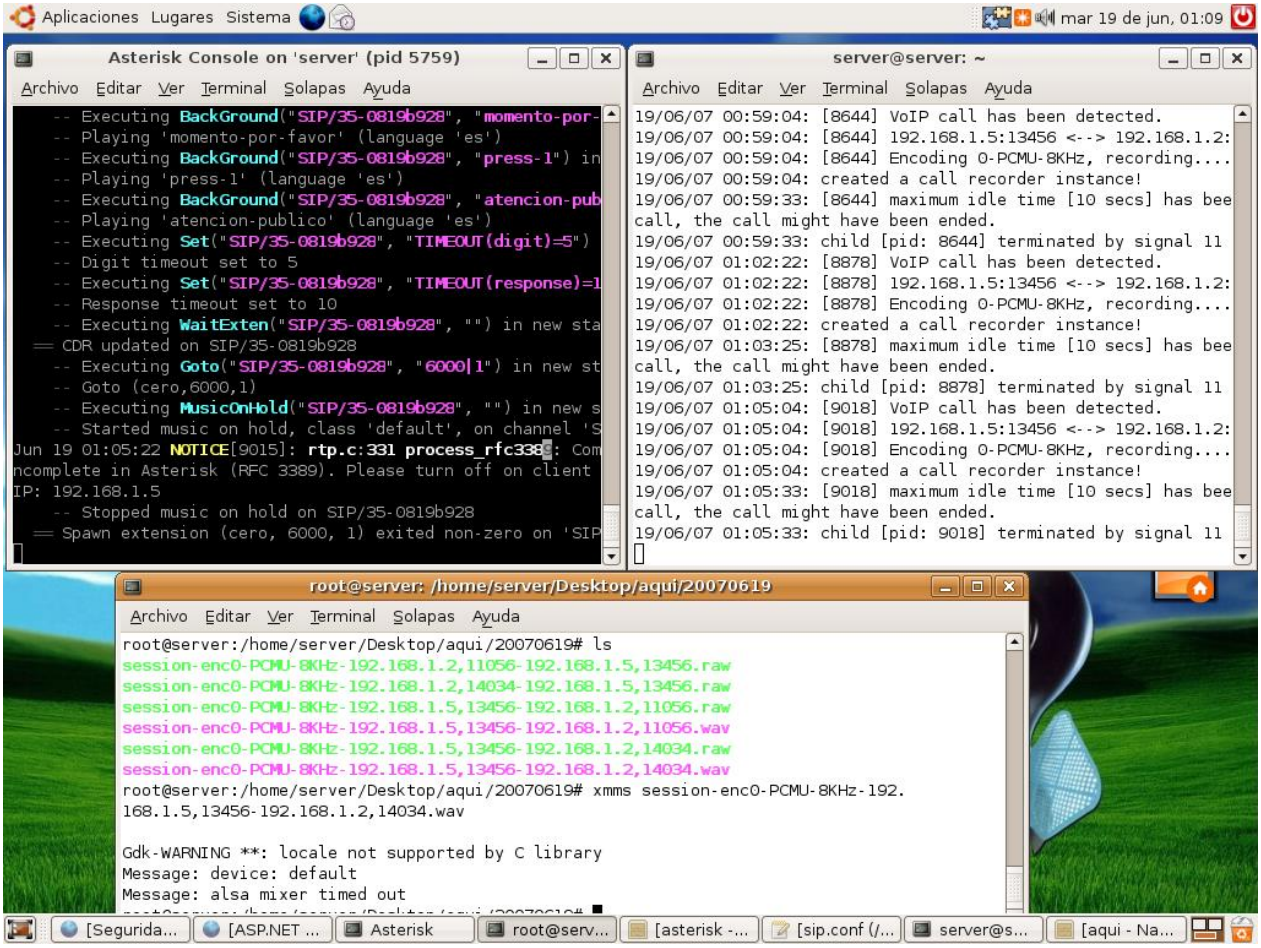
El eavesdropping en VoIP presenta pequeñas diferencias frente la interceptación de datos en las redes tradicionales. En VoIP vamos a diferenciar básicamente dos partes dentro de la comunicación: la señalización y el flujo de datos. Los cuales utilizarán protocolos diferentes. En la señalización nos centraremos durante todo el documento en el protocolo SIP mientras que en el flujo de datos normalmente se utilizará el protocolo RTP sobre UDP.

El impacto de esta técnica es más que evidente, interceptando comunicaciones es posible obtener toda clase información sensible y altamente confidencial. Y aunque en principio se trata de un técnica puramente pasiva, razón por la cual hace difícil su detección, es posible intervenir también de forma activa en la comunicación insertando nuevos datos (que en el caso de VoIP se trataría de audio) redireccionar o impedir que los datos lleguen a su destino.

Las formas de conseguir interceptar una comunicación pueden llegar a ser tan triviales como esnifar el tráfico de la red si los datos no van cifrados. Existen excelentes sniffers como ethereal/wireshark, software que se utilizo en el trabajo de titulacion, que permitirán capturar todo el tráfico de el segmento de la red. Por el contrario, lo normal es que nos encontramos dentro de redes conmutadas por lo que para esnifar el tráfico que no vaya dirigido a nuestro equipo serán necesarias otras técnicas más elaboradas como realizar un “Main in the Midle” utilizando Envenenamiento ARP. Entre las herramientas que podremos utilizar se encuentra el conocido programa ettercap, Cain & Abel, la suite de herramientas para Linux Dsniff y vomit (Voice over misconfigured Internet telephones) por citar algunos ejemplos.

Hay que señalar también la creciente utilización de redes inalámbricas supone en muchos casos un vía más a explotar por parte del intruso. Redes Wifi mal configuradas junto con una infraestructura de red insegura puede facilitar e trabajo del intruso a la hora de acceder a la red VoIP para lanzar sus ataques.

En el trabajo de titulacion se realizo este ataque a una conversación en una red LAN con un servidor Linux con el programa voipong, primero se realiza el ataque apuntando a la conversación y después el mismo programa crea un archivo wav con la conversación escuchada, este programa se explicara mas adelante para seguir con este tema.



(Figura 3-2)

3.1.3.3 Ataques de denegación de servicio

Los ataques de denegación de servicio son intentos malintencionados de degradar seriamente el rendimiento de la red o un sistema incluso llegando al punto de impedir la utilización del mismo por parte de usuarios legítimos. Algunas técnicas se basan en el envío de paquetes especialmente construidos para explotar alguna vulnerabilidad en el software o en el hardware del sistema, saturación de los flujos de datos y de la red o sobrecarga de procesos en los dispositivos.

Llegan a ser especialmente dañinos los llamados DDoS o ataques de denegación distribuidos. Son ataques DoS simples pero realizados desde múltiples computadores de forma coordinada. Las redes y sistemas VoIP son especialmente vulnerables a los DDoS por diversas razones:

La primera y quizás más importante es la dependencia y la necesidad de garantías en la calidad de servicio, que hacen que las redes IP donde se mantengan llamadas telefónicas tengan una tolerancia mucho menor a problemas de rendimiento.

Otra razón es que en una red VoIP existen multitud de dispositivos con funciones muy específicas por lo que ataques contra casi cualquier dispositivo de la red pueden afectar seriamente los servicios de telefonía IP. Muchos de estos dispositivos son muy susceptibles de no manejar, priorizar o enrutar el tráfico de forma fiable si presentan un consumo de CPU alto. Por lo que muchos de los ataques de DoS se centran en atacar los dispositivos de red y/o inundar la red de tráfico inútil para degradar su funcionamiento y que los paquetes pertenecientes a comunicaciones telefónicas se pierdan o retrasen.

3.1.3.4 Ataques a los dispositivos

Muchos de los ataques realizador hoy en día por hackers y crackers hacia las redes de datos tienen como objetivo principal el hardware y el software de los dispositivos. Por lo tanto, en redes VoIP, los gateways, call managers, Proxy servers sin olvidar los teléfonos IP serán potencialmente objetivos a explotar por parte de un intruso. Hay que tener en cuenta que los dispositivos VoIP son tan vulnerables como lo es el sistema operativo o el firmware que ejecutan. Son muy frecuentes los ataques de fuzzing con paquetes malformados que provocan cuelgues o reboots en los dispositivos cuando procesan dicho paquete. Otros ataques de denegación de servicio llamados “flooders” tienen como objetivo los servicios y puertos abiertos de los dispositivos VoIP.

3.2.3.5 Descubriendo objetivos

Una vez que el hacker ha seleccionado una red como su próximo objetivo, sus primeros pasos consistirán en obtener la mayor información posible de su victima. Cuando el intruso tenga información suficiente evaluará sus siguientes pasos eligiendo el método de ataque más adecuado para alcanzar su objetivo. Normalmente el método de obtención de información se realiza con técnicas de menos a más nivel de intrusión. De este modo en las primeras etapas el atacante realizará un footprinting u obtención de toda la información pública posible del objetivo. Más adelante una de las acciones más comunes consiste en obtener la mayor información posible de las máquinas y servicios conectados en la red atacada. Después de tener un listado de servicios y direcciones IP consistente, tratará de buscar agujeros de seguridad, vulnerabilidades y obtener la mayor información sensible de esos servicios (enumeración) para poder explotarlos y conseguir una vía de entrada.

Un ejemplo de ataque de enumeración, podría ser utilizar la fuerza bruta contra servidores VoIP para obtener una lista de extensiones telefónicas válidas. Información que seria extremadamente útil para lanzar otros ataques como inundaciones INVITE o secuestro de registro.

3.2.3.6 Representación de Ataques

3.2.2 Herramientas del Hacker

Es difícil describir el ataque “típico” de un hacker debido a que los intrusos poseen diferentes niveles de técnicos por su experiencia y son además son motivados por diversos factores. Algunos hackers son intrigosos por el desafío, otros más gozan de hacer la vida difícil a los demás, y otros tantos substraen datos delicados para algún beneficio propio.

Recolección de información

Generalmente, el primer paso es saber en que forma se recolecta la información y además que tipo de información es. La meta es construir una base de datos que contenga la organización de la red y colectar la información acerca de los servidores residentes.

Esta es una lista de herramientas que un hacker puede usar para colectar esta información:

- El protocolo SNMP puede utilizarse para examinar la tabla de ruteo en un dispositivo inseguro, esto sirve para aprender los detalles más íntimos acerca del objetivo de la topología de red perteneciente a una organización.
- El programa TraceRoute puede revelar el número de redes intermedias y los ruteadores en torno al servidor específico.
- El protocolo Whois que es un servicio de información que provee datos acerca de todos los dominios DNS y el administrador del sistema responsable para cada dominio. No obstante que esta información es anticuada.
- Servidores DNS pueden accesarce para obtener una lista de las direcciones IP y sus correspondientes Nombres (Programa Nslookup).

- El protocolo Finger puede revelar información detallada acerca de los usuarios (nombres de Login, números telefónicos, tiempo y última sesión, etc.) de un servidor en específico.
- El programa Ping puede ser empleado para localizar un servidor particular y determinar si se puede alcanzar. Esta simple herramienta puede ser usada como un programa de escaneo pequeño que por medio de llamadas a la dirección de un servidor haga posible construir una lista de los servidores que actualmente son residentes en la red.

Sondeo del sistema para debilitar la seguridad

Después que se obtienen la información de red perteneciente a dicha organización, el hacker trata de probar cada uno de los servidores para debilitar la seguridad.

Estos son algunos usos de las herramientas que un hacker puede utilizar automáticamente para explorar individualmente los servidores residentes en una red:

- Una vez obtenida una lista no obstantemente pequeña de la vulnerabilidad de servicios en la red, un hacker bien instruido puede escribir un pequeño programa que intente conectarse a un puerto especificando el tipo de servicio que esta asignado al servidor en cuestión. La corrida del programa presenta una lista de los servidores que soportan servicio de Internet y están expuestos al ataque.
- Están disponibles varias herramientas del dominio publico, tal es el caso como el Rastreador de Seguridad en Internet (ISS) o la Herramienta para Análisis de Seguridad para Auditar Redes (SATAN), el cual puede rastrear una subred o un dominio y ver las posibles fugas de seguridad. Estos programas determinan la debilidad de cada uno de los sistemas con respecto a varios puntos de vulnerabilidad comunes en un sistema. El intruso usa la información colectada por este tipo de rastreadores para intentar el acceso no autorizado al sistema de la organización puesta en la mira.

Un administrador de redes hábil puede usar estas herramientas en su red privada para descubrir los puntos potenciales donde esta debilitada su seguridad y así determina que servidores necesitan ser remendados y actualizados en el software.

Acceso a sistemas protegidos

El intruso utiliza los resultados obtenidos a través de las pruebas para poder intentar acceder a los servicios específicos de un sistema.

Después de tener el acceso al sistema protegido, el hacker tiene disponibles las siguientes opciones:

- Puede atentar destruyendo toda evidencia del asalto y además podrá crear nuevas fugas en el sistema o en partes subalternas con el compromiso de seguir teniendo acceso sin que el ataque original sea descubierto.
- Pueden instalar paquetes de sondeo que incluyan códigos binarios conocidos como “Caballos de Troya” protegiendo su actividad de forma transparente. Los paquetes de sondeo colectan las cuentas y contraseñas para los servicios de Telnet y FTP permitiendo al hacker expandir su ataque a otras maquinas.
- Pueden encontrar otros servidores que realmente comprometan al sistema. Esto permite al hacker explotar vulnerablemente desde un servidor sencillo todos aquellos que se encuentren a través de la red corporativa.
- Si el hacker puede obtener acceso privilegiado en un sistema compartido, podrá leer el correo, buscar en archivos

3.1.3.7 Explotando el Nivel de Aplicación

Autenticación en VoIP

En toda comunicación, servicio o transmisión de dato existe la necesidad de demostrar que los clientes son quien dicen ser. En VoIP la autenticación requiere que los dos dispositivos que se van a comunicar se autentiquen uno al otro antes de que se produzca cualquier intercambio de información. Esta autenticación mutua esta basada en algún tipo de secreto compartido que es conocido a priori por los dos.

Autenticación del protocolo SIP

El protocolo SIP utiliza la autenticación digest para comprobar la identidad de sus clientes. La autenticación digest fue originalmente diseñada para el protocolo HTTP, y se trata de un mecanismo bastante simple, basado en hashes que evita que se envíe la contraseña de los usuarios en texto claro. Cuando el servidor quiere autenticar un usuario genera un desafío digest que envía al usuario. Un ejemplo de desafío podría ser:

Digest realm="iptel.org", qop="auth,auth-int",
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093", opaque="", algorithm=MD5

Destacar que **nonce** es la cadena que genera como desafío utilizando el algoritmo MD5 de algún otro dato.

Después de recibir el desafía el UA pedirá al usuario el nombre y la contraseña (si no están presentes en la configuración del dispositivo) y a partir de ellos y del desafío enviado por el servidor generará una respuesta digest como la siguiente:

Digest username="jan", realm="iptel.org",
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093", uri="sip:iptel.org",
qop=auth, nc=00000001, cnonce="0a4f113b",
response="6629fae49393a05397450978507c4ef1", opaque=""

De una forma similar el campo respones contendrá la respuesta generada por el UA. Cabe destacar el significado del uri que indica la dirección sip a la que se quiere acceder y el cnonce que es una cadena utilizada por el cliente y el servidor que ofrece cierta protección de integridad al mensaje.

Cuando recibe la respuesta del cliente, el servidor realiza exactamente los mismos pasos. Generando una respuesta digest a partir del desafío y del password del usuario que tiene almacenado en su configuración. Si el hash generado coincide con la respuesta del cliente, el usuario acaba de autenticarse demostrando ser quien dice ser. Cuando el servidor SIP recibe alguna petición SIP, comprueba si en el mensaje se encuentran las credenciales que autentiquen al usuario, en caso contrario, generará un mensaje de error 401 Unauthorized al cliente incluyen el desafió digest para iniciar el proceso de autenticación.

El siguiente ejemplo muestra un mensaje REGISTER que contiene las credenciales digest.

REGISTER sip:iptel.org SIP/2.0.
Via: SIP/2.0/UDP 195.37.78.121:5060.
From: sip:jan@iptel.org.
To: sip:jan@iptel.org.
Call-ID: 003094c3-bcfea44f-40bdf830-2a557714@195.37.78.121.
CSeq: 102 REGISTER.
User-Agent: CSCO/4.
Contact: <sip:jan@195.37.78.121:5060>.
Authorization: Digest username="jan",realm="iptel.org",
uri="sip:iptel.org",response="dab81127b9a7169ed57aa4a6ca146184",
nonce="3f9fc0f9619dd1a712b27723398303ea436e839a",algorithm=md5.
Content-Length: 0.
Expires: 10.

3.1.3.7.1 Crackeo de contraseñas SIP

Una vez entendido el proceso de autenticación se demostrara los métodos y las herramientas para romper esa autenticación y crackear los hashes digest con el fin de obtener el password de un usuario y poder utilizar la identidad de la víctima de forma maliciosa. Entre las herramientas se debe tener SIPCrack , que como su nombre indica, crackea las contraseñas del protocolo SIP en Linux. Contiene dos programas sipdump para esnifar los hashes de la autenticación y sipcrack para crackear los logins capturados. Se puede descargar de las siguientes direcciones: página oficial http://www.codito.de o PacketStorm http://packetstormsecurity.org.

En caso de tener una vez más en redes conmutadas puede que sea necesario el uso de herramientas como ettercap para realizar la técnica de man in the middle y poder esnifar el tráfico necesario.

El programa sipdump actúa a modo de sniffer, analizando el tráfico y extrayendo autenticaciones SIP que encuentre.

```
# ./sipdump -i eth0 -d captura.dump
SIPdump 0.1 ( MaJoMu | www.remote-exploit.org )
* Using dev 'eth0' for sniffing
* Starting to sniff with filter 'tcp or udp'
```

sipdump puede también analizar una captura realizada de algún otro sniffer como tcpdump. Localiza los paquetes SIP dentro de la captura, los decodifica y extrae los logias que encuentre.

 # ./sipdump -f capturaSIP.pcap -d fichdump
SIPdump 0.1 (MaJoMu | www.remote-exploit.org)
** Using tcpdump data file 'capturaSIP.pcap' for sniffing*
** Starting to sniff with filter 'tcp or udp'*
** Adding 192.168.0.35:50451 <-> 192.168.0.1:50195 to monitor list...id*
0
** New traffic on monitored connection 0 (192.168.0.35 -> 192.168.0.1)*
** Found challenge response (192.168.0.35:50451 <-> 192.168.0.1:50195)*
** Wrote sniffed login 192.168.0.35 -> 192.168.0.1 (User: '200') to*
dump file
** Exiting, sniffed 1 logins*
** Adding 192.168.1.35:50451 <-> 192.168.1.100:50195 to monitor*
list...id 0
** New traffic on monitored connection 0 (192.168.1.35 ->*
192.168.1.100)
** Found challenge response (192.168.1.35:50451 <->*
192.168.1.100:50195)
** Wrote sniffed login 192.168.1.35 -> 192.168.1.100 (User: '100') to*
dump file

Una vez que se tiene el hash de la contraseña del usuario, se pueden crackear de dos modos diferentes: Por fuerza bruta y utilizando diccionario. La forma de ejecutar sipcrack es la siguiente:

 # ./sipcrack -w /usr/share/dict/spanish -d captura.dump
SIPcrack 0.1 (MaJoMu | www.remote-exploit.org)
--
** Reading and parsing dump file...*
** Found Accounts:*

Num Server Client User Algorithm Hash
/ Password
1 192.168.1.100 192.168.1.35 100 MD5
140c0b72f294abd9f4e13eea081a0307
** Select which entry to crack (1 - 1): 1*
** Generating static MD5 hash...495ff79e6c8f0378a7c029289a444573*
** Starting bruteforce against user '100' (MD5 Hash:*
'140c0b72f294abd9f4e13eea081a0307')
** Loaded wordlist: '/usr/share/dict/spanish'*
** Tried 47492 passwords in 1 seconds*
** Found password: 'hola'*
** Updating 'captura.dump'...done*

Como es normal, el éxito de este ataque dependerá de lo bueno y preciso que sea el diccionario que se utilice. Los ataques de fuerza bruta se encargan de probar todas las palabras generadas por todas las combinaciones posibles de cierto grupo de caracteres. Para ello vamos a utilizar uno de los crackeadores más famosos de la historia: John the Ripeer, el cual se puede descargar en la página oficial: http://www.openwall.com/john

John presenta diferentes opciones y formas de configurarse para conseguir el resultado y rendimiento optimo que no se tratara en este documento. Con el john the ripper generaremos un diccionario con todas las posibles combinaciones de cierto grupo de caracteres que se indique.

En el ejemplo solo letras y por defecto de hasta 5 caracteres:

 # john --incremental=alpha --stdout > fichero.txt
words: 11881376 time: 0:00:00:03 w/s: 3960458 current: uxjqv

 # ./sipcrack -w fichero.txt -d captura.dump
SIPcrack 0.1 (MaJoMu | www.remote-exploit.org)

** Reading and parsing dump file...*
** Found Accounts:*
Num Server Client User

Algorithm Hash / Password

1 192.168.1.100 192.168.1.35 101 MD5

d666ff953dff9b05a54d0457ab671c78

2 192.168.1.100 192.168.1.35 200

PLAIN hola

3 192.168.1.100 192.168.1.35 200

PLAIN hola

4 192.168.1.100 192.168.1.35 101 MD5

da08487896afd6920a077661bfd3997d

** Select which entry to crack (1 - 4): 4*

** Generating static MD5 hash...495ff79e6c8f0378a7c029289a444573*

** Starting bruteforce against user '101' (MD5 Hash:*

'da08487896afd6920a077661bfd3997d')

** Loaded wordlist: 'fichero.txt'*

** Tried 5585 passwords in 0 seconds*

** Found password: 'asdfg'*

** Updating 'captura.dump'...done*

3.3 Como defenderse

Lo primero que se debe tener en mente a la hora de leer sobre VoIP es la encriptación. Aunque lógicamente no es sencillo capturar y decodificar los paquetes de voz, puede hacerse. Y encriptar es la única forma de prevenirse ante un ataque. Desafortunadamente, toma ancho de banda. Existen múltiples métodos de encriptación o posibilidades de encriptación: VPN (virtual personal network), el protocolo Ipsec (IP segura) y otros protocolos como SRTP (secure RTP). La clave, de cualquier forma, es elegir un algoritmo de encriptación rápido, eficiente, y emplear un procesador dedicado de encriptación.

Esto debería aliviar cualquier riesgo de amenaza. Otra opción podría ser QoS (Quality of Service); los requerimientos para QoS asegurarán que la voz se maneja siempre de manera oportuna, reduciendo la pérdida de calidad.

Lo próximo, como debería esperarse, podría ser el proceso de securizar todos los elementos que componen la red VoIP: servidores de llamadas, routers, switches, centros de trabajo y teléfonos. Necesitas configurar cada uno de esos dispositivos para asegurarte de que están en línea con tus demandas en términos de seguridad. Los servidores pueden tener pequeñas funciones trabajando y sólo abiertos los puertos que sean realmente necesarios. Los routers y switches deberían estar configurados adecuadamente, con acceso a las listas de control y a los filtros. Todos los dispositivos deberían estar actualizados en términos de parches y actualizaciones. Se trata del mismo tipo de precauciones que podrías tomar cuando añades nuevos elementos a la red de datos; únicamente habrá que extender este proceso a la porción que le compete a la red VoIP. Tal como se ha mencionado, la disponibilidad de la red VoIP es otra preocupación. Una pérdida de potencia puede provocar que la red se caiga y los ataques DdoS son difíciles de contrarrestar. Aparte de configurar con propiedad el router, recordemos que estos ataques no solo irán dirigidos a los servicios de datos, sino también a los de voz.

Por último, podemos emplear un firewall y un IDS (Intrusion Detection System) para ayudar a proteger la red de voz. Los firewalls de VoIP son complicados de manejar y tienen múltiples requerimientos. Los servidores de llamada están constantemente abriendo y cerrando puertos para las nuevas conexiones. Este elemento dinámico hace que su manejo sea más dificultoso. Pero el coste está lejos de verse oscurecido por la cantidad de beneficios. Un IDS puede monitorizar la red para detectar cualquier anomalía en el servicio o un abuso potencial. Las advertencias son una clave para prevenir los ataques posteriores.

3.3.1 IPSec

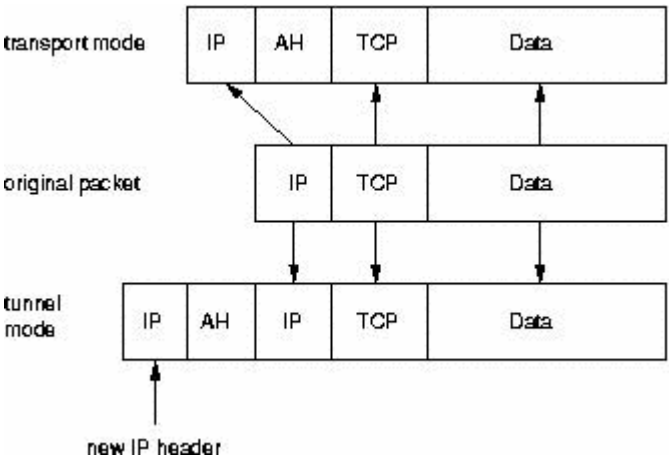
La meta de este protocolo es proporcionar varios servicios de seguridad para el tráfico de la capa IP, tanto a través de IPv4 e IPv6. Los componentes fundamentales de la arquitectura de seguridad IPSec son los siguientes:

- Protocolos de Seguridad: Cabecera de autenticación (AH) y los Datos Seguros Encapsulados (ESP).
- Asociaciones de Seguridad.
- Manejo de Clave: manual y automática (Internet Key Exchange, IKE).
- Algoritmos para la autenticación y encriptación.

IPsec es una extensión al protocolo IP que proporciona seguridad a IP y a los protocolos de capas superiores. Fue desarrollado para el nuevo estándar IPv6 y después fue portado a IPv4. La arquitectura IPsec se describe en el RFC2401. Los siguientes párrafos dan una pequeña introducción a IPsec.

IPsec emplea dos protocolos diferentes - AH y ESP - para asegurar la autenticación, integridad y confidencialidad de la comunicación. Puede proteger el datagrama IP

completo o sólo los protocolos de capas superiores. Estos modos se denominan, respectivamente, modo túnel y modo transporte. En modo túnel el datagrama IP se encapsula completamente dentro de un nuevo datagrama IP que emplea el protocolo IPsec. En modo transporte IPsec sólo maneja la carga del datagrama IP, insertándose la cabecera IPsec entre la cabecera IP y la cabecera del protocolo de capas superiores.



(Figura 3-3)

IPsec: modos túnel y transporte

Para proteger la integridad de los datagramas IP, los protocolos IPsec emplean códigos de autenticación de mensaje basados en resúmenes (HMAC - Hash Message Authentication Codes). Para el cálculo de estos HMAC los protocolos HMAC emplean algoritmos de resumen como MD5 y SHA para calcular un resumen basado en una clave secreta y en los contenidos del datagrama IP. El HMAC se incluye en la cabecera del protocolo IPsec y el receptor del paquete puede comprobar el HMAC si tiene acceso a la clave secreta.

Para proteger la confidencialidad de lo datagramas IP, los protocolos IPsec emplean algoritmos estándar de cifrado simétrico. El estándar IPsec exige la implementación de NULL y DES. En la actualidad se suelen emplear algoritmos más fuertes: 3DES, AES y Blowfish.

Para protegerse contra ataques por denegación de servicio, los protocolos IPsec emplean ventanas deslizantes. Cada paquete recibe un número de secuencia y sólo se acepta su recepción si el número de paquete se encuentra dentro de la ventana o es posterior. Los paquetes anteriores son descartados inmediatamente. Esta es una medida de protección eficaz contra ataques por repetición de mensajes en los que el atacante almacena los paquetes originales y los reproduce posteriormente.

Para que los participantes de una comunicación puedan encapsular y desencapsular los paquetes IPsec, se necesitan mecanismos para almacenar las claves secretas, algoritmos y direcciones IP involucradas en la comunicación. Todos estos parámetros se almacenan en asociaciones de seguridad (SA - Security Associations). Las asociaciones de seguridad, a su vez, se almacenan en bases de datos de asociaciones de seguridad (SAD - Security Asocciation Databases).

Cada asociación de seguridad define los siguientes parámetros:

- Dirección IP origen y destino de la cabecera IPsec resultante. Estas son las direcciones IP de los participantes de la comunicación IPsec que protegen los paquetes.
- Protocolo IPsec (AH o ESP). A veces, se permite compresión (IPCOMP).
- El algoritmo y clave secreta empleados por el protocolo IPsec.
- Índice de parámetro de seguridad (SPI - Security Parameter Index). Es un número de 32 bits que identifica la asociación de seguridad.

Algunas implementaciones de la base de datos de asociaciones de seguridad permiten almacenar más parámetros:

- Modo IPsec (túnel o transporte)
- Tamaño de la ventana deslizante para protegerse de ataques por repetición.
- Tiempo de vida de una asociación de seguridad.

En una asociación de seguridad se definen las direcciones IP de origen y destino de la comunicación. Por ello, mediante una única SA sólo se puede proteger un sentido del tráfico en una comunicación IPsec full duplex. Para proteger ambos sentidos de la comunicación, IPsec necesita de dos asociaciones de seguridad unidireccionales.

Las asociaciones de seguridad sólo especifican cómo se supone que IPsec protegerá el tráfico. Para definir qué tráfico proteger, y cuándo hacerlo, se necesita información adicional. Esta información se almacena en la política de seguridad (SP - Security Policy), que a su vez se almacena en la base de datos de políticas de seguridad (SPD - Security Policy Database).

Una política de seguridad suele especificar los siguientes parámetros:

- Direcciones de origen y destino de los paquetes por proteger. En modo transportes estas serán las mismas direcciones que en la SA. En modo túnel pueden ser distintas.
- Protocolos y puertos a proteger. Algunas implementaciones no permiten la definición de protocolos específicos a proteger. En este caso, se protege todo el tráfico entre las direcciones IP indicadas.
- La asociación de seguridad a emplear para proteger los paquetes.

La configuración manual de la asociación de seguridad es proclive a errores, y no es muy segura. Las claves secretas y algoritmos de cifrado deben compartirse entre todos los participantes de la VPN. Uno de los problemas críticos a los que se enfrenta el administrador de sistemas es el intercambio de claves: ¿cómo intercambiar claves simétricas cuando aún no se ha establecido ningún tipo de cifrado?

Para resolver este problema se desarrolló el protocolo de intercambio de claves por Internet (IKE - Internet Key Exchange Protocol). Este protocolo autentica a los participantes en una primera fase. En una segunda fase se negocian las asociaciones de seguridad y se escogen las claves secretas simétricas a través de un intercambio de

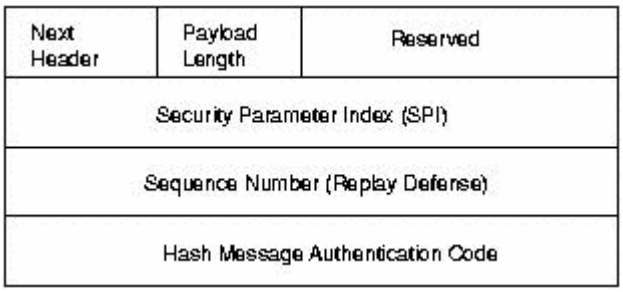
claves Diffie Hellmann. El protocolo IKE se ocupa incluso de renovar periódicamente las claves para asegurar su confidencialidad.

Los protocolos IPsec

La familia de protocolos IPsec está formada por dos protocolos: el AH (Authentication Header - Cabecera de autenticación) y el ESP (Encapsulated Security Payload - Carga de seguridad encapsulada). Ambos son protocolos IP independientes. AH es el protocolo IP 51 y ESP el protocolo IP 50.

AH - Cabecera de autenticación

El protocolo AH protege la integridad del datagrama IP. Para conseguirlo, el protocolo AH calcula una HMAC basada en la clave secreta, el contenido del paquete y las partes inmutables de la cabecera IP (como son las direcciones IP). Tras esto, añade la cabecera AH al paquete.



(Figura 3-4)

La cabecera AH protege la integridad del paquete

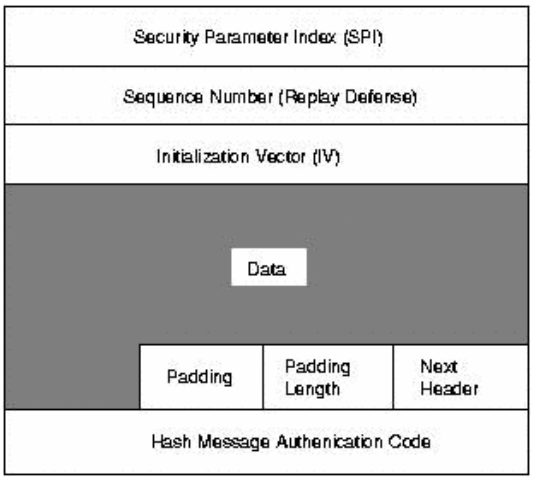
La cabecera AH mide 24 bytes. El primer byte es el campo Siguiente cabecera. Este campo especifica el protocolo de la siguiente cabecera. En modo túnel se encapsula un datagrama IP completo, por lo que el valor de este campo es 4. Al encapsular un datagrama TCP en modo transporte, el valor correspondiente es 6. El siguiente byte especifica la longitud del contenido del paquete. Este campo está seguido de dos bytes reservados. Los siguientes 4 bytes especifican en Índice de Parámetro de Seguridad (SPI). El SPI especifica la asociación de seguridad (SA) a emplear para el desencapsulado del paquete. El Número de Secuencia de 32 bit protege frente a ataques por repetición. Finalmente, los últimos 96 bit almacenan el código de resumen para la autenticación de mensaje (HMAC). Este HMAC protege la integridad de los paquetes ya que sólo los miembros de la comunicación que conozcan la clave secreta pueden crear y comprobar HMACs.

Como el protocolo AH protege la cabecera IP incluyendo las partes inmutables de la cabecera IP como las direcciones IP, el protocolo AH no permite NAT. NAT (Network address translation - Traducción de direcciones de red) también conocido como Enmascaramiento de direcciones reemplaza una dirección IP de la cabecera IP (normalmente la IP de origen) por una dirección IP diferente. Tras el intercambio, la HMAC ya no es válida. La extensión a IPsec NAT-transversal implementa métodos que evitan esta restricción.

ESP - Carga de Seguridad Encapsulada

El protocolo ESP puede asegurar la integridad del paquete empleando una HMAC y la confidencialidad empleando cifrado. La cabecera ESP se genera y añade al paquete tras cifrarlo y calcular su HMAC. La cabecera ESP consta de dos partes.

La cabecera ESP



(Figura 3-5)

Los primeros 32 bits de la cabecera ESP especifican el Índice de Parámetros de Seguridad (SPI). Este SPI especifica qué SA emplear para desencapsular el paquete ESP. Los siguientes 32 bits almacenan el Número de Secuencia. Este número de secuencia se emplea para protegerse de ataques por repetición de mensajes. Los siguientes 32 bits especifican el Vector de Inicialización (IV - Initialization Vector) que se emplea para el proceso de cifrado. Los algoritmos de cifrado simétrico pueden ser vulnerables a ataques por análisis de frecuencias si no se emplean IVs. El IV asegura que dos cargas idénticas generan dos cargas cifradas diferentes.

IPsec emplea cifradores de bloque para el proceso de cifrado. Por ello, puede ser necesario rellenar la carga del paquete si la longitud de la carga no es un múltiplo de la longitud del paquete. En ese caso se añade la longitud del relleno (pad length). Tras la longitud del relleno se coloca el campo de 2 bytes Siguiente cabecera que especifica la siguiente cabecera. Por último, se añaden los 96 bit de HMAC para asegurar la integridad del paquete. Esta HMAC sólo tiene en cuenta la carga del paquete: la cabecera IP no se incluye dentro de su proceso de cálculo.

El uso de NAT, por lo tanto, no rompe el protocolo ESP. Sin embargo, en la mayoría de los casos, NAT aún no es compatible en combinación con IPsec. NAT- Transversal ofrece una solución para este problema encapsulando los paquetes ESP dentro de paquetes UDP.

El protocolo IKE

El protocolo IKE resuelve el problema más importante del establecimiento de comunicaciones seguras: la autenticación de los participantes y el intercambio de claves simétricas. Tras ello, crea las asociaciones de seguridad y rellena la SAD. El protocolo IKE suele implementarse a través de servidores de espacio de usuario, y no suele implementarse en el sistema operativo. El protocolo IKE emplea el puerto 500 UDP para su comunicación.

El protocolo IKE funciona en dos fases. La primera fase establece un ISAKMP SA (Internet Security Association Key Management Security Association - Asociación de seguridad del protocolo de gestión de claves de asociaciones de seguridad en Internet). En la segunda fase, el ISAKMP SA se emplea para negociar y establecer las SAs de IPsec.

La autenticación de los participantes en la primera fase suele basarse en claves compartidas con anterioridad (PSK - Pre-shared keys), claves RSA y certificados X.509.

La primera fase suele soportar dos modos distintos: modo principal y modo agresivo. Ambos modos autentican al participante en la comunicación y establecen un ISAKMP SA, pero el modo agresivo sólo usa la mitad de mensajes para alcanzar su objetivo. Esto, sin embargo, tiene sus desventajas, ya que el modo agresivo no soporta la protección de identidades y, por lo tanto, es susceptible a un ataque man-in-the-middle (por escucha y repetición de mensajes en un nodo intermedio) si se emplea junto a claves compartidas con anterioridad (PSK). Pero sin embargo este es el único objetivo del modo agresivo, ya que los mecanismos internos del modo principal no permiten el uso de distintas claves compartidas con anterioridad con participantes desconocidos. El modo agresivo no permite la protección de identidades y transmite la identidad del cliente en claro. Por lo tanto, los participantes de la comunicación se conocen antes de que la autenticación se lleve a cabo, y se pueden emplear distintas claves pre-compartidas con distintos comunicantes.

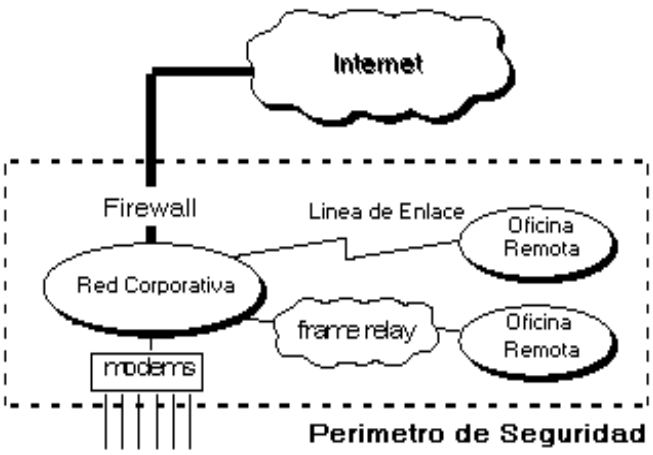
En la segunda fase, el protocolo IKE intercambia propuestas de asociaciones de seguridad y negocia asociaciones de seguridad basándose en la ISAKMP SA. La

ISAKMP SA proporciona autenticación para protegerse de ataques man-in-the-middle. Esta segunda fase emplea el modo rápido.

Normalmente, dos participantes de la comunicación sólo negocian una ISAKMP SA, que se emplea para negociar varias (al menos dos) IPsec SAs unidireccionales.

3.3.2 Firewalls

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.



(Figura 3-6)

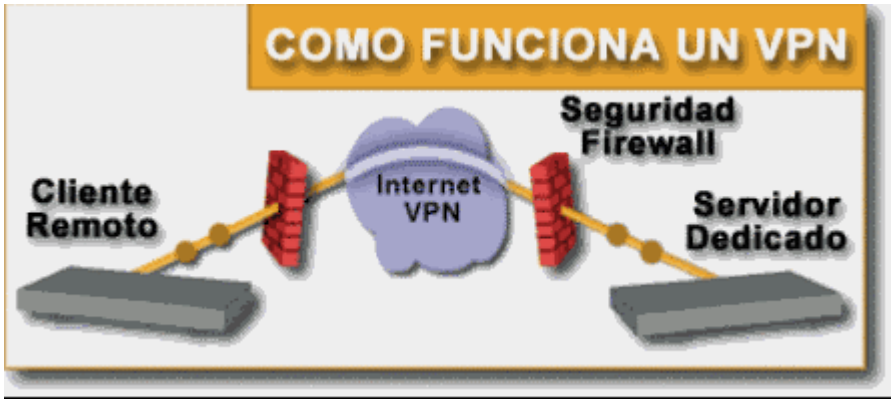
La Política De Seguridad Crea Un Perímetro De Defensa.

Esto es importante, ya que se debe notar que un firewall de Internet no es justamente un ruteador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial-in y dial-out, reglas de enciptacion de datos y discos, normas de protección de virus, y entrenamiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad. Un firewall de Internet sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda.

3.3.3 Redes Privadas Virtuales – VPN

Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte.

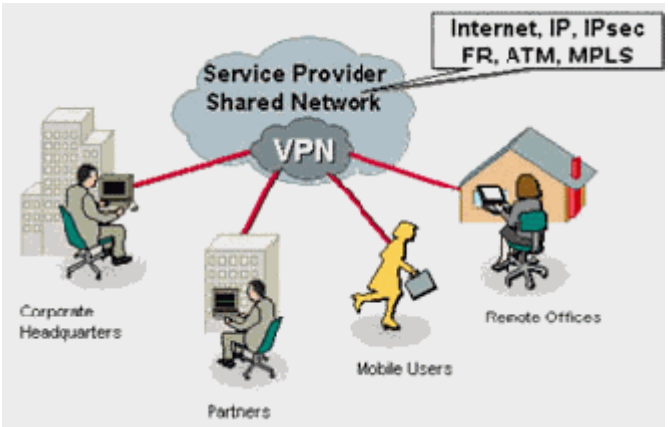
Los paquetes de datos de la red privada viajan por medio de un “túnel” definido en la red pública.



(Figura 3-7)

En la figura anterior se muestra como viajan los datos a través de una VPN ya que el servidor dedicado es del cual parten los datos, llegando a firewall que hace la función de una pared para engañar a los intrusos a la red, después los datos llegan a nube de internet donde se genera un túnel dedicado únicamente para nuestros datos para que estos con una velocidad garantizada, con un ancho de banda también garantizado y lleguen a su vez al firewall remoto y terminen en el servidor remoto.

Las VPN pueden enlazar oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos como internet, IP, Ipsec, Frame Relay, ATM como lo muestra la figura siguiente.



(Figura 3-8)

4.0 Marco regulatorio de la telefonía IP en Chile

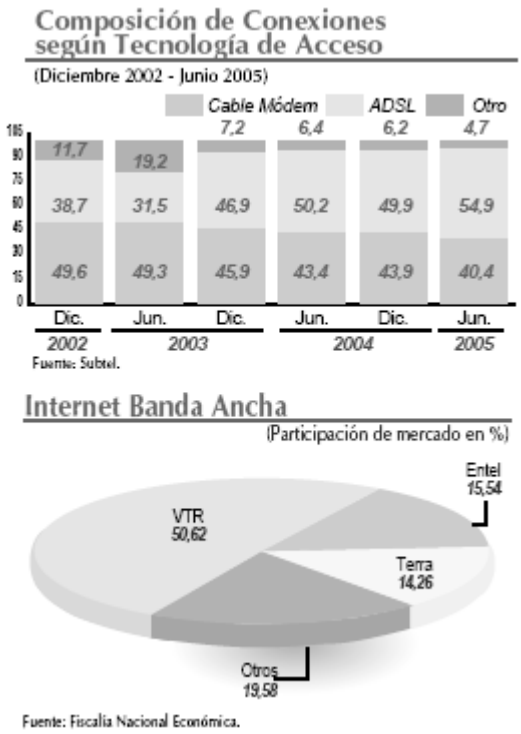
En siguiente capitulo es un resumen de un especial de telefonía ip en chile, es entrevistado el subsecretario de Telecomunicaciones, Pablo Bello,

La telefonia IP viajara a través de la linea adsl ,por lo tanto según la empresa que preste el servicio tendrá calidad de servicio o no,tambien dependiendo de la llamada si es nacional,local o internacional, por lo que no todas la empresas proveedoras de internet prestaran este servicio y como es obio nadie quiere que aparezca otro competidor de telefonia desplazando sus redes de telefonia y ocupando sus redes de internet

Habrá concesión para esta tecnología. Hay concesiones hace tiempo sobre telefonía IP que no utilizan internet, sino que usan este protocolo para redes dedicadas.
Lo que se está regulando es la red pública de internet que utiliza IP, se va atener un título concesional adecuado para aquellos operadores de telefonía sobre internet que cumplan con estas condiciones: interconectarse a la red pública y tener numeración telefónica.

Hay un segmento de la población con ingresos medios y altos que tiene competencia, pero hay una gran mayoría que no puede optar por distintos proveedores y que no tiene acceso a internet. El modelo actual supone que los sectores de mayores ingresos comparten y ayudan a financiar a los de menores ingresos, mediante el subsidio cruzado al interior de una misma compañía. Es decir, se calcula una tarifa promedio y aquellos que hacen más uso de la tecnología subsidian a aquellos que la utilizan

menos. Con lo que se está dando hoy, este modelo deja de funcionar y esto significa que los incentivos para invertir en tecnología y servicios en los sectores de menores ingresos dejan de estar presentes. Con eso se pretende tener una telefonia integral para todos



(Figura 4.0)

Cobro en la telefonía IP

SUBTEL ha propuesto clasificar las aplicaciones de VoIP en tres categorías con diferentes características y así regular estos servicios respectivamente. Las categorías incluyen: (1) Servicio Web unidireccional (PC-a-PC; PC-a-Red Pública); 2) Servicio Privado y/o Restringido (para grupo privado que no requiere numeraciones) y 3) Servicio Público (acceso directo o con acceso Internet, asignación numérica e interconexiones con Red Pública). Dentro de estas propone no regular los servicios del tipo 1) y 2). Para la categoría 3), SUBTEL propone hacer un tratamiento distinto a los servicios VoIP prestados a través de un acceso directo o a través de un acceso a través de Internet, esta última modalidad permitida bajo una Concesión de Servicio Público de Telecomunicaciones de Voz sobre Banda Ancha ("SPTVBA"). SUBTEL desarrolla así, un mecanismo para minimizar la regulación necesaria para los servicios que no requieren asignación de numeración nacional y así enfocar los objetivos de regulación apropiados para los servicios que si necesiten numeración nacional.

Para los servicios VoIP que requieran recursos de numeración en Chile y que se ofrecerían al público para interconectarlos con la Red Pública, SUBTEL propone que estos sean tratados como servicios públicos. Bajo esta categoría, AT&T sugiere que se aplique un enfoque regulatorio mínimo que asegure que la telefonía tradicional del Siglo XX no impida innecesariamente la innovación de las nuevas tecnologías VoIP del Siglo XXI. Con este objetivo en mente, la creación de la concesión del SPTVBA demuestra un prometedor reconocimiento a que las aplicaciones avanzadas de VoIP utilizando acceso IP no deberían ser regulados de la misma manera que la telefonía tradicional o que otros proveedores con "acceso directo" que usen su propia red.

Numeración:

Numeración no-geográfica:

SUBTEL ha propuesto establecer una numeración nacional específica para los operadores SPTVBA que serían utilizados para identificar los servicios VoIP que requieren numeración.

La numeraciones no-geográficas, particularmente creará eficiencias que permitan a los nuevos operadores de servicios VoIP usar y obtener estos rangos de números. Para las aplicaciones de VoIP que se apoyan fuertemente en el servicio por su movilidad o larga distancia, una numeración no-geográfica será preferible dada la independencia de esta numeración por distancia o ubicación específica. Adicionalmente, durante la fase inicial de adopción de servicios VoIP, una numeración no-geográfica podría ser preferible para los clientes y el organismo regulador al mismo tiempo al señalar una clara intención por parte del organismo regulador y el supuesto conocimiento por parte de los consumidores que estos rangos de números son nuevos y tendrán un bajo nivel de regulación.

Al establecer este rango, SUBTEL debería tratar de asegurar que los cargos por llamados a números no-geográficos sean competitivamente equivalentes al estándar nacional de cargos para los llamados a números geográficos, de ser así, los cargos inapropiadamente altos podrían afectar el desarrollo y la aceptación por parte de los clientes para los servicios VoIP.

La disponibilidad de numeraciones geográficas facilitará la adopción de VoIP, la cual a su vez promoverá servicios eficientes, innovadores y competitivos. Para los usuarios que se están acostumbrandos a un rango de numeración conocido, la numeración geográfica puede ser preferible, restricciones excesivas en el cual los operadores pueden obtener estas numeraciones podrían elevar una barrera innecesaria para la entrada a niveles competitivos. Cuando un operador VoIP ofrece numeraciones geográficas, existe una serie de alternativas que implican un bajo nivel de regulación para proteger los intereses de los usuarios. En primer lugar, la percepción de calidad de los usuarios y las características asociadas con el servicio no deberían cambiar en base a su naturaleza de asignación geográfica o no-geográfica, sino que en como el operador del servicio eduque a sus potenciales clientes sobre los atributos de su servicio específico – con limitaciones y beneficios. No sería una buena política regulatoria de largo plazo para una prometedora tecnología emergente asumir que servicios con características limitadas, están en los rangos de numeración no-geográficas y que los servicios que son un sustituto efectivo a la telefonía conmutada tradicional están en las numeraciones geográficas. A medida que los servicios VoIP avancen y nuevos operadores se incorporen, esta distinción será incrementalmente menos relevante.

Para principio del 2007 empezaran a analizar el tema para tener un proyecto robusto de recuperación de inversiones en las comunas mas pobres, para que los empresarios que quieran invertir en telefonía IP obtengan ganancias y se abra el mercado para todos

4.0 Costos

Costos de una central de Telefonía IP comercial en comparación con una central domestica

Central de Telefonía IP Comercial

Item	Descripción de central IP-PBX
IP-PBX VoIPPLus Telco	Dell PowerEdge 9G 1950
Capacidad:	2 x Procesador Xeox 3.0Ghz
50 entronques SIP	2 GB Ram
concurrentes	Disco duro 73 Gb x 2 (raid 1)
	Formato 1U/Rackeable
	Fuente de Poder Redundante
	Licenciamiento CODECS/G.729
	4 x puertas E1/Pri
	Instalación y configuración
Respuestos	4 x puertas E1/Pri (no compatible con E1 corporativo)
Total Neto US$	***$ 14.433***

Nota: Los valores son Neto y no incluyen IVA.

El costo de la central de telefonía IP es de $14.433 dolares , 7.317.531 pesos, este valor corresponde a 50 teléfonos que se pueden configurar en la central, la mantención de la central es de $200.000 mensuales , que incluye los 7 días de la semana , los 30 dias del mes.

Central de telefonía domestica

La central domestica tiene un costo por cada teléfono de $20.000 pesos , que es lo que cuesta la tarjeta para conectarla a la red Telefónica conmutada, con un computador de 1 Gb de RAM , de un costo aproximado de $150.000 pesos , ya tenemos la central de telefonía IP, con un costo no mayor a los &170.000 pesos.

La capacitación para el uso de la central es de $50.000, que incluye un manejo de la central a nivel de configuración de script, que es mas complicado que la configuración de la central comercial, y la manutención para que el servicio funcione correctamente

5.0 Conclusiones

Lo mas importante de la telefonía IP en comparación de la telefonía tradicional es que la telefonía IP es mas económica su implementación, no requiere de una línea dedicada como la telefonía tradicional, y es escalable para brindar al usuario todas las prestaciones que se requiera dar.

Hoy en día el costo de implementar una central telefónica es mucho menor que antiguamente ya que no se requiere de mucho recurso para hacerlo, como se demostro en este trabajo de titulacion

Uno de los aspectos relevantes para que la telefonía IP funcione correctamente es el BW que esta disponible para la llamada y que no exista atochamiento en las redes, ya que si esto ocurre la información puede llegar desfasada y los buffer (almacenadores de información) pueden no soportar tanto retardo y descartar paquetes, con lo que se pierde parte de la información y por lo tanto parte de la comunicación.

Para implementar este tipo de telefonía se debe montar sobre una red robusta, esto se puede implementar aplicando calidad de servicio, para priorizar los paquetes de voz sobre los de datos, implementando un codec que requiera del menor BW para su transmisión, implementando VPN para asegurar una velocidad de transmisión de la voz, esto podría ser suficiente para que la voz llegue en forma aceptable hasta el receptor.

La utilización del protocolo SIP a cambio del protocolo H323 es que este protocolo H323 es un protocolo complejo y extenso, por lo que implementarlo es un poco complicado ya que consume mucho recurso de la red, porque posee sus propios protocolos, en cambio SIP funciona sobre protocolos ya existentes, por esto es mas factible implementar en cualquier parte SIP

En el único aspecto que decae esta tecnología es en la parte de seguridad, ya que al no tener una línea dedicada como en la telefonía tradicional, los paquetes viajan por todas las redes y estos pueden ser capturados en cualquier parte de la red que no este protegida, lo cual hace vulnerable la información de la conversación.

Todavía en telefonía IP hay una discusión en el cobro ya que el cobro de trafico ip a IP no se va a normar se dará como una aplicación mas de internet, pero el trafico hacia la PSTN va a estar normado, en esta parte se llega a una discusión , si la numeración se cobrara igual que a nivel nacional o como una llamada local , y si la numeración va a ser geografica o una nueva, esto apunta tambien a los posibles clientes, el paso de la numeración acostumbrada a una atipica, pero lo que si es conocido es que esta regulación es por el momento, ya que mas adelante no se preocupara por esta numeración por la migración que esta ocurriendo hacia la telefonia IP

Los proveedores de telefonía en Chile como CTC van a tratar de lidiar con esta telefonía, tratando de bloquearla a nivel de puerto , firewall, provocando colisiones de paquetes, cuellos de botella, trafico innecesario, priorizacion de paquetes, por esto va ha tener una larga batalla jurídica hasta que las compañías de telefonía tradicional puedan dejar acceder en sus redes en forma normal esta tecnología

A través de las redes de acceso, como es MPLS, se ha dado una mayor calidad de servicio a cada usuario, ya que estas redes manejan prioridad en las colas de paquetes, con esto se evita que se produzca un retardo en la llamada y una degradación del servicio, por lo tanto el servicio se torna mas robusto.

La central de telefonía domestica en comparación con la central de telefonía Ip comercial es mucho mas barata, ya que los costos que tiene por teléfono no sobrepasan los $20000 pesos , lo unico inconveniente es la gestión que tiene para el manejo de la central, la cual debe ser con script, pero para solucionar este problema existen capacitaciones que debe dar el proveedor que entregue este producto, las soluciones de telefonía que entrega cada una son iguales, ya que se entregan sobre la misma plataforma y el hardware es similar en todas las tarjetas, por esto no es que se este comprando alo mas malo con una central de telefonía IP domestica, sino que es mas económica solamente

Hacer este proyecto de tesis me sirvió para conocer, esta tecnología y saber hacia donde apunta la tecnología de hoy, para desarrollarme en la compañía Telefónica del Sur, con los conocimientos necesarios para entender que hacen los equipos y poder encontrar fallas en estos, en lo personal me enriqueció hacer este proyecto para ser mas ordenado con mi tiempo y fortalecer el área de telecomunicaciones que es donde en este momento me desenvuelvo.

6.0 Referencias Bibliográficas

Libros

- Título: Asterisk el The Future of Telephony Jim Van Meggelen, Jared Smith, y Leif Madsen

- Voice over IP Fundamentals Jonathan Davidson , James Peters , Brian Gracely .

-Converged Networks and Services: Internetworking IP and the PSTN Igor Faynberg, Lawrence Gabuzda, Hui-Lan Lu

-Título: Ubuntu primeros pasos Ubuntu-es | Portal hispano de Ubuntu www.ubuntu-es.org/

- Especial de telefonia IP ,Diario: Estrategia,- Titulo: Nueva Normativa Para Telefonía IP Incluirá Régimen de Concesiones

- Asterisk Guia de la Configuración V.Office Networks

- Título: Curso de interplus de telefonía IP, realizado en la empresa telefónica del sur en el mes de junio del presente año

- Título: Internet
  - http://www.asterisk.org/
  - http://www.digium.com/en/index.php
  - http://www.asterisk-guru.com.ar/

7.0 Anexo

Configuración

Sip.conf

[general]

videosupport=yes

port=5060

bindaddr = 0.0.0.0

allow=ulaw

nat=no

[33]

type=friend

language=es

username=33

secret=1234

host=dynamic

nat=no

dtmfmode=rfc2833

qualify=yes

canreinvite=no

context=cero

allow=h263

allow=h263p

mailbox=77@mb_tutorial

```
[34]
type=friend
language=es
username=34
secret=1234
host=dynamic
nat=no
dtmfmode=rfc2833
qualifi=yes
canreinvite=no
context=cero
allow=h263
allow=h263p
mailbox=78@mb_tutorial


[35]
type=friend
language=es
username=35
secret=1234
host=dynamic
```

nat=no

dtmfmode=rfc2833

qualifi=yes

canreinvite=no

context=cero

allow=h263

allow=h263p

mailbox=79@mb_tutorial

[36]

type=friend[general]

videosupport=yes

port=5060

bindaddr = 0.0.0.0

allow=ulaw

nat=no

[33]

type=friend

language=es

username=33

secret=1234

host=dynamic

nat=no

dtmfmode=rfc2833

qualify=yes

canreinvite=no

context=cero

allow=h263

allow=h263p

mailbox=77@mb_tutorial

[general]

videosupport=yes

port=5060

bindaddr = 0.0.0.0

allow=ulaw

nat=no

[33]

type=friend

language=es

username=33

secret=1234

host=dynamic

nat=no

dtmfmode=rfc2833

qualify=yes

canreinvite=no

context=cero

allow=h263

allow=h263p

mailbox=77@mb_tutorial

[34]

type=friend

language=es

username=34

secret=1234

host=dynamic

nat=no

dtmfmode=rfc2833

qualifi=yes

canreinvite=no

context=cero

allow=h263

allow=h263p

mailbox=78@mb_tutorial

[35]

type=friend

language=es

username=35

secret=1234

host=dynamic

nat=no

dtmfmode=rfc2833

qualifi=yes

canreinvite=no

context=cero

allow=h263

allow=h263p

mailbox=79@mb_tutorial

[36]

type=friend

language=es

username=36

secret=1234

host=dynamic

nat=no

dtmfmode=rfc2833

qualifi=yes

canreinvite=no

context=cero

allow=h263

allow=h263p

mailbox=80@mb_tutorial

[34]

type=friend

language=es

username=34

secret=1234

host=dynamic

nat=no

dtmfmode=rfc2833

qualifi=yes

canreinvite=no

context=cero

allow=h263

allow=h263p

mailbox=78@mb_tutorial

[35]

type=friend

language=es

username=35

secret=1234

host=dynamic

nat=no

dtmfmode=rfc2833

qualifi=yes

canreinvite=no

context=cero

allow=h263

allow=h263p

mailbox=79@mb_tutorial

[36]

type=friend

language=es

username=36

secret=1234

host=dynamic

nat=no

dtmfmode=rfc2833

qualifi=yes

canreinvite=no

context=cero

allow=h263

allow=h263p

mailbox=80@mb_tutorial

language=es

username=36

secret=1234

host=dynamic

nat=no

dtmfmode=rfc2833

qualifi=yes

canreinvite=no

context=cero

allow=h263

allow=h263p

mailbox=80@mb_tutorial

Extensions.conf

[general]

```
static=yes
writeprotect=yes

[cero]
include => anexos
include => grabar
include => musica



include => grabar

exten => _33,1,Answer
exten => _33,2,Wait,3
exten => _33,3,Background(bienvenido)
exten => _33,4,Background(main-menu)
exten => _33,5,Background(momento-por-favor)
exten => _33,6,Background(press-1)
exten => _33,7,Background(atencion-publico)
exten => _33,n,Set(TIMEOUT(digit)=5)
exten => _33,n,Set(TIMEOUT(response)=10)
exten => _33,n,WaitExten
```

```
exten => _1,1,Goto(6000,1)



exten => _34,1,Dial(SIP/34,10,tT)
exten => _34,2,VoiceMail(78@mb_tutorial)
exten => _34,3,PlayBack(vm-goodbye)
exten => _34,4,Hangup

exten => _35,1,Dial(SIP/35,10,tT)
exten => _35,2,VoiceMail(79@mb_tutorial)
exten => _35,3,PlayBack(vm-goodbye)
exten => _35,4,Hangup

exten => _36,1,Dial(SIP/36,10,tT)
exten => _36,2,VoiceMail(80@mb_tutorial)
exten => _36,3,PlayBack(vm-goodbye)
exten => _36,4,Hangup
```

```
exten => _2999,1,VoicemailMain(77@mb_tutorial)
exten => _3000,1,VoicemailMain(78@mb_tutorial)
exten => _3001,1,VoicemailMain(79@mb_tutorial)
exten => _3002,1,VoicemailMain(80@mb_tutorial)
exten => _6000,1,MusicOnHold()


exten => 123,1,Goto(conf,1)
exten => conf,1,Answer
exten => conf,2,Playtones,ring
exten => conf,3,Wait,3
exten => conf,4,MeetMe(600|M)
exten => conf,5,Hangup


exten => 601,1,Playback(conf-thereare)
exten => 601,2,MeetMeCount(600,3)
exten => 601,3,Playback(conf-peopleinconf)

exten => 120,1,GotoIf($["${CALLERIDNUM}" = "36"]?3:2)
exten => 120,2,Hangup
exten => 120,3,Goto(33,1)

[grabar]
```

```
exten => 205,1,Answer

exten => 205,2,Wait(2)

exten => 205,3,Record(mensaje-inicio%d:gsm)

exten => 205,4,Wait(2)

exten => 205,5,Playback(${RECORDED_FILE})

exten => 205,6,Wait(2)

exten => 205,7,Hangup
```

Voicemail.conf

```
[general]

attach=yes

format=gsm

maxmessage=180

minmessage=5

[zonemessages]

Chile24=America/Chile|'vm-received'Q'digits/at'R

[mb_tutorial]

77 => 111,33,joel@server,tz=Chile|attach=yes
```

78 => 222,34,server@server,tz=Chile|attach=yes

79 => 333,35,juanito@server,tz=Chile|attach=yes

80 => 123,36,jose@server,tz=Chile|attach=yes

Esta es la configuración que utilizare en mi proyecto de tesis

Definición de Codec

CODEC comprime la secuencia de datos, y proporciona la cancelación del eco. **La compresión de la forma de onda representada puede permitir el ahorro del ancho de banda**. Esto es especialmente interesante en los enlaces de poca capacidad y permite tener un mayor numero de conexiones de VoIP simultaneamente. **Otra manera de ahorrar ancho de banda es el uso de la supresión del silencio, que es el proceso de no enviar los paquetes de la voz entre silencios en conversaciones humanas.**

A continuación se muestra una tabla resumen con los códecs más utilizados actualmente:

- El Bit Rate indica la cantidad de información que se manda por segundo.
- El Sampling Rate indica la frecuencia de muestreo de la señal vocal.(cada cuanto se toma una muestra de la señal analógica)
- El Frame size indica cada cuantos milisegundos se envia un paquete con la información sonora.
- El MOS indica la calidad general del códec (valor de 1 a 5)

Nombre	Estandarizado	Descripción	Bit rate (kb/s)	Sampling rate (kHz)	Frame size (ms)	Observaciones	MOS (Mean Opinion Score)
G.711 *	ITU-T	Pulse code modulation (PCM)	64	8	Muestreada	Tiene dos versiones u-law (US, Japan) y a-law (Europa) para muestrear la señal	4.1
G.721	ITU-T	Adaptive differential pulse code modulation (ADPCM)	32	8	Muestreada	Obsoleta. S e ha transformado en la G.726.	
G.722	ITU-T	7 kHz audio-coding within 64 kbit/s	64	16	Muestreada	Divide los 16 Khz en dos bandas cada una usando ADPCM	
G.722.1	ITU-T	Codificación a 24 y 32 kbit/s para sistemas sin manos con baja perdida de paquetes	24/32	16	20		
G.723	ITU-T	Extensión de la norma G.721 a 24 y 40 kbit/s para aplicaciones en circuitos digitales.	24/40	8	Muestreada	Obsoleta por G.726. Es totalmente diferente de G.723.1.	
G.723.1	ITU-T	Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s	5.6/6.3	8	30	Parte de H.324 video conferencing. Codifica la señal usando linear predictive analysis-by-synthesis coding. Para el codificador de high rate utiliza Multipulse Maximum Likelihood Quantization (MP-MLQ) y para el de low-rate usa Algebraic-Code-Excited Linear-Prediction (ACELP).	3.8-3.9
G.726	ITU-T	40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM)	16/24/32/40	8	Muestreada	ADPCM; reemplaza a G.721 y G.723.	3.85
G.727	ITU-T	5-, 4-, 3- and 2-bit/sample embedded adaptive	var.		Muestreada	ADPCM. Relacionada con G.726.	

		differential pulse code modulation (ADPCM)					
G.728	ITU-T	Coding of speech at 16 kbit/s using low-delay code excited linear prediction	16	8	2.5	CELP.	3.61
G.729 **	ITU-T	Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction (CS-ACELP)	8	8	10	Bajo retardo (15 ms)	3.92
GSM 06.10	ETSI	RegularPulse Excitation Long-Term Predictor (RPE-LTP)	13	8	22.5	Usado por la tecnología celular GSM	
LPC10	Gobierno de USA	Linear-predictive codec	2.4	8	22.5	10 coeficientes.La voz suena un poco "robotica"	
Speex			8, 16, 32	2.15-24.6 (NB) 4-44.2 (WB)	30 (NB) 34 (WB)		
iLBC			8	13.3	30		
DoD CELP	American Department of Defense (DoD) Gobierno de USA		4.8		30		
EVRC	3GPP2	Enhanced Variable Rate CODEC	9.6/4.8/1.2	8	20	Se usa en redes CDMA	
DVI	Interactive Multimedia Association (IMA)	DVI4 uses an adaptive delta pulse code modulation (ADPCM)	32	Variable	Muestreada		
L16		Uncompressed audio data samples	128	Variable	Muestreada		

Codificación:

Este proceso de conversión analógico digital o modulación por impulsos codificados (PCM) **se realiza mediante tres pasos**:

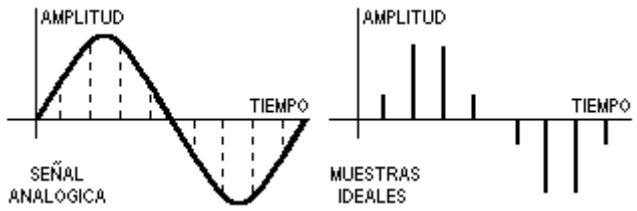
- Muestreo (sampling)
- Cuantificación (quantization)
- Codificación (codification)

En el proceso de cuantificación como explicaremos se puede realizar una compresión de la voz utilizando diferentes esquemas:

Muestreo

El proceso de muestreo consiste en tomar valores instantáneos de una señal analógica, a intervalos de tiempo iguales. A los valores instantáneos obtenidos se les llama muestras.

Este proceso se ilustra en siguiente figura:



El muestreo se efectúa siempre a un ritmo uniforme, que viene dado por la frecuencia de muestreo fm o sampling rate.

La condición que debe cumplir fm viene dada por el teorema del muestreo "Si una señal contiene únicamente frecuencias inferiores a f, queda completamente determinada por muestras tomadas a una velocidad igual o superior a 2f."

De acuerdo con el teorema del muestreo, las señales telefónicas de frecuencia vocal (que ocupan la Banda de 300 a - 3.400 Hz), se han de muestrear a una frecuencia igual o superior a 6.800 Hz (2 x 3.400).

En la practica, sin embargo, se suele tomar una frecuencia de muestreo o sampling rate de fm = 8.000 Hz. Es decir, se toman 8.000 muestras por segundo que corresponden a una separación entre muestras de:

T=1/8000= 0,000125 seg. = 125 µs

Por lo tanto, dos muestras consecutivas de una misma señal están separadas 125 µs que es el periodo de muestreo.

Cuantificación

La cuantificación es el proceso mediante el cual se asignan valores discretos, a las amplitudes de las muestras obtenidas en el proceso de muestreo. Existen varias formas de cuantificar que iremos detallando según su complejidad.

Cuantificación uniforme

Hay que utilizar un número finito de valores discretos para representar en forma aproximada la amplitud de las muestras. Para ello, toda la gama de amplitudes que pueden tomar las muestras se divide en intervalos iguales y a todas las muestras cuya amplitud cae dentro de un intervalo, se les da el mismo valor.

El proceso de cuantificación introduce necesariamente un error, ya que se sustituye la amplitud real de la muestra, por un valor aproximado. A este error se le llama error de cuantificación.

El error de cuantificación se podría reducir aumentando el número de intervalos de cuantificación, pero existen limitaciones de tipo práctico que obligan a que el número de intervalos no sobrepase un determinado valor.

Una cuantificación de este tipo, en la que todos los intervalos tienen la misma amplitud, se llama cuantificación uniforme.

En siguiente figura se muestra el efecto de la cuantificación para el caso de una señal analógica. El número de intervalos de cuantificación se ha limitado a ocho.

La señal original es la de trazo continuo, las muestras reconstruidas en el terminal distante, se representan por puntos y la señal reconstruida es la línea de trazos.

El error de cuantificación introducido en cada muestra, da lugar a una deformación o distorsión de la señal reconstruida que se representa por línea de trazos y puntos.

Cuantificación no uniforme

En una cuantificación uniforme la distorsión es la misma cualquiera que sea la amplitud de la muestra. Por lo tanto cuanto menor es la amplitud de la señal de entrada mayor es la influencia del error. La situación se hace ya inadmisible para señales cuya amplitud analógica está cerca de la de un intervalo de cuantificación.

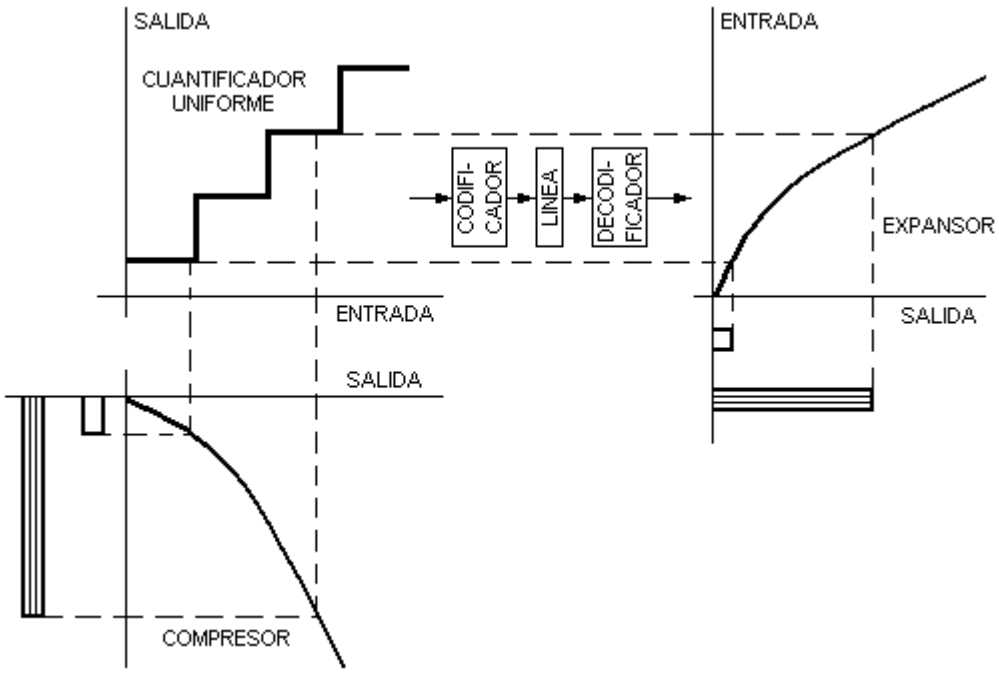
Para solucionar este problema existen dos soluciones:

- Aumentar los intervalos de cuantificación - si hay más intervalos habrá menos errores

pero necesitaremos más números binarios para cuantificar una muestra y por tanto acabaremos necesitando mas ancho de banda para transmitirla.

- Mediante una cuantificación no uniforme, en la cual se toma un número determinado de intervalos y se distribuyen de forma no uniforme aproximándolos en los niveles bajos de señal, y separándolos en los niveles altos. De esta forma, para las señales débiles es como si se utilizase un número muy elevado de niveles de cuantificación, con lo que se produce una disminución de la distorsión. Sin embargo para las señales fuertes se tendrá una situación menos favorable que la correspondiente a una cuantificación uniforme, pero todavía suficientemente buena.

Por lo tanto lo que podemos hacer es realizar una cuantificación no uniforme mediante un codec (compresor-decompresor) y una cuantificación uniforme según se ve en la siguiente figura:



Ley de codificación o compresión

El proceso de cuantificación no uniforme responde a una característica determinada

llamada ley de Codificación o de compresión.

Hay dos tipos de leyes de codificación: las continuas y las de segmentos.

En las primeras, los intervalos de cuantificación son todos de amplitud distinta, creciendo ordenadamente desde valores muy pequeños, correspondientes a las señales de nivel bajo, a valores grandes, correspondientes a las señales de nivel alto

En las segundas, la gama de funcionamiento se divide en un número determinado de grupos y dentro de cada grupo los intervalos de cuantificación tienen la misma amplitud, siendo distinta de unos grupos a otros.

Normalmente se utilizan las leyes de codificación de segmentos.

G.711 Ley A (a-law) y ley μ (u-law)

Actualmente, las dos leyes de compresión de segmentos mas utilizadas son la ley A (a-law) y la ley μ (u-law) que dan lugar al codec g.711. La ley A (a-law) se utiliza principalmente en los sistemas PCM europeos, y la ley μ (u-law)se utiliza en los sistemas PCM americanos.

La ley A esta formada por 13 segmentos de recta (en realidad son 16 segmentos, pero como los tres segmentos centrales están alineados, se reducen a 13). Cada uno de los 16 segmentos, esta dividido en 16 intervalos iguales entre si, pero distintos de unos segmentos a otros.

La formulación matemática de la Ley A es:

y= Ax / 1+ LA ---------- para 0 =< x =< 1/A
y= 1+ L (Ax) / 1+ LA ---------- para 1/A=< x =< 1

siendo L logaritmo neperiano.

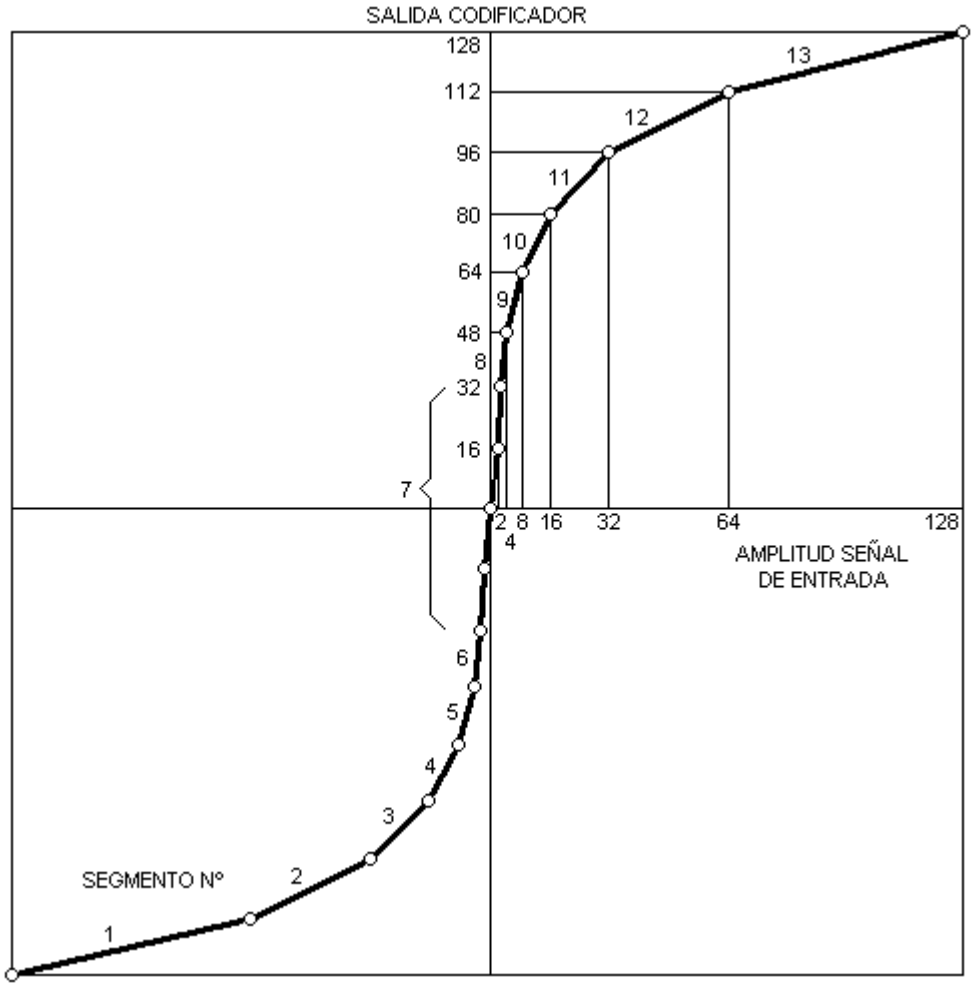
El parámetro A toma el valor de 87,6 representando x e y las señales de entrada y salida al compresor.

La ley μ se representa matemáticamente como:

y= L(1+μx) / L (1+μ)---------- para 0 =< x =< 1

donde μ= 255

En siguiente figura se representa gráficamente la ley A (a-law):



Cuantificación diferencial

En las señales de frecuencia vocal, predominan generalmente las bajas frecuencias, por ello las amplitudes de dos muestras consecutivas difieren generalmente en una cantidad muy pequeña. Aprovechando esta circunstancia, se ha ideado la cuantificación diferencial.

En la cuantificación diferencial, en lugar de tratar cada muestra separadamente, se cuantifica y codifica la diferencia entre una muestra y la que le precede. Como el número de intervalos de cuantificación necesarios para cuantificar la diferencia entre dos muestras consecutivas es lógicamente inferior al necesario para cuantificar una muestra aislada, la cuantificación diferencial permite una reducción sensible de la frecuencia de transmisión en línea, ya que esta es proporcional al numero de intervalos de cuantificación

Cuantificación diferencial delta y ADPCM (Adaptative delta PCM)

Si en un sistema DPCM vamos aumentando la frecuencia de muestreo, llega un momento en que dos muestras consecutivas tienen una amplitud tan próxima, que no se necesita más que un solo intervalo de cuantificación para cuantificar la diferencia.

En este caso solo se necesitaría un bit por muestra, y la velocidad de transmisión en línea (bit rate) sería igual a la velocidad de muestreo. Este tipo de modulación se conoce con el nombre de modulación delta.

La modulación delta descrita, se denomina modulación delta porque la magnitud de la variación producida a la salida es fija. Existen otros tipos de modulación delta mas sofisticados, en los cuales dicha variación no es fija sino que depende de las variaciones de la señal de entrada. Por ejemplo ADPCM o Adaptative delta PCM se basa en ajustar la escala de cuantificación de forma dinámica para adaptarse mejor a las diferencias pequeñas o grandes.

Codificación - Decodificación

La codificación es el proceso mediante el cual se representa una muestra cuantificada, mediante una sucesión de "1's" y "0's", es decir, mediante un número binario.

En el punto anterior va hemos indicado que cada muestra cuantificada se representa, o codifica mediante un numero binario. Normalmente en telefonía se utilizan 256 intervalos de cuantificación para representar todas las posibles muestras (por ejemplo para G.711 tanto ley A como ley μ), por tanto se necesitarán números binarios de 8 bits para representar a todos los intervalos (pues $2^8 = 256$). Otros codecs que usan ADPCM o cuantificación delta utilizan menos intervalos y por tanto menos bits.

El dispositivo que realiza la cuantificación y la codificación se llama codificador.

La decodificación es el proceso mediante el cual se reconstruyen las muestras, a partir de la señal numérica procedente de línea. Este proceso se realiza en un dispositivo denominado decodificador.

Al conjunto de un codificador y de un decodificador en un mismo equipo, se le llama codec.

IMPORTANTE: **De esta explicación se deduce que si queremos calcular el bit-rate de un codec necesitamos solamente multiplicar la frecuencia de muestreo (sample rate) expresada en muestras por segundo o Herzios por los bits necesarios para cuantificar cada muestra y nos da como resultados los bits por segundo (bit-rate) del codec en cuestión.**