



Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

TELEFONÍA IP UNA ALTERNATIVA A LA TELEFONÍA TRADICIONAL

Víctor Américo Marroquín Quic
Asesorado por el Ing. Enrique Edmundo Ruiz Carballo

Guatemala, agosto de 2008

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Inga. Glenda Patricia García Soria
VOCAL II	Inga. Alba Maritza Guerrero de López
VOCAL III	Ing. Miguel Angel Dávila Calderón
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
SECRETARIA	Inga. Marcia Ivónne Véliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

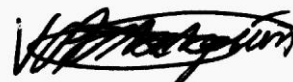
DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Enrique Edmundo Ruiz Carballo
EXAMINADOR	Inga. Ingrid Rodríguez de Loukota
EXAMINADOR	Ing. Armando Alonso Rivera Carrillo
SECRETARIA	Inga. Marcia Ivónne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

TELEFONÍA IP UNA ALTERNATIVA A LA TELEFONÍA TRADICIONAL,

tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 6 de septiembre de 2007.



Víctor Américo Marroquín Quic



FACULTAD DE INGENIERIA

Guatemala, 21 de Mayo de 2008


Ing. Julio Cesar Solares Peñate
Coordinador del Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería
Universidad de San Carlos de Guatemala
Presente.

Estimado Ingeniero:

Por este medio me dirijo a usted para informarle que habiendo asesorado al estudiante **Víctor Américo Marroquín Quic** con número de carné **1999-11387**, en el trabajo de graduación **"Telefonía IP una alternativa a la telefonía tradicional"** y llenando éste los objetivos trazados, extendiendo la aprobación del mismo.

Por lo tanto, el autor de este trabajo y yo como asesor, nos hacemos responsables del contenido y conclusiones del mismo.

Atentamente,


Ingeniero Enrique Edmundo Ruiz Carballo
Asesor





Guatemala, 25 de julio 2008.

FACULTAD DE INGENIERIA

Señor Director
Ing. Mario Renato Escobedo Martinez
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado:
Telefonía IP una alternativa a la telefonía tradicional, del
estudiante: Victor Américo Marroquín Quic por considerar que
cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,

ID Y ENSEÑAD A TODOS


Ing. Julio César Solares Peñate
Coordinador Área de Electrónica



JCSP/sro



El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante: Victor Américo Marroquín Quic, titulado: Telefonía IP una alternativa a la telefonía tradicional, procede a la autorización del mismo.

Ing. Mario Renato Escobedo Martínez

DIRECTOR



GUATEMALA, 29 DE JULIO 2008.



El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al trabajo de graduación titulado: **TELEFONIA IP UNA ALTERNATIVA A LA TELEFONIA TRADICIONAL**, presentado por el estudiante universitario **Victor Américo Marroquín Quic**, autoriza la impresión del mismo.

IMPRÍMASE.


Ing. Murphy Olimpo Paiz Recinos
DECANO

Guatemala, agosto de 2008



/gdech

DEDICATORIA

“El principio de la sabiduría es el temor de Jehová...”

Los proverbios 1:7

Con el mayor de los agradecimientos dedico el presente trabajo a Dios, por permitirme iniciarlo y finalizarlo, con la ayuda de mis padres: Victor Manuel Marroquin y María Esperanza Quic de Marroquin, de mis hermanos: Olga, Virginia, Manuel y Sandra Patricia, y de mi asesor el ingeniero Enrique Edmundo Ruiz Carballo.

Una dedicatoria especial a mis padres y a mi hermana Virginia, por ser un gran apoyo no solamente en el período de elaboración de este trabajo, sino también, durante los años de estudio.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES	VII
GLOSARIO	XI
RESUMEN	XVII
OBJETIVOS	XIX
INTRODUCCIÓN	XXI
1. TELEFONÍA TRADICIONAL	1
1.1 Red Telefónica Pública Conmutada.....	1
1.1.1 Terminales telefónicas.....	2
1.1.2 Lazo local.....	3
1.1.3 Central de Conmutación.....	3
1.1.4 Troncales.....	6
1.1.5 Señalización.....	7
1.1.5.1 SS7.....	9
1.1.6 Medios de transmisión.....	15
1.6.1.1 Medios alambritos.....	15
1.6.1.2 Fibra óptica.....	16
1.6.1.3 Medios inalámbricos.....	17
1.2 PABX.....	19
1.3 ISDN.....	20
2. REDES DE DATOS	23
2.1 Conmutación de paquetes.....	23
2.1.1 Circuitos virtuales.....	24

2.1.2	Datagramas.....	24
2.2	Protocolo TCP/IP.....	26
2.2.1	Protocolo IP.....	29
2.2.2	Dirección IP.....	32
2.2.2.1	Mascara de red.....	33
2.2.2.2	Subredes.....	34
2.2.2.3	CIDR y super-redes.....	36
2.2.2.4	IP versión 6.....	36
2.2.3	Protocolo TCP.....	40
2.2.4	Protocolo UDP.....	45
3.	TELEFONÍA IP	47
3.1	Voz sobre IP.....	47
3.2	Digitalización de la voz.....	51
3.3	Codecs de voz.....	53
3.4	Protocolo de transporte.....	57
3.5	Protocolos de señalización y arquitecturas.....	60
3.5.1	H.323.....	60
3.5.1.1	Arquitectura H.323.....	62
3.5.2	Protocolo RAS.....	65
3.5.3	Establecimiento y señalización de llamada en H.323.....	69
3.5.4	SIP.....	72
3.5.4.1	Arquitectura.....	73
3.5.4.2	Mensajes SIP.....	75
3.5.4.2.1	Mensajes de solicitud.....	76
3.5.4.2.2	Mensajes de respuesta.....	77
3.5.5	SDP.....	77
3.5.6	Establecimiento de sesión en SIP.....	80
3.5.7	MEGACO.....	83

3.5.8	Plan de Enumeración.....	84
3.5.8.1	E.164.....	86
3.5.8.2	DNS.....	88
3.5.8.3	DNS-ENUM.....	91
4.	TELEFONÍA IP COMO UNA ALTERNATIVA.....	97
4.1	Seguridad.....	99
4.1.1	Protocolos de seguridad.....	104
4.1.1.1	IPsec.....	104
4.1.1.2	TLS.....	106
4.1.1.3	SRTP.....	107
4.1.2	Firewall.....	107
4.1.3	VPN.....	113
4.1.4	NAT.....	115
4.1.5	VLAN.....	123
4.1.6	Seguridad H.323.....	126
4.1.6.1	H.235.....	126
4.1.6.1.1	H.235.1.....	127
4.1.6.1.2	H.235.2.....	129
4.1.6.1.3	H.235.3.....	129
4.1.6.1.4	H.235.4.....	130
4.1.6.1.5	H.235.5.....	131
4.1.6.1.6	H.235.6.....	132
4.1.6.1.7	H.235.7.....	133
4.1.6.1.8	H.235.8.....	133
4.1.6.1.9	H.235.9.....	134
4.1.6.2	Firewall.....	135
4.1.7	Seguridad en SIP.....	135
4.1.7.1	Http digest.....	136

4.1.7.2	TLS.....	137
4.1.7.3	S/MIME.....	137
4.1.7.4	Firewall.....	138
4.1.8	Monitoreo de la red.....	138
4.2	Qos.....	141
4.2.1	Ancho de banda.....	143
4.2.1.1	Supresores de silencio.....	145
4.2.1.2	Compresión de cabecera.....	145
4.2.2	RSVP.....	146
4.2.3	Int-Serv.....	148
4.2.4	Diff-Serv.....	149
4.2.5	MPLS.....	150
5.	HARDPHONE, SOFTPHONE Y PBX IP.....	155
5.1	Hardphone.....	155
5.2	Softphone.....	158
5.3	PBX IP.....	161
5.3.1	IAX2.....	161
5.3.2	Asterisk.....	165
	CONCLUSIONES.....	179
	RECOMENDACIONES.....	181
	BIBLIOGRAFÍA.....	183
	ANEXOS.....	185
1.	Empresas guatemaltecas interesadas en migrar a telefonía IP.....	185
2.	Universidad Francisco Marroquin; sistema de telefoía IP ofrece Mejoras en la comunicación y atención de los estudiantes y personal Administrativo.....	187
3.	VOIP al alcance de su mano.....	191

4. Crece oferta de voz IP.....	196
--------------------------------	-----

ÍNDICE DE ILUSTRACIONES

FIGURAS

1	Red Telefónica Conmutada	2
2	Conexión de abonados	4
3	Trama T1	7
4	Red SS7	12
5	Enlace inalámbrico	18
6	Circuitos virtuales	25
7	Datagramas	26
8	Relación entre arquitecturas	28
9	Datagrama IP	29
10	Valores del campo Next Header	38
11	Segmento TCP	41
12	Segmento UDP	45
13	Cabecera y Pseudos-cabecera UDP	46
14	Cuantización	52
15	Estructura de la cabecera RTP	58
16	Pila del protocolo H.323	62
17	Arquitectura H.323	65
18	Señalización directa	70
19	Flujo de señalización directa	70
20	Señalización encaminada por Gatekeeper	71
21	Flujo de información de señalización encaminada por Gatekeeper	71
22	Mensaje SDP	79
23	Inicio de sesión simple	80
24	Inicio de sesión con Proxy Server	81

25	Inicio de sesión con Redirect Server	81
26	Encaminamiento de llamada SIP-RTPC y H.323-SIP	82
27	Formato de enumeración E.164	87
28	Árbol DNS	89
29	Distribución de los servidores de dominio genérico gTLD	91
30	Registro NAPTR	93
31	Llamada telefónica de la RTPC hacia una red SIP	95
32	Llamada telefónica de una red SIP hacia la RTPC	96
33	Modo de operación del protocolo IPsec	105
34	Uso del firewall	109
35	Arquitectura DMZ	112
36	Red privada virtual	115
37	VLANs en un mismo espacio físico	124
38	VLANs en distinto espacio físico	125
39	Mecanismo de señalización H.225	128
40	Mensajes de reservación de recursos	147
41	Arquitectura MPLS	152
42	Teléfono IP SI-150	157
43	Teléfono IP 7975G	157
44	Softphone	160
45	Arquitectura Asterisk	166
46	Trixbox	178

TABLAS

I	Codecs y puntuación MOS	56
II	Servidores STUN	120
II	Requerimientos de firewall para H.323	135
IV	Requerimientos de firewall para SIP	138
V	Retardo introducido por codecs en aplicaciones basada en IP	142
VI	Ancho de banda en VOIP	144

GLOSARIO

Ancho de banda

Rango de frecuencias en el que se concentra la mayor parte de la información contenida en una señal analógica. Para señales digitales corresponde a la cantidad de datos que pueden ser enviados en un determinado tiempo.

Binario

Sistema en el que las señales se representan usando dos estados o valores. En sistema binarios digitales estos estados son 1 y 0.

Bit

Representa el elemento de información más pequeño que puede ser utilizadas en sistemas digitales, suelen representarse como 1 y 0.

Byte

Conjunto de 8 bits.

Conmutación

Técnica utilizada para cambiar de una posición o de un nivel a otro. En la telefonía la conmutación permite la conexión entre los usuarios.

DHCP

Protocolo de red que permite a las terminales conectadas a esta obtener sus parámetros de configuración (máscara de red, dirección IP y otros) automáticamente.

Endpoint (Terminal)

En redes de datos o telefonía suele referirse al punto en donde se originan o se reciben datos o llamadas.

Enrutador (Router)

Dispositivo de red encargado en encaminar hasta el destino final la información transmitida, determinando la ruta que deben seguir los paquetes.

Full-duplex

Tipo de transmisión en donde se envía información en ambos sentidos simultáneamente.

Inmunidad electromagnética

Capacidad de rechazar cualquier interferencia externa que pueda ocasionar la degradación de la calidad en el funcionamiento de los equipos de comunicación.

Licencia GPL

Licencia utilizadas por desarrolladores de *Software* para indicar que su producto pertenece al llamado *Software* libre, en donde la ejecución, distribución y readecuación del programa puede hacer sin restricciones.

Microondas

Señales utilizadas comúnmente en sistemas inalámbricos (por ejemplo, telefonía celular) con un rango de frecuencia entre los 300 MHz y los 300 GHz.

Multicast

Servicio de red en el cual un único flujo de datos, proveniente de una determinada fuente, se puede enviar simultáneamente a diversos receptores que requieran de la información.

Orbita Geo-estacionaria

Zona en el espacio, en la que se puede colocar un objeto que visto desde la tierra parecerá inmóvil.

Paquete

Bloque de información utilizado en redes de datos.

Protocolo X.25

Protocolo de acceso a redes públicas de conmutación de paquetes definido por la Unión Internacional de las Telecomunicaciones (UIT-T).

Señal analógica

Tipo de señal que varía de forma continua a lo largo del tiempo. En su mayoría las señales obtenidas a nuestro alrededor son de este tipo, la voz, la temperatura y presión son ejemplos de este tipo de señal.

Señal digital

Tipo de señal que se representa por valores discretos en el tiempo. Típicamente suelen utilizarse dos valores para representar a una señal de este tipo.

Sistema operativo

Software encargado de gestionar los recursos en sistemas de cómputo, permite la interacción con elementos externos (impresoras, celulares) y la ejecución de programas (Word, Internet Explorer) compatibles con este.

Texto Plano

Son aquellos que están compuestos únicamente por texto sin formato, sólo caracteres, que dependen del idioma utilizado.

Unicast

Servicio de red en el cual un único flujo de datos, proveniente de una determinada fuente, es enviada a un único receptor.

RESUMEN

VOIP es una tecnología que permite transportar señales de voz sobre redes de datos y es parte fundamental de la telefonía IP, la cual se basa en la conmutación de paquetes, a diferencia de la telefonía tradicional basada en conmutación de circuitos. Además, está fundamentada en cuatro protocolos de señalización los cuales son: H.323, SIP, MGCP e IAX2. Cada uno de estos protocolos está diseñado para trabajar en conjunto con una serie de dispositivos que permiten la interacción entre los distintos usuarios de redes IP o telefonía tradicional.

La seguridad es una parte fundamental dentro de la telefonía tradicional, y lo es de igual manera dentro de la IP. Los usuarios deben de estar confiados de que sus conversaciones serán únicamente escuchadas por aquellos que estén autorizados a hacerlo, para esto se hace necesario hacer uso de una serie de herramientas que garantizan la confiabilidad, disponibilidad y autenticación de los datos transmitidos y recibidos.

Para los usuarios de la telefonía IP, realizar una llamada será como siempre lo han hecho y lo podrán hacer desde un teléfono IP basada en *Hardware* o *Software*, o desde su teléfono tradicional adicionado un dispositivo que acople ambas tecnologías, además se podrá hacer uso de la PBX, de igual manera que en la telefonía tradicional.

Actualmente, la arquitectura de la telefonía tradicional se encuentra bien sustentada, desplazarla será todo un reto para la telefonía IP, pero el aumento del uso de la Internet es un punto a favor a la expansión de esta, además de las opciones y ventajas que presenta su implementación.

OBJETIVOS

- General

Proporcionar un texto de referencia con el fin de transmitir al lector los conocimientos básicos que le ayuden a conocer y comprender todo lo relacionado con la telefonía IP.

- Específicos

1. Conocer el funcionamiento de las redes de voz, de datos y la convergencia de ambas tecnologías, como base para la comprensión de la telefonía IP.
2. Conocer las herramientas que permiten proporcionar seguridad y calidad de servicio en la telefonía IP, para mantener un nivel similar al que entrega la PSTN.
3. Describir los teléfonos y PBX utilizados en telefonía IP que permiten realizar llamadas desde y hacia una red IP o la PSTN.

INTRODUCCIÓN

La actual globalización de nuestra sociedad hace imprescindible estar comunicados, para poder seguir el paso a esta tendencia es necesario avanzar paralelamente con los avances tecnológicos. La VOIP aunque no es una tecnología relativamente nueva, en los últimos años ha empezado a ganar relevancia en el mundo de las telecomunicaciones, porque permite transportar señales de voz en las actuales y muy usadas redes IP. Su avance se debe en gran medida a que ahora es posible transportar estas señales sin mayores retardos y pérdidas, con lo que se logra mantener la fluidez de una conversación, parecido a lo que se está acostumbrado en la red telefónica tradicional. En sus inicios esto no era posible porque la calidad de las conversaciones era muy baja.

El creciente uso de la Internet y la posibilidad de disponer de transmisiones de banda ancha, han hecho que esta tecnología le gane terreno a la actual red telefónica. Como ingenieros debemos estar preparados para afrontar la creciente evolución y el surgimiento de nuevas tecnologías que podrían cambiar las actuales arquitecturas que permiten comunicarnos, y aunque esto es casi siempre transparente para el usuario, un ingeniero debe ir más allá de únicamente usar la tecnología, debe comprenderla, y aún más si se desempeña laboralmente dentro de este ambiente.

Grandes empresas como Cisco y 3Com han apostado a la telefonía IP, estas empresas fueron principalmente desarrolladoras de tecnología para redes de datos, ahora además diseñan tecnología VOIP. Al parecer el mercado para esta tecnología promete ser rentable tanto para desarrolladores, proveedores y usuarios. El usar la misma red para datos y voz permite a las empresas reducir costos de mantenimiento y diseño, los actuales precios por llamada han hecho de esta tecnología una buena opción de reemplazo de la telefonía tradicional, en algunos países se ha detectado una baja de usuarios de la red tradicional.

En países en desarrollo como el nuestro, aún es difícil poder contar con una conexión a la Internet y aun más que sea de banda ancha, pero la tecnología sigue una tendencia de bajar su precio con el tiempo, por lo cual en algunos años podría convertirse también en una buena alternativa o reemplazo y poder gozar de sus beneficios, esto para usuarios domésticos y pequeños empresarios, para empresas grandes puede representar una buena alternativa a muy corto plazo.

El sistema actual se fundamenta sobre las telecomunicaciones porque las empresas se comunican con sus clientes, sucursales y trabajadores nacionales e internacionales y los países deben estar comunicados para negociaciones económicas y políticas. Por lo que es de gran relevancia conocer y comprender a la telefonía IP, pues si continúa su crecimiento es muy probable que se convierta en una importante red de comunicaciones.

Conocer esta tecnología implica tener que relacionarse con la telefonía tradicional y las redes de datos, porque la telefonía IP permite relacionar ambas tecnologías. La telefonía IP implica una arquitectura en la que interaccionan una serie de dispositivos, que permiten interconectar a diferentes usuarios y protocolos de señalización, y la VOIP conforma una parte fundamental, al igual que la seguridad y la calidad.

El presente trabajo se inicia con una descripción de la telefonía tradicional y las redes de datos, para posteriormente iniciar con los protocolos y arquitecturas usadas en telefonía IP, también se incluye temas de importancia como seguridad y calidad de servicio. Además se explica el concepto de teléfono IP tanto software como hardware, y se describen algunos teléfonos encontrados comercialmente, por último se hace una introducción a la PBX IP Asterisk, considerada como una herramienta muy útil a la hora de desarrollar un sistema de telefonía IP empresarial.

El trabajo se basa en información bibliográfica debido a que las empresas que prestan el servicio de telefonía IP en el país están reacias a proporcionar información y la poca que se obtuvo no aportó datos de relevancia que se pudieran incluir. Por lo que se espera que los datos incluidos permitan dar a conocer esta tecnología a los futuros lectores.

1. TELEFONÍA TRADICIONAL

1.1 Red Telefónica Pública Conmutada

La red telefónica pública conmutada (RTPC) interconecta a los diferentes usuarios que desean establecer una comunicación vocal, esta interconexión puede ser local o internacional. Debido al gran desarrollo que ha sufrido esta red se ha convertido en una de las más importantes redes de comunicación.

En sus inicios esta red era totalmente analógica, con los años se empezaron a utilizar técnicas digitales tanto en los medios de transmisión como en la conmutación, lo cual permitió la transmisión de voz y de datos (texto, imágenes y audio) sobre un mismo canal. Los elementos que conforman la RTPC son los siguientes:

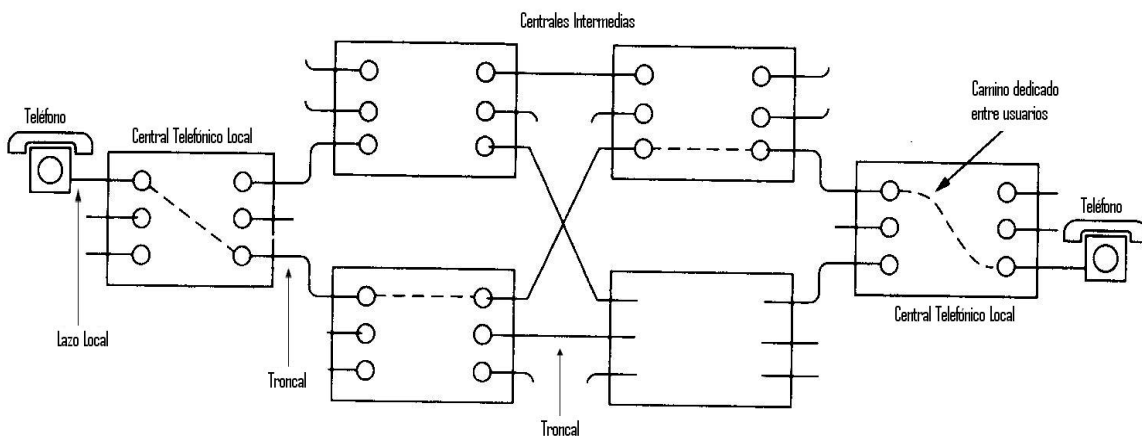
- Terminales telefónicas (teléfonos)
- Lazo local
- Centrales de conmutación
- Troncales telefónicos

La figura 1 muestra la relación entre cada uno de los elementos de la RTPC, la cual es una red de conmutación de circuitos. La conmutación de circuitos en telefonía, es un sistema en el cual se establece un canal dedicado durante la duración de una llamada telefónica. Terminada la llamada se libera el canal y éste podrá ser usado por otro par de usuarios de la red. La conmutación telefónica es el proceso mediante el cual se establece y mantienen un circuito entre dos usuarios cualesquiera.¹

¹ Huidobro, José Manuel. **Manual de Telefonía. Telefonía fija y móvil.** (España: Editorial Paraninfo, 1997). p.16

La conmutación de circuitos es ideal para la transmisión de señales de voz, ya que no introduce retardos y es transparente, es decir que una vez establecido un circuito está aparece como una conexión directa entre los usuarios. Esta tecnología desde sus inicios ha tenido un gran dominio sobre las comunicaciones de voz, y este dominio aun permanece dentro de la era de la transmisión digital.

Figura 1. Red telefónica Conmutada.



Fuente: Tanenbaum Andrew. **Redes de computadoras**. Pág. 131.

1.1.1 Terminales telefónicas

Los teléfonos tienen la tarea de convertir las señales de voz en señales eléctricas y viceversa, además de esto tienen a cargo indicarle a la central que se desea realizar una llamada o finalizarla, reciben de la central tonos que le indican al usuario que debe marcar el número al cual se desea comunicar (tono de marcación), que la terminal con la cual desea comunicarse esta desocupada y se realiza la llamada al usuario con el que deseamos comunicarnos (tono de llamada) o que el usuario con el que desea comunicarse no esta disponible, además se recibe la señal que hace que el teléfono timbre, lo cual indica una llamada entrante.

Las señales enviadas y recibidas desde un teléfono son del tipo analógico con un ancho de banda limitado de los 300 a los 3400 Hz. Las terminales telefónicas han evolucionado desde los antiguos teléfonos de disco, los cuales permitían la marcación a través de un disco giratorio a los actuales DTMF (*Dual Tone MultiFrequency*). En estos teléfonos cada tecla tiene asignada dos frecuencias las cuales son combinadas al momento de la marcación, la combinación de estas dos frecuencias representa al número marcado².

1.1.2 Lazo local

El lazo local o lazo del suscriptor es el encargado de unir a los terminales telefónicos con la central de conmutación. Por lo que cada abonado tiene una conexión dedicada desde su teléfono hasta la central de conmutación a la cual pertenece, este enlace comúnmente esta hecho por un par de alambres trenzados de cobre³ aunque también se puede usar DLC (*Digital Loop Carrier*), con este método el teléfono es conectado al sistema DLC y de este a una central de conmutación digital con lo cual se consiguen transmisiones de mayor ancho de banda. La tecnología inalámbrica también es utilizada en el lazo local (*Wireless Local Loop*) la cual reduce los costos de instalación y mantenimiento, se suele utilizar en áreas remotas o rurales.

1.1.3 Central de Conmutación

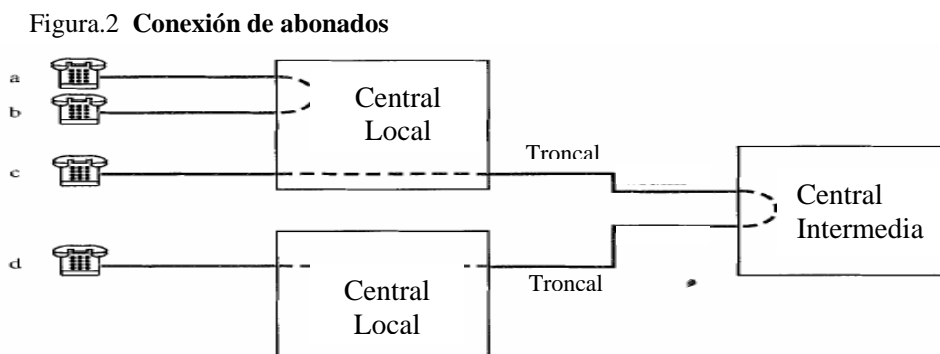
Cada suscriptor de la red telefónica esta conectado a una central que contiene todo el equipo de conmutación, de señalización y de energía eléctrica necesaria para la operación de los teléfonos.

² Los símbolos utilizados en DTMF incluye a los números del 0 al 9, las letras de la A hasta la D y los caracteres # y *.

³ El nombre de los cables del lazo local son conocidos como T (TIP) y R (RING).

La central es la encargada de crear el enlace de comunicación entre el usuario llamante y el usuario llamado, debido a los altos costos que representa tener un circuito dedicado por cada abonado hacia las posibles terminales con las que desee comunicarse, este circuito es dedicado a la llamada únicamente durante el tiempo que esta dura, para luego estar nuevamente disponible en espera de otra llamada.

Al realizar una llamada telefónica esta viaja sobre el lazo local hasta la central local a la cual se encuentra suscrito el abonado, si esta es para otro usuario suscrito a la misma central la llamada es conmutada hacia la línea del suscriptor. Si la llamada es para un usuario suscrito en otra central telefónica la llamada es conmutada a un troncal telefónico el cual conecta a las dos centrales, en áreas urbanas con un gran número de centrales locales se utilizan centrales intermedias que realizan la conexión entre centrales locales ya que la conexión directa no resulta practico. Lo anteriormente dicho se ilustra en la figura 2, en donde el usuario “a” desea comunicarse con el usuario “b” al estar ambos suscritos a la misma central esta se encarga de crear el enlace entre ambos usuarios. En el caso del usuario “c” que desea comunicarse con el usuario “d” y ambos usuarios se encuentran suscritos a distintas centrales, el enlace entre ambos abonados se crea a través de la central intermedia, la cual se encarga de unir a ambas centrales locales.



Fuente: Stallings, William . **Data and Computer Communications**. Pág. 234.

La central telefónica para poder unir a dos abonados o enlazarse con otra central hace uso de la señalización, la cual se encarga de que tanto el abonado como la central local o centrales puedan entenderse y lograr así el objetivo de unir a los abonados de la red. Tomando en cuenta que se utilizan dos tipos de señalización, la central de conmutación debe de proveer señalización tanto para la vinculación con el suscriptor como con otras centrales. En el inciso 1.1.1 se detalla la señalización entre el usuario y la central local.

Si un usuario de la red desea comunicarse con otro que se encuentra abonado en una central distinta se da inicio a la señalización entre centrales. La central de origen toma un enlace libre entre centrales, se envía una señal de descolgado a la otra central y se solicita un registro a la cual enviar la dirección del destino, seguido el conmutador al cual se le solicito el registro envía una señal de descolgar seguida de otra de colgar, esta secuencia es conocida como “*wink*”, lo cual indica que el registro esta listo y la central origen envía los dígitos de la dirección al conmutador destino y así lograr el enlace entre los abonados.

En los inicios de la telefonía la conmutación se realizaba manualmente. Se utilizaba un jack para cada línea y dos plugs en un cable flexible, con lo cual se lograba crear el canal de comunicación entre dos teléfonos. Posteriormente se utiliza lo que se conoció como “*The Strowger*” o “*Step-by-Step Switch*”, la conexión hacia el teléfono receptor se realizar a través de una serie de interruptores que generaban pasos verticales y horizontales, todos los pasos eran directamente controlados por los pulsos generados en el dial del teléfono.

Seguidamente se usa el sistema conocido como “*Crossbar Switching*”, el cual utilizaba una matriz de interruptores en la cual se energizaba la línea horizontal y la vertical de la matriz para encaminar la llamada telefónica.

Dentro de las tecnologías utilizadas está también la de los circuitos lógicos a base de relés. Actualmente la lógica de conmutación es realizada por circuitos digitales, con lo que se logra la transmisión de datos y voz sobre un mismo canal, además de disponer de mayor capacidad y mayores velocidades de conmutación.

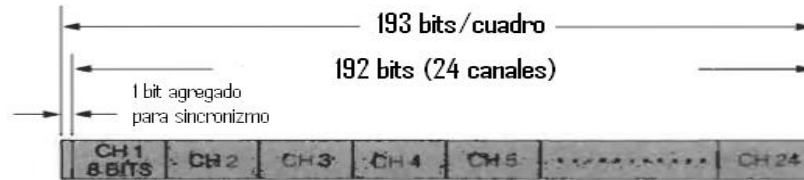
1.1.4 Troncales

Los troncales son los encargados de conectar a las centrales telefónicas. Actualmente, los troncales tienden a la digitalización, las conversaciones son convertidas en formato PCM (*Pulse Code Modulation*), multiplexadas y transmitido sobre estos. Pequeñas centrales pueden ser enlazadas con troncales digitales los cuales utilizan portadoras T1 (sistema Norteamericano) o E1 (sistema Europeo).

El sistema de portadora T1 es un método digital de transmisión de voz, capaz de transportar 24 canales. Utiliza multiplexión por división de tiempo (TDM) con velocidades de transmisión de 1.544 Mbps. Si el flujo de datos es al alto y la portadora T1 es insuficiente, se pueden utilizar portador T2, T3, T4, las cuales son obtenidas por la multiplexación de portadoras T1, con lo que se consiguen velocidad de transmisión de 6.312 Mbps (4 portadoras T1), 44.736 Mbps (7 portadoras T2) y 274.176 Mbps (6 portadoras T3).

La figura 3 ilustra una trama T1, la cual consiste de 193 bits de los cuales 192 corresponden a 24 canales de datos y uno corresponde al bit de sincronización de trama, los 193 bits son enviados en un tiempo de 125 μ seg. El sistema E1 es capaz de transportar 30 canales de voz a una velocidad de 2.048 Mbps. La trama está dividida en 32 ranuras de tiempo de TS0 a TS31, donde TS0 es para la señalización y TS16 para sincronización, el resto es para los canales de voz.

Figura 3. **Trama T1**



Fuente: Stephen J. Bigelow, Joseph J. Carr, Steve Winder. **Understanding Telephone Electronics**. Pág. 195.

1.1.5 Señalización

La función principal de una central de conmutación es establecerle contacto temporal entre dos usuarios que desean comunicarse, gracias a la información proporcionada (numeración) por el solicitante, por lo que se debe establecer un intercambio de señales tanto entre este y la central local como ésta y las otras, para completar la llamada⁴.

Tradicionalmente se ha utilizado la señalización troncal o intra-canal (*In Channel Signaling*). Con esta señalización se emplea el mismo canal para la transmisión de voz como para la señalización de control.

En banda o fuera de banda son dos formas de la señalización intra-canal. En banda además de utilizar el mismo canal que la información también usa la misma banda de frecuencia. La principal ventaja de la señalización en banda es que puede ser usada sobre cualquier medio de transmisión. Su principal desventaja reside en la necesidad de eliminar la interferencia entre las dos señales.

⁴ Huidobro, José Manuel. **Manual de Telefonía. Telefonía fija y móvil**. (España: Editorial Paraninfo, 1997). p.26

Fuera de banda también utiliza el mismo canal que la señal de voz pero en una banda de frecuencia distinta. Para el envío de las señales de control se utiliza una banda angosta dentro de los 4Khz asignados a las señales de voz pero no utilizado por estas. Su principal ventaja es que permite la continua supervisión y control de una llamada, esto debido a que las señales de control pueden ser enviadas haya o no señales de voz en el medio de transmisión. La desventaja de este método es que requiere de equipo extra para el manejo de la banda de señalización.

Señalización por canal común (*Common Channel Signaling*), es otro método de señalización en el cual las señales de voz y las señales de control se conducen en caminos independientes. Las señales de control se conducen sobre canales que están dedicados a estas y son comunes a un grupo de canales de voz. La señalización por canal común utiliza dos modos de operación, el modo asociado y el modo no asociado.

En el modo asociado las señales de control están en canales distintos de las señales del suscriptor, y dentro del conmutador las señales de control se encaminan directamente hacia un procesador de control de señal. El modo no asociado aumenta la complejidad, pero también se vuelve más potente. En este sistema nodos adicionales conocidos como puntos de transferencia de señal amplían la red, ya que ahora se tiene dos redes separadas con enlaces entre ellas y no existe relación entre los canales de control y el grupo de troncales. Con este modo se pueden asignar tareas a los canales de control de una forma más flexible haciendo más fácil la gestión de la red.

La señalización intra-canal es usada para la comunicación con el suscriptor, por ejemplo, las señales de ocupado, marcado o de llamada alcanzan al suscriptor utilizando esta señalización. La señalización por canal común es usada para la comunicación entre centrales telefónicas, lo que hace que esta señalización sea muchos más compleja que la intra-canal.

1.1.5.1 SS7

El Protocolo de control SS7 (*Signaling System 7*) es una estandarización para señalización telefónica compatible con la red digital e ISDN (*Integrated Service Digital Network*), que contiene los mecanismos necesarios para que los elementos dentro de la red puedan intercambiar información de control. Su robustez, flexibilidad, confiabilidad, capacidad de interconexión y otras características han hecho de SS7 un importante recurso dentro de las redes de transporte de voz y datos⁵.

SS7 es una red de conmutación de paquetes que controla a una red de conmutación de circuitos, con el propósito principal de conectar llamadas telefónicas. La señalización se basa en paquetes cortos de información que son encaminados a través de la red de señalización. El protocolo provee dos tipos de servicios: Circuitos relacionados y no relacionados. La señalización con circuitos relacionados es utilizada para establecer, supervisar y liberar las conexiones de voz en redes TDM y VoIP. Los no relacionados se utilizan para el resto de servicios que presta la red como: Acceso a base de datos para información de usuarios y administración de la red.

La red de señalización mundial se divide en dos niveles: La internacional y la nacional. El plan internacional se basa en la estandarización de la ITU-T (SS7), mientras que las nacionales pueden utilizar variaciones del estándar. Para llevar a cabo las comunicaciones entre los niveles nacionales e internacionales, se hace uso de gateway que convierten las distintas variaciones de las señalizaciones nacionales a la internacional. Esta estructura hace posible que el plan de enumeración SS7 de los nodos pertenecientes al plan internacional y las diferentes redes nacionales puedan ser independientes unas de otras, además provee una división en la responsabilidad de la administración de la red de señalización.

⁵ Russel, Travis. **Signaling System #7**. (5^{ta} Edición; EE.UU: McGraw-Hill, 2006). pp. 1-3

Los nodos son los encargados de manejar los mensajes SS7 y son los componentes fundamentales de la red. A los nodos también se les llama SP (*signaling points*) y cada uno de los SP tiene una única dirección llamada PC (*Point Code*). En SS7 se manejan tres tipos de nodos SP, los cuales son:

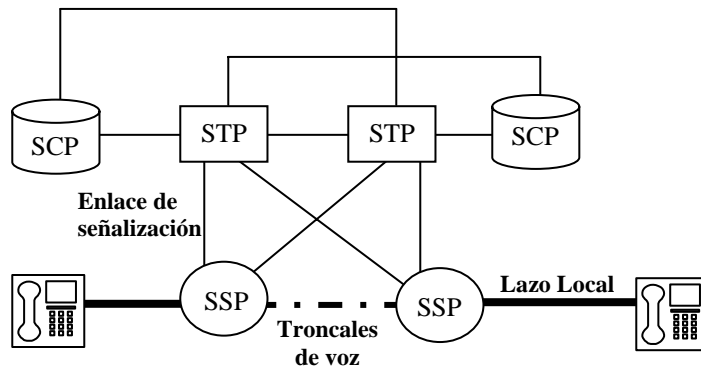
- *Service Switching point (SSP)*: Es el encargado de los intercambios locales en la red telefónica, se conectan directamente a la línea del suscriptor. Cualquier conmutador de voz con funciones SS7 es considerado un SSP, sin tomar en cuenta si son conmutadores locales o conmutadores tandem. Los SSP deben de convertir la señalización de los conmutadores de voz a mensajes de señalización SS7 para ser enviados a otros conmutadores en la red, pueden generar y terminar mensajes pero no puede transferirlos. Sin un mensaje llega con un PC distinto al de SSP el mensaje es descartado. Un SSP utiliza la información provista por los usuarios al marcar los dígitos del número telefónico para saber como conectar la llamada. Determinan donde se origina y donde termina una llamada para obtener la ruta a seguir, ya que cada mensaje de señalización contiene la dirección PC de la fuente y el destino. La ruta se obtiene por el uso de una tabla de ruteo en el propio SSP. Los mensajes con servicio de circuitos relacionados y no relacionados son generados en los SSP.
- *Signal Transfer Point (STP)*: Son los encargados de encaminar los mensajes de señalización de un nodo a otro, lo cual permite el acceso a la red. Tienen gran similitud a un router en una red IP. Proveen la lógica necesaria para conectar SSPs sin requerir conexiones directas entre de ellos. Son configurados en pares para proveer redundancia y alta disponibilidad, si un STP falla el otro se hace cargo del tráfico de la red. Los STP configurados en pares son conocidos como autónomos (*standalone*). La otra forma de STP es la integrada, esta forma conjuga las funciones de un SSP y un STP. Se manejan tres distintos tipos de STP: STP nacionales, STP internacionales y STP gateway.

Los primeros proveen el encaminamiento de los mensajes de señalización para el tráfico nacional, los internacionales encaminan el tráfico entre los distintos países y los gateway son los encargados de la traducción de los distintos protocolos o variaciones del estándar al utilizado en las redes internacionales. También sirven como una interfaz de red para la seguridad de la misma, ya que determinan a que operadores (*carriers*) se les permite el acceso a la red.

- *Service Control Point (SCP)*: Establecen el enlace hacia la base de datos de los proveedores telefónicos. El acceso al sistema de la base de datos es comúnmente hecha a través de X.25, por lo que el SCP debe de proveer la conversión entre SS7 y X.25. Si no se utiliza este protocolo para el acceso a la base de datos, SCP provee la capacidad de comunicación a través de primitivas. Las bases de datos son direccionadas utilizando un número de sub-sistema, el cual es único para cada base. El número de sub-sistema es conocido como nivel SSP. Una solicitud originada dentro de la PSTN contiene a este identificador, que es utilizado para identificar en que base de datos se ha guardado la información para el SCP puede responder a la solicitud. Al igual que los STP trabajan en pares para proveer redundancia a la red, en condiciones normales el par de SCPs comparten la carga, si por alguna razón uno de ellos falla, el otro se hace carga de toda la carga de la red hasta que se haya restablecido la operación normal. Los SCP guardan información sobre los servicios del suscriptor, asignación de rutas para llamadas de números especiales, como los números para llamadas gratis, también permiten la validación de llamadas por tarjeta.

La figura 5 muestra la relación entre los distintos nodos en una red SS7.

Figura 4. Red SS7



Todos los puntos de señalización son unidos a través de enlace bidireccionales, estos enlaces pueden ser terrestres o satelitales. Típicamente los enlaces son de 56 ó 64 Kbps. Se manejan 3 modos de señalizaciones que dependen de la relación que exista entre nodos SS7 que se comunican, los tipos de enlaces son: Asociado, no asociado y cuasi- asociado.

En el modo asociado tanto los enlaces de voz como de señalización unen directamente a dos SSP, si se utiliza un STP para unir a dos SSP, entonces se está utilizando el modo cuasi-asociado. En este modo, el enlace de voz une directamente a dos SSP pero los mensajes de señalización deben de pasar por el mínimo número de STPs para poder llegar a su destino. Este modo de señalización minimiza el retardo de los mensajes pero es mucho más costoso ya que se debe utilizar el mínimo número de STP. El modo no asociado es similar al cuasi-asociado, con la diferencia de que los mensajes pasan por múltiples STP para llegar a su destino. Este modo es el más común en las redes SS7. Los enlaces utilizados para unir a los distintos nodos de la red son etiquetados de acuerdo a su relación con esta. Seis tipos de enlaces son utilizados:

- Enlaces de acceso (A-Links): Son utilizados para interconectar los SSP con los STP y los STP con SCP. Estos enlaces proveen el acceso a la red y a las bases de datos a través de los STP. El máximo número de enlaces hacia cualquier STP es de 16, por lo que se consiguen 32 para el par STP (configuración *Standalone*).
- Enlaces de puente (B-Links): Son utilizados para conectar dos pares de STPs que tiene el mismo nivel de jerarquía dentro de la red.
- Enlaces de cruce (C-Links): Son utilizados para conectar dos STP y formar el par redundante, se utilizan si ocurre algún error o existe congestión. En condiciones normales transportan mensaje de administración de la red. Un máximo de ocho C-links pueden ser colocados entre pares STP.
- Enlaces diagonales (D-links): Son utilizados para conectar un par STP a otro par que pertenece a un nivel de jerarquía distinto, o pares de STP que pertenecen a distintas redes. Estos enlaces son utilizados en redes SS7 muy grandes y que manejen una arquitectura de red con jerarquía. Un máximo de ocho D-Links pueden ser utilizados entre dos pares STP.
- Enlaces extendidos (E-Links): Son utilizados para conectar a los SSP y SCP a un par STP no local mediante A-Links, el enlace local también se hace con este tipo de enlace. Los E-Links se usan para proveer fiabilidad adicional a la red o en caso de fallas o congestión en el par STP local.
- Enlace asociado completo (F-Links): Son usados para unir directamente a dos SSP sin el uso de los STP, ya sea porque no están disponibles o existe demasiado tráfico en la red. Este es el único tipo de enlace en el cual el tráfico de señalización sigue el mismo camino que el tráfico de voz.

El protocolo SS7 sigue una estructura de capas similar a las del modelo OSI, aunque únicamente 4 niveles son utilizados por SS7. Las capas 1, 2 y 3 del modelo OSI corresponden con los niveles 1, 2 y 3 de SS7, las capas 4, 5, 6, 7 se corresponden con el nivel 4 en SS7. El nivel 1, 2 y 3 de SS7 es usado por MTP (*Message Transfer Part*), el nivel 1 corresponde a MTP L1, el nivel 2 a MTP L2 y al nivel 3 MTP L3. MTP provee el protocolo de transporte de un SP a otro, proporciona un esquema básico de detección y corrección de errores. Además proporciona asignación de rutas, discriminación de mensajes y funciones de distribución dentro de un nodo.

MTP L1 tiene la función de transportar información de un SP a otro y define las características físicas y eléctricas de los enlaces. MTP L2 se ocupa del chequeo de secuencia, control de flujo, permite la detección de errores, efectúa la confirmación o rechazo del mensaje para la retransmisión automática en mensajes con errores. Este protocolo tiene a su cargo la transferencia segura de los mensajes de señalización en un enlace. MTP L3 se encarga de: asignación de rutas a los mensajes, discriminación de mensajes, distribución de mensajes y administración de la red.

El nivel 4 de SS7 contiene a los protocolos: SCCP (*Signaling connection control part*), TCAP (*Transactions capabilities application part*), ISUP (*ISDN user part*) y TUP (*Telephone user part*). SCCP efectúa funciones de direccionamiento adicionales a MTP3, la combinación de SCCP y el MTP3 se denomina NSP (*Network Service Part*), lo que suma una mayor flexibilidad en el encaminamiento de los mensajes y provee mecanismos para transmitir datos sobre las redes SS7. Este protocolo permite el transporte de mensaje tanto orientados a conexión como sin conexión. TCAP permite a las aplicaciones poder comunicarse entre si a través de elementos de datos conocidos como componentes, los cuales pueden ser vistos como instrucciones envidadas entre aplicaciones. También permite el acceso remoto a base de datos y solicitud remota de las capacidades de los elementos de la red.

TUP e ISUP se sitúan sobre MTP para establecer, mantener y liberar llamadas telefónicas. Ambos son protocolos de señalización de circuitos relacionados. TUP fue el primer protocolo de control y soporta únicamente el plan antiguo de servicios telefónicos (POTS) que es el servicio estándar de telefonía, mientras que ISUP soporta POST e ISDN.

1.1.6 Medios de transmisión

A través de los medios de transmisión se transportan las señales eléctricas generadas y recibidas por el teléfono y las centrales telefónicas. El lazo local del abonado y los troncales son las secciones de la red telefónica que hacen uso de los medios de transmisión para la transportación de señales de voz y señalización. Los medios de transmisión pueden pertenecer a tres categorías: Medios alámbricos, inalámbricos y fibra óptica.

1.1.6.1 Medios alámbricos

Los cables de cobre son los medios más comunes de transmisión a pesar de tener altos niveles de atenuación y poca inmunidad electromagnética pero es un buen conductor y de bajo costo en comparación con otros conductores. Los cables de par trenzado y el cable coaxial son hechos de cobre y se encuentran comúnmente en el lazo del suscriptor y la conexión entre centrales.

El par trenzado consiste de dos cables de cobre aislados típicamente de 0.4 a 0.7 mm de espesor. El par de cables son trenzados juntos para reducir la interferencia externa y la interferencia que pueda producirse entre el par de cables.

El cable es simétrico, la diferencia de voltaje entre los dos cables lleva la señal transmitida. Es utilizado en el lazo del suscriptor, en transmisiones digitales puede alcanzar velocidades de 2 Mbps a distancias superiores a los 2 km., es fácil de instalar y ocupa poco espacio.

El cable coaxial está formado de un núcleo rígido de cobre rodeado de un material aislante, este aislante es revestido con un conductor cilíndrico. El exterior del conductor es recubierto con una protección plástica. El cable coaxial tiene buenas características de ancho de banda y buena inmunidad al ruido eléctrico, es utilizado en sistemas de transmisión analógicos y digitales de alta capacidad.

1.1.6.2 Fibra Óptica

La fibra óptica es el medio más reciente de transmisión, ofrece un gran ancho de banda, gran inmunidad a la interferencia electromagnética y baja atenuación. La fibra óptica tiene un núcleo de vidrio de alta calidad de un diámetro de alrededor de 8 a 60 μm rodeado de un revestimiento de vidrio con un índice de refracción un poco menor al del núcleo.

Las señales transportadas por la fibra son pulsos de luz que luego son convertidas a señales eléctricas en el receptor, en el transmisor pasan de eléctricas a pulsos de luz. Las señales de luz introducidas en el núcleo de la fibra se transportan por continuas refracciones entre el núcleo y el revestimiento. Pueden transmitir a velocidades superiores a los 2 Gbps y transportar hasta 30, 000 canales de voz simultáneamente a largas distancias y con poca atenuación por kilómetro.

La fibra óptica se divide en dos categorías: Las fibras monomodo y las multimodo. Las fibras multimodo tiene diámetros de 125/60 μm (revestimiento/núcleo), se les llama multimodo debido a que los rayos de luz que viaja por ellas se refractan durante todo el recorrido lo que provoca que los rayos lleguen a su destino con distintas fases, se utilizan diodos emisores de luz que transiten longitudes de onda de 850 nm en donde la atenuación de la fibra es de 2 dB/Km. Esta fibra es utilizada en enlaces entre centrales de corta distancia donde no se requiere alta capacidad de transporte ni tampoco se requieren repetidores.

Las fibras monomodo tienen diámetros aproximados de 125/5 μm y son utilizadas en redes de alta capacidad de transporte, enlace de larga distancia y enlaces con repetidores. Se denominan monomodo debido a que solo una longitud de onda puede viajar a través de la fibra con lo que se consigue un mayor ancho de banda pero mayor atenuación. Como elementos de transmisión se utilizan diodos láser con longitudes de onda entre 1.3 ó 1.55 μm .

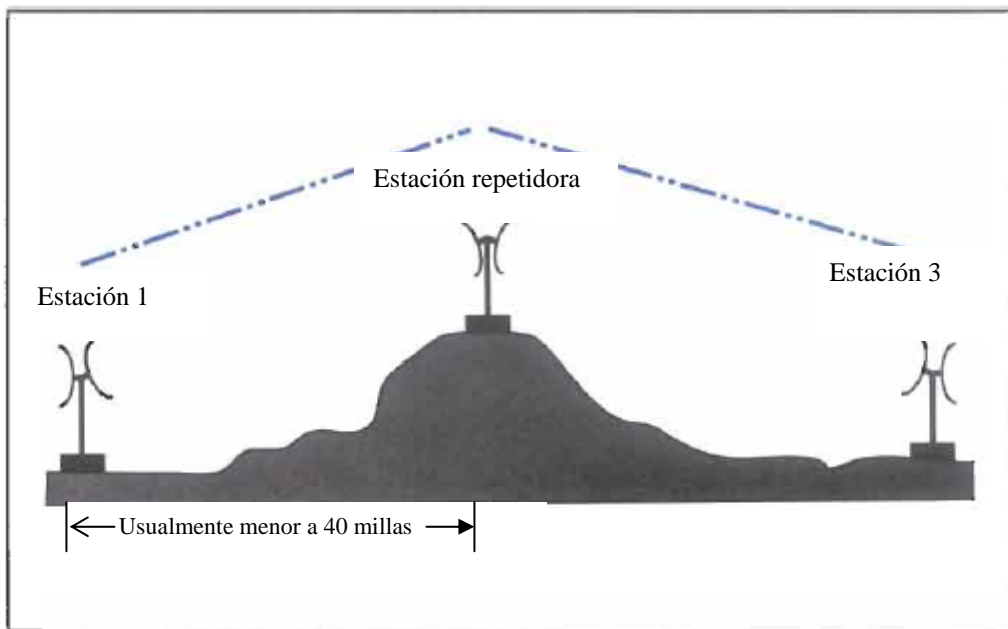
1.1.6.3 Medios inalámbricos

Una de las principales ventajas de los medios inalámbricos es que no se utiliza ningún medio físico para el transporte de la información. La falta de bandas de frecuencias es una de las más importantes restricciones de los sistemas inalámbricos.

En un enlace inalámbrico un repetidor de microondas puede situarse en un satélite localizado comúnmente en una orbita geo-estacionaria, la distancia de esta orbita es de 36,000 km desde la superficie terrestre. Una estación terrestre transmite hacia el satélite en una banda de frecuencia, el satélite la regenera y retransmite en otra banda de frecuencia, la banda de frecuencia se encuentra entre 1 a 30 Ghz. Un retardo de aproximadamente 250 ms se tiene desde que una estación terrestre transmite y la otra recibe en un sistema satelital.

La estación repetidora no necesariamente debe estar ubicada en un satélite, esta puede estar en la tierra, y se puede prescindir de un repetidor si entre las estaciones a comunicarse existe un enlace visual, es decir que no existen obstáculos visuales entre las estaciones, además de esto la potencia de recepción debe de estar entre los rangos establecidos por la estación receptora. La figura 4 muestra un típico enlace inalámbrico con una estación repetidora terrestre.

Figura 5. Enlace Inalámbrico



Fuente: Stephen J. Bigelow, Joseph J. Carr, Steve Winder. **Understanding Telephone Electronics**. Pág. 40.

1.2 PABX

Las PABX (*Private Automatic Branch Exchange*) o comúnmente llamadas PBX son conmutadores telefónicos utilizados en empresas grandes. A través de una PBX se pueden conmutar las llamadas internas de la empresa, además también permiten el acceso a la red telefónica pública⁶. En el caso de usar una PBX es esta quien se enlaza directamente a la central local y no los teléfonos. El uso de un PBX evita conectar todos los teléfonos de una empresa de manera separada a la red telefónica, con lo cual se logra evitar el cobro por llamadas dentro de la misma empresa, ya que estas son encaminadas por el PBX y no por la RTPC.

Estos conmutadores son similares a los utilizados en la RTPC pero de menor capacidad, pero al igual que estos contiene todo lo necesario para la conmutación y señalización. En una PBX la unidad de conmutación puede ser del tipo con bloqueo o del tipo sin bloqueo.

En la PBX con unidad de conmutación sin bloqueo, el número de posiciones de conmutación es igual a la multiplicación de los usuarios de entrada por los de salida con lo que se consigue tener siempre un enlace. En la PBX con bloqueo el número de posiciones de conmutación es limitado, si dicho número es extra limitado se provocara una congestión en la PBX.

A continuación se lista algunas de las funciones realizadas por las PBX

1. Transferencia de llamadas.
2. Sistema para conocer el estado de las extensiones.
3. Sistema de espera en caso de que la extensión solicitada este ocupada.

⁶ Huidobro, José Manuel. **Manual de Telefonía. Telefonía fija y móvil.** (España: Editorial Paraninfo, 1997). p.39

4. Mantener un archivo con información sobre las comunicaciones.
5. Sistema de contraseñas.
6. Desvió de llamadas.
7. Cola de llamadas en caso de que todas las líneas estén ocupadas.

1.3 ISDN

ISDN es una red de conmutación telefónica totalmente digital, que integra los servicios de voz, datos, y video. Su principal objetivo es el reemplazar a la RTPC que se basa en una tecnología analógica, con ISDN no solamente se transforma la red a digital sino que también se le agrega inteligencia, además provee una integración hacia la RTPC.

Se han desarrollado dos tipos de servicios ISDN, ISDN de banda angosta que soporta transmisiones de 144 Kbps hasta los 2.048 Mbps, y los de banda ancha con velocidades de 155.52 Mbps hasta los 622.08 Mbps. En ISDN de banda angosta el servicio que funciona con 144 Kbps se le conoce como BRI (*Basic Rate Interface*) y al que provee 1.544 y 2.048 Mbps como PRI (*Primary Rate Interface*). Para tener acceso a los servicios ISDN se debe de contar con terminales que soporten aplicaciones ISDN ya sea este un teléfono o una computadora. Al igual que en la PSTN el enlace dedicado que une a los suscriptores con las centrales de conmutación ISDN es el lazo local.

BRI funciona con dos canales básicos tipo B y uno tipo D. Una canal B permite transmisiones de voz y datos a 64Kbps bidireccional, este canal no transporta información de señalización, de esto se encarga el canal tipo D, el cual se puede implementar con 16 o 64 Kbps también bidireccionales. Para poder alcanzar los 144kbps provistos por BRI se necesitan 2 canales tipo B y un canal tipo D de 16 Kbp, comúnmente escrito como 2B+D ISDN.

Para alcanzar las velocidades provistas por PRI se necesitan 23 canales B y uno D de 64 Kbps (23B+D ISDN) para alcanzar los 1.544 Mbps y 30 canales B mas un canal D (30B+ D ISDN) para los 2.048 Mbps. Los diferentes tipos de conexiones que se pueden establecer sobre un canal B son: Llamadas por conmutación de circuitos, conexiones semi-permanentes y llamadas por conmutación de paquetes. Las llamadas por conmutación de circuitos son similares a las hechas en la RTPC, la diferencia está en que la señalización es enviada por una canal tipo D. Las semi-permanentes son similares a las líneas arrendadas por la RTPC, pero no se requiere un procedimiento de establecimiento de llamada. En las llamadas por conmutación de paquetes los usuarios son conectados a una red de paquetes y los datos son intercambiados a través del protocolo X.25.

La arquitectura ISDN soporta dos elementos, los cuales son: TE (*Terminal Equipment*) y los NT (*Network Terminations*). Los TE dividen dentro de dos grupos los cuales son: TE1 y TE2. Los TE1 son equipos que soportan ISDN directamente, mientras que los TE2 son equipos que no soportan ISDN y se debe utilizar un TA (*Terminal Adapter*) para conectarlos a la red ISDN. Los NT se agrupan en tres tipos: NT1, NT2 y NT12. La NT1 es la que proporciona la terminación física y eléctrica de la red, permite una adecuada monitorización y mantenimiento, provee un aislamiento entre el bucle del abonado y las TE, además transforman los dos cables de lazo local a cuatro para los TE.

Los NT2 son dispositivos inteligentes que permiten realizar funciones de conmutación, PBX digitales y redes de área local son ejemplos de dispositivos ST2. Los ST12 son dispositivos que unen las funciones de un ST1 y ST2 en un solo equipo. La arquitectura también maneja interfaces entre los dispositivos de la red definidos como puntos de referencia. Se manejan 4 diferentes puntos de referencia, los cuales son: T, R S y U.

Los puntos de referencia S (*System*) representan la conexión entre los equipos ISDN y los separa de las funciones de comunicación relacionadas a la red. Los puntos de referencia T (*Terminal*) permiten el acceso a la red de los dispositivos NT2 a través de los NT1. Los puntos R (*Rate*) son la interfaz de los dispositivos no ISDN y su TA para permitirles conectarse a la red. Los puntos U es la interfaz entre un conmutador ISDN y los ST1.

Los mensajes de señalización utilizados en el canal D se basan en la recomendación ITU Q.931 para proveer las funciones control de llamada, no provee control de flujo ni retransmisión. Al ser un canal bidireccional los mensajes de señalización son enviados de los usuarios a la red y viceversa. Los mensajes provistos por Q.931 son:

- SETUP: Usado para iniciar una llamada
- ALERTING: Indica el inicio de generación del tono.
- CONNECT: Usado para indicar el comienzo de la conexión.
- CONNECT ACKNOWLEDGE: Reconocimiento local del mensaje de conexión.
- DISCONNECT: Usado para terminar una llamada.
- RELEASE: Respuesta a un mensaje de desconexión.
- RELEASE COMPLETE: Confirmación de la liberación correcta de la llamada.
- CALL PROCEEDING: Mensaje enviado por la central a un terminal para establecer una llamada.
- SETUP ACKNOWLEDGEMENT: Confirmación por la central de la recepción del mensaje de SETUP.
- USER INFORMATION: Usado para la señalización usuario a usuario.
- NOTIFY: La central utiliza estos mensajes para enviar información a un terminal durante una llamada.

2. REDES DE DATOS

2.1 Conmutación de paquetes

La conmutación de paquetes es una técnica diseñada para la transmisión de datos digitales en redes de larga distancia. En este tipo de redes la información se divide en paquetes de tamaños específicos para su transmisión y contrario a las redes conmutadas de circuitos¹³ no se dispone de una conexión dedicada durante el tiempo que dure la transmisión de información sino que la ruta se establece por cada paquete transmitido a la red.

Para poder llevar a cabo una transmisión con este tipo de conmutación se hace necesario el uso de conmutadores de paquetes, estos elementos disponen de puertos entrada-salida para la recepción y transmisión de paquetes. Al momento de recibir un paquete este es almacenado y analizado por el conmutador para encontrar la dirección de destino y basado en esta dirección se envía nuevamente a la red, es decir, que el paquete viaja de conmutador en conmutador hasta llegar a su destino final. Debido a que cada paquete puede viajar por un camino distinto al de los demás para llegar a su punto final, cada uno de ellos debe transporta la dirección de destino e información de secuencia (enumeración), para el correcto ensamblaje de los paquetes en el receptor.

¹³ Para transportar señales digitales provenientes de redes de computo a través de la red telefónica analógica, se hace uso del módem (modulador-demodulador) el cual se encarga de convertir las señales para poder ser transportadas por este medio, y en el destino entregar la señal digital nuevamente.

2.1.1 Circuitos Virtuales

Una de las formas de transportar paquetes en una red de datos es a través de circuitos virtuales, también conocido como *connection-oriented service*. Con esta técnica primero se crea una ruta entre la fuente y el destino antes del envío de los paquetes de información. Un paquete de control denominado *Call-Request* se envía hacia el destino a través de los conmutadores, si este está listo para aceptar una conexión envía un paquete *Call-Accept* hacia el terminal que inició la comunicación, establecido el camino y la conexión se procede a intercambiar datos sobre la ruta por la cual pasó el paquete de control *Call-Request*. La conexión dura hasta que alguna de las terminales envía un paquete *Clear-Request*, cada una de las terminales puede tener más de un circuito virtual activo a la vez hacia otras terminales.

El nombre de circuito virtual se debe a que antes de transferir datos se establece una ruta por la cual viajarán todos los paquetes de datos y esta queda establecida el tiempo que dure la conexión, de manera similar a lo que sucede en la conmutación de circuitos pero, en este caso el camino no es dedicado. El uso de un camino común para todos los paquetes en circuitos virtuales hace que sea más fácil el reensamblaje de estos en el receptor ya que se reciben con la misma secuencia con que fueron enviados. La ventaja de usar circuitos virtuales es que primero se debe de establecer una ruta, establecida esta se envían los datos por lo que no se debe agregar una dirección de destino a cada paquete únicamente el identificador del circuito y número de secuencia.

2.1.2 Datagramas

Datagramas es otra técnica para el transporte de paquetes a través de una red de datos. Con esta técnica cada paquete es tratado de manera independiente, por lo que cada conmutador por donde pase un paquete tendrá a su cargo encaminarlo hacia su destino.

Ya que cada paquete puede viajar por caminos distintos, en caso de pérdida de paquetes los conmutadores no pueden determinar cual de ellos se perdió, por lo que es responsabilidad del receptor determinar cual de los paquetes no llegó y enviar a la fuente una petición de reenvío. Además de esto, viajar por caminos diferentes puede provocar que los paquetes se adelanten o atrasen con respecto al ordenamiento con que fueron enviados, por lo que el receptor también es el encargado del ordenamiento de los paquetes.

Una ventaja de la técnica con datagramas es que no se requiere de una llamada para establecer una comunicación ni tampoco una señal de finalización lo cual lo hace más eficiente que circuitos virtuales. La principal diferencia entre ambas técnicas es que, con datagramas el conmutador tiene que tomar decisiones de encaminamiento por cada paquete, mientras que con circuitos virtuales se hace una sola vez para todos los paquetes que utilizan dicho circuito. El envío de datos a través de datagramas suele ser más confiable que con circuitos virtuales ya que si un conmutador falla, todos los circuitos que pasen por ese conmutador se pierden, mientras que con datagramas si un conmutador falla los paquetes subsiguientes pueden viajar por una ruta alternativa que no pase por el conmutador defectuoso. Las figuras 6 y 7 muestran ambas técnicas de conmutación.

Figura 6. Circuitos Virtuales

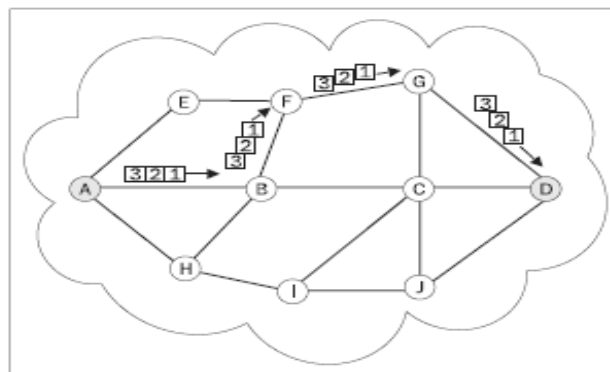
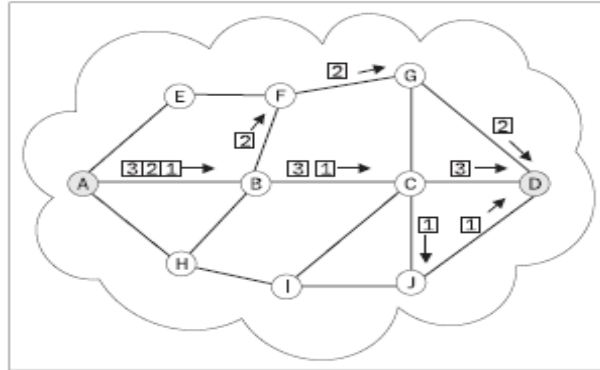


Figura 7. Datagramas



Fuente: Dostálek, Libor. Alena Kabelov. **Understanding TCP-IP**
Pág. 18, 19

2.2 Protocolo TCP/IP

El protocolo TCP/IP (*Transmission Control Protocol/Internet Protocol*) fue desarrollado por el Departamento de Defensa de los Estados Unidos para garantizar y preservar la integridad de los datos y poder mantener una comunicación en caso de una guerra, esta arquitectura se desarrolla en base de la ARPANET (*Advanced Research Projects Agency Network*). El rápido crecimiento de la Internet ha hecho del protocolo TCP/IP una parte integral de la mayoría de sistemas operativos como Windows, Unix, Linux y una de las arquitecturas de red más empleadas en el mundo.

El protocolo está conformado por 4 capas, las cuales se enumeran a continuación:

1. Capa física y enlace de datos: Define las características de transmisión tales como: la tasa de transferencia y el esquema de codificación. Es responsable del intercambio de datos entre el sistema final y la red a la que se está conectado.

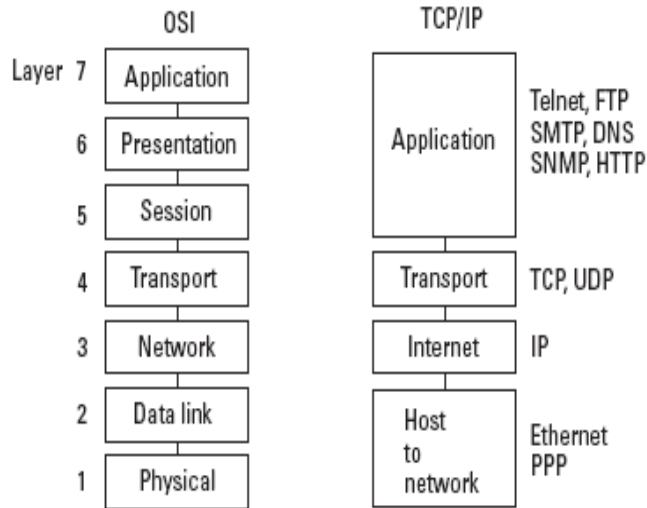
2. Capa del protocolo de Internet (IP): Usada para transmitir datagramas IP entre computadoras remotas. Transporta paquetes de información a su destino correspondiente.
3. Capa de transporte (TCP y UDP): Permite la comunicación extremo a extremo desde un programa de aplicación a otro. Puede proveer un transporte confiable asegurándose de que los datos lleguen sin errores y en la secuencia correcta. En esta capa se encuentran los protocolos TCP y UDP (User Datagram Protocol). TCP es un protocolo orientado a conexión, utilizado si se requiere un enlace confiable. UDP al contrario es un servicio no orientado a la conexión, utiliza datagramas para el transporte y no es un servicio fiable.
4. Capa de aplicación: Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET) y el protocolo HTTP (Hypertext Transfer Protocol).

A pesar de que el protocolo TCP/IP es el más utilizado, otra arquitectura conocida como OSI (*Open Systems Interconnection*) es la más aceptada. Este modelo está formado por 7 capas: Capa física, capa de enlace de datos, capa de red, capa de transporte, capa de sesión, capa de presentación y la capa de aplicación. La figura 8 muestra la relación entre ambas arquitecturas.

El modelo fue desarrollado por la necesidad de interconectar sistemas de distintos fabricantes, por lo que fue hecho con base en necesidades generales de todos los sistemas, de tal forma que los fabricantes pudieran apearse a estas funciones¹⁴.

¹⁴ Gascon, Aldo. Jorge Silis. GS comunicaciones. **Telecomunicaciones: Redes de datos**. (México: McGraw-Hill, 1997). p.58

Figura 8. Relación entre arquitecturas



Fuente: Anttalainen, Tarmo. **Introduction to Telecommunications Network Engineering**. Pág. 256.

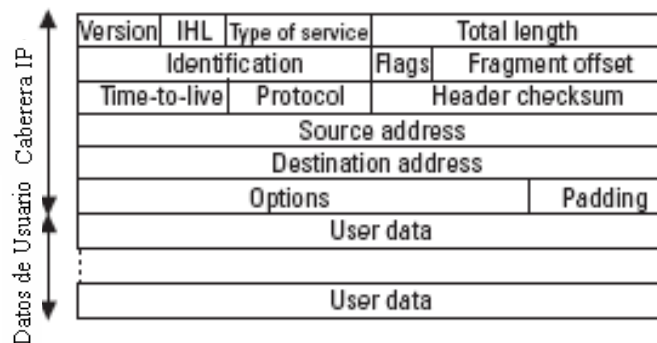
Cada capa en el protocolo TCP/IP se relaciona con las capas adyacentes inmediatas. En la fuente, la capa de aplicación hace uso de la capa de transporte y envía datos hacia las capas inferiores. Una relación similar existe entre la interfaz de transporte y la capa de Internet, en la interfaz de Internet y la capa de acceso. En el destino cada capa distribuye datos hacia las capas superiores. El uso individual de las capas no es requerido en la arquitectura, lo que hace posible desarrollar aplicaciones que recurran directamente a los servicios de una de las capas.

2.2.1 Protocolo IP

Este protocolo es utilizado para habilitar conexiones de redes individuales dentro de la red mundial de Internet¹⁵. Define el formato de los datos enviados a través de las redes, además, especifica los mecanismos de direccionamiento y encaminamiento. El protocolo proporciona un servicio de distribución de paquetes entre host y enrutador o entre enrutadores, no es orientado a conexión y no garantiza fiabilidad en la transmisión de datos.

El enrutador es el elemento básico necesario para enlazar redes individuales dentro de la red mundial, el protocolo IP debe de ejecutarse tanto en terminales de usuario como en los enrutadores. La unidad básica de transferencia de datos es llamado datagrama IP, un datagrama IP consta de una cabecera y un campo de datos de usuario, usualmente la cabecera consta de 20 bytes pero puede hacerse mayor debido a que contiene campos opcionales. La figura 9 muestra un datagrama IP:

Figura 9. Datagrama IP



Fuente: Anttalainen, Tarmo. **Introduction to Telecommunications Network Engineering**. Pág 310.

¹⁵ Dostálek, Libor. Kabelová Alena. Understanding TCP/IP. (UK: Packt Publishing, 2006) p.129

- Campo versión (*Version*): Especifica la versión utilizada del protocolo, actualmente se utiliza la versión 4, como reemplazo eventual se desarrolla la versión 6.
- La longitud de la cabecera (*IHL*): Contiene la longitud de la cabecera del datagrama IP. La longitud mínima de la cabecera es de 20 bytes y el menor valor del campo es de 5.
- Campo tipo de servicio (*Service Type*): Especifica como el datagrama es manejado por el sistema, el campo determina la calidad del servicio, aunque el protocolo IP no garantiza la calidad deseada. Tiene una longitud de 8 bits, los 3 primeros bits son usados para definir la prioridad, los bits 4, 5, 6 son usados para: solicitud de bajo retardo, solicitud de alto nivel de procesamiento y solicitud de alta fiabilidad, hay que tomar en cuenta que la solicitud de fiabilidad no garantiza que esta sea proporcionada.
- Campo longitud de datagrama (*Total Length*): Contiene la longitud total del datagrama (cabecera y datos), su longitud es de 2 bytes, por lo que el máximo tamaño del datagrama debe de ser de 65, 535 bytes.
- El identificador de datagrama (*Identification*): Sirve para identificar a un datagrama y permite al destino saber que fragmentos pertenecen a un datagrama en particular, en caso de que este haya sido fragmentado.
- Las banderas (*Flags*) especifican si un determinado datagrama ha sido fragmentado, tiene una longitud de 3 bits, el primero de ellos indica que el datagrama no ha sido fragmentado (colocado en 1), el segundo indica que el fragmento llegado es el último si el bit está colocado en 0, el tercer bit permanece sin uso.

- Campo desplazamiento de fragmento (*Fragment offset*): Es utilizado para que el destino puede reensamblar todos los fragmentos recibidos, empezando con 0 al valor más alto.
- El tiempo de vida (*Time to live*) contiene la duración de un paquete en la internet, es decir, un paquete para poder llegar a su destino puede pasar por muchos enrutadores, el valor del campo comúnmente es de 64, lo que indica que un paquete puede pasar por 64 enrutadores antes de ser descartado. Cada enrutador por donde pasa el paquete debe de disminuir en uno el valor del campo TTL.
- Campo de protocolo (*protocol*): Contiene al número que identifica que protocolo de la capa superior (TCP o UDP) es encapsulada dentro del área de datos del datagrama IP. El número usado para TCP es el 6 y para UDP es el 17.
- La cabecera de suma de verificación (*Header Checksum*) contiene la suma de verificación pero únicamente para la cabecera del datagrama IP. El valor del campo debe de ser ajustada por cada enrutador por el que pasa el paquete IP, esto debido a que los campos de la cabecera del datagrama IP pueden cambiar de enrutador en enrutador, como por ejemplo el valor del campo *time to live*.
- Campos de dirección IP fuente y destino (*Source Address, Destination Address*): Contienen las direcciones de envío y de recepción de los datagramas.
- Campo opciones (*options*): Contiene información para el testeo y depuración de la red.
- Campo de relleno (*Padding*): Es usado para hacer la cabecera IP múltiplo exacto de 32 bits. Se colocan únicamente si son necesarios.

- Campo datos: Es variable y su longitud es especificada en la cabecera del datagrama. Debe de ser un múltiplo entero de 8 bits.

2.2.2 Dirección IP

Una dirección IP sirve para identificar redes y a los nodos (terminales) conectados a ellas. La dirección tiene una longitud de 32 bits (4 bytes) para la versión 4. Las direcciones comúnmente se escriben en formato decimal, cada byte se separa por un punto, por ejemplo la dirección 127.0.0.1 está escrita en el formato anteriormente dicho.

La primera estructura de una dirección IP estaba compuesta por una dirección de red y una dirección de computadora. Dentro de esta estructura las direcciones se dividieron en 5 clases: Clase A, B, C, D y E. A continuación se explican las características de cada una de las clases:

- La clase A es utilizada si se requiere un pequeño número de redes y un gran número de terminales. Se pueden acomodar 126 redes y cada red contener $2^{24}-2$ computadoras. El primer bit de la clase A es 0 los restantes 7 bits del primer byte representan la dirección de red, los 24 sobrantes de la dirección son utilizados para las direcciones de computadora.
- La clase B puede contener 2^{14} redes y cada red $2^{16}-2$ computadoras. Los primeros dos bits de el primer byte son 10_2 los siguientes 6 bits restantes y el segundo byte corresponden a la dirección de red y el resto la dirección de computadoras.

- La clase C es utilizada si se requiere un número grande de redes y uno menor de computadoras. Los primeros bits del primer byte son 110_2 los 5 bits restantes y los 2 bytes siguientes representan la dirección de red, el último byte es utilizado para las direcciones de computadora. Se pueden acomodar 2^{21} redes y cada red contener 2^8-2 computadoras.
- La clase D no se divide en dirección de red ni de computadoras, debido a que es usada para direccionamiento multi-cast. El direccionamiento multi-cast es utilizado si se requiere el envío de datagramas de manera simultánea a varios computadores. Los primeros 4 bits del primer bytes son 1110_2 los 28 siguientes representan la dirección multi-cast.
- La clase E es reservada para usos futuros.

Debido al gran auge de la Internet, el uso del direccionamiento anteriormente descrito hace probable que se puedan agotar rápidamente las direcciones IP. Para solventar el problema se desarrollo un sistema de subredes, el cual consiste en dividir las redes clase A, B, C en redes más pequeñas, es decir que cada red contendrá a otras redes dentro de ella.

2.2.2.1 Mascara de red

Una mascara de red es un número compuesto de 4 bytes, utilizada para ayudar a definir las direcciones de red¹⁶. La dirección de red puede ser determinada por la multiplicación lógica de cada bit de la dirección IP por los correspondientes bits de la mascara de red.

¹⁶ Dostálek, Libor. Kabelová Alena. Understanding TCP/IP. (UK: Packt Publishing, 2006) p.170

Las clases A, B y C tiene definidas mascararas de red y son conocidas como mascararas de red estándar. La clase A tiene definida la mascara 255.0.0.0, la clase B tiene la mascara 255.255.0.0 y la clase C tiene la mascara 255.255.255.0.

2.2.2.2 Subredes

Una sub-red es una división de una red principal, la cual debe tener su propia dirección IP y una mascara de subred. El direccionamiento IP a través de sub-redes permite que muchas redes físicas compartan la misma dirección IP de red. La estructura de la dirección IP ahora es dividida en 3 partes: dirección de red, la dirección de sub-red y la dirección de computadora, la dirección de computadora de la estructura explicada en la sección 2.2.2 se divide en la dirección de sub-red y de computadora, por lo que se tiene una estructuras jerárquica la cual es interpretada de manera local. Desde el punto de vista externo la red sigue siendo única aunque internamente este sub-dividida en otras redes. El enrutamiento interno de la red debe realizarse usando direccionamiento de sub-red, para ejecutar las funciones de ruteo cada terminal necesita conocer su dirección IP y mascara de sub-red, la cual es la misma para todas las sub-redes pertenecientes a la red principal.

La función de la máscara de subred es indicar qué parte de una dirección IP corresponde a la dirección de la red (red y subred), y que parte es la correspondiente a la dirección de computadora. Al igual que la una dirección IP esta se puede escribir en formato decimal con punto y esta formada por 32 bits (4 bytes).

La sección de la dirección IP que corresponda con los unos de la mascara es la parte que corresponde a la dirección de red y sub-red, y la parte de la dirección que corresponda con los ceros de la mascara corresponde a la dirección de computadora.

Por ejemplo, si se tiene una dirección IP 204.15.5.0 y una máscara de sub-red 255.255.255.224, procedemos a pasar la dirección IP la máscara a su forma binaria:

204.15.5.0 = 1100 1100. 0000 1111. 0000 0101. 0000 0000
255.255.255.224 = 1111 1111. 1111 1111. 1111 1111. 1110 0000

Se puede notar que esta es una dirección clase C (los primeros bytes son 110_2), esta clase utiliza el último byte para las direcciones de computadora. Pero con el direccionamiento de sub-red esta es ahora dividida en dirección de sub-red y de computadora. Podemos notar que se han tomado 3 bits para dirección de sub-red y 5 para direcciones de computadora, por lo que podemos tener 8 sub-redes y 32 computadoras por sub-red. El número de sub-redes y computadoras dependerá de las características que se deseen para la red.

En el direccionamiento por sub-red todas las sub-redes deben usar la misma máscara de red, lo que puede llevar al desaprovechamiento de direcciones si no se dimensionan de manera igual (se dimensiona para la sub-red más grande), en el ejemplo anterior se tenían 8 sub-redes con 32 computadoras cada una, si una de las redes únicamente contiene 6 computadoras se desaprovecharían 26 direcciones, a menos que se tenga en cuenta una ampliación posterior de la sub-red. Utilizar direccionamiento por sub-red permite un mejor manejo ante una creciente demanda de direcciones IP.

Para solucionar el problema del desaprovechamiento del uso de direcciones se desarrolló el sistema VLSM (*Variable Length Subnet Mask*), en donde cada sub-red puede utilizar una máscara diferente que se ajuste a las necesidades de la sub-red, lo que permite un mejor manejo del espacio de direcciones. El uso de VLSM hace que el manejo y mantenimiento de la red sea más complejo.

2.2.2.3 CIDR y Súper-Redes

Una súper-red es un conjunto de redes tipo C contiguas que pueden ser asignadas en lugar de una dirección tipo B, en la máscara estándar de la red tipo C los bits de dirección de computadora pueden ser extendidos hacia los bits de dirección de red para obtener un mayor número de direcciones que puedan ser asignadas a las computadoras. La implementación del direccionamiento por súper-red, es debido a que una sola red tipo C es demasiado pequeñas para cumplir con los requisitos de las actuales de las empresas, lo que provoca el rápido agotamiento de las redes tipo B.

El asignar varias direcciones tipo C ayuda al problema de la redes clase B, pero esto conlleva un nuevo problema, los datos que los routes almacenan e intercambian crecer considerablemente. Un método conocido como CIDR (*Classless Inter Domain Routing*) usado actualmente para el direccionamiento IP, resuelve el problema anteriormente descrito. CIDR agrupa redes tipo C representadas por la dirección de red más baja y una máscara de red de 32 bits. CIDR no utiliza únicamente direcciones tipo C, más bien con este sistema se hace caso omiso de las clases de direcciones, lo que se requiere es que cada grupo de direcciones sea potencia de dos, y la utilización de una máscara para identificar el tamaño del grupo. La forma de representar una dirección con sistema CIDR es el siguiente: 198.192.10.30 / 21, donde 198.192.10.30 representa la dirección más baja del grupo y 21 la máscara.

2.2.2.4 IP Versión 6

Con la versión 6 de IP se consiguen resolver todos los problemas descritos anteriormente para la versión 4. Los sistema de super-redes y CIDR son únicamente medios por los cuales se consigue alargar la vida de la versión 4, mientras se logra consolidar la nueva versión.

IPv6 no solo incrementa la longitud de la dirección de 32 bits (4 bytes) a 128 (16 bytes) sino que además mejora la seguridad, modifica el formato de la cabecera IP para reducir el procesamiento de los enrutadores, tiene soporte para audio y video en tiempo real y es compatible con la IPv4.

La cabecera base de la versión 6 consta de 8 campos los cuales se explican a continuación:

- Versión (*Version*): Contiene el número de versión del protocolo. En este caso 6.
- Clase de tráfico (*Traffic Class*): Si una red se llega a sobrecargar los enrutadores deben descartar algunos datagramas, en este campo se indica la prioridad de los datos y así saber cuales datos son menos importantes y ser los primeros en ser descartados.
- Etiqueta de flujo (*Flow Label*): Este campo especifica el tipo de manejo que deben recibir datos especiales como: audio y video.
- Longitud de carga útil (*Payload length*): Este campo especifica la longitud del datagrama IP con excepción de la cabecera base.
- Próxima cabecera (*Next Header*): Indica la próxima cabecera seguida de la cabecera base. La figura 10 muestra los valores que puede tomar el campo.

Figura 10. Valores del campo Next Header

0	Hop-by-Hop Header
4	IP protocol
6	TCP protocol
17	UDP protocol
43	Routing Header
44	Fragment Header
45	IRP Protocol
46	RRP protocol
50	Encapsulating Security Payload
51	Authentication Header
58	ICMP protocol
59	No next header follows
60	Destination Options

Fuente: Libor Dostálek, Alena Kabelov. Understanding TCP-IP

Pág. 215.

- Limite de salto (*Hop Limit*): Este campo es disminuido en 1 por cada enrutador por el que pasa el paquete, si llega a cero el paquete es descartado.
- Dirección Fuente (*Source Address*): Especifica la fuente de los datos, tiene una longitud de 128 bits.
- Dirección Destino (*Destination Address*): Especifica el destino de los datos tiene una longitud de 128 bits.

Dentro del protocolo IPv6 se utilizan tres tipos de direccionamiento:

- Unicast: Identifica a una sola interface de red. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección.

- Multicast: Identifica a un grupo de interfaces de red. Un paquete enviado a una dirección multicast es entregado a todo el grupo identificado con dicha dirección.
- Anycast: Al igual que multicast identifica a un grupo de interfaces, pero con la diferencia que un paquete enviado a una dirección anycast es entregado a la interface más cercana identificada con dicha dirección. La medida de cercanía se realiza con protocolos de ruteo.

La forma de representar la direcciones IPv6 es a través de dígitos hexadecimales de la forma: hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh donde cada “h” representa un dígito hexadecimal. Si algunos de los bloque contiene ceros a la izquierda no es necesario escribirlos, pero por lo menos debe existir un número por cada bloque. Por ejemplo: AB34 : 4589 : 3: 4567 : 9: FCDA : 9867 : 8123.

Para las cadenas largas de ceros se tiene la notación especial ::, la cual deberá ir una sola vez por cada dirección. Por ejemplo la dirección AB34: 4589: 0: 0: 0: 0: 9867: 8123 puede representarse de la siguiente forma: AB34 : : 9867 : 8123.

Para situaciones en las que se trabaje con IPv4 e IPv6 de manera conjunta se utiliza la notación: hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:d.d.d.d, donde cada “d” representa un número decimal (8 bits cada uno). Ejemplo: DCAB::FCAA: 192.165.10.128.

Las direcciones de red son identificadas de la misma manera que en el sistema CIDR en IPv4: dirección de red / prefijo de red. Donde la dirección de red representa una dirección en cualquiera de los formatos expuestos con anterioridad. El prefijo de red es un número decimal que especifica cuantos bits de la parte superior representan a la dirección de red.

2.2.3 Protocolo TCP

TCP es un protocolo de transporte orientado a la conexión, es decir, que se crea una conexión (circuito virtual) entre dos aplicaciones que corren en las terminales conectadas. El enlace creado es *full-duplex* y se transfieren datos en ambas direcciones simultánea y independientemente.

Un protocolo orientado a conexión es frecuentemente descrito como un servicio fiable y secuencial en la transferencia de datos. La conexión puede ser deshabilitada en cualquier tiempo por cualquiera de las partes involucradas en la comunicación o por el protocolo mismo¹⁷.

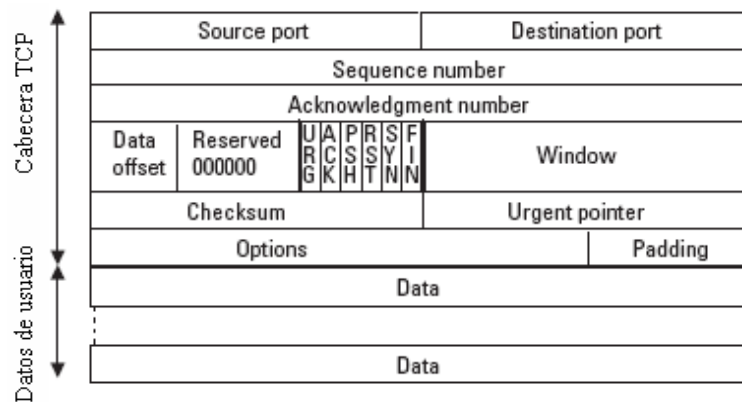
Los bytes transferidos son enumerados, en caso de pérdida o daño los datos son solicitados nuevamente. Una suma verificación (*checksum*) es utilizada para garantizar la transferencia de los datos. En TCP tanto el destino como la fuente son identificados por un número de puerto, este número está constituido por 2 bytes, y tienen un rango de enumeración de 0 a 65535.

El número de puerto es usado por el sistema operativo para reconocer a que aplicación debe entregar el segmento TCP recibido. Por ejemplo la transferencia de ficheros (FTP) tiene asignado el puerto 21, la conexión remota (TELNET) el puerto 23, http (HiperText Transfer Protocol) el puerto 80. Ya que UDP también utiliza números de puerto en el mismo rango que TCP y estos no son comunes a los protocolos, se hace necesario colocar junto al número de puerto el nombre del protocolo utilizado (23/TCP, 23/UDP).

¹⁷ Leon Silva, Arturo. Carlos Alonso Alcántara. GS comunicaciones. **Telecomunicaciones: Redes de datos**. (México: McGraw-Hill, 1997). p.135

La unidad básica de transferencia del protocolo es llamada segmento TCP o paquete TCP. El segmento esta constituido por una cabecera con una longitud mínima de 20 bytes y una unidad de datos de usuario de longitud variable. La figura 11 muestra el formato de un segmento TCP.

Figura 11. Segmento TCP



Fuente: Tarmo Anttalainen. **Introduction to Telecommunications Network Engineering**
Pág. 321.

- Puerto de origen (*Source Port*): Es el número de puerto que identifica a la aplicación de origen.
- Puerto destino (*Dest. Port*): Identifica a la aplicación destino, ambos números de 16 bits.
- Número de secuencia (*Sequence No.*): Necesario debido a que un segmento TCP es una parte de un gran flujo de datos entre la fuente y el destino. Tiene una longitud de 32 bits y normalmente la enumeración no inicia de cero, mas bien el número de secuencia inicia por un número elegido aleatoriamente.
- Número de reconocimiento (*Ack. No.*): Representa el número del próximo byte que el destino esta dispuesto a aceptar.

- Longitud de cabecera (*Header Length*): Especifica la longitud de la cabecera del segmento TCP en múltiplos de 32 bits, requerida porque la longitud de la cabecera varía debido a la presencia de campos opcionales.
- Bits de código (code bits): Esta compuesto por seis bits que especifican el propósito y contenido del segmento, si estos bits son colocados la siguiente información es transmitida:
 - URG: Indica que el campo de urgencia es válido.
 - ACK: El segmento tiene un número de reconocimiento válido.
 - PSH: Especifica que los datos deben ser enviados inmediatamente. Cuando una aplicación requiere el envío de datos, TCP toma los datos acumulados sin esperar que el segmento este lleno y los marca con la bandera PSH.
 - RST: Restablece la conexión TCP.
 - SYN: La fuente inicia un nuevo conteo de secuencia.
 - FIN: Indica que la fuente ha enviado todos los datos.
- Campo Windows: Especifica el tamaño del buffer, indicando la cantidad de datos listos a ser aceptados, se inicia con el byte indicado en el campo ACK.
- Checksum: Es usado para garantizar la integridad de los datos enviados, es calculado a partir de las cabeceras TCP e IP y el campo de datos. Una estructura llamada pseudos-cabecera es utilizada para el calculo del checksum, la pseudos-cabecera esta formada por los bits de la dirección IP fuente (32 bits), la dirección IP destino (32 bits), bits de ceros (8 bits), bits de protocolo (8 bits) y bits de longitud TCP (16 bits). El checksum es calculado a partir del complemento a uno de palabras de 16 bits y al resultado se aplica nuevamente el complemento a uno.

- Puntero de urgencia (*Urgent Pointer*): Tiene una longitud de 16 bits y sirve para indicar que los datos del segmento TCP son urgentes. La aplicación destino debe de procesar este segmento antes que cualquier otro segmento.
- Campo opción (*options*): Es utilizado para negociar el máximo tamaño del segmento TCP, usualmente de 536 bytes. Además, incluye otras opciones como: *Windows scale factor*, *timestamp value*, *timestamp echo reply*, *connection count*, *new connection count* y *connection count echo*.
- Campo *padding*: Es usado para completar el segmento TCP.
- Campo dato (*data*): Es donde se incluyen la información que el usuario desea enviar.

Al iniciarse una conexión TCP, quien recibe la petición puede aceptarla o rechazarla, desde el punto de vista de la capa de aplicaciones quien inicia una conexión es el cliente y quien espera por una es el servidor.

Antes del envío de datos a través del protocolo TCP se hace necesario establecer una conexión. Esta conexión se divide en tres fases: Inicio de conexión, transferencia de datos y fin de la conexión.

Para establecer la conexión se realizan los siguientes pasos:

1. El cliente envía una petición de conexión. Se transmite un número de secuencia, esto provoca el levantamiento de la bandera syn, ya que se inicia un nuevo conteo de secuencia.

2. El servidor responde a la petición. Se transmite nuevamente el número de secuencia enviado por el usuario más uno, el número de secuencia generado por el servidor más un número de reconocimiento (Ack No.).
3. El cliente responde nuevamente. Se transmite un número de reconocimiento más el número de secuencia recibido, con este último paso se da por finalizada la fase de establecimiento de conexión, quedando ambos terminales a la espera de la transferencia de datos.

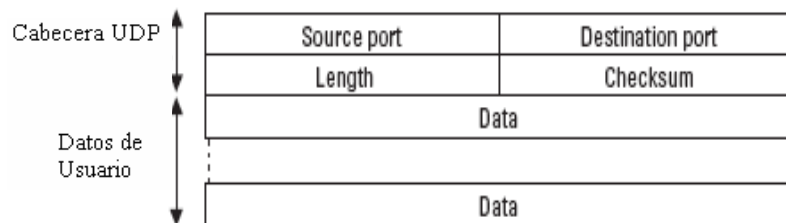
Para finalizar una conexión se realizan los siguientes pasos:

1. Para finalizar la conexión se envía un paquete con la bandera fin, este puede ser enviado por el cliente o el servidor.
2. El que recibe la petición de finalizar conexión envía un número de reconocimiento. La conexión en una de las vías queda finalizada. Esto debido a que la conexión creada es full-duplex, por lo que se pueden finalizar las conexiones independientemente.
3. Para que la otra parte puede finalizar conexión envía un paquete con la bandera fin.
4. Se finaliza la conexión luego de recibir un número de reconocimiento.

2.2.4 Protocolo UDP

UDP es un protocolo no orientado a conexión (datagrama) perteneciente a la capa de transporte que proporciona una comunicación sencilla entre aplicaciones. Además permite la comunicación punto-punto y punto-multi-punto. Al igual que TCP utiliza puertos para identificar tanto al destino como a la fuente. Su cabecera es más pequeña lo que lo hace útil en aplicaciones de tiempo real, ya que es más rápido procesarla. Al ser no orientado a conexión no garantiza la llegada de los datos, además no hay procedimientos para recuperación de datos. El tamaño de su cabecera es de ocho bytes y consta de cuatro campos la figura 12 muestra el segmento UDP.

Figura 12. Segmento UDP



Fuente: Tarmo Anttalainen

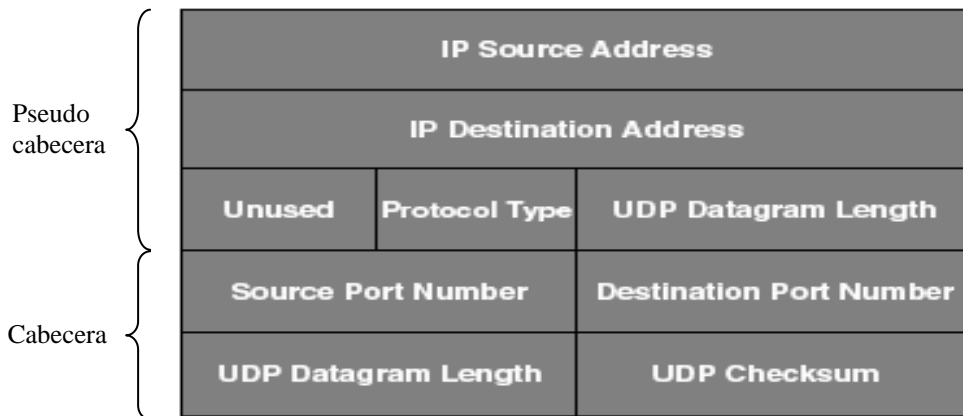
Introduction to Telecommunications Network Engineering

Pág. 326.

Los dos primeros campos *Source Port Address* y *Destination Port Address*, indican respectivamente las direcciones de puerto fuente y destino ambos tiene una longitud de 16 bits. El puerto origen puede ser opcional ya que UDP no solicita una respuesta de recepción de dato, si no se usa debe colocarse a cero. El campo *Message Length* indica la longitud del datagrama UDP (cabecera y datos), como mínimo debe de tener un valor de 8 bytes si no se agregan datos.

El campo Checksum es un campo opcional y se coloca a cero si no se utiliza, envuelve tanto a la cabecera como a los datos y contiene información para la protección de datagramas mal encamidos. UDP incluye una pseudo-cabecera de 12 bytes utilizada para el cálculo del *checksum* en conjunto con la cabecera UDP. La figura 13 muestra tanto la cabecera como pseudo-cabecera UDP.

Figura 13. Cabecera y pseudos-cabecera UDP



Fuente: Shepard, Steven. **Voip Crash Course**. Pág. 95.

La pseudo-cabecera incluye la dirección IP de la fuente y el destino, un campo de protocolo (17 para UDP) y la longitud del datagrama. La pseudo-cabecera es rellena con octetos de valor cero en la parte final necesario si la pseudo-cabecera no es un múltiplo de dos octetos. Muchas aplicaciones cliente-servidor que tienen una solicitud y una respuesta usan el UDP para evitar tener que establecer y luego liberar una conexión, como en el caso de TCP. Algunas de las aplicaciones que utilizan UDP son: DNS, TFTP, NetBios, SNMP.

3. TELEFONÍA IP

3.1 Voz sobre IP

Con el tiempo, las redes telefónicas han experimentado cambios evolutivos importantes, impulsados esencialmente por el progreso tecnológico en varios campos (conmutación, transmisión, acceso y mantenimiento), el último de esos cambios ha sido la digitalización de su tecnología de transporte, que ha tenido una considerable influencia en la integración²³.

El uso de paquetes IP para el transporte de señales de voz sobre redes de datos es conocido como voz sobre IP (VoIP), y es una de las más importantes tendencias en las telecomunicaciones. Esta tecnología no es nueva y debido al gran auge del Internet empieza a popularizarse ya que unifica las redes de voz y datos. Transportar señales de voz sobre redes de datos conlleva problemas que no existen en la RTPC o que ya se habían solucionado. Problemas como ancho de banda, delay, jitter, pérdida de paquetes, son algunos de los problemas que afectan la calidad de servicio en VoIP.

Las señales de voz son del tipo analógico y es necesario su digitalización para poder viajar por redes de datos, lo que hace necesario el uso de codec (Coder-Decoder) que son los encargados de convertir la señal analógica en una señal digital, codificarla y comprimirla y viceversa.

²³ Grupo de expertos sobre telefonía IP del UIT-D. Informe Esencial sobre Telefonía IP. (Suiza: Unión Internacional de Telecomunicaciones, 2003). p.13

Existen diferentes tipos de codecs cada unos con distintas características de ancho de banda y tipo de codificación, entre los estándares establecidos por la ITU tenemos: G.711, G.721, G.728, G.729 y G.723.1²⁴. Para negociar y entablar una comunicación entre usuarios en una red VoIP se hace uso de protocolos de señalización, entre los más utilizados actualmente tenemos: H.323, SIP y MGCP.

La principal aplicación de VoIP es la telefonía IP, con lo cual se logra transportar conversaciones telefónicas a través de redes conmutadas de datos en vez de las típicas redes de conmutación de circuitos. Debido a que TCP/IP es esencialmente un protocolo para el transporte de datos no se obtienen buenos resultados si se desea transportar paquetes de voz, por lo que las redes VoIP utilizan RTP (*Real-Time Transport Protocol*) en conjunto con UDP/IP para el transporte de los paquetes de voz. La unión de estos protocolos es comúnmente escrito como RTP/UDP/IP y actualmente es utilizado por la mayoría de protocolos de señalización de VoIP.

UDP es utilizado para aplicaciones de tiempo real debido a que con este protocolo no se requiere confirmación de parte del receptor, contrario a TCP que si requiere confirmación para continuar el envío de paquetes lo que provoca altos retardos inaceptables en aplicaciones de tiempo real como VoIP. Además de esto la cabecera UDP es mucho mas pequeña que la TCP lo que hace que su procesamiento sea mucho mas rápida.

La calidad de servicio (QoS) es una parte fundamental en las transmisiones VoIP, ya que permite una buena o mala recepción de la voz transmitida. Los principales problemas que limitan la QoS en redes VoIP se listan a continuación²⁵:

²⁴ En la pagina oficia de la ITU se puede encontrar explicación detallada de cada uno de estos codec, en algunos se incluye los archivos que contienen los código fuente.

²⁵ Los documentos G.1010 y G.114 de la ITU proporcionan información relacionada a la calidad de servicios en ambientes multimedia y tiempos de transmisión en un sentido extremo-extremo.

1. Retardo (*Delay*): En redes de transmisión de voz un retardo denominado también latencia, es el tiempo que le toma a una señal de voz alcanzar al usuario que toma parte en una conversación y pueda escuchar lo que se le ha transmitido. Los retardos pueden ocasionar la degradación de la calidad de la voz, lo que puede provocar la dificultad de mantener una conversación. Dos tipos de efectos son ocasionados por el retardo: Eco y traslape. El eco se debe a la reflexión de la señal enviada al equipo distante, es decir, que la señal enviada regresa nuevamente a la fuente con cierto desfase y atenuada. Si el retardo llega a ser mayor a los 50 ms el eco se convierte en un serio problema, por lo que se debe de disponer del equipo necesario para llevar a cabo la cancelación de la señal reflejada. El traslape se origina si el retardo en una vía es superior a los 250 ms. Tres tipos de retardos son inherente a las redes de telefonía actual pero que también afectan a las redes de datos: Retardo de propagación, retardo de manejo o de procesamiento y el retardo de serialización. El retardo de propagación es debido a la longitud del medio físico de transporte por el cual viajan las señales, ya sea por fibra optica, cables de cobre o aire. El retardo de procesamiento es debido a los codec, el empaquetado (RTP/UDP/IP para VoIP) y por los procedimientos de encaminado que realizan los enrutadores en la red. El retardo de serialización es el tiempo que toma poner los datos dentro del enlace físico que interconecta a los equipos. Otro tipo de retardo originado en las redes de conmutación de paquetes y conocido como retardo de cola, es originado por la retención de paquetes en una red congestionada. La ITU recomienda que para tener una buena calidad de servicio no se debe pasar los 150 ms en una vía en retardos punto a punto (*end to end*).
2. Variación del retardo (*Jitter*): Es la variación de retardo con que llegan los paquetes de voz a su destino y es un problema que existe solamente en las redes de conmutación de paquetes.

Debido al congestionamiento en una red, pérdida de sincronización o el camino tomado por cada paquete, hace que el retardo sea distinto entre ellos, lo que causa un mayor problema que si todos llegaran con el mismo retardo. Para minimizar este efecto se suele utilizar buffers de retención de paquetes de manera que se envíe al decodificador los bloques codificados de manera sincrónica. Una práctica recomendada es contar el número de paquetes que llegan parte y calcular la razón entre estos paquetes y el número de los paquetes que se han procesado con éxito, y utilizarlo para ajustar el buffer de jitter. Este ajuste al buffer de jitter es efectivo para compensar los retardos en los paquetes recibidos. El uso de estos buffer ayuda además a solucionar los problemas de la llegada de tramas RTP fuera de orden, valiéndose del número de secuencia de cada trama. El retardo total es aumentado por el uso de estos buffer, esto debido a que a más jitter el tamaño del buffer debe ser mayor.

3. Pérdida de paquetes: Las redes IP no garantizan la calidad de servicio, y debido al congestionamiento en la red, algunos paquetes deben de ser desechados. Algunos protocolos de transporte como TCP corrigen el error solicitando una retransmisión, pero en VoIP se utiliza UDP por lo que se debe utilizar otras técnicas para compensar la pérdida de paquetes. La interpolación de pérdida de paquetes, es una técnica en la cual se reemplaza el paquete previo en el lugar del paquete perdido, suele ser una tarea realizada por los codecs en el lado del receptor. Esta técnica es funcional si el número de paquetes perdidos es pequeño y no se pierden paquetes consecutivos. Enviar información redundante es otra técnica en la cual la información acerca de n th paquetes es enviada juntamente con $(n+1)$ th paquetes. Si un paquete se pierde el próximo contiene información acerca del paquete previo y con esta información se puede reconstruir el paquete perdido. La recuperación de la información perdida es a expensas de la utilización del ancho de banda, pero se logra una buena calidad de voz.

3.2 Digitalización de la voz

La voz es una señal de tipo analógica incompatible con las redes de datos, lo que hace necesario la digitalización de la señal. Para llevar a cabo esto, primero se debe de muestrear la señal de voz, luego cuantificarla y seguidamente codificarla.

El proceso de muestreo consiste en obtener valores instantáneos de la señal a intervalos de tiempo iguales, a este intervalo de tiempo se le conoce como periodo de muestreo y al inverso del periodo como frecuencia de muestreo²⁶.

El ancho de banda de la voz está limitada entre los 300-3400 Hz. para conocer la frecuencia a la que se debe muestrear se hace uso del teorema del muestreo, el cual dice que si una señal está limitada en banda la frecuencia de muestreo debe de ser como mínimo igual a $2f_m$ (frecuencia Nyquist) donde f_m es la máxima componente de frecuencia que contiene la señal, si se cumple esto será posible recuperar la señal a partir de las muestras tomadas. Para el rango de 300-3400 Hz. la frecuencia de muestreo sería igual a $3400 * 2 = 6800$ Hz, en la práctica se suele tomar una frecuencia de 8000 Hz que corresponde a una separación entre muestras de 125 μ seg (1/8000).

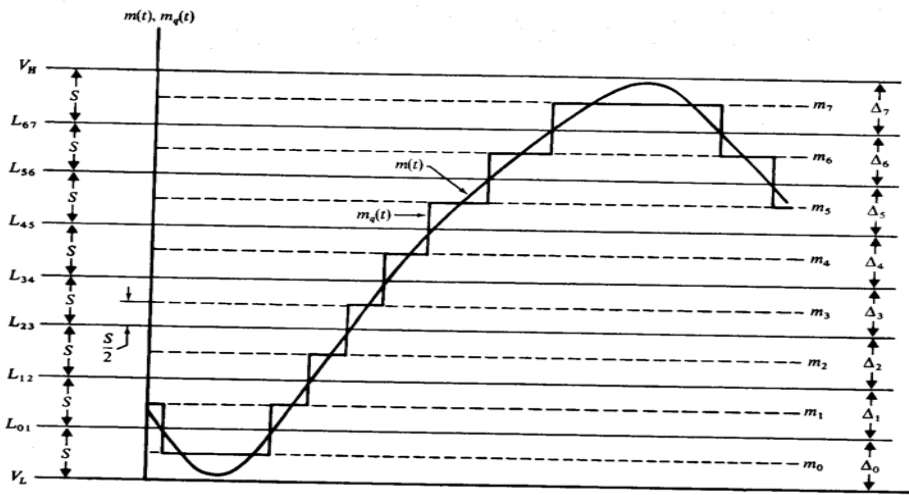
En el proceso de cuantificación se asigna un valor discreto a cada muestra tomada, durante este procedimiento se puede llevar a cabo el proceso de compresión de la voz. A través de la cuantización se crea una nueva señal la cual es aproximadamente igual a la original, la diferencia entre la señal original y la señal cuantizada se conoce como error de cuantización. En la figura 14 se muestra una señal $m(t)$ y su señal cuantizada $m_q(t)$, la señal está dividida en intervalos de tamaño S y se le asignan 8 niveles de cuantización.

²⁶ Taub, Herbert. Donald Shillin. **Principles of Communication Systems**. (2da Edición; EE.UU: McGraw-Hill, 1986). p. 185

El tamaño del paso S es igual a $(V_H - V_L)/M$ donde M en este caso es igual a 8 (de m_0 a m_7). Un nivel de cuantización es mantenido mientras la señal se mantenga en el cualquiera de los intervalos Δ_0 a Δ_7 , por ejemplo m_0 será asignado mientras la señal se encuentre en Δ_0 , un cambio de Δ_0 a Δ_1 ocurre cuando la señal pasa el nivel de transición L_{01} .

La calidad de la señal cuantizada con respecto a la original dependerá del tamaño del paso que se seleccione, para los sistemas PCM (Pulse Code Modulation) utilizados en los sistemas telefónicos se utilizan 256 niveles de cuantización.

Figura 14. Cuantización



Fuente: Taub, Herbert. Donald Shillín. **Principles of Communication Systems**. Pág. 206.

Con la codificación cada muestra cuantificada es representada por unos y ceros, es decir que la señal esta representada por números binarios. En PCM cada nivel de cuantización es representado por una serie de 8 bits. La codificación se realiza del lado del transmisor, del lado receptor se realiza la acción contraria, decodificar y obtener nuevamente la señal de voz analógica.

3.3 Codecs de voz

Como se explicó con anterioridad un codec es el conjunto de un codificador y un decodificador, estos además de codificar una señal de voz también tiene a su cargo: La compresión de la señal vocal y supresión de silencios para un mejor manejo del ancho de banda disponible, cancelación de ecos y manejo de pérdida de paquetes para una mejor calidad de servicio de voz.

La mayoría de codecs son estándares de la ITU, a continuación se lista los más populares:

- G.711: Es la estandarización de PCM, con ancho de banda de 3.4 Khz. y transmisiones a 56 o 64 Kbps. Existen dos variantes de acuerdo al algoritmo de compresión utilizados: la ley A utilizada en Europa y la ley μ utilizada en Estados Unidos. PCM es el sistema de codificación de voz ampliamente utilizado en la red telefónica pública para canales de 64 Kbps en sistemas T1 o E1.
- G.726: Es la estandarización para ADPCM (Adaptive Differential PCM), con ancho de banda de 3.4 Khz. y transmisiones a 40, 32, 24 y 16 Kbps. ADPCM es una variante de PCM en el cual se utilizan estimaciones basándose en dos muestras consecutivas para reducir el ancho de banda.
- G.728: Codifica una señal de voz con ancho de banda de 3.4 Khz. con transmisiones a 16 Kbps, utiliza una variante del algoritmo de compresión CELP (*Code Excited Linear Prediction Compression*) de bajo retardo. Es comúnmente utilizado en sistemas de video conferencias que funcionan a 56 ó 64 Kbps. Proporciona la misma calidad que G.711 a un cuarto del índice de datos necesarios.

- G.729: Utiliza el algoritmo de compresión CS-ACELP (Conjugate Structure-Algebraic Code Exited Linear Prediction), codifica señales de audio con ancho de banda de 3.4 Khz y velocidad de transmisión a 8 Kbps. G.729A es una variante con la única diferencia de que necesita una menor capacidad computacional que G.729, ambas generan una buena calidad de voz comparable con la calidad de ADPCM a 32 Kbps. Se espera que G.729A encuentre mayor aplicación en transmisiones sobre redes inalámbricas.
- G.723.1: Codifica señales de audio con un ancho de banda de 3.4 Khz. y transmisiones a 5.3 y 6.3 Kbps. Las transmisiones a 6.3 Kbps se basan en la técnica de compresión MP-MLQ (*MultiPulse MultiLevel Quantization*) y provee una gran calidad de voz. La velocidad de 5.3 Kbps se basa en la compresión CELP y provee una calidad un poco menor. VoIP Forum ha seleccionado a este codec como el básico para aplicaciones de telefonía IP de bajo índice de bits. Este codec se puede utilizar tanto para comprimir voz como señales de audio en los servicios multimedia.
- ILBC (*Internet Low Bitrate Codec*): Es un codec libre (Open Source) y gratuito para comunicaciones robustas de voz sobre redes IP. Está diseñado para trabajar con anchos de banda reducidos a dos velocidades distintas que dependen del tamaño de la muestra usada, si se usan 20 ms se transmite a 15.20 Kbps con 30 ms se utiliza 13.33 Kbps. Soporta una degradación leve de la calidad de voz debido a pérdida de datos o retardos en la red, la tolerancia a la degradación leve es debido a que utiliza interpolación de los paquetes perdidos. Es utilizado por algunas aplicaciones PC a teléfono como Skype, Google Talk, Yahoo! Messenger (con voz) y MSM Messenger.

Hay tres atributos de cualquier algoritmo de codificación que determina su adecuación en VoIP: Tasa de transmisión (*data rate*), el aumento en el delay asociado con el uso y la calidad de audio resultante tras la aplicación del algoritmo. Los codecs son desarrollados y afinados en base a medidas subjetivas de la calidad de la voz. Las medidas de calidad objetivas estándar como la distorsión armónica total y la relación señal a ruido no correlacionan bien con la percepción humana de la calidad de voz, la cual es al final el principal objetivo de las técnicas de compresión de voz.

La Calificación Promedio de Opinión (*Mean Opinion Score: MOS*) es una medida subjetiva de la calidad del sonido y sirve para valorar la calidad de los codecs que comprimen la voz y los efectos de la red sobre esta. La calificación se consigue a través de un grupo de personas, que deben escuchar innumerables llamadas telefónicas por IP con distintos codecs y evaluar así cada uno de ellos. Tiene un rango de calificación de 1 (malo) a 5 (excelente), en la tabla I se colocan los codecs explicados con anterioridad y su puntuación MOS.

Además del MOS también existe la Medida perceptual de la calidad del habla (*Perceptual Speech Quality Measurement: PSQM*), recomendación P.861 de la ITU para determinar la calidad del habla de manera objetiva²⁷. Está diseñado para evitar la naturaleza subjetiva del MOS, sin embargo, estas medidas fueron diseñadas para analizar únicamente los efectos de la compresión y descompresión de los codecs, por lo que PSQM no tiene capacidad de analizar los efectos causados por la pérdida o el jitter de paquetes.

²⁷ La determinación subjetiva de la voz se encuentra detallada en la recomendación P.800 de la ITU.

Los sistemas de codificación han evolucionado considerablemente en los últimos años, y esto ha permitido reducir de manera importante la necesidad de anchura de banda de diversos servicios de telecomunicaciones, particularmente la transmisión vocal, actualmente estos sistemas de codificación han alcanzado la madurez, y hay actividades en curso para desarrollar nuevos e incluso más eficaces sistemas de codificación.²⁸

Tabla I. Codecs y puntuación MOS

Método de compresión	Bit Rate (Kbps)	Tamaño muestra (ms)	Puntuación MOS
G.711 PCM	64	0.125	4.1
G.726 ADPCM	32	0.125	3.85
G.728 CELP de bajo retardo (LD-CELP)	15	0.625	3.61
G.729 (CS-ACELP)	8	10	3.92
G.729a CS-ACELP	8	10	3.7
G.723.1 MP-MLQ	6.3	30	3.9
G.723.1 ACELP	5.3	30	3.65
iLBC Freeware	15.2	20	3.9
	13.3	30	

Fuente: Paul J. Fong y otros. **Configuring Cisco Voice over IP**. Pág. 67.

²⁸ Grupo de expertos sobre telefonía IP del UIT-D. **Informe Esencial sobre Telefonía IP**. (Suiza: Unión Internacional de Telecomunicaciones, 2003). p.42

3.4 Protocolo de Transporte

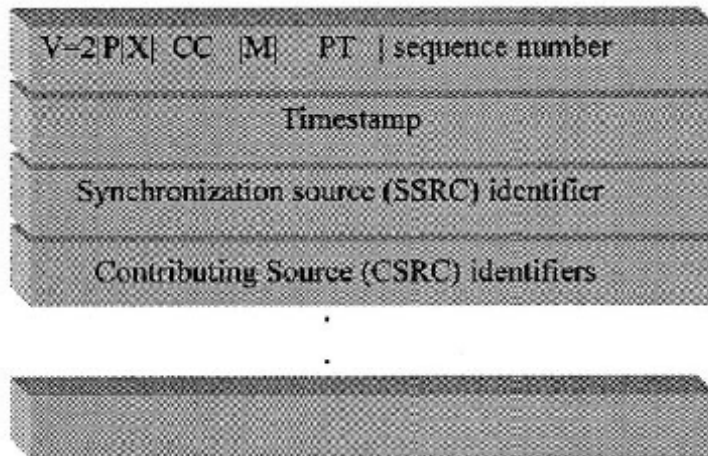
RTP es un protocolo estándar de la IETF (*Internet Engineering Task Force*) que utiliza al protocolo UDP/IP para el transporte de voz y video. RTP es bastante similar a TCP, con una excepción, no se reenvían datos en caso de error por pérdida de paquetes. Esto hace de RTP adecuado para el envío de información con requerimientos de tiempo real, aunque no garantice la calidad del servicio. Este protocolo se encuentra sobre UDP e IP, es decir que opera en la capa de aplicación de la pila TCP/IP, por lo que cada paquete RTP es encapsulado dentro de un paquete UDP y este dentro de uno IP, por lo que VoIP es transportado con RTP/UDP/IP. Entre los servicios prestados por RTP están: Identificación del tipo de carga útil (*Payload*), números de secuencia (*Sequence Number*), tiempo de sellado (*TimeStamp*), supervisión de entrega (*Delivery Monitoring*).

RTP no garantiza el tiempo de entrega, aun así su contribución a los intercambios en tiempo real es muy importante. Este protocolo suministra información de alta utilidad para el transporte de contenido. Además, asigna a los paquetes indicaciones del tiempo en que fueron generados, lo que simplifica su entrega al destinatario en orden correcto, también incluye mecanismos para detectar y sincronizar diferentes flujos, lo que permiten reconocer a que flujo pertenece cada paquete.

Otro protocolo que trabaja conjuntamente con RTP es RTCP (*Real-Time Transport Control Protocol*), y es el encargado de los mecanismos de control e identificación en transmisiones RTP. Una de sus principales funciones es proveer retroalimentación de la calidad de distribución de la información. Además provee información que ayuda al receptor a sincronizar audio y video, también establece una identificación CNAME (*Canonical Name*) para poder transmitir paquetes de control a los participantes de una sesión multimedia, puede utilizarse tanto en ambientes multicast como en unicast, pero es particularmente más efectivo en multicast.

La figura 15 muestra la estructura de la cabecera RTP. A continuación se explica cada uno de los campos que la componen.

Figura 15. Estructura de la cabecera RTP



Fuente: Atul Puri, Tsuhan Shen. **Multimedia Systems, Standards, and Networks**
Pág. 509.

- V: Especifica la versión RTP actualmente la 2.
- P: Bit de relleno (padding). Si está colocado, existe uno o más bytes al final del paquete que no son parte de la carga útil. Algunos algoritmos de encriptación hacen uso de este bit.
- X: Bit de extensión. Una extensión de cabecera es agregada a la cabecera fija si el bit está colocado. Permite adicionar información para ser enviada en la cabecera.

- CC: Conteo CSCR. Si la cuenta es cero, entonces la fuente de la sincronización es la fuente de la carga útil. Si se tiene una comunicación uno a uno, como en una llamada telefónica típica CC debe ser colocado a cero.
- M: Bit de marca. Es definido como una descripción o formato de carga útil. Es utilizado para tramas de video codificado, el bit es puesto a uno en el último paquete para indicar el fin de trama.
- PT: Tipo de carga útil. Identifica los medios codificados y permite interpretar el tipo el tipo de aplicación que transporta el paquete.
- Sequence Number (Número de Secuencia): Número que identifica la posición de un paquete dentro de una trama. El número del paquete es incrementado en uno para cada paquete transmitido. El número de secuencia inicial es generado aleatoriamente. Para aplicaciones de telefonía en tiempo real el receptor puede utilizar el número de secuencia para determinar cuales paquetes se han perdido, pero no dispone de ningún mecanismo de recuperación.
- TimeStamp (Tiempo de Sellado): Refleja el instante de muestreo del primer byte en la carga útil. Varios paquetes consecutivos pueden tener el mismo sellado si son lógicamente generados en el mismo tiempo. Todos los paquetes que pertenezcan a una trama en particular deben de tener mismo tiempo de sellado. Es utilizado para medir el jitter de arribo de cada paquete. Se debe obtener de una fuente confiable de reloj para garantizar la sincronización.
- SSRC (*Synchronization Source Identifier*): Identificador de la fuente de sincronización, asignado de forma aleatoria al inicio de un flujo RTP. Cada paquete generado por la misma fuente (cámara o micrófono) debe de contener el mismo SSRC, y puede ser utilizado para ayudar al receptor a agrupar los paquetes del mismo medio para su reproducción.

- CSRC (*Contributing Source Identifiers*): Identifica las fuentes que aportan carga útil en un flujo RTP. El número de fuentes está indicado por el campo de la cuenta CSRC, y puede haber un máximo de 16 fuentes de carga útil. Para aplicaciones uno a uno el campo CSRC no está presente en la cabecera RTP.

La longitud de la cabecera RTP puede ser calculada de la siguiente forma: $(3 + n) * 32$ bits. Donde n es el número de CSRC. La longitud de la cabecera es de 12 bytes (96 bits), cuando no hay CSRC.

3.5 Protocolos de señalización y arquitecturas

3.5.1 H.323

H.323²⁹ es una estandarización de la ITU-T (*International Telecommunication Union Telecommunication*), que proporciona los requerimientos técnicos necesarios para las comunicaciones multimedia en sistemas basados en redes de conmutación de paquetes, es una variante del estándar H.320 necesario en video conferencias sobre ISDN. La meta del estándar era proveer soluciones futuras a la industria en lo que respecta al desarrollo de video-conferencias y sistemas telefónicos.

Este protocolo permite a la red el uso de mecanismos avanzados de control y gestión tales como: Control de admisión, gestión del ancho de banda de punto a punto y multipunto, autorización de llamadas, traducción de direcciones entre la RTPC y las redes de paquetes. También maneja la interfaz entre redes LAN y otras redes, H.323 puede interactuar en el traslado de llamadas y señalización entre las redes IP y la RTPC.

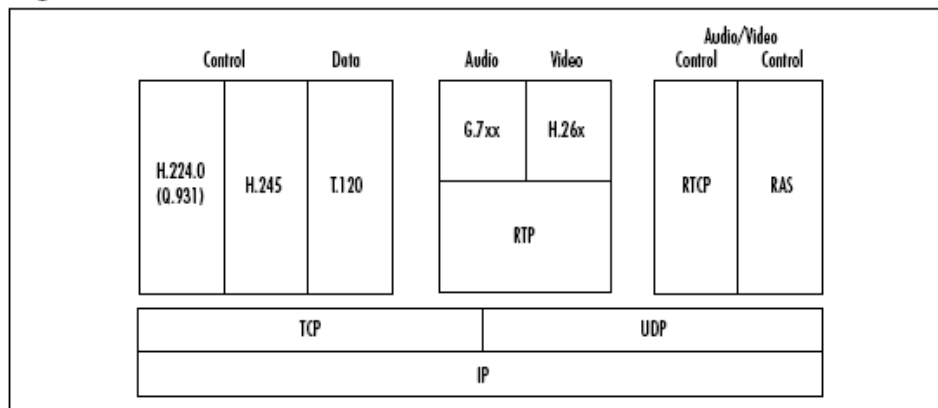
²⁹ H.323 fue uno de los primeros protocolos utilizados en telefonía IP, su dominio comienza a ser desplazado por protocolos como SIP e IAX2 que se acoplan mejor a las actuales redes.

El estándar está conformado por un conjunto de especificaciones que se encargan del flujo de voz y video sobre las redes de paquetes. H.225, H.235, H.245 y los miembros de la serie de señalización Q.900 son los más importantes en aplicaciones de telefonía IP. A continuación se lista las especificaciones más importantes.

- H.225-Q931: Definen la señalización de llamada usado para estabilizar y liberar la conexión. Incluye la dirección IP de fuente y destino, puertos, código de ciudad e información del puerto para H.245.
- H.225.0-RAS: Especifica los mensajes que describen la señalización, el registro, admisión y estatus, que permite a los terminales y gateways hablar con el Gatekeeper.
- H.235: Maneja la seguridad de los mensajes entre gateways y gatekeeper.
- H.245: Cubre el protocolo de estabilización y control de llamada para habilitar la comunicación entre dos terminales H.323, limita la velocidad de transmisión, negocia capacidades, controla la apertura y cierre de canales para el flujo multimedia.
- H.320: Define el estándar para video conferencias sobre redes ISDN.
- H.261 y H.263: Estándar específico para video conferencias.
- H.450: Tiene a su cargo el control de los servicios suplementarios entre terminales H.323 como espera de llamada o transferencia de llamada.
- T.120: Usado para transferencia de datos multipunto en tiempo real para video conferencias.

La pila de protocolos de H.323 se muestra en la Figura 16. Esta incluye tanto el transporte de medios como el transporte de protocolos de señalización.

Figura 16. Pila del protocolo H.323



Fuente: Paul J. Fong y otros. **Configuring Cisco Voice Over IP**. Pág. 134.

3.5.1.1 Arquitectura H.323

H.323 está conformado por algunos elementos los cuales se pueden implementar separadamente o en conjunto en un solo dispositivo. Los principales elementos que componen la arquitectura H.323 son: Terminales, gateways, gatekeepers y unidades de control multipunto MCU.

- Terminales: Una terminal H.323 es un dispositivo que debe de ser capaz de manejar comunicaciones bidireccionales en tiempo real, debe de entregar servicio de voz, voz y datos, voz y video o voz, datos y videos. Además debe de soportar H.225 para establecer llamadas, H.245 para el control de la capacidad y canales, RTP y RTCP para el flujo multimedia, comunicación RAS con un gatekeeper, interfaz de red y codecs para la compresión de audio y opcional para video, G.711 es obligatorio para garantizar una mínima compatibilidad entre los terminales.

Pueden implementarse en software (softphone) o dispositivos *stand-alone*, como un teléfono o un MCU, y son asignados a un alias (nombre de usuario) o números telefónicos. Las terminales H.323 pueden establecer una comunicación vocal sin la intervención de ningún elemento adicional.

- **Gateway:** Permite la comunicación entre diferentes tipo de redes. Por ejemplo, en telefonía IP permite la interacción entre la red IP y la RTPC, una PBX o un fax. Por lo que el Gateway se conecta por una parte a una central telefónica y por otra a una red IP, encargándose de la traducción entre los formatos de transmisión y los protocolos de señalización. Los gateways pueden comunicarse con otros gateways, gatekeeper, MCU, terminales o una PBX. Los gateway IP-IP son un caso especial, ya que estos unen dos redes VoIP independientes, lo cual permite a los usuarios de distintos dominios administrativos intercambiar voz y video sobre IP en lugar de tener que pasar por la PSTN. Son utilizados por proveedores de servicios de telefonía IP para enrutar tráfico de voz sobre otras redes y para obtener información de facturación o para proveer servicio VoIP entre oficinas remotas de una misma empresa. A los gateways IP-IP también se les conoce como controladores de sesión de frontera.
- **Gatekeepers:** El GK es un elemento opcional de la arquitectura, lo que permitió inicialmente el desarrollo de terminales que podían comunicarse directamente entre sí sin la necesidad de este. Es el encargado de manejar a uno o más gateway y permite la traducción de alias a direcciones IP, al estar presente todas las terminales y gateways deben utilizar sus servicios. Su uso también permite la autorización de llamadas, control de admisión, control de zonas, gestión de ancho de banda, gestión de llamadas, reserva de ancho de banda, servicios de directorio. Una red H.323 con control de llamadas centralizado en un gatekeeper se estructura en zonas H.323. Cada zona se conforma de terminales, gateways y MCU que son gestionadas por un único gatekeeper.

Los GK permiten a los terminales H.323 encontrarse entre sí a través de un alias que pueden ser: números telefónicos, direcciones de correo o nombre de usuario. El uso de alias es debido a que es más común utilizar un nombre de usuario o número telefónico que la dirección de red de cada dispositivo. Para que el gatekeeper tenga conocimiento de todos los terminales dentro de su zona, cada terminal debe de registrarse con el, y así poder realizar la conversión de direcciones basándose en los registros de su base de datos. Al igual que las terminales, los gateway deben registrarse con el gatekeeper de la zona, para que este pueda encontrar al mejor gateway para una sesión en particular. Con respecto a la gestión de ancho de banda, este es aplicado únicamente al tráfico H.323 de la red dentro de la zona controlada por el gatekeeper.

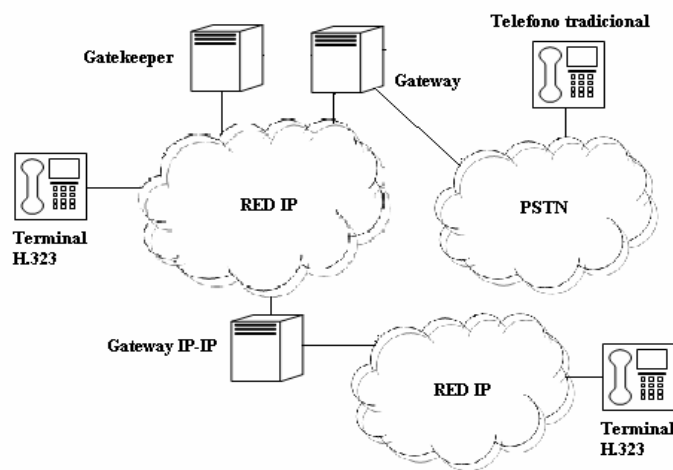
Los GK simplifican el despliegue y uso de sistemas de VoIP, ya que centralizan y coordinan la administración de señalización de llamadas para todos los dispositivos en su zona.

- MCU: Es el equipo que permite soportar comunicaciones multipunto. Se encarga del intercambio de capacidades entre terminales para el establecimiento de comunicación de audio y video. El establecimiento y procesamiento de la multiconferencia se apoya en dos componentes principales:
 - Controlador multipunto (CM): Se encarga de establecer un canal H.245 por cada participante.
 - Procesador multipunto (PM): Se encarga de mezclar, procesar y conmutar el envío de un único flujo multimedia hacia todos o parte de los participantes de la conferencia. La funcionalidad del MCU puede ser integrada en un terminal H.323.

Este estándar funciona bajo una arquitectura distribuida, es decir que todos los componentes manejan funciones de inteligencia, en especial si no se considera al gatekeeper dentro de las funciones de control de llamadas.

La figura 17 muestra los elementos que intervienen en la comunicación entre una red IP1 y la RTPC, y entre las redes IP 1 y 2, la terminal, el gatekeeper y el gateway en la red 1 forman parte de la zona H.323.

Figura 17. Arquitectura H.323



3.5.2 Protocolo RAS

La señalización RAS (*Registration, Admission and Status*) utiliza mensajes H.225.0 para llevar a cabo los procedimientos de registro, admisiones, cambios de anchura de banda, establecimiento y liberación entre puntos extremos y gatekeeper, el canal de señalización RAS es independiente del canal de señalización de llamada y del canal de control H.245³⁰. En los entornos de red que no tienen gatekeeper, no se utiliza el canal de señalización RAS. Mientras que en entornos de red que sí lo tienen, el canal de señalización RAS se abre entre el punto extremo (Terminal) y su correspondiente gatekeeper. El canal de señalización RAS se abre antes de que se establezca cualquier otro canal entre puntos extremos H.323.

³⁰ UIT-T H.323. **Sistemas de Comunicación Multimedia basados en Paquetes**. (Suiza: Unión Internacional de telecomunicaciones, 2006). p.29

Los mensajes de RAS se engloban dentro de las siguientes categorías:

1. Hallazgo del gatekeeper`

1.1 GRQ (*Gatekeeper Request*): Mensaje enviado por un *endpoint* durante el proceso de hallazgo de un gatekeeper. El proceso puede ser manual o automático. Si el *endpoint* dispone previamente de la dirección y número de puerto del gatekeeper el proceso es manual. Si puede determinar en todo momento un gatekeeper con el cual se pueda registrar se dice que el proceso es automático. Esto permite les permite buscar a otro gatekeeper en caso de fallas.

1.2 GCF (*Gatekeeper Confirm*): Confirmación del gatekeeper al *endpoint*, el cual indica el puerto UDP del canal RAS. Si responde más de un gatekeeper, se puede elegir cual usar.

1.3 GRJ (*Gatekeeper Reject*): Rechazo del mensaje GRQ debido a errores de configuración en el *endpoint* o gatekeeper.

2. Registro en Gatekeeper

2.1 RRQ (*Registration Request*): Solicitud de registro que envía un *endpoint* a la dirección de transporte (puerto UDP) y dirección IP del gatekeeper.

2.2 RCF (*Registration Confirm*): Mensaje de confirmación a la solicitud de registro.

2.3 RRJ (*Registration Reject*): Mensaje de rechazo a la solicitud de registro.

2.4 URQ (*Unregister Request*): Mensaje de cancelación de registro, enviado por el *endpoint* al gatekeeper.

2.5 UCF (*Unregister Confirmation*): Mensaje de confirmación de que se ha cancelado el registro.

2.6 URJ (*Unregister Reject*): Mensaje enviado al *endpoint* cuando este no se encuentra registrado en el gatekeeper.

3. Localización de endpoint

3.1 LRQ (*Location Request*): Mensaje enviado por un gatekeeper o *endpoint* hacia otro Gatekeeper solicitando la ubicación de un *endpoint*.

3.2 LCF (*Location Confirmation*): El gatekeeper con el que se encuentra registrado el *endpoint* solicitado envía la información de localización, dirección IP y puertos TCP/UDP.

3.3 LRJ (*Location Reject*): Mensaje de rechazo de localización enviado si el *endpoint* solicitado no se encuentra en el gatekeeper al cual se le envió un mensaje LRQ.

4. Admisión

4.1 ARQ (*Admission Request*): Mensaje enviado para inicializar una llamada, se especifica ancho de banda, tipo de llamada (multicast o unicast), alias de fuentes y destino.

4.2 ACF (*Admission Confirm*): Confirmación a la solicitud de admisión de llamada.

4.3 ARJ (*Admisión Reject*): Rechazo a la solicitud de admisión de llamada, debido a insuficiente ancho de banda o porque un alias no puede ser convertido a una dirección IP.

5. Manejo de ancho de banda

5.1 BRQ (*Bandwidth Request*): Solicitud enviada por un *endpoint* hacia un gatekeeper donde se pide un aumento o disminución del ancho de banda de una llamada en particular.

5.2 BCF (*Bandwidth confirm*): Mensaje enviado hacia un *endpoint* donde se confirma el cambio en el ancho de banda.

5.3 BRJ (*Bandwidth Reject*): Mensaje enviado hacia un *endpoint* donde se niega el cambio de ancho de banda solicitado.

6. Consulta de estatus

6.1 IRQ (*Information Request*): Mensaje enviado por un Gatekeeper donde se pregunta a un *endpoint* su estado actual.

6.2 IRR (*Information Response*): Mensaje de respuesta a la petición de información.

6.3 IACK (*Information Request Acknowledgement*): Respuesta de un gatekeeper a un mensaje IRR reconocido.

6.4 INAK (*Information Request Negative Acknowledgement*): Respuesta de un gatekeeper a un mensaje IRR no reconocido.

7. Fin de llamada

7.1 DRQ (Disengage Request): Mensaje enviado por un endpoint o gatekeeper para finalizar una llamada.

7.2 DCF (Disengage Confirm): Mensaje que confirma la finalización de una llamada.

7.3 DRJ (Disengage Reject): Mensaje donde se indica que se ha negado la finalización de llamada.

3.5.3 Establecimiento y señalización de llamada en H.323

En una red H.323 una llamada puede ser estabilizada de acuerdo a los dos modelos mostrados en las figuras 18 y 20. El modelo de la figura 18 es conocido como señalización directa debido a que toda la información de señalización es transmitida entre ambos *endpoint*. El gatekeeper es opcional, si se toma en cuenta en la comunicación será únicamente para el envío de los mensaje RAS.

La comunicación da inicio con el envío hacia el gatekeeper del mensaje ARQ, el cual responderá con un ACF o ARJ. Si se recibe un ACF, se procede a enviar directamente un mensaje de apertura de puertos TCP para el canal Q.931, seguido se envía los mensajes *Setup* y *Call Proceeding* hacia el destino, ahora este envía un mensaje ARQ al gatekeeper y espera recibir un ACF, si se recibe este mensaje, el destino enviara los mensaje *Alerting* y *Connect* hacia la fuente. El canal de control H.245 es utilizado para negociar las capacidades comunes entre los *endpoint* y abrir los canales para el flujo de voz. Con esto queda establecido el canal de comunicación para el envío y recepción de paquetes de voz. La figura 19 muestra el flujo de la información de señalización al iniciar una llamada desde el *endpoint* 1 hacia el 2.

Figura 18. Señalización directa

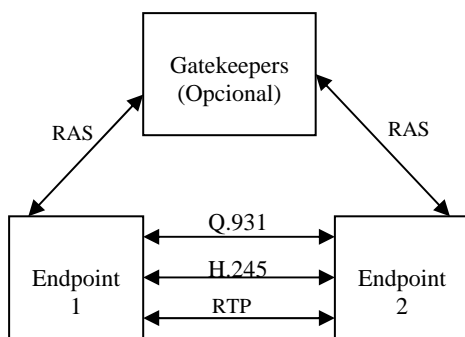
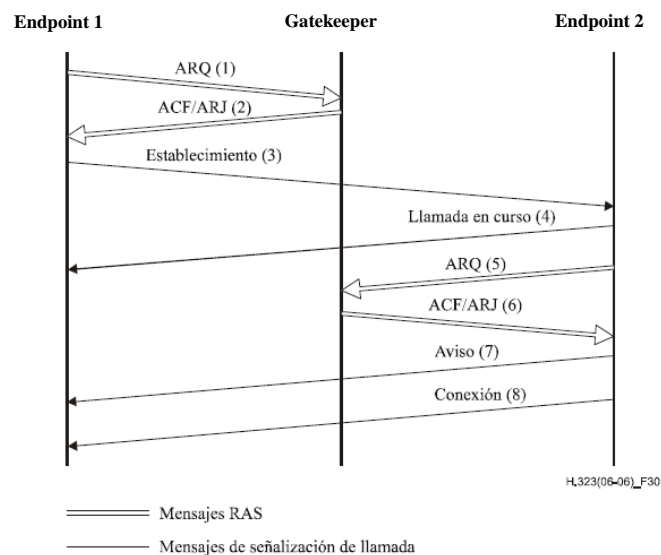


Figura 19. Flujo de información de señalización directa



Fuente: UIT-T H.323. **Sistemas de Comunicación Multimedia basados en Paquetes.** Pág 94.

El modelo de la figura 20 es conocido como señalización encaminada por gatekeeper. Aquí toda la señalización es conducida por el GK y la única información que fluye entre los *endpoint* son los paquetes de voz. La figura 21 muestra el flujo de información de señalización al iniciarse una llamada desde el endpoint 1 hacia el 2. El gatekeeper es común a ambos endpoint.

Figura 20. Señalización encaminada por Gatekeeper

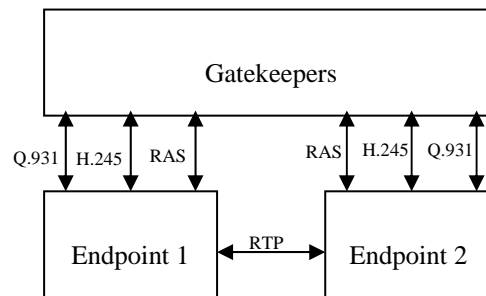
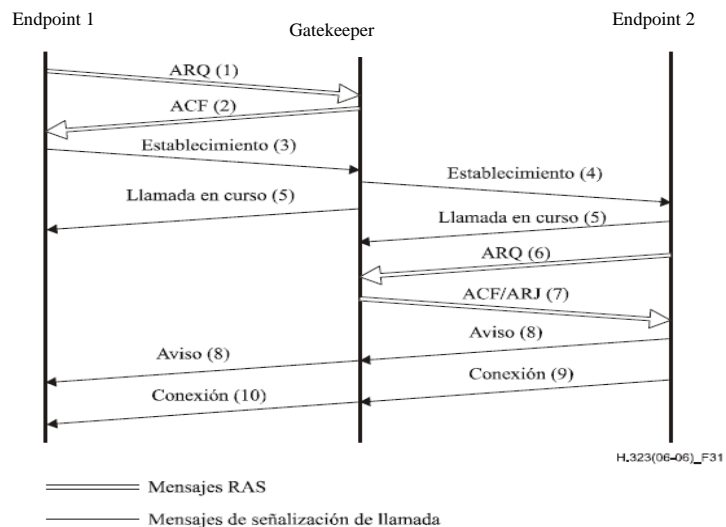


Figura 21. Flujo de información de señalización encaminada por gatekeeper



Fuente: UIT-T H.323. **Sistemas de Comunicación Multimedia basados en Paquetes.** Pág 95

3.5.4 SIP

SIP³¹ (*Session Initiation Protocol*) es un protocolo de señalización que se utiliza para establecer, modificar y terminar llamadas vocales y sesiones multimedia a través de redes IP (redes intranet y/o Internet). Se trata de un protocolo cliente-servidor similar en cuanto a sintaxis y semántica al protocolo HTTP que se utiliza en la web, de hecho, los servidores de la web (http) y los SIP pueden coexistir e integrarse³².

SIP es principalmente un protocolo de señalización de nivel de aplicación para el establecimiento, modificación y terminación de sesiones de comunicación multimedia entre usuarios, las sesiones incluye: llamadas telefónicas, transferencia de datos multimedia, y conferencias en tiempo real. Al igual que H.323 SIP permite el encaminamiento de llamadas hacia la RTPC a través de gateways conectados a la red IP.

El protocolo al manejarse bajo el esquema cliente-servidor, todos sus procesos se realizan a través de un intercambio de mensajes en forma de petición (cliente) y respuesta (servidor), además es un protocolo punto a punto con inteligencia distribuida en los extremos de la red, incluida en los terminales, ya sea mediante hardware o software. SIP no trabaja de manera solitaria, lo hace en conjunto con otros protocolos de la IETF para estructurar un sistema multimedia más completo. Entre los protocolos utilizados por SIP se encuentran: el RTP-RTCP, MEGACO (*Media Gateway Control*) para controlar las conmutaciones con la red RTPC u otras redes de paquetes, y SDP (*Session Description Protocol*) usado para la descripción de las diferentes sesiones.

³¹ SIP se encuentra definido dentro de la recomendación RFC 2543 de la IETF.

³² Grupo de expertos sobre telefonía IP del UIT-D. **Informe Esencial sobre Telefonía IP**. (Suiza: Unión Internacional de Telecomunicaciones, 2003). p.111

Las principales funciones de SIP dentro de una sesión multimedia son:

- Localización de usuarios.
- Determinar la disponibilidad de los usuarios. El o los usuarios tiene la habilidad de indicar si desean establecer una comunicación.
- Determinar las capacidades de las terminales involucradas en la comunicación.
- Establecer los parámetros de sesión. Configuración de llamada.
- Administración de la sesión. Inicialización, transferencia, modificación y terminación de sesiones.

Al igual que H.323 a las terminales SIP se les asigna un identificador, en H.323 es conocido como alias en SIP como URI (*Uniform Resource Identifiers*). Estos identificadores son similares a la direcciones de correo electrónico e indican que el usuario pertenece a un dominio (sip:usuario@dominio), a una determinada computadora (sip:usuario@computadora), a una dirección IP (sip:usuario@dirección_IP) o incluso a un número telefónico E.164 accesible a través de un gateway IP-RTPC (sip:número_teléfono@gateway). URI también puede llevar otro tipo de información que permita conectarse con un determinado usuario como: Número de puerto, password u otros parámetros.

3.5.4.1 Arquitectura

La arquitectura SIP esta conformada por dos elementos fundamentales, los cuales son:

- User Agent (UA): Son los usuarios que inician o responden a una sesión SIP, se pueden registrarse, invitar a nuevas sesiones o modificar sus características. Se dividen dentro de dos categorías las cuales son:

- User Agent Client (UAC): Es el responsable de iniciar y enviar una petición de sesión, también puede dar por terminado una sesión.
 - User Agent Server (UAS): Responsable de atender y contestar las peticiones de sesión. Al igual que UAC puede terminar con una sesión.
- SIP Server: Son los encargados de la localización de usuarios y de la resolución de nombres de usuario a direcciones IP, necesario para que las peticiones enviadas hacia un UA puedan encaminarse apropiadamente. En caso de que el destinatario no pertenece al dominio del remitente, el SIP Server puede transferir la petición a otros SIP Servers. Aunque una llamada básica con SIP puede hacerse sin la intervención de estos, las funciones avanzadas no se podrían llevar a cabo, lo que necesario su uso. Existen 4 tipos de SIP Server, los cuales se listan a continuación:
 - Proxy Server: Es el responsable primario del encaminamiento de mensajes entre los UA. Se encargan de interpretar las peticiones que reciben para reenviarla hacia su destino final, ya sea de forma directa o remitiéndola hacia otro Proxy. Además pueden proveer funciones como: control de acceso a la red, seguridad, autenticación y autorización.
 - Redirect Server: Son utilizados por los UA y los Proxy Server para encontrar el destino final. Son particularmente útiles en redes con usuarios móviles. A diferencia del Proxy, este acepta peticiones pero no la encamina, si no que retorna la petición con información acerca de los SIP Server a los cuales debe contactar para alcanzar otro UA o la forma de contactarlo directamente. Permiten el establecer llamadas entre clientes sin necesidad de usar el Proxy Server.

- Registrar Server: Esto servidores son usados comúnmente para registrar a un usuario que ha iniciado una sesión y poder mantener su localización actual, de modo que si llega alguna invitación destinadas a él, los SIP Server puedan proporcionar su dirección. Esto facilita la movilidad de los usuarios ya que se actualizan las localizaciones.
- Location Server. Suministra información sobre la posible localización del destinatario de la llamada al mantener una base de datos de los usuarios registrados. Brinda los servicios de resolución de direcciones a los SIP Proxy Server y a los Redirect Server.

3.5.4.2 Mensajes SIP

La comunicación entre componentes SIP se realiza a través de mensaje que pueden ser divididos como mensaje de solicitud y mensajes de respuesta. Son mensajes de texto plano de acuerdo al estándar de mensajes de texto de internet, lo cual ayuda a solucionar problemas por la facilidad de lectura, pero se debe de conocer y entender cada uno de los mensajes y los formatos usados. Un mensaje SIP generalmente esta compuesto por: Una línea de inicio, uno o más campos de cabecera, un espacio vacío que indica el fin de cabecera y el cuerpo del mensaje que es opcional.

La línea de inicio especifica el tipo de mensaje, es decir si es una solicitud o una respuesta. La cabecera comúnmente especifica los campos To (Destinatario), From (Remitente), Call ID que identifica cada uno de los mensajes que pertenecen a la misma sesión, Via el cual contiene a todos los equipos que componen el camino que siguió la solicitud y es utilizada por la respuesta para seguir el mismo camino, CSeq identifica el número de orden de los mensajes en la sesión SIP.

Si se coloca un cuerpo de mensaje se debe agregar los campos Content-Type y Content-Length, los cuales especifican el tipo de contenido enviado con la solicitud o la respuesta y la longitud del mensaje respectivamente. Cada campo de la cabecera esta formado por el nombre del campo seguido de dos puntos (:) y el valor del campo.

3.5.4.2.1 Mensajes de solicitud

El formato de la línea de inicio de una solicitud es la siguiente: Método “espacio en blanco” solicitud URI “espacio en blanco” versión SIP “secuencia CRLF” (Secuencia de nueva línea). Existen seis métodos que pueden ser utilizados en la línea de inicio de una solicitud, y son:

- **INVITE:** Indica a un usuario que se le invita a participar en una sesión. Se incluye una descripción de los parámetros de la sesión en formato SDP.
- **ACK:** Mensaje de confirmación enviado hacia el destino, en donde se indica que se ha recibido la respuesta a la solicitud. Se puede incluir en el cuerpo de mensaje los parámetros de la sesión si no fueron enviados con INVITE o si se han hecho modificaciones.
- **OPTIONS:** Usado para obtener las capacidades de otros UA y poder establecer una comunicación.
- **BYE:** Utilizado para finalizar una sesión. Puede ser enviado por un UAC o un UAS.
- **CANCEL:** Un UA puede cancelar una petición pendiente o en progreso al utilizar este método. No se pueden cancelar peticiones ya contestadas.

- REGISTER: Los UA lo utilizan para registrar y actualizar su dirección IP y SIP en un SIP Registrar Server.

3.5.4.2.2 Mensaje de respuesta

Al igual que los mensajes de solicitud los de respuesta tienen un formato similar, como se muestra a continuación: Version SIP “Espacio en blanco” Código de estado “Espacio en blanco” Frase-Razón “Secuencia CRLF”). La Frase-Razón es una descripción textual del código de estado.

Los mensajes de respuesta se clasifican en seis tipos de acuerdo a su código de estado, el cual esta compuesta por una secuencia de 3 dígitos. Los códigos de estado inician en 100 y terminan en 699. El primer dígito del código determina el tipo de mensaje, los cuales pueden ser: Informativo (1xx), de éxito (2xx), redirección (3xx), errores de cliente (4xx), errores de servidor (5xx) y fallas globales (6xx). A continuación se muestra un ejemplo de la línea de inicio de un mensaje de solicitud y su correspondiente línea de inicio del mensaje de respuesta.

Mensaje de Solicitud	Mensaje de respuesta
INVITE sip:Ingenieria@Usac.com SIP/2.0	SIP/2.0 200 OK

3.5.5 SDP

SDP es utilizado para enviar información descriptiva sobre los parámetros de sesiones multimedia a través de la red, también se le utiliza para negociar capacidades entre usuarios SIP, aunque no este diseñado para esto, lo que hace que sea poco eficiente en esa área. Es un protocolo textual y cada descripción SDP proporciona la siguiente información:

- Nombre y propósito de la sesión
- Tipo y formato de los medios que se intercambian durante la sesión.
- Tiempo que permanece activa la sesión.
- Parámetros necesarios para la recepción e interpretación de datos multimedia, como: direcciones IP, puertos, tipo de dato (audio, video), esquema de codificación por ejemplo: G.711 o G.729.

Las descripciones SDP están formadas por campos que tienen el siguiente formato: Tipo = valor1 valor2... valorN, a continuación se lista los campos que se pueden encontrar en un mensaje SDP, el cual puede estar dentro del cuerpo de mensaje de una solicitud o una respuesta:

- v= Número de versión del protocolo.
- o= Creador e identificador de sesión.
- s= Nombre de la sesión.
- i= Información de la sesión.
- u= URI
- e= Dirección de correo electrónico
- p= Número de teléfono.
- c= Información de conexión.
- b= Información de ancho de banda.
- t= Tiempo de inicio y fin de session.
- r= Tiempos de repetición.
- z= Ajustes de la zona de tiempo
- k= Llave de cifrado

- a= Atributos de la presente sesión. Usado para extender la información acerca de la sesión.
- m= Información del tipo de medios: Audio, video, medio de transporte, número de puerto.

A continuación se muestra en la figura 22 un mensaje SDP con algunos de los campos listados con anterioridad.

Figura 22. Mensaje SDP

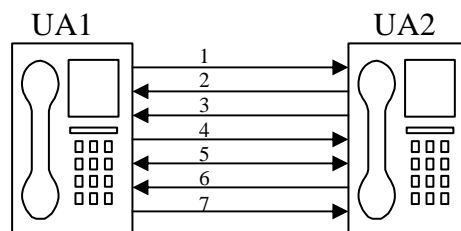
v=0
o=usuario 3400544316 3360854676 IN IP4 168.10.134.100
s=Session SDP
c=IN IP4 172.18.193.109
t=0 0
m=audio 48140 RTP/AVP 0
a=rtpmap:0 PCMU/8000

En el campo “o” se especifica el nombre de usuario, el identificador de sesión, versión, número que se incrementa por cada cambio en la sesión, tipo de red (IN corresponde a internet), tipo de dirección (IP versión 4 o 6), dirección IP. El campo “c” especifica el tipo de red, tipo de dirección y la dirección de quién envía los datos. El campo “t” especifica los tiempos de inicio y fin de sesión, al estar ambos en cero se indica que la sesión es permanente. El campo “m” especifica el tipo de dato, puerto, tipo de transporte (*Real time transport protocol/Audio Video Profile*) y la carga útil. En RTP/AVP el cero corresponde con una carga útil G.711 (PCM de ley μ con audio a 64kbps). El campo “a” amplía la información de los atributos de la sesión, rtpmap es el valor para RTP/AVP, cero tiene el mismo significado que se le dio en el campo “m”, PCMU/8000 corresponde a PCM ley μ con velocidad de muestreo de 8000 bit/s.

3.5.6 Establecimiento de sesión en SIP

La forma más simple de iniciar una sesión SIP es directamente ente dos UA. La figura 23 muestra los mensajes de solicitud y de respuesta necesarios para iniciar y terminar una sesión.

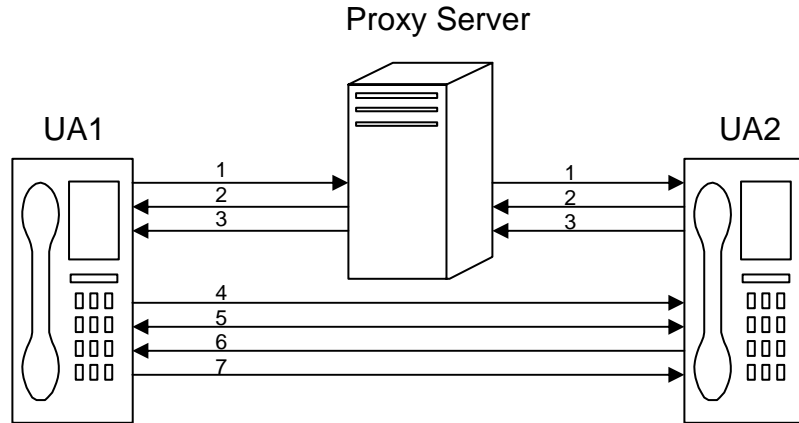
Figura 23. Inicio de sesión simple



1. INVITE: Invitación de inicio de sesión
2. RINGING (180): Se lleva a cabo el aviso a UA2
3. OK (200): Se acepta la invitación.
4. ACK: UA1 ha recibido la respuesta a la invitación.
5. Flujo multimedia
6. BYE: UA2 termina con la sesión
7. OK (200): UA1 acepta.

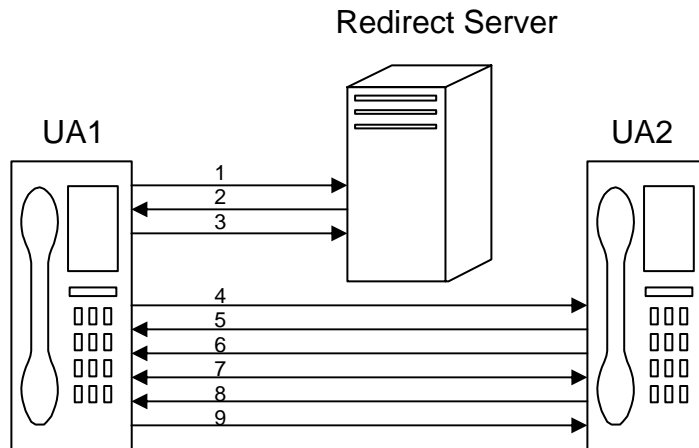
Podemos utilizar un Proxy Server para transportar los mensajes de solicitud de inicio de sesión. La figura 24 muestra esta arquitectura. Podemos notar que el Proxy no establece la comunicación ni tampoco la termina, solamente encamina los mensajes. Se pueden utilizar más de un Proxy para encaminar los mensajes hasta su destino.

Figura 24. Inicio de sesión con Proxy Server.



La secuencia de los mensajes de la figura 23 es similar a la secuencia de mensajes de la figura 24. También es posible utilizar un Redirect Server, este acepta peticiones pero no las envía al destino sino que las retorna con información de cómo localizarlo. La figura 25 muestra esta arquitectura.

Figura 25. Inicio de sesión con Redirect Server

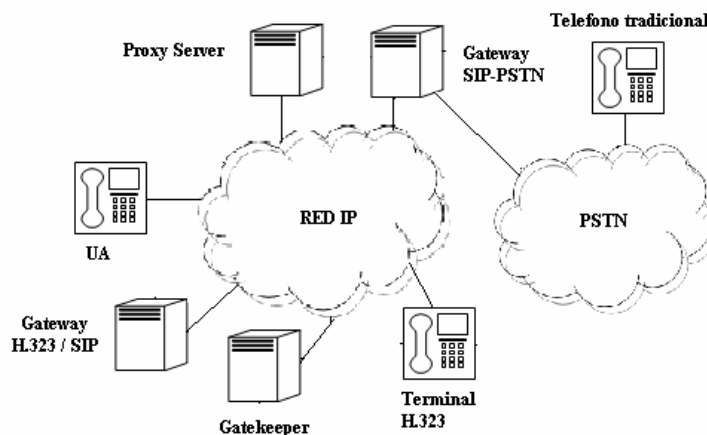


1. INVITE: Invitación de inicio de sesión.
2. Moved Temporarily (302): Retorna la dirección de UA2. No es permanente.
3. ACK: Termina el flujo de información.
4. INVITE: Invitación de inicio de sesión.
5. RINGING (180): Se lleva a cabo el aviso a UA2
6. OK (200): Se acepta la invitación.
7. ACK: UA1 ha recibido la respuesta a la invitación.
8. Flujo multimedia.
9. BYE: UA2 termina con la sesión
10. OK (200): UA1 acepta.

Los *Location Server* y *Registrar Server* puede ser agregado a las arquitecturas de las figuras 2 y 3. En una misma arquitectura se puede tener más de un SIP Server, en la figura 3 en lugar de entregar directamente la dirección de UA2, se le pudo haber entregado la dirección de un Proxy Server para que este se encargara de encaminar los mensajes hacia el destino.

Al igual que H.323, SIP puede encaminar llamadas desde y hacia la RTPC con la ayuda de gateways SIP/RTPC. De igual forma usuarios H.323 y SIP pueden comunicarse, esto se logra a través de un gateway H.323/SIP, que es el encargado de la traducción entre los protocolos. La figura 26 muestra esta arquitectura.

Figura 26. Encaminamiento de llamada SIP-RTPC y H.323-SIP



3.5.7 MEGACO

Megaco³³ (IETF) o H.248 (ITU) es un protocolo que permite la interacción entre las redes conmutadas de circuitos y las redes conmutadas de paquetes, es un protocolo de control de gateway. El gateway Megaco se dividen en tres partes: Media Gateway (MG), Signalling Gateway (SG) y Controller Media Gateway (MGC). El MG es la parte que se encarga de proporcionar una interfaz entre la red de circuitos y la de paquetes, por una parte se conecta a una central telefónica y por otra a una red de paquetes. MGC es el encargado de realizar el control de los MG para una buena gestión de los servicios, además provee funciones de procesamiento y control de llamadas. La función de los SG es proporcionar la traducción entre la señalización SS7 y los protocolos de señalización SIP o H.323. El SG puede ser incluido dentro de un MGC.

El protocolo H.248 consiste fundamentalmente en un modelo de conexión que ofrece una pasarela de medios (MG) al controlador de pasarela de medios (MGC); un conjunto de instrucciones que actúan sobre los objetos de ese modelo; y una función de agrupación de instrucciones en transacciones³⁴.

El protocolo se basa en dos conceptos: Terminación y contextos. Las terminaciones pueden ser una o más fuentes de flujo multimedia. Los contextos son una asociación entre un conjunto de terminaciones que describen una llamada. H.248 maneja una serie de comandos para la manipulación de terminaciones, contextos, eventos y señales, a continuación se lista y explica cada uno de ellos:

³³ Para la IETF se define dentro de la recomendación RFC 3015

³⁴ Grupo de expertos sobre telefonía IP del UIT-D. **Informe Esencial sobre Telefonía IP**. (Suiza: Unión Internacional de Telecomunicaciones, 2003). p.115

- Add: Suma una terminación a un contexto.
- Modify: Modifica las propiedades, eventos y señales de una terminación.
- Subtract: Desconecta una terminación de su contexto.
- Move: Mueve una terminación hacia otro contexto.
- AuditValue: Determina el estado actual de las propiedades, eventos y señales de las terminaciones.
- AuditCapabilities: Permite a un MCG preguntar a un determinado MG todos los valores posibles de las propiedades, eventos y señales de que puede tomar una terminación.
- Notify: El MG informa al MGC que ha sucedido un determinado evento en una terminación.
- ServiceChange: El MG informa al MGC que se pondrá fuera de servicio o de que ya se encuentra disponible.

3.5.8 Plan de enumeración

Debido a la integración de las redes de datos con las redes de circuitos en telefonía IP, se hace necesario un método para dirigir las llamadas que pasan de una red a otra, además del método de acceso para los usuarios, esto debido a que existen métodos de acceso basados en E.164 para las redes de circuitos, alias H.323 en H.323 y URI-SIP en SIP.

ENUM es un protocolo propuesto para relacionar los números telefónicos de la recomendación E.164 de la ITU con el DNS (*Domain Name Service*), lo que hace posible asociar un número E.164 con cualquier recurso que pueda ser identificado mediante el uso de URI, el cual es un esquema de direccionamiento comúnmente utilizado en Internet. Los URI son cadenas de caracteres que identifican recursos tales como documentos, imágenes, archivos, bases de datos, direcciones de correo electrónico y otros recursos. Una de las formas más comunes de URI son las URL, utilizadas para localizar recursos en la WWW, por ejemplo www.google.com.

ENUM hace posible contactar a un usuario mediante su número E.164 independientemente si se encuentra en la red IP (SIP o H.323) o en la red de circuitos (PSTN o ISDN), mediante una consulta DNS ENUM la cual es completamente transparente para la red. Con ENUM se hace necesario el uso de gatekeeper (H.323) y Proxy (SIP) para poder acceder a la información necesaria para localizar y contactar al usuario. DNS ENUM no realiza ni procesa llamadas ya que únicamente hace la relación entre números E.164 y URI's para poder ser utilizada por una aplicación o dispositivo, y así poder contactar con un usuario en particular.

El protocolo ENUM³⁵ no está limitado a llamadas telefónicas también es posible que un número E.164 pueda ser relacionado a diferentes servicios, es decir, que un cliente puede ser contactado mediante una o varias formas. Mediante ENUM es posible tener un número de teléfono como único contacto para voz (fija y móvil), correo electrónico, web, etc., para lo cual se hace uso del sistema de nombres de dominio (DNS).

³⁵ ENUM es desarrollado con la idea de tener un único identificador en lugar de los muchos que actualmente se manejan.

Aspectos políticos y regulatorios han hecho que ENUM no despegue completamente. Uno de los mayores obstáculos es debido al dominio primario .arpa asociado a cada número E.164 en un registro DNS. Esto debido a que el dominio .arpa tiene sus servidores en Estados Unidos lo que daría cierto poder sobre la telefonía IP a esta nación, lo cual no es bien recibido por algunos países, lo que ha dificultado su implementación.

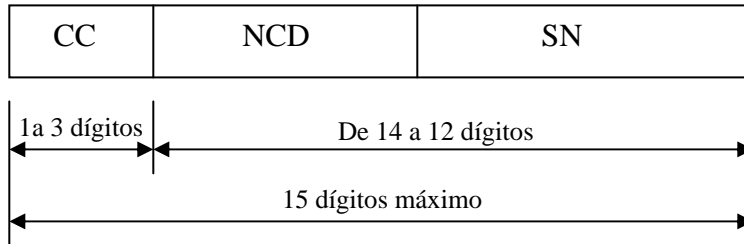
3.5.8.1 E.164

E.164 es el nombre que recibe el plan de numeración internacional que especifica la estructura, formato y jerarquía de encaminamiento que deben mantener los números de teléfono. Un número de teléfono acorde con el plan de numeración E.164 debe contener un código de país, un código de área o de ciudad y el número de teléfono.

Debido a que el sistema de numeración empleado en la actualidad garantiza el alcance internacional y establece un método de acceso estático entre terminales, resulta apropiado para los fines perseguidos por ENUM. De esta manera, será posible disponer de un solo número para alcanzar una página web, dirección de correo electrónico, teléfono fijo, móvil, etc.

Un número E.164 es identificado por el signo “+” antes de la cadena de números que lo componen, tiene una longitud máxima de 15 dígitos de los cuales 1 ó 3 dígitos componen el código de país, el resto identifica el código de área o de ciudad (opcional) y el número del abonado. La figura 27 muestra el formato utilizado en la enumeración telefónica E.164.

Figura 27. Formato de enumeración E.164



CC: Código de país (*Country Code*)

NDC: Código de destino (*Nacional Destination Code*)

SN: Número del suscriptor (*Subscriber Number*)

Para realizar una llamada internacional se debe de incluir el CC, mientras que para el plan nacional únicamente el NDC y el SN. Para nuestro país el CC corresponde al +502 por lo que se tiene 12 dígitos para la enumeración nacional. El NDC para telefonía fija depende del área geográfica, el 2 corresponde a la zona metropolitana, el 6 corresponde a la zona metropolitana suburbana y el 7 a la zona interurbana. La zona metropolitana incluye el municipio de Guatemala y de manera parcialmente a algunos municipios del departamento de Guatemala. La zona metropolitana suburbana incluye a los excluidos de la zona metropolitana. La zona interurbana incluye los departamentos de: Quetzaltenango, Huehuetenango, El Quiché, Totonicapán, Sololá, San Marcos, Retalhuleu, Sacatepéquez, Chimaltenango, Escuintla, Santa Rosa, Jutiapa, Suchitepéquez, El Petén, Izabal, Zacapa, Chiquimula, El Progreso, Jalapa, Alta Verapaz y Baja Verapaz. Para la telefonía móvil se utilizan los NDC 5 y 4. Un ejemplo de número E.164 sería el siguiente: +502 2XXX XXXX. Donde las X corresponden al número del suscriptor.

3.5.8.2 DNS

El sistema de nombres de dominio DNS es una base de datos jerárquica y distribuida utilizada principalmente para la resolución o traducción de nombres a direcciones IP y viceversa. Por ejemplo `www.paginaejemplo.com` se traduciría a través de servidores DNS a `169.168.99.100`. La utilización de nombres en lugar de direcciones IP, que es la forma como encontramos servicios como páginas web, servidores FTP correo electrónico, es debido a que comúnmente es más fácil recordar un nombre que una dirección.

DNS tiene una estructura en forma de árbol, y a cada rama del árbol se le conoce como dominio y a las hojas como host. Los datos guardados en el DNS se identifican a través de nombres de dominio, que es la unión de varios dominios separados por puntos. En el ejemplo anterior el nombre de dominio sería `paginaejemplo.com`.

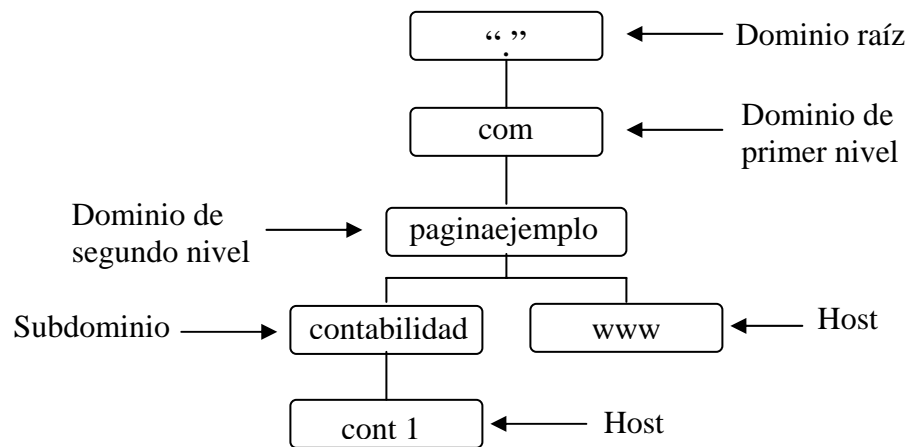
Como se dijo anteriormente DNS es jerárquico, por lo que se tiene dominios primarios o de nivel superior TLD (*Top Level Domain*), dominios de segundo nivel, dominios de tercer nivel o subdominios, y el nombre de recurso o host, aunque puede haber más niveles no es muy común. Sobre estos niveles se encuentra el dominio raíz que agrupa a todos los demás y se coloca antes que los dominios primarios, se le identifica por “.”. Si al ejemplo anterior se le agrega un punto al final del dominio primario (`www.paginaejemplo.com.`) se dice que está escrito como FQDN (Full Quality Domain Name) y especifica una ubicación exacta en el árbol de dominios.

Dentro de los dominios de nivel superior o TLD (Top Level Domain) se encuentran los gTLD o dominios de nivel superior genéricos entre los cuales tenemos: “.com”, “.net”, “.org”, “.int”, “.edu”. También se tiene los ccTLD o dominios de nivel superior de indicativo de país, por ejemplo: “.gt”, “.mx”, “.us”.

En el ejemplo el TLD es “.com”. La sección “paginaejemplo” compone el dominio de segundo nivel y www compone el nombre de recurso o de host, también se le suele llamar CNAME (Canonical Name).

En este ejemplo no se tiene un dominio de tercer nivel, los subdominios se manejan a nivel de organizaciones para dividir una empresa o universidad en secciones, si dentro del dominio “paginaejemplo.com” se desea crear un subdominio para el departamento de contabilidad, entonces tendríamos un nuevo dominio el cual sería “contabilidad.paginaejemplo.com”, y si dentro del departamento de contabilidad se tiene un host de nombre cont1, el nombre que identificaría a este host en una red local o en Internet sería “cont1.contabilidad.paginaejemplo.com”. El árbol DNS para el ejemplo que se ha explicado se muestra en la figura 28.

Figura 28. **Árbol DNS**



Una de las principales características del DNS es que puede delegar autoridad sobre los subdominios a partir del dominio de segundo nivel a otros servidores DNS, a esto se le conoce como zonas. Por lo que se debe saber diferenciar entre un dominio y una zona. Un dominio incluye a todas las ramas del árbol y hojas (host), mientras que una zona incluye subdominio y host dentro de la zona. Por ejemplo, el dominio “paginaejemplo.com” incluye a todos los subdominios y host que existan, mientras que la zona “paginaejemplo.com” incluye únicamente al host “www” y no tiene ninguna autoridad sobre “contabilidad” que es una zona distinta, a menos que dentro de la zona “paginaejemplo.com” se incluya al subdominio “contabilidad”.

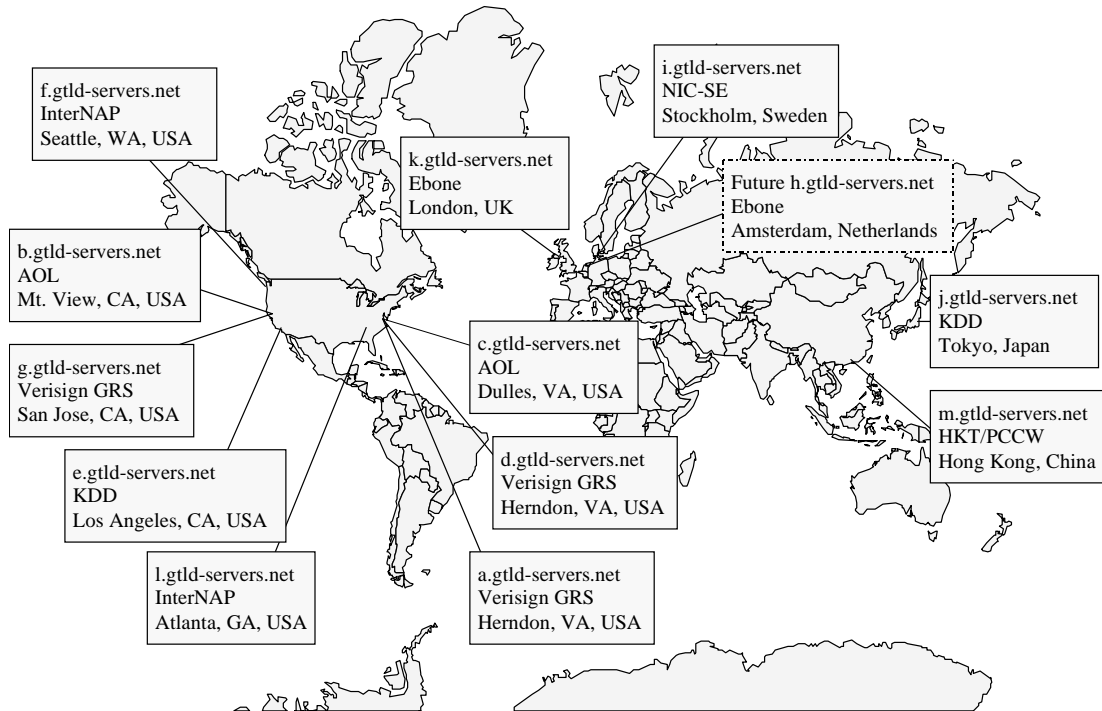
Comúnmente DNS es utilizado para resolver nombres de dominio a direcciones IP, pero también resuelve direcciones IP a nombres de dominio, lo cual se conoce como DNS inverso. Para este sistema se ha creado un dominio especial conocido como in-addr.arpa, que contiene la dirección de los host de manera invertida, es decir, para la dirección 169.168.99.100, le corresponde el nombre 100.99.168.169.in-addr.arpa que corresponde al host www.paginaejemplo.com.

Se suele utilizar el DNS inverso para verificar la identidad del usuario en algunas aplicaciones de red. Es decir, que si se tiene la dirección del host podemos saber a quien corresponde.

Una de las aplicaciones más utilizadas por los servidores DNS es BIND (Berkeley Internet Name Domain), el cual trabaja como una aplicación cliente/servidor, al igual que otras aplicaciones para servidores DNS. Se suele utilizar los puertos TCP y UDP 53 para las peticiones y respuesta DNS.

El mapa de la figura 29 muestra la ubicación de los 13 servidores (mayo de 2001) para los dominios genéricos, como se puede observar 8 de estos servidores se encuentran en los Estados Unidos, mientras que los demás se ubican en: Londres, Suecia, Holanda, China, Japón.

Figura 29. Distribución de los servidores de dominios genéricos gTLD



Fuente: http://www.itu.int/itudoc/itu-t/workshop/enum/004_ww9-es.doc

3.5.8.3 DNS-ENUM

La telefonía tradicional ha prevalecido por más de 100 años y sigue siendo una de las mayores redes tanto en infraestructura como en uso en el mundo. La forma de contactar a otros usuarios conectados a la red es a través del uso de número telefónicos los cuales son únicos para cada usuario. La telefonía IP surge como una aplicación del uso de la digitalización de la voz y su transmisión por redes de datos. Esta telefonía se fundamenta principalmente en dos arquitecturas H.323 y SIP y la forma de contactar con otros usuarios es a través de alias H.323 o SIP URI. Aunque estas arquitecturas puedan unirse a la red tradicional a través de Gateways o Proxy SIP, el iniciar una llamada desde una red IP y terminarla en la RTPC es posible, pero es poco común poder terminar una llamada iniciada en la RTPC en una red IP.

Además de esto existe incompatibilidad con respecto a las forma de contactar a los usuarios, ya que los números telefónicos son inútiles en la Internet al que igual que las URI en la red tradicional, todo esto hace surgir la interrogante de cómo hacer conjugar ambas tecnologías y poder tener un único identificador que nos permita iniciar una llamada telefónica sin importar en donde se encuentra conectado el usuario destino, es decir que no importa si este se encuentra en la RTPC, en una red ISDN, en una red H.323 o una red SIP, además que este único identificador nos permita utilizar todos los recursos tanto de la red tradicional como los de la Internet.

La IETF propone lo que muchos creen unirá a estas dos tecnología y se conoce como ENUM, y no es más que la correspondencia entre números telefónicos de la recomendación E.164 y los URI, a través del uso de DNS inverso y un nuevo dominio conocido como “e164.arpa”, por lo que cada solicitud DNS ENUM³⁶ devuelve una serie de registro llamados NAPTR (*Naming Authority Pointer*) que contiene toda la información de cómo contactar al usuario destino, ya sea mediante su e-mail, número de celular, número telefónico o cualquier otro recurso, todo esto definido por el propietario del número E.164.

Para poder traducir un número E.164 y poder ser almacenado en la base de datos DNS se deben ejecutar ciertos pasos, los cuales se enumeran a continuación:

1. Para el número 21234567, se coloca el código de país mas el signo + para indicar un número E.164: +502 21234567.
2. Se eliminan todos los caracteres excepto los números: 50221234567.
3. Se colocan puntos entre los dígitos y se invierte el orden:
7.6.5.4.3.2.1.2.2.0.5

³⁶ Enum requiere una infraestructura DNS confiable, robusta y sin ningún punto de fallo, redimensionable a medida que se incrementa la demanda del servicio.

4. Se agrega el dominio e164.arpa a lo obtenido en el paso 2: 7.6.5.4.3.2.1.2.2.0.5.e164.arpa. El dominio e164.arpa aun se encuentra en discusión, por lo que su uso puede ser temporal.

Con lo obtenido en el paso, es ahora posible localizar los URI que identifican al usuario y la prioridad establecida para cada una de las formas de contacto. Toda esta información es almacenada como se menciono anteriormente en registros NAPTR. Un ejemplo de este tipo de registro se muestra en la figura 30.

Figura 30. Registro NAPTR

```
$ORIGIN 7.6.5.4.3.2.1.2.2.0.5.e164.arpa.  
IN NAPTR 100 10 "u" "sip+E2U" "!^.*$!sip:usuario@midominio.gt!" .  
IN NAPTR 101 10 "u" "h.323+E2U" "!^.*$!h323:usuario@midominio.gt!" .  
IN NAPTR 102 10 "u" "msg+E2U" "!^.*$!mailto:usuario@midominio.gt!" .  
IN NAPTR 103 10 "u" "tel+E2U" "!^.*$!tel:+502 21234567!" .
```

Este registro se obtendría al realizar una consulta DNS ENUM, mediante la marcación del número +50221234567. El registro nos muestra que existen cuatro formas de contacto asociadas al número telefónico para este usuario, ya sea por SIP, H.323, correo electrónico o su número telefónico. Estos contactos se encuentran en orden de prioridad definidos por el usuario. El orden de prioridad especifica como desea el usuario ser contactado. Al momento de marcar el número telefónico y realizar la consulta DNS ENUM el sistema encaminara la llamada hacia la red SIP que tiene la mayor prioridad, si no se obtiene una respuesta entonces procederá con H.323 y así sucesivamente hasta que se acaben las direcciones de contacto o se establezca una conexión.

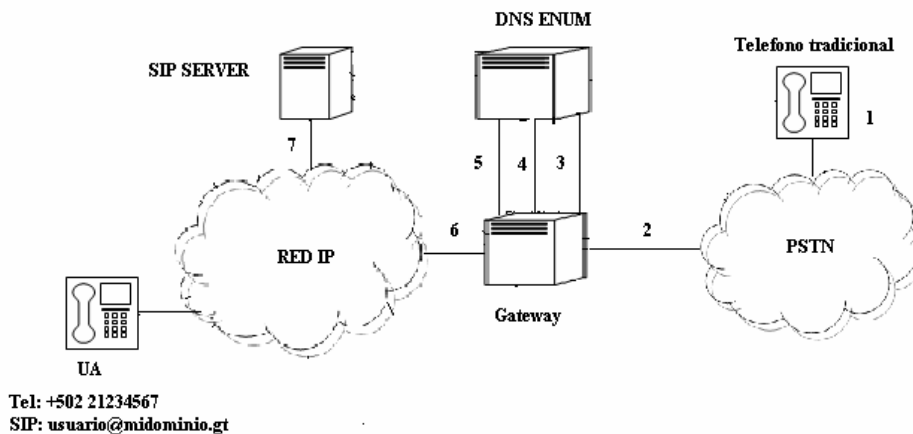
Dentro del registro NAPTR se pueden observar algunos campos los cuales se explican a continuación:

- CAMPO CLASS: Este identifica la familia de protocolo usado, en este caso IN identifica el sistema de Internet.
- CAMPO TYPE: Este identifica el tipo de recurso del registro, para este caso se usa el registro NAPTR.
- CAMPO ORDER: Este identifica el orden en el cual los registros NAPTR deberán de ser procesados, se inicia desde el valor más bajo hasta el valor más alto. Si dos campos de orden tienen el mismo valor, entonces se procede a ver el campo Preference.
- CAMPO PREFERENCE: Este identifica el orden en el cual los registros NAPTR con igual valor en el campo Order deben de ser procesados.
- CAMPO FLAG: Este campo contiene aspectos sobre el control, reescritura e interpretación de los campos en el registro. Actualmente existen cuatro banderas las cuales son: “S”, “A”, “U” y la “P”. Las primeras tres banderas se denominan terminales de búsqueda. La bandera “U” significa que el próximo paso no es una búsqueda DNS pero que la salida del campo Regexp es una URI que contiene la información necesaria para contactar al usuario.
- CAMPO SERVICES: Este campo identifica el tipo de servicio que será dado al número marcado. E2U es un mnemónico que identifica la resolución de E.164 a (to) URI.

- CAMPO REGEXP: Este campo contiene lo que sustituirá al número marcado por el usuario llamante. Es decir la dirección de contacto del usuario destino.

La figura 31 ilustra el procedimiento para realizar una llamada desde la RTPC hacia una red SIP.

Figura 31. Llamada telefónica de la RTPC hacia una red SIP

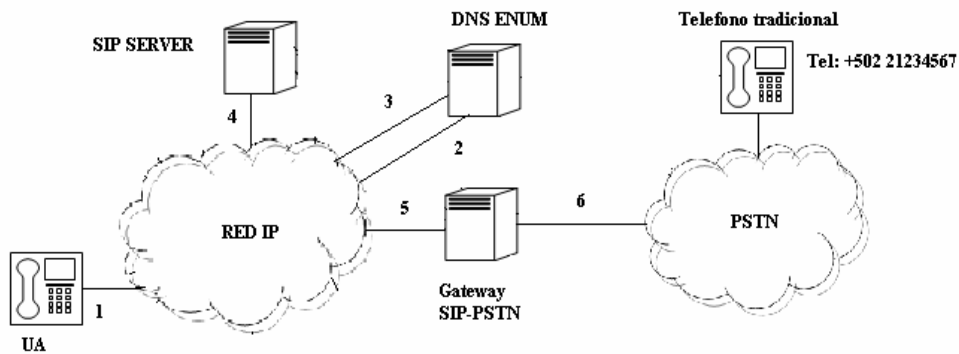


1. Se marca el número telefónico +502 21234567
2. Se encamina la llamada hacia un gateway.
3. El gateway pregunta al DNS ENUM sobre 7.6.5.4.3.2.1.2.2.0.5.e164.arpa.
4. El DNS ENUM devuelve los registros NAPTR con el orden y la prioridad de los contactos. Para este caso el de mayor prioridad es SIP por lo que devuelve el URI SIP: usuario@midominio.gt.
5. El gateway pregunta por el anfitrión de la URI obtenida.
6. El DNS retorna la dirección IP del SIP Server y el gateway envía la URI obtenida a este.
7. El SIP Server obtiene la dirección IP del destino y encamina la llamada.

En el paso 5 de la explicación anterior se ha supuesto que el SIP Server ya se ha registrado al DNS juntamente con todos los UA bajo su control.

La figura 32 ilustra el procedimiento a seguir para realizar una llamada desde una red SIP a la RTPC.

Figura 32. Llamada telefónica desde una red SIP hacia la RTPC.



1. Se marca el número telefónico +502 21234567.
2. El UA pregunta al DNS ENUM sobre 7.6.5.4.3.2.1.2.2.0.5.e164.arpa.
3. El DNS responde con la URI del usuario destino. En este caso es Tel: +502 21234567.
4. El UA inicia una sesión hacia el SIP Server con la información del URI destino.
5. El SIP Server consigue la dirección del gateway y encamina la llamada hacia el.
6. El gateway encamina la llamada hacia la PSTN y esta hacia el usuario destino.

4. TELEFONÍA IP COMO UNA ALTERNATIVA

Una de las características que ha hecho de la telefonía IP una opción atractiva a los usuarios, empresariales y domésticos, es la reducción de costos en las llamadas y en el mantenimiento de la red, ya que se utiliza la misma para datos como para voz.

La telefonía IP promete proporcionar la capacidad para ofrecer a los usuarios finales servicios de telecomunicaciones convergentes y novedosos de una manera rentable. Las inversiones en las redes IP se pueden considerar como inversiones en el futuro, independientemente del desarrollo económico del Estado Miembro de la ITU⁵¹ de que se trate. El argumento comercial para la inversión en las tecnologías IP no se basaría en el solo potencial de la telefonía IP, sino en el potencial más amplio que ofrecen las redes IP para transmitir datos, texto, vídeo y voz. Casi todos los operadores del mundo están en preparación de diversas estrategias para afrontar el desafío que representa una telefonía basada en la conmutación de paquetes, como es el caso de la telefonía IP⁵².

Mientras algunos expertos opinan que los ahorros resultantes de precios bajos se deben a la supresión de las tasas de acceso y de liquidación de cuentas, otros creen que la telefonía IP tiene el potencial de beneficiar a los clientes gracias a la prestación eficaz de servicios convergentes en una sola red. El ahorro del costo de ancho de banda es sustancial cuando el volumen de tráfico de datos es alto y supera al tráfico vocal⁵³.

⁵¹ Guatemala forma parte de la ITU desde el 10 de Julio de 1914.

⁵² Grupo de expertos sobre telefonía IP del UIT-D. **Informe Esencial sobre Telefonía IP.** (Suiza: Unión Internacional de Telecomunicaciones, 2003). p.69

⁵³ Grupo de expertos sobre telefonía IP del UIT-D. **Informe Esencial sobre Telefonía IP.** (Suiza: Unión Internacional de Telecomunicaciones, 2003). p.51

En países en vías de desarrollo, disponer de conexión de banda ancha y aun más de Internet es aun privilegio de algunos, y en áreas rurales el problema es más acentuado. Por lo que la telefonía IP⁵⁴ por el momento será una tecnología de uso limitado, posiblemente grandes empresas y uno que otro usuario domestico o pequeña empresa puedan hacer uso de esta, al menos en nuestro país es probable que así sea.

La mayoría de fabricantes y proveedores de servicios VOIP se han enfocado en llevar el establecimiento de llamadas tanto dentro de las mismas redes como hacia otras, dejando de lado la seguridad y la calidad del servicio. Aunque con el aumento de usuarios de esta tecnología estos temas empiezan hacer eco, lo que ha provocado que fabricantes y proveedores pongan mayor interés en solventar estas debilidades inherentes a las redes de datos.

Es bien conocido que la Internet es un ambiente hostil para la transmisión de datos, por lo que la seguridad juega un papel importante en el desempeño de la telefonía IP, y si no se toman las mínimas medidas de seguridad cualquiera con poco conocimiento sobre el tema de las redes de datos y con la ayuda de programas fácilmente encontrados en la Internet puede capturar nuestras llamadas, lo cual para muchas empresas sería catastrófico. La calidad de servicio es otro tema de gran importancia en la telefonía IP, ya que si se espera que la telefonía tradicional sea sustituida por esta tecnología, al menos debe de tener la misma calidad, es decir que los ecos, los retardos y las pérdidas de paquetes no perjudiquen drásticamente la calidad de la voz, como para hacer una conversación poco inteligible.

⁵⁴ Desde el punto de vista económico, la telefonía IP es innegablemente más barata que la telefonía tradicional. Será una buena opción si llega a cumplir con requisitos como: calidad, seguridad, robustez y algunas otras características deseables en las comunicaciones de multimedia.

El tema de la seguridad en telefonía IP ha provocado la creación de la organización denominada VOIPSA (VOIP Security Alliance), grupo que se encarga de fomentar la seguridad en las redes VOIP, esta formada por proveedores de servicios VOIP, fabricantes de VOIP, universidades e investigadores de seguridad.

Este grupo pretende ayudar a las organizaciones a evitar y comprender los riesgos de seguridad que presentan estas redes, a través del desarrollo de herramientas, listas de discusión, informes y metodologías de uso público.

4.1 Seguridad

El tema de la seguridad ya sea en una red de datos o de circuitos es un fundamental, ya que los usuarios esperan que sus llamadas o envío de datos solo sean escuchados o recibidos por el usuario destino. Este tema en conjunto con las regularizaciones⁵⁵ y aspectos políticos, podrían frenar el avance de la telefonía IP si no se toma con seriedad, ya que la telefonía IP hereda en su mayoría las fallas de seguridad de las redes de datos. Ataques a los servidores DNS, usurpación de identidad (*spoofing*), denegación de servicio (*DoS*), interceptación de paquetes de voz y SPIT (Spam Over IP Telephony), son solo algunos de los problemas de seguridad que enfrenta la telefonía IP. La confiabilidad, la integridad y la disponibilidad son las tres categorías que engloban a la mayoría de riesgos de seguridad en las redes VOIP o cualquier red sobre la cual se transporte información.

⁵⁵ En Guatemala el organismo encargado de las regularizaciones en el campo de las comunicaciones es la SIT (Superintendencia de telecomunicaciones).

La apertura del mercado mundial de telecomunicaciones a la competencia, por un lado, y la evolución de las tecnologías de transporte en las redes de telecomunicaciones, por el otro, han servido para acentuar la importancia de la seguridad para los distintos actores, es decir, los usuarios que exigen que sus comunicaciones se mantengan confidenciales a fin de salvaguardar su vida privada; los operadores de red, que necesitan proteger sus actividades e intereses financieros; y por último, los organismos de reglamentación, que requieren e imponen medidas de seguridad mediante la publicación de directrices y de reglamentos para garantizar la disponibilidad de los servicios⁵⁶.

Los ataques a la confiabilidad y privacidad, integridad y disponibilidad pueden darse por muchos motivos, algunos de los más típicos son los siguientes:

- La vulnerabilidad que presentan los conmutadores, enrutadores y terminales VOIP con el password y login que viene predeterminado para poder acceder al equipo a través de interfaces web para su administración local o remota. Es un error grave y común el no cambiar el password predeterminado, en su mayoría se da en usuarios inexpertos, lo que permitiría a un atacante poder capturar todos los paquetes que pasan por ese dispositivo. Es recomendable utilizar la versión segura del protocolo http (https), o deshabilitar el acceso remoto a la interfaz de usuario para evitar la captura de sesiones administrativas.
- Programas de captura o protocolos de análisis para redes VOIP, los cuales se encargan de interceptar el tráfico de voz en la red.

⁵⁶ Grupo de expertos sobre telefonía IP del UIT-D. **Informe Esencial sobre Telefonía IP**. (Suiza: Unión Internacional de Telecomunicaciones, 2003). p.37

El programa Cain & Abel es un programa para administradores que sirve para medir el nivel de seguridad en su red ya que captura claves utilizadas en protocolos como http, ftp, POP3 y otros, dentro de las tareas que puede realizar también se encuentra su capacidad de ataque a http-digest en paquetes SIP. Http-digest es el método de autenticación VOIP. Este programa también incluye la captura de paquetes de voz (flujo RTP), los cuales pueden ser guardados en formato WAV.

- *ARP (Address Resolution Protocol)* es un protocolo de red encargado de encontrar la dirección MAC (*Media Access Control*), que corresponde a una dirección IP. El envenenamiento de la cache de este protocolo puede provocar que el tráfico de datos y voz sea re-encaminado para su captura. Un buen mecanismo de autenticación puede evitar esta vulnerabilidad.
- Se puede engañar a un teléfono IP asignándole una máscara de red y una dirección de enrutador para causar que algunos o todos los paquetes sean enviados a la dirección MAC de alguien no autorizado, efecto similar al del inciso anterior. El uso de firewall puede reducir el riesgo de este tipo de ataques al igual que evitar que se pueda acceder remotamente a los teléfonos IP.
- Un intruso puede enmascararse como un usuario legítimo, al hacer uso de los privilegios otorgados a algún usuario puede ejecutar funciones dañinas para la integridad de la red, descubrir datos confidenciales, modificar la seguridad y mucho más. Ya que el intruso puede borrar sus huellas, los accesos no autorizados difícilmente se detectan a tiempo.
- Es posible cambiar la configuración de un teléfono IP por el aprovechamiento de una respuesta DHCP al iniciar una sesión. Un servidor no autorizado puede enviar respuesta al teléfono con información falseada.

En lo posible es mejor asignar direcciones estáticas a los teléfonos, por lo que el servidor DHCP no es necesario. Si esto no fuera posible, es necesario filtrar las salidas DHCP desde los puertos del teléfono IP, lo que permite solamente el tráfico de servidores autorizados.

- La denegación de servicio es una vulnerabilidad generada por la sobrecarga del sistema. Esto ocurre al momento que alguien sobrecargue la red con enormes cantidades de peticiones, paquetes especiales o el envío de paquetes inválidos al equipo, lo que ocasiona que el sistema colapse y se deje de prestar el servicio.

Los teléfonos IP y su software, los SIP Server, los gateway, los gatekeeper y sus sistemas operativos, son puertas de entrada a los ataques a las redes VOIP, y aunque existen muchas formas de burlar la seguridad, también existen medios para evitarlos. Una de las formas más comunes de seguridad es el cifrado del flujo VOIP, lo cual provoca un mayor consume de ancho de banda, pero podría solucionarse al migrar a la versión 6 de IP (IPv6). También existen muchos métodos de cifrado o posibilidades de cifrado, como por ejemplo las VPN (Virtual Private Network), IPsec (IP Security) y SRTP (Secure RTP). El uso de firewall y VLANs (Virtual LAN) también ayuda a minimizar el riesgo de un ataque. A continuación se listan algunas de las herramientas disponibles para garantizar la confiabilidad, la integridad y la disponibilidad de los datos en redes VOIP o cualquier red de datos.

- Clave compartida (*Shared-Key*): Es un sistema de autenticación donde el remitente y el destinatario comparten una clave secreta, que no es conocida por terceros. La clave compartida puede ser utilizada por el remitente para cifrar el mensaje enviado al destinatario, por lo que el mensaje no se envía en texto plano, y para recuperarlo se deberá usar la clave compartida en el algoritmo de descifrado.

En caso de que una clave se vea comprometida, ya sea por pérdida o robo, el administrador del sistema debe proveer una nueva clave a los usuarios. A este tipo de cifrado también se le conoce como cifrado simétrico.

- Cifrado de clave pública (*Public-Key Cryptography*): En este tipo de cifrado se manejan dos clases: claves asimétricas y las firmas digitales. En las claves asimétricas se tiene un par de claves, una pública y otra privada las cuales se basan en funciones matemáticas, ambas claves pertenecen al mismo propietario. El uso de dos claves se debe a que una es relacionada al cifrado y la otra al descifrado, así únicamente la clave pública puede descifrar los datos que han sido cifrados con la clave privada, de igual forma únicamente una clave privada puede descifrar datos que han sido cifrados con clave pública.

La clave pública es repartida entre los quienes la requieran, mientras que la privada es una clave secreta. Uno de los algoritmos más utilizados para claves públicas es RSA inventado por Rivest, Shamir y Adleman, de ahí el nombre del algoritmo. Este se fundamenta en la dificultad de factorizar cantidades que son producto de dos números primos muy grandes en un tiempo razonable.

- Firma digital (*Digital Signature*): Es un atributo del contenido del mensaje y de quien firma el mensaje. Para la creación de una firma digital se hace uso de una función denominada “Hash”, la cual permite calcular un valor resumen de los datos que se desean firmar, a este resultado se le aplica el algoritmo de firma, el cual hace uso de la clave privada de quien firma (remitente), la firma es adjunta al documento para que puede ser verificada con el algoritmo de verificación y la clave pública del remitente en el lado del destinatario.

4.1.1 Protocolos de seguridad

IPsec, TLS y SRTP son protocolos de seguridad que utilizan las claves públicas para el transporte en redes VOIP, aunque no están limitados a este tipo de redes ya que pueden ser utilizados en cualquier otro servicio.

4.1.1.1 IPsec

Este protocolo brinda seguridad a los datagramas IP a través del uso del cifrado de claves públicas, opera en base a dos protocolos definidos como: AH (*Authentication Header*) y ESP (*Encapsulating Security Payload*).

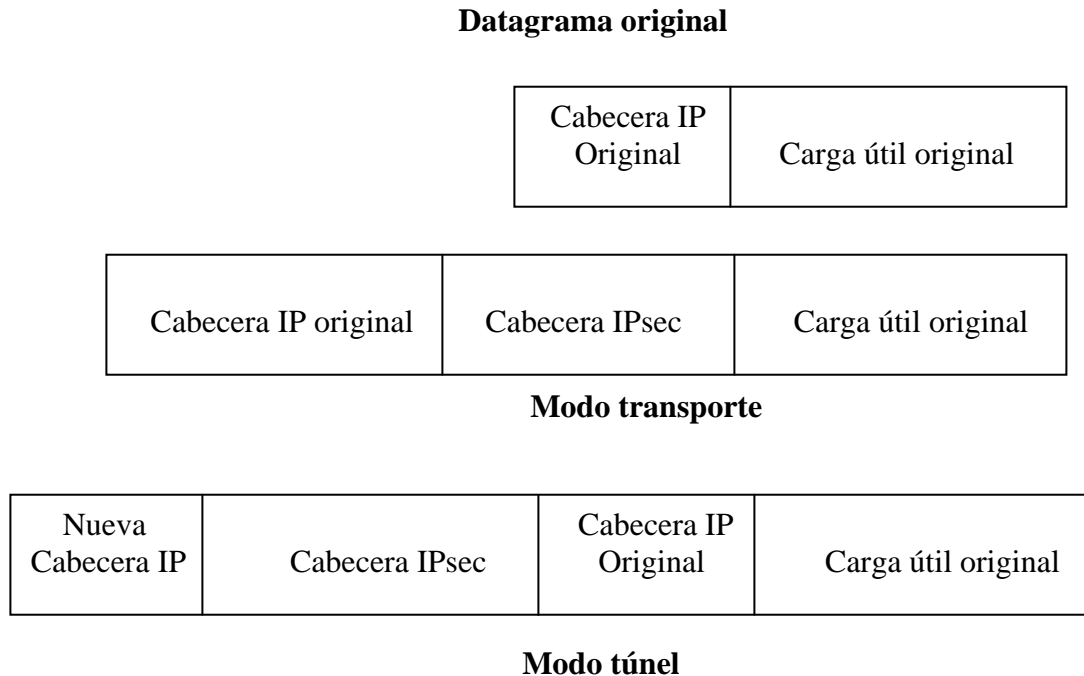
AH provee autenticación e integridad mientras que ESP provee integridad, autenticación y cifrado, su uso reduce la posibilidad de ataques de negación de servicio al igual que AH, una diferencia importante entre ambos protocolos es que AH se aplica a paquetes no fragmentados mientras que ESP si se aplica a estos. AH al no aplicarse a paquetes fragmentados no permite que se pueda cambiar el orden de los paquetes para burlar a un firewall, por lo que evita el uso de paquetes solapados. IPsec se incluye dentro de la pila del protocolo IPv6 y funciona en la capa de red que corresponde a la capa 3 en el modelo OSI, en el protocolo IPv4 es opcional su uso pero puede ser agrado a la pila. Un flujo unidireccional de datos entre dos puntos es un enlace seguro IPsec y se le denomina SA (Security Association), y define el acuerdo entre las dos partes comunicadas en el método a utilizar para la comunicación segura. El flujo de datos puede ser entre dos host o entre un host y un gateway o entre dos gateway.

IPsec puede operar en dos modos distintos, los cuales son: Modo transporte y el modo túnel. En el modo transporte solamente la carga útil del datagrama IP es protegida, la cabecera IPsec es insertada entre la cabecera original IP y la carga útil.

Este modo es utilizado en comunicaciones punto a punto entre hosts y provee confidencialidad total de la comunicación. En el modo túnel todo el datagrama es protegido e insertado dentro de otro datagrama IP, la cabecera IPsec es insertada entre la nueva cabecera IP y la cabecera original. Este modo es utilizado en comunicaciones punto a punto entre gateways, también se le emplea para introducir el protocolo IPsec en redes IPv4 y para la creación de islas IPsec en VPNs, provee confidencialidad de la comunicación solo dentro del túnel.

La figura 33 muestra el uso del protocolo AH en los dos distintos modos de operación del protocolo IPsec.

Figura 33. **Modos de operación del protocolo IPsec**



El protocolo encargado de manejar la seguridad de las claves se denomina IKE (*Internet Key Exchange*) y utiliza las claves públicas para negociar una clave autenticada y el protocolo de seguridad a usar, ya sea AH o ESP. Este protocolo tiene a su cargo la infraestructura IPSec ya que proporciona un entorno previo seguro para el intercambio de una clave secreta y autenticación de los extremos, ya que provee seguridad contra la interceptación de la comunicación y denegación de servicio. El protocolo funciona sobre el puerto 500 UDP para establecer el intercambio de mensajes.

4.1.1.2 TLS

El protocolo TLS (*Transport Layer Security*), como su nombre lo indica opera en la capa del transporte del modelo OSI, es utilizado para establecer una conexión segura entre dos aplicaciones que se comunican, autenticándolos y creando una conexión cifrada entre los dos. Se compone de dos capas las cuales son: Protocolo TLS de registro y el protocolo TLS Handshake. El protocolo de registro provee la seguridad al utilizar el cifrado simétrico en los datos, se suelen utilizar algoritmos de cifrado como: DES (Data Encrytion Standard) y RC4. Las claves utilizadas en el cifrado simétrico son generadas únicamente para cada conexión y se basan en una negociación secreta llevada a cabo por el protocolo Handshake. Para dar integridad a los datos cada mensaje lleva un mensaje de comprobación de integridad que usa un código de autenticación de mensaje (MAC). El MAC usa funciones Hash seguras como MD5 o SHA. El protocolo Handshake permite a un cliente y a un servidor poder autenticarse, negociar el algoritmo de cifrado y la clave a utilizar, las claves negociadas pueden ser del tipo simétrico o claves públicas.

4.1.1.3 SRTP

El protocolo SRTP provee seguridad, confiabilidad, autenticación de mensajes y protección de reenvío al flujo RTP y RTCP, por lo que SRTP provee una arquitectura para el cifrado y autenticación de mensajes para el flujo de audio y video, además tiene un alto nivel de procesamiento de información, bajos costos computacionales y de ancho de banda, puede ser implementado en aplicaciones unicast y multicast. SRTP es independiente de cualquier sistema de gestión de claves, pero MIKEY (*Multimedia Internet Keying*) ha sido propuesto para trabajar con el protocolo.

MIKEY soporta la negociación de claves cifradas y parámetros de seguridad para uno o más protocolos de seguridad, y para una o múltiples sesiones. Puede ser implementado de forma independiente debido a su fácil integración en protocolos de comunicación multimedia (H.323, SIP). MIKEY utiliza cuatro opciones para la distribución de claves las cuales son: Claves simétricas, Claves públicas, claves Diffie-Hellman con intercambio protegido por cifrado de claves públicas y claves Diffie-Hellman con intercambio protegido con claves compartidas y funciones Hash.

El algoritmo Diffie-Hellman permite el intercambio de claves en un medio inseguro entre dos usuarios que no han tenido conexión previa, el intercambio es secreto y de manera no autenticada. Su seguridad se basa en la dificultad que presenta el cálculo de algoritmos discretos en un campo finito.

4.1.2 Firewall

El Firewall es un dispositivo utilizado en redes de datos para proveer seguridad, ya que permite controlar el flujo de información que sale y entra de los puertos, es decir, permite abrir los puertos necesarios para cierta aplicación y mantener cerrados lo que no se utilizan.

El uso del firewall minimiza accesos no autorizados a la red, y evita así que intrusos tengan acceso a información de importancia para una empresa o persona, ya que se crea un perímetro de defensa en torno a la red local, su ubicación suele ser entre la red local y la Internet, aunque también se pueden colocar dentro de la misma red local para evitar el acceso a áreas no autorizadas a usuarios de la red, su implementación se realiza por *Software* o *Hardware*, y su utilidad no se limita a evitar acceso no autorizados también puede evitar ataque de negación de servicio a nivel de red y los ataques de robo de identidad, pero no puede evitar que terceras personas escuchen y capture datos en la red, tampoco puede evitar el uso por parte de un atacante de debilidades en los servicios de red o programas utilizados.

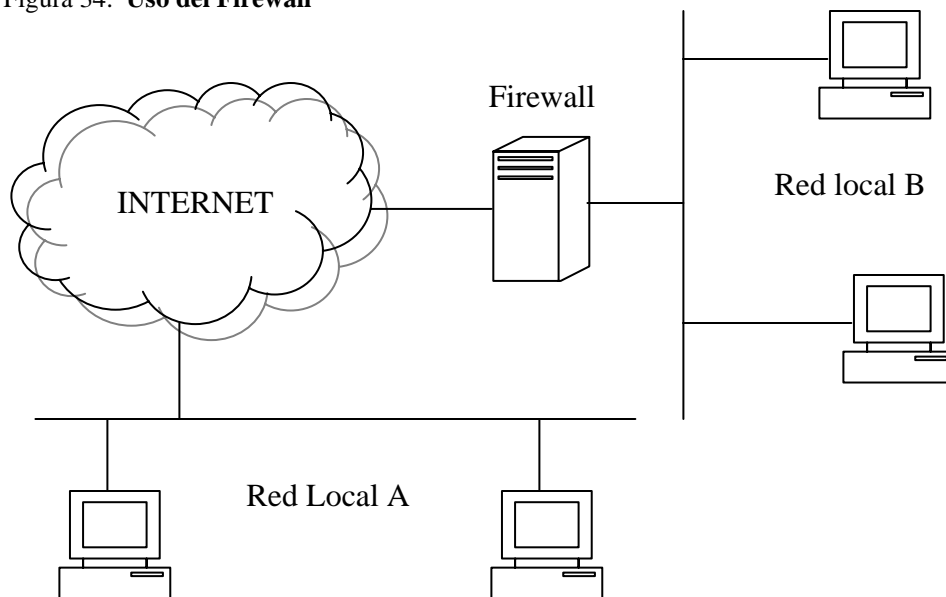
La zona protegida por un firewall es comúnmente llamada “zona protegida”, mientras que la zona de la que nos protegemos se le denomina “zona de riesgo”. Aunque el firewall provee una buena seguridad se recomienda su utilización con otras herramientas para reforzar la seguridad en la red, esto debido a que se centraliza toda la seguridad en un único sistema y si por cualquier motivo el firewall se ve comprometido toda la red estaría en riesgos si únicamente se utiliza esta herramienta.

Hoy día no es necesario ser un experto en redes o informática para acceder ilegalmente a una red si esta no cuenta con la seguridad necesaria para evitarlo. Con el uso de programas de dominio público que generalmente se encuentran en la Internet o con herramientas disponibles en los propios sistemas operativos, cualquier puede escanear puertos, obtener direcciones y nombres de host o encontrar fugas en el sistema de seguridad. Herramientas como ISS (*Internet Security Scanner*) o SATAN (*Security Analysis Tool for Auditing Networks*) que auditan y buscan fugas de seguridad en las redes, se puede obtener la suficiente información como para iniciar un acceso no autorizado o un ataque a la red.

Herramientas disponibles en los sistemas operativos como ping, con el cual podemos saber si es posible alcanzar a un servidor o host, enviando una solicitud, si se recibe una respuesta el host es accesible, sino es porque este se encuentra protegido por firewall o no esta activo. Con Nslookup podemos obtener de un servidor DNS direcciones IP y nombres de host o con Traceroute se podría obtener información acerca del número de redes intermedias y enrutadores en torno a un servidor objetivo. Aunque estas herramientas puede ser utilizadas para provocar daños o simplemente acceder a una red, los administradores pueden utilizarlas para encontrar vulnerabilidad en sus redes, y así evitar o minimizar posible ataques.

La figura 34 ilustra una red local A conectada directamente a Internet y otra red local B conectada través de un firewall a la zona de riesgo Internet.

Figura 34. **Uso del Firewall**



Todo Firewall maneja tres componentes básicos los cuales son:

- Filtrado de paquetes: Consiste en analizar la cabecera de cada paquete recibido, y en función de reglas establecidas como protocolo utilizado (TCP, UDP, RTP), dirección IP de fuente y destino, puerto destino, determinar si el paquete puede o no pasar ya sea hacia dentro o hacia fuera de la red.
- Proxy de aplicación: Se utilizan para bloquear o permitir la ejecución de aplicaciones, aunque los permisos pueden ser parciales, ya que se le puede permitir ejecutarse pero con limitaciones en los comandos utilizados, por lo que el bloqueo o el pase no se limita únicamente a examinar la cabecera del paquete recibido. Para una red en la que se tenga un Proxy de aplicación para html solamente este podrá ejecutarse y ninguna otra aplicación estará disponible, por lo que se hace necesario un Proxy para cada aplicación que se desee ejecutar.
- Monitoreo y detección de actividades sospechosas: Esta es una parte fundamental en la implementación de un firewall ya que a través de esta actividad podemos obtener información de todo lo ocurrido en la zona protegida como posibles intentos de ataque, cual ha sido el flujo de información, intentos de acceso a áreas no autorizadas para un determinado usuario, uso de protocolos no autorizados. Toda esta información es almacenada en registros, los cuales deben de ser leídos frecuentemente por el administrador de la red, para tomar acción en caso de una actividad sospechosa.

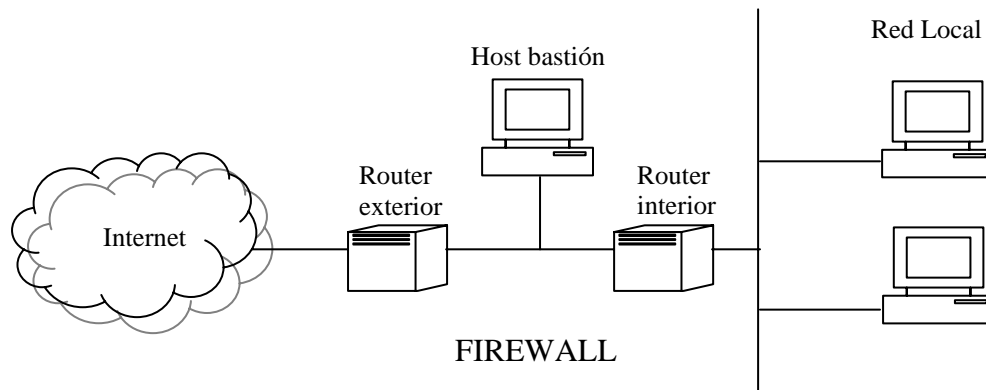
Como se comento con anterioridad los firewall pueden implementarse a nivel de software o hardware. Actualmente existe una gran variedad de software para firewall y suelen ejecutarse sobre sistemas Unix, Linux o Windows NT.

Uno de los más utilizados en sistemas Unix es el FireWall-1, este opera a nivel del núcleo del sistema operativo, por debajo de la capa de red en el modelo OSI, lo que garantiza que ningún paquete podrá acceder a un nivel más alto sin antes haber sido inspeccionado por el firewall y así asegurarse que cumple con las políticas de seguridad establecidas.

Dentro de los firewall implementados a nivel de hardware se tiene cuatro arquitecturas las cuales son: Firewall de filtrado de paquetes, Dual Homed-Host, Screened Host y los Screened Subnet (DMZ). Dentro de estos el más utilizado actualmente es el DMZ también conocido como *De-Militarized zone*. Esta arquitectura crea una subred entre la red interna y la externa. Se compone de dos enrutadores denominados interno y externo que se conectan directamente a la subred que constituye el firewall, además se tiene un host denominado bastión, el cual es el punto de contacto entre usuarios de la red interna y otras redes exteriores, habitualmente la red exterior es la Internet, y al estar conecta a la zona de riesgo será el que reciba todos los ataques procedentes de esta zona, por lo que tiene altos niveles de seguridad, el host bastión también tiene a su cargo el filtrado de aplicaciones de entrada y salida necesarias para la comunicación con la red exterior (http, ftp, telnet).

Con el enrutador exterior se bloquea todo el tráfico no deseado desde la red exterior hacia la subred en ambos sentidos, de igual manera el router interior bloquea desde la red interna hacia la subred, el uso de estos dos router disminuye la posibilidad de que un intruso comprometa al host bastión, y que a través de este pueda acceder a la red local. La figura 35 muestra la arquitectura DMZ, con la cual se une a una red local al Internet.

Figura 35. **Arquitectura DMZ**



El tráfico en redes VOIP comúnmente viaja a través de puertos UDP, la información para el establecimiento de llamada también usa algunos puertos UDP, la asignación de los puertos para el tráfico VOIP suele ser dinámico, comúnmente se asignan puertos del 1024 al 65535, por lo que el uso de firewall complica de cierto modo la administración de la red ya que se dejaría un rango bastante amplio de puertos abiertos, lo que crearía una brecha en la seguridad. En el procedimiento de filtrado de paquetes se tiene dos sistemas los cuales son: filtrado con memoria (*Stateful Firewall*) y filtrado sin memoria (*Stateless firewall*). Un *stateful firewall* es un firewall que provee mecanismos para dar seguimiento al flujo de datos, es decir que la información referente a cada conexión es almacenada en memoria y cada vez que un paquete cruza el filtro, la decisión de rechazar o recibir un paquete es realizada en base a la información de conexión almacenada en memoria, lo que lo hace útil para aplicaciones que asignan puertos de forma dinámica como VOIP, ya que solo se abrirán puertos el tiempo suficiente para que cierto paquete pase y luego serán nuevamente cerrados, lo que ayuda a evitar que los puertos permanezcan abiertos a posibles ataques. Además permiten controlar el número de conexiones, lo que evita ataques de negación de servicio debido al envío de demasiadas peticiones.

4.1.3 VPN

La red privada virtual o VPN es un canal de comunicación entre dos host que permite el tráfico de datos de forma segura entre ellos, al negociar un esquema de cifrado y autenticación para el transporte de los datos. Una forma habitual de VPN es el uso de IPsec con cabecera ESP en modo túnel, con la cual se puede atravesar de manera segura una red pública como la Internet. El uso de VPN brinda seguridad contra ataques internos y externos en la red local, provee integridad y autenticación, permite la separación lógica del flujo de datos y de voz, protege contra ataques de negación de servicio, además permite evitar ataques de captura, interceptación de llamadas, y robo de servicio al hacer uso del cifrado de datos.

Los cuatro requisitos que hacen de una VPN un enlace seguro son los siguientes:

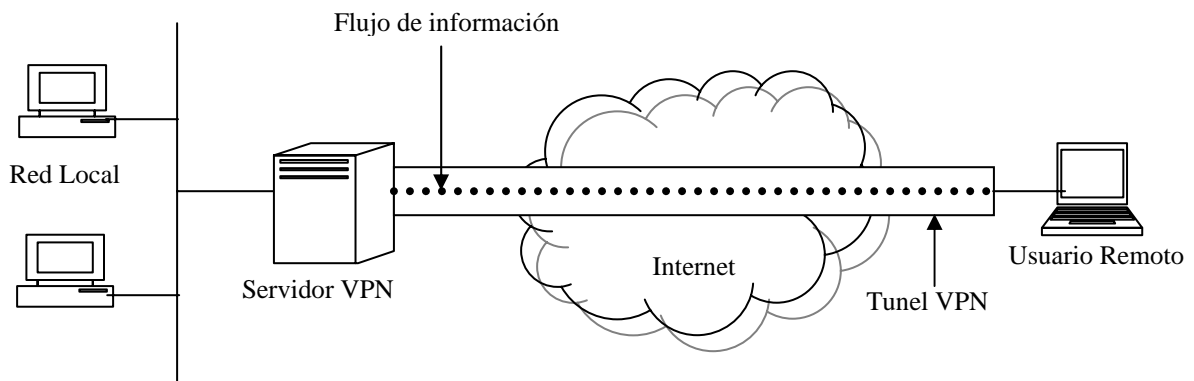
- Confidencialidad de los datos: Esto garantiza que solo el remitente y el destinatario podrán ver los datos transmitidos, lo que minimiza que terceros puedan ver información confidencial.
- Integridad de los datos: Esto garantiza que el destinatario recibirá datos confiables, que no han sido alterados por terceros durante su recorrido por el canal.
- Autenticación de mensajes: Con esto se asegura que los mensajes enviados por un remitente son auténticos y que el recipiente que los recibe de igual manera sea auténtico.
- No repudio de mensajes enviados: Utilizado para garantizar que un remitente no pueda negar que ha sido el quién ha enviado un mensaje.

Aunque existen algunas formas de crear canales seguros como el uso Extranets o líneas privadas, lo que hace de VPN una mejor opción son la reducción de costos al no tener que contratar líneas privadas para el envío de datos confidenciales, ya no se hacen necesarios los servidores de accesos remotos ya que la VPN es quien se encarga de dar acceso a los usuarios a la red, ya no se hace importante la ubicación física de un usuario para hacer uso de la red privada, permitiéndoles el uso de los servicios de la red, como impresora o el sistema de archivos compartidos o cualquier otro servicio prestado por la red local, permiten la administración y ampliación de las redes corporativas al mejor costo-beneficio.

Actualmente los servicios VPN pueden ser encontrados en un enrutador con capacidad de cifrado o en un firewall, existen también programas para crear y administrar VPNs. Los enrutadores utilizados para VPN tiene la tarea de cifrar o descifrar el flujo de datos que pasen por ellos. Los firewall que incluye servicios VPN ofrecen además su capacidad de bloquear los accesos a la red y proveer registro de intentos de ataque a la red.

El uso de IPsec como se menciono con anterioridad está ganado terreno en el mundo de las VPN en gran medidas debido a su compatibilidad con las redes IP actuales, pero existen otros protocolos como PPTP (*Point-to-Point Tunneling Protocol*) desarrollada por Microsoft, una de las principales características de este protocolo es su capacidad de soportar clientes no IP, su principal problema es su falta de capacidad de definir un protocolo de cifrado estándar. Otro protocolo para VPN conocido L2TP (*Layer Two Tunneling Protocol*) desarrollado con la colaboración de la IETF, Cisco y Microsoft, reúne las mejores características de PPTP con un protocolo anterior a L2TP conocido como L2F (*Layer 2 Forwarding*) desarrollado por Cisco, ambos PPTP y L2TP son aplicaciones cliente-servidor. La figura 36 muestra un esquema básico de una arquitectura VPN.

Figura 36 **Red privada virtual**



El uso de las VPN puede causar una fuerte sensación de seguridad, lo que puede causar que se baje la guardia en torno al tema, pero como toda tecnología es propensa a sufrir ataques y alguien con la suficiente capacidad puede llegar a autenticarse como un usuario válido lo que le daría acceso a toda la red, lo que abriría camino para realizar cualquier tipo de ataque sobre esta, por lo que el administrador del sistema debe tomar todas las medidas necesarias para no permitir ataques que puedan comprometer a toda la red.

4.1.4 NAT

La traducción de direcciones de red o NAT (*Network Address Translation*) es una herramienta utilizada para que una red local pueda hacer el mapeo de su rango de direcciones privadas a un rango de direcciones públicas, de manera transparente para el usuario.

Esta traducción es debido a que el rango de direcciones privadas solo son aplicables dentro del dominio al que pertenecen y no se puede acceder a redes públicas como la Internet, tampoco se puede acceder desde una red pública a red privada, por lo que NAT daría en cierta forma seguridad a la red al ocultarla de una red pública.

Comúnmente NAT es implementada en router o firewalls que permiten el acceso a los hosts pertenecientes a una red privada a la Internet, por lo que únicamente el router o firewall será accesible desde la red pública, por lo que cualquier ataque hacia la red privada se iniciaría sobre el servidor NAT, por lo que no es recomendable si se tiene un router NAT conectarlo directamente a una red pública, en todo lo posible se debe de conectar a través de un firewall, para evitar posibles intromisiones. Aunque su uso es muy común actualmente en redes de datos basadas en IPv4, debido al agotamiento de direcciones IP públicas, su implementación en VOIP ha ocasionado ciertos problemas debido a la traducción de direcciones y por que los protocolos usados en VOIP dividen la señalización y los datos en canales separados, por lo cual se han desarrollado otras herramientas que trabajan de forma conjunta con el NAT para resolver estos problemas.

Diferentes tipos de NAT son actualmente utilizados, a continuación se explica cada uno de ellos.

- NAT estático: En este tipo de NAT el mapeo de direcciones se realiza uno a uno, es decir que por cada dirección IP privada se tiene una dirección IP pública. NAT mantiene una tabla de búsqueda que contiene direcciones privadas y públicas necesarias para realizar la traducción, al ser estático el mapeo la dirección pública para cada host será siempre la misma. Esto es necesario si los hosts deben de mantener una misma dirección en cada una de sus conexiones a la Internet. Además permite el mapeo de direcciones IP internas en redes privadas e iniciar una conexión desde el exterior con servidores Web, de correo electrónico o DNS que se encuentren en una red privada, es decir que el inicio de una sesión se puede iniciar desde adentro o fuera de la red privada.
- NAT dinámico: El NAT dinámico está diseñado para el mapeo de una dirección IP privada a una dirección pública de entre un conjunto de direcciones públicas. Es decir, que cualquier dirección IP pública de este conjunto se asigna a un host de la red interna, no necesariamente la misma.

- NAT de cono completo o NAPT (*Network Address Port Translation*): Este tipo de NAT permite compartir una dirección IP pública única entre el conjunto de hosts de la red privada, se logra compartir la dirección al asignar a cada host un número de puerto distinto, por ejemplo las direcciones privadas 192.168.1.2 y 192.168.1.3 serían traducidas a la dirección IP pública 200.150.100.50 con puerto 1010 y 2020 respectivamente. La mayoría de router usados en redes privadas hogareñas y en pequeñas oficinas, utilizan este tipo de NAT y es el que más se ha difundido ya que ayudo a evitar el rápido agotamiento de la direcciones IP públicas.
- NAT de cono restringido: Todos las solicitudes desde la misma dirección IP interna y su respectivo puerto son traducidos a la misma dirección IP externa y puerto respectivo. Este tipo de NAT es unidireccional ya que para que un host externo pueda enviar datos hacia un host interno solamente si ha recibido previamente datos de este, es decir que un host externo no puede iniciar una sesión. Por ejemplo si el host externo con dirección 300.250.150.100 trata de enviar datos a 192.168.1.2:80 (200.150.100.50:1010), pero este no le ha enviado datos al host externo, los datos provenientes de la dirección externa serán rechazados.
- NAT de cono restringido a puerto: Este trabaja de manera similar al cono restringido con la diferencia de que ahora también se incluye el número de puerto. Es decir que un host externo puede enviar datos a un host interno solamente si este ha enviado datos a la dirección IP y puerto del host externo. Si a la hora de enviar datos el host externo no incluye el número de puerto al que se le enviaron datos, estos no podrán ser encaminados correctamente hacia su destino.

- NAT simétrico: Todas las solicitudes desde una dirección IP interna y puerto respectivo son traducidas a una dirección externa y puerto externo y enviados al destino. Si la misma dirección interna y puerto interno envían datos hacia otro destino se utiliza una traducción distinta, y únicamente un host externo que haya recibido datos desde el host interno puede enviar datos de vuelta. Este tipo de NAT es más comúnmente encontrado en empresas.

Actualmente la mayoría de redes privadas se encuentran detrás de cualquiera de los distintos tipos de NAT, y como se comentó con anterioridad NAT causa problemas en los protocolos utilizados por la telefonía IP (H.323 y SIP). Uno de estos problemas es debido a la traducción de direcciones y puertos hecha por NAT. Al iniciarse una sesión los terminales negocian las direcciones y puertos que se utilizarán, las direcciones en este caso serían las que le fueron asignadas en la red privada. A la hora de iniciar el flujo multimedia, los protocolos usados en telefonía IP agregan esta dirección en cada uno de los mensajes enviados, al pasar por NAT este cambia únicamente la dirección privada por la pública solo a nivel de la cabecera IP, pero no mira las contenidas dentro de los mensajes, lo cual causará un desacople que no permitirá la recepción de los mensajes correctamente, lo que podría ocasionar que se reciba audio en un solo sentido, generalmente desde dentro de la red hacia fuera, si únicamente uno de los usuarios se encuentra tras de un router NAT, esto debido a que el cliente ha indicado en el mensaje su dirección IP que corresponde a una dirección privada la cual no es accesible desde fuera de NAT. El problema se agrava al estar ambos usuarios de tras de un router NAT, ya que provocaría que no se reciba audio en ninguna vía.

Otro problema común relacionado a NAT es el de no poder recibir llamadas entrantes, ya que cualquier aplicación IP que necesite crear una conexión con un host dentro de la red privada necesita saber la dirección IP y puerto que ha sido asignada por NAT al host interno. Lo que permitiría realizar únicamente llamadas salientes de la red privada.

La mayoría de problemas relacionados con NAT se resuelven fácilmente al utilizar el protocolo IAX2 (*Internet Asterisk Exchange*), el cual fue pensado por su creador para poder atravesar firewall y NAT, lo que no ocurrió con H.323 y SIP. El protocolo IAX2 será abordado en el siguiente capítulo.

Algunas de las soluciones que se han presentado para corregir los problemas relacionados con NAT, y aplicables en su mayoría a SIP, ya que es más popular que H.323, son: STUN (*Simple Traversal of UDP through NATs*), TURN (*Traversal Using Relay NAT*), ICE (*Interactive Connectivity Establishment*), ALG (*Application Level Gateways*) y UPnP (*Universal Plug and Play*).

STUN es un protocolo cliente-servidor que permite conocer a una aplicación el tipo de NAT entre el y la Internet, además se puede obtener el mapeo entre una dirección IP privada y su puerto respectivo y la dirección IP pública y puerto asignado. Esto ayuda a facilitar la recepción de los paquetes de voz por UDP. La aportación de este protocolo ha ayudado en mayor medida a las aplicaciones residenciales, ya que STUN no trabaja en presencia de NAT simétrico, el cual como se dijo con anterioridad es mayormente encontrado en empresas.

TURN es un protocolo similar a STUN, una solución para NAT simétrico. A diferencia de STUN este protocolo puede recibir datos sobre TCP y UDP, por lo que se podría decir que TURN es un complemento de STUN.

El uso de estos protocolos no causa mayores complicaciones a los usuarios de la red ni para NAT ya que comúnmente son agregados dentro de las aplicaciones, como pueden un softphone o un teléfono IP, por lo que al iniciar una sesión automáticamente se envía la petición de reconocimiento a un servidor STUN o TURN.

El acceso a estos servidores es restringido ya que se debe ser usuario autorizado para poder hacer uso del servidor, el acceso se realiza a través de un password y nombre de usuario, los cuales son enviados por TLS. La mayoría de estos servidores pueden ser encontrados a través del registro DNS SRV, el cual permite especificar de forma genérica la ubicación de servidores para un servicio, protocolo y dominio DNS determinados. La tabla II muestra algunos servidores STUN y sus respectivas direcciones IP.

Tabla II. **Servidores STUN**

Stun.fwdnet.net	69.90.168.14
Stun.fwd.org	64.186.56.73
Stun01.sipphone.com	69.0.208.27
Stun.softjoys.com	69.3.254.11
Stun.voxgratia.org	83.103.82.85
Stun1.vovida.org	182.107.250.38
Xtunnels1.xten.net	64.69.76.23

Fuente: Porter, Thomas y otros. **Practical VOIP Security**. Pág. 402.

ICE a diferencia de los protocolos anteriores, es más bien un método utilizado para habilitar el tráfico entre terminales SIP, para lo cual hace uso de protocolos como STUN y TURN, para descubrir la dirección externa y puerto.

ICE para realizar su trabajo requiere la cooperación de los terminales involucrados en la comunicación, autorizándolos para descubrir el tipo de NAT que existe entre de ellos y proponiendo una lista con las direcciones IP por las cuales pueden comunicarse. Su uso es independientemente del número o tipo de NAT. La única adaptación necesaria es a nivel de mensajes SDP ya que se deben agregar algunos atributos para su funcionamiento.

Otra de las soluciones utilizadas en NAT es ALG, el cual es un software agregado a NAT que permite a éste entender los paquetes pertenecientes a los protocolos H.323 o SIP. ALG abre los paquetes VOIP y los reconfigura con la nueva dirección IP pública o privada correcta para que la comunicación a través de NAT sea posible. Estos cambios los realiza nivel de cabecera IP y a nivel de mensaje SDP, además permite el mapeo del tráfico RTP entre los puertos, al hacer la lectura desde y hacia un host interno. El uso de ALG puede reducir considerablemente el rendimiento de NAT si debe de procesar muchas llamadas consecutivamente, además el tráfico de datos también es procesado por ALG.

UPnP es otra de las soluciones que pretenden mejorar la relación NAT-telefonía IP. Un cliente SIP UPnP puede dialogar con un NAT actualizado para tal efecto y comunicarle sus necesidades de puertos activos y direcciones IP. Por lo que el cliente puede preguntar a NAT directamente acerca de su dirección IP externa y número de puerto asignado. Una de las debilidades de UPnP es su vulnerabilidad a ataques de negación de servicio. Además no funciona correctamente en casos de NAT en cascada.

Otro problema agregado al uso de NAT es su incompatibilidad con el cifrado IPsec, más concretamente con AH y ESP los dos protocolos que pueden ser usados por IPsec. La incompatibilidad con AH se debe a que este protege los datos al verificar que el paquete no haya cambiado durante su transportación al destino, NAT cambia la dirección IP y puerto, lo que hace que falle la autenticación de los paquetes y que estos sean desechados. ESP es un protocolo dependiente del campo checksum de TCP y UDP, debido al cambio generado en la dirección IP y puerto de la fuente el checksum de la cabecera IP y del protocolo de transporte, ya sea TCP o UDP se tiene que calcular nuevamente, lo que causa que falle la autenticación ESP, y de igual manera que los datos sean descartados.

También hay que tomar en cuenta a IKE, ya que es el encargado de negociar las claves utilizadas y el protocolo a utilizar (AH o ESP) durante una conexión, la principal incompatibilidad es debido a que IKE utiliza el puerto 500 UDP el cual al ser cambiado por NAT crea un desacople entre los participantes de la conexión, lo que conlleva no poder iniciar la sesión, ya que si falla la negociación de las claves y protocolos no es posible la comunicación.

Algunos métodos usados para evitar estos problemas son: Realizar NAT antes que IPsec, es decir que NAT es colocado lógicamente detrás de IPsec o hacer uso de RSIP (*Realm Specific IP*) o el encapsulado UDP. RSIP viene a ser un sustituto de NAT, el cual hace uso de gateways RSIP los cuales funcionan de manera similar a NAT, con la diferencia de que en vez de asignar direcciones privadas se arriendan direcciones desde un espacio público las cuales son pasadas a los hosts RSIP, además permite la conectividad extremo-extremo a través de IPsec. RSIP soporta AH y ESP, y aunque demuestra ser mejor que NAT para su implementación es necesario realizar una revisión de las arquitecturas actuales de las redes locales, lo que lo hace poco factible.

El encapsulado UDP es la opción más usada para resolver los problemas de NAT e IPsec, lo que permite el tráfico ESP a través de NAT en ambas direcciones ya sea en modo túnel o transporte.

Los puertos utilizados por esta opción son los mismos que utiliza IKE, esto debido a su fácil implementación y configuración ya que únicamente un puerto debe de ser configurado en un firewall, si este está presente en la red, para diferenciar entre paquetes IKE y ESP encapsulados se hace uso del campo SPI (*Security Parameters Index*) de la cabecera de ESP el cual es colocado a cero. La encapsulación se puede implantar tanto en IPv4 como en IPv6 siempre y cuando las negociaciones se realicen con IKE.

4.1.5 VLAN

La separación del tráfico de voz y datos para ayudar en la seguridad de las redes VOIP ha hecho necesario el uso de las VLAN, las cuales dividen de forma lógica una red LAN, es decir que la red es segmentada en distintas subredes o dominios broadcast, por lo que una VLAN es una agrupación lógica de hosts y dispositivos de red que no se limitan a un segmento de red físico. La función principal de esta separación es evitar que los problemas que afectan al tráfico de datos afecten al tráfico de voz e igualmente que los problemas del tráfico de voz no afecte al de datos, además permite mejorar la utilización del ancho de banda, permitir que únicamente los hosts pertenecientes a una VLAN puedan acceder a ella y niega el acceso a cualquier otro host, reduce la carga de procesamiento en hosts y teléfonos IP al reducir el flujo de paquetes broadcast innecesarios en algunos casos para las estaciones.

Las VLAN son implementadas en la capa dos del modelo OSI a nivel de software en los conmutadores de red (*switch*), la conectividad entre las distintas VLAN se realiza con routers y puede coexistir más de una VLAN en un mismo switch. Por ejemplo un switch con 12 puertos puede dividirse en 4 VLAN donde cada una contendrá 3 hosts o teléfonos IP, cada una de estas VLAN se dividen de acuerdo a criterios requeridos por el administrador.

En una empresa se podría crear una VLAN de contabilidad, otra de ventas, una de administración y otra de VOIP y cada una de ellas será independiente una de la otra, es decir que el flujo de datos será visto por una VLAN, a la que le pertenezcan los datos. Los hosts en una VLAN también pueden agruparse por protocolo, por puerto o por dirección MAC que son las tres formas básicas de agrupación. Las VLAN al ser segmentos lógicos de una red, no hacen importante la conexión física o la ubicación de los usuarios.

Durante la creación de las VLAN es necesario crear una de administración que se encargue de gestionar el switch, se debe de asignar al menor un puerto, los demás se reparten entre las otras VLAN que se deseen crear. La asignación de los puertos puede hacerse de forma estática o dinámica. En la forma estática cada puerto es asignado a una VLAN por el administrador, en la forma dinámica se usa una base de datos que contiene direcciones MAC que se asocian a una VLAN en particular, la base debe de ser configurar primeramente por el administrador.

La forma de identificar a que VLAN corresponde una trama en particular se hace a través del etiquetado de tramas. Existen dos métodos comunes de etiquetado estos son: ISL (*Inter Switch Link*) desarrollado por Cisco y el 802.1Q desarrollado por IEEE (*Institute of Electrical and Electronics Engineers*), aunque el ISL era en un principio el más común, ahora el 802.1Q se ha vuelto más popular.

La figura 37 muestra 3 VLAN configuradas en un switch y un router el cual se encarga de enlazar a las VLAN, en esta configuración los hosts comparten el mismo espacio físico, de igual manera se podría crear las mismas 3 VLAN sin compartir el mismo espacio físico, es decir que cada uno de los hosts que pertenecen a VLAN 1, 2 y 3 se podrían encontrar en pisos diferentes en un edificio, para poder realizarlo se emplearían 3 switch y un router para enlazarlos, esto es mostrado en la figura 38.

Figura 37. VLANs en un mismo espacio físico

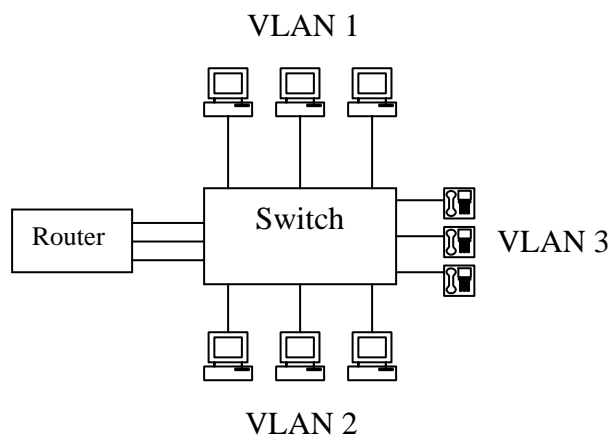
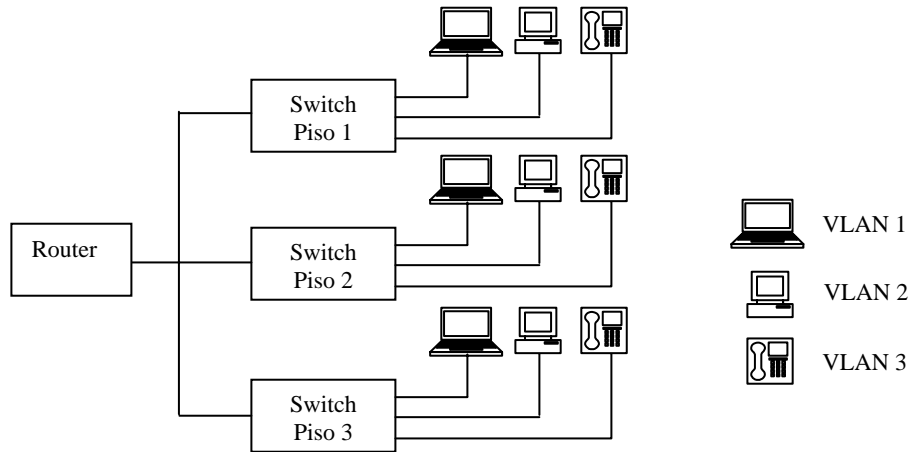


Figura 38 VLANs en distinto espacio físico



La utilización de softphone en las VLAN crea conflicto en la función principal de esta, que es la de separar el tráfico de voz y datos. Los hosts que contiene softphone deben de coexistir en ambas dominios: Voz y datos. Una solución a este problema es proveer a los hosts con dos tarjetas de red para que una de ellas resida en el dominio de datos y la otra en el dominio de la voz. La presencia de softphone en los ambientes VOIP puede disminuir la seguridad en la red, ya que son tan vulnerables como el sistema operativo sobre el que se ejecutan, por lo que cualquier virus, gusano o cualquier malware en el host residente también puede afectar a los softphone, por lo que se debe de prohibir softphone que contengan algún tipo de publicidad o que almacene información de los usuarios sin ningún tipo de cifrado.

4.1.6 Seguridad H.323

4.1.6.1 H.235

El protocolo encargado de la seguridad en H.323 es el H.235, interactúa con H.245, H.225.0-RAS, H.225-Q931 y RTP, para el establecimiento, señalización y flujo de audio de la llamada, lo que provee a la arquitectura seguridad y autenticación. Una de las características principales de H.235 es su capacidad de incorporar claves de cifrado para proteger la señalización y el flujo multimedia a través de los mensajes de establecimiento de llamada, lo cual se realiza canal por canal, lo que permite que múltiples canales puedan ser cifrados de distinta manera, útil en aplicaciones de comunicación multipunto, el uso de TLS a nivel de capa de transporte o IPsec a nivel de capa de red provee seguridad al dar confiabilidad al canal de comunicación, aunque también puede ser implementada en las aplicaciones o servicios H.323 como una capa agregada de protección. La autenticación es considerada como una parte fundamental en el establecimiento de llamadas confiables entre dispositivos H.323 y puede ser implementada al hacer uso de claves simétricas, función hash y mecanismos de claves públicas. Los elementos que finalicen la creación de un canal de control o un canal de datos codificado son considerados un elemento de confianza en la conexión. Si los terminales involucrados en la comunicación tienen capacidades de seguridad compatibles se crea el canal de comunicación, si no se logra establecer un canal H.245 seguro la conexión termina.

El protocolo se divide en varias secciones que van desde H.235.1 a H.235.9 y son perfiles de H.235.0, el cual es el marco de seguridad para sistemas basados en H.323 y H.245, estos perfiles son negociados durante el intercambio de mensajes de señalización. Los perfiles se agrupan dentro de las recomendaciones H de la ITU, a continuación se describen las características más importantes de cada uno de ellos.

4.1.6.1.1 H.235.1

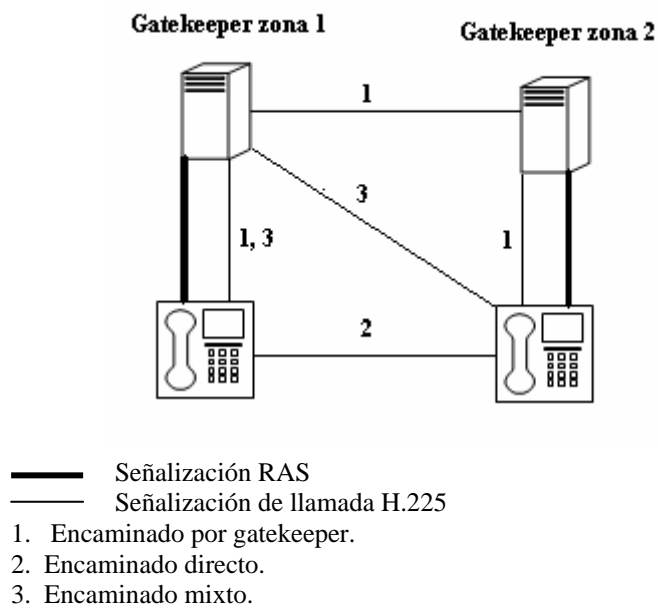
El perfil de seguridad básico se basa en las técnicas criptográficas seguras basadas en claves (secreto compartido), las cuales son usadas para proveer autenticación e integridad o solamente autenticación a H.225.0 RAS, mensajes de señalización y H.245 encapsulado, el cual consiste en la inserción de mensajes H.245 dentro de una conexión rápida H.225. El perfil de seguridad hace uso de HMAC (*Hashed Message Authentication Codes*) en conjunto con el algoritmo hash SHA1-96 (*Security Hash Algorithm*) para cumplir el propósito de integridad y autenticidad, aplicable a comunicaciones entre terminales H.323 y gatekeeper, entre gatekeeper y gatekeeper y entre gateway y gatekeeper. En algunos casos es requerido el uso de dos claves, una para los mensajes RAS y otra para los mensajes de señalización. En este perfil es obligatorio el uso del procedimiento de conexión rápida, procedimiento por el cual se crea una conexión extremo-extremo básico con un único intercambio de mensajes de ida y vuelta, para una entrega rápida del flujo multimedia. Además se incluye para la gestión de claves el algoritmo Diffie-Helman.

El uso del perfil para dar únicamente autenticación es utilizado si los mensajes de señalización deben atravesar NAT y Firewall. Existen tres formas de autenticar los mensajes de señalización H.225 entre terminales H.323, los cuales son: Encaminado por gatekeeper, Directo y el mixto.

En el encaminado por gatekeeper, los mensajes de señalización son transportados entre los correspondientes gatekeeper de zona, se recomienda el uso de IPsec o TLS para asegurar los mensajes de señalización que deben atravesar distintas zonas H.323. En el encaminado directo, los mensajes de señalización son enviados directamente entre los terminales H.323 que se desean comunicar, este sistema brinda una verdadera seguridad de extremo a extremo, ya que no depende de elementos intermedios de confianza.

En el encaminamiento mixto, se hace uso únicamente de uno de los gatekeeper de zona para transportar la señalización entre los terminales H.323. La figura 39 ilustra los mecanismos de señalización comentados con anterioridad.

Figura 39 Mecanismos de señalización H.225



4.1.6.1.2 H.235.2

Este perfil de seguridad es una implementación de firmas digitales para proteger mensajes de señalización H.225, RAS y H.245, al igual que el perfil anterior provee autenticación e integridad o únicamente autenticación, hace uso de los algoritmos hash SHA1 o MD5. Al hacer uso de firma digitales se agrega una característica a la seguridad, y consiste en el no repudio de los mensajes. El perfil puede ser utilizado en redes de gran escala donde el cifrado simétrico no es factible, donde pueden existir bastantes terminales, en conferencias multipunto y autenticación extremo-extremo, su implementación debe de hacerse en base al encaminado por gatekeeper y debe soportar H.245 encapsulado. Con este perfil pueden evitarse situaciones que pueden comprometer la seguridad de la red VOIP como: Ataque de negación de servicio, accesos no autorizados, robo de identidad. Además su implementación puede permitir el intercambio compartido de claves secretas para el cifrado del tráfico RTP.

4.1.6.1.3 H.235.3

Este es un perfil de seguridad híbrido, basado en H.235.1 y H.235.2, el perfil hace uso de firmas digitales pero solamente si es absolutamente necesario, de lo contrario se hace uso de las claves simétricas del H.235.1. Con El uso de los perfiles H.235.1 y 2 se logra un perfil de seguridad escalable basado en una infraestructura de claves públicas, que permite superar las limitaciones de H.235.1 y mejorar las características de H.235.2, al hacer uso de un menor ancho de banda y mejorar la calidad del procesamiento. Su implementación se realiza en base al encaminamiento por gatekeeper y por el uso de la conexión rápida, además permite el uso de H.245 encapsulado.

En este perfil se utiliza los términos primer mensaje y ultimo mensaje. El primer mensaje es el encargado de establecer el contexto de seguridad al poner a disposición de los terminales el conjunto de claves simétricas, mientras que el último mensaje termina con el contexto de seguridad establecido. También se introduce el uso de un gatekeeper de procesos de seguridad (GKSP), el cual es usado para aliviar la carga de procesamiento, como por ejemplo para el cálculo y la verificación de firma digitales, su uso mejora la escalabilidad y robustez del sistema. El perfil puede ser implementado en terminales H.323, gatekeeper y gateway, y provee protección a los mensajes H.225, RAS y H.245.

4.1.6.1.4 H.235.4

Este es el perfil de seguridad de llamada con encaminamiento directo y selectivo, a diferencia de los anteriores no hace uso del encaminamiento por gatekeeper, si no como su nombre lo indica se basa en el encaminamiento directo, el perfil permite una mayor flexibilidad y escalabilidad en comparación con el modelo de encaminado por gatekeeper al permitir el manejo de múltiples canales paralelos.

El uso de la configuración asume que los terminales que se comunican lo hacen sobre una red insegura, al inicio de la comunicación cada terminal debe de crear una comunicación de confianza con su respectivo gatekeeper de zona, ya sea por H.235.1 o H.235.3, en algunos casos se requiere que los gatekeeper de zona también creen una conexión de confianza. La conexión directa entre ambos terminales permite compartir claves secretas a través de una red insegura y así proteger los mensajes de señalización de llamada y el flujo multimedia. El uso del gatekeeper en esta configuración asume la responsabilidad del manejo de registros, admisión, resolución de direcciones y manejo del ancho de banda.

El perfil maneja tres tipos de implementación los cuales son: DRC1 (*Direct Routed Call*), DRC2 y DRC3. El DRC1 es usado en ambientes corporativos donde los gatekeeper de zona se encuentran bajo las mismas políticas de seguridad al pertenecer al mismo dominio administrativo. DRC2 y 3 son utilizados en ambientes donde existen múltiples dominios administrativos y cada uno de ellos sujetos a distintas políticas de seguridad. La diferencia entre ambos radica en que DRC2 es utilizado en ambientes donde los terminales llamantes o los gatekeeper no soportan el algoritmo Diffie-Hellman, mientras que DRC3 se implementa en ambientes en donde los terminales llamantes no soportan el algoritmo pero los gatekeeper de zona si lo soportan.

4.1.6.1.5 H.235.5

Este perfil define una estructura de seguridad para la autenticación en mensajes RAS a través del uso de secretos compartidos débiles. Las propiedades de los secretos compartidos, como password o un PIN y toda clave criptográfica derivada de ellos y usados para crear una relación de confianza entre distintos dispositivos no son lo suficientemente resistentes a los ataques por búsquedas exhaustivas, como por ejemplo las búsquedas por diccionario, en donde se tiene un listado de palabras usadas comúnmente como password o PIN, este listado se prueba una a una hasta encontrar cual fue el secreto compartido usado para cifrar una clave publica, la implementación de H.235.5 se basa en el uso de mensajes iniciales RAS para negociar un conjunto de secretos compartidos más fuerte para cifrar y autenticar los mensajes RAS y los mensajes de señalización de llamada, esto evita que un atacante obtenga un mensaje en texto simple conocido y lo utilice para un ataque exhaustivo.

Existen protocolos que combinan la seguridad de un intercambio Diffie-Hellman fuerte con el uso de un secreto compartido para evitar que terceros usen un ataque por búsqueda exhaustiva que les permita obtener el secreto compartido, entre los protocolos utilizados están EKE (*Encrypted Key Exchange*) y SPEKE (*Simple Password Exponential Key Exchange*). El uso del perfil se limita a la estructura de encaminamiento por gatekeeper.

4.1.6.1.6 H.235.6

El perfil de encriptación vocal con manejo de claves H.235/H.245 nativo, es una implementación que puede ser utilizada en conjunto con H.235.1 para proveer confidencialidad al flujo multimedia. El perfil define un conjunto de algoritmos de cifrado entre los que se encuentran: AES, RC2, DES y 3DES, cada uno de estos algoritmos trabaja de manera conjunta con los codec. La negociación del perfil se lleva a cabo durante el intercambio de capacidad de seguridad del terminal a través de H.245 y la conexión rápida.

H.235.6 establece un componente en la arquitectura conocido como maestro, que no es más que un terminal, el cual tiene a su cargo generar y difundir las claves de cifrado, de gran utilidad en aplicaciones en donde se manejan múltiples canales, además soporta la autenticación de igual forma que se hace para dos terminales. Otro punto importante de perfil es que permite el cifrado de tonos DTMF.

4.1.6.1.7 H.235.7

Este perfil hace uso del protocolo de gestión de claves MIKEY conjuntamente con SRTP para negociar claves de encriptación y proveer seguridad al flujo multimedia, además provee la capacidad de interactuar con terminales SIP que hayan implementado MIKEY y SRTP. Los mensajes MIKEY son transportados dentro de los mensajes señalización H.245 negociados por los terminales. El perfil recomienda la utilización de H.245 encapsulado, en caso de no hacerlo se requiere el uso de un protocolo de transporte seguro, ya sea TLS o IPsec, además se debe implementar la conexión rápida. H.235.7 se basa en dos perfiles de seguridad los cuales son: La arquitectura basada en claves simétricas con soporte para múltiples gatekeepers, y la arquitectura basada en claves asimétricas con soporte para múltiples gatekeepers. Este último se basa en una infraestructura de claves públicas (PKI).

4.1.6.1.8 H.235.8

Este perfil define el intercambio de claves para SRTP al hacer uso de canales de señalización seguros como IPsec o TLS, el proceso de autenticación y la negociación del algoritmo de cifrado a utilizar también se realizan durante el intercambio de claves.

El perfil esta enfocado a comunicaciones unicast, aunque se espera ampliarlo a multicast. Una comunicación unicast crea dos canales unidireccionales encargados de mantener los distintos parámetros SRTP, el intercambio de parámetros de cifrado SRTP sobre mensajes H.245 permite funciones como el intercambio y negociación de capacidades de cifrado e integridad de medios SRTP, negociación y establecimiento de el cifrado inicial y los algoritmos, claves y parámetros de sesión que habrán de utilizarse para los flujos SRTP en cada sentido y modificación del cifrado y los algoritmos, claves y parámetros de sesión en cualquier momento durante la sesión SRTP.

El perfil permite además añadir el procedimiento de claves públicas para garantizar la autenticación y confiabilidad de extremo a extremo de las claves de sesión SRTP.

4.1.6.1.9 H.235.9

Este perfil introduce el uso de gateways de seguridad (SG), el cual es un dispositivo ALG que sabe reconocer a los protocolos de señalización H.323. El gateway de seguridad se instala entre dos o más dominios de red IP para realizar las funciones relacionadas a la seguridad, como la validación o restricción de los flujos de paquetes y la traducción de direcciones de transporte entre los dominios.

La introducción de este perfil obedece al hecho de que dispositivos como firewall o NAT crean problemas al flujo H.323, por lo que los SG tendrán la tarea de manipular los mensajes multimedia y de señalización según se haga necesario. En el perfil se detalla un mecanismo sencillo para informar a los ALG que se encuentran en el camino de la señalización e intercambiar con estos la clave de autenticación de señalización negociada, lo que le permitirá a los ALG poder modificar datos no privados como direcciones de transporte de los mensajes de señalización y autenticar el resultado antes de retransmitir los mensajes modificados hacia su destino, cosa que no sucede con NAT, por lo que su uso provoca que la autenticación y integridad de los datos falle al ser verificado. El uso de estos dispositivos permite mantener la privacidad de extremo a extremo de todo elemento cifrado que tome parte en la señalización.

4.1.6.2 Firewall

Para poder utilizar un firewall en una red H.323 es necesario conocer los puertos TCU/UDP, por los cuales los mensajes de establecimiento de llamada, señalización y flujo RTP deben pasar, la tabla III muestra cada uno de los puertos relacionados a los mensajes H.323.

Tabla III. **Requerimientos de firewall para H.323**

	PUERTO
Descubrimiento de Gatekeeper	1718/UDP
Mensajes RAS	1719/UDP
Señalización Q.931	1720/TCP
Señalización H.245	1024-65535/TCP
Señalización H.235	1300/TCP
RTP-RTCP	1024-65535/UDP

Fuente: Porter, Thomas y otros. **Practical VOIP Security**. Pág. 396.

4.1.7 Seguridad en SIP

Al igual que en H.323 la seguridad en SIP es un punto importante dentro del protocolo, es necesario que dentro de las red SIP exista autenticación e integridad de los datos para minimizar cualquier tipo de ataque. La recomendación RFC 3261 de la IETF describe el funcionamiento de SIP, incluye además procedimientos y herramientas que pueden ser usados para proveer de seguridad a los usuarios SIP.

Dentro de las vulnerabilidades más conocidas que presenta SIP se encuentran: Secuestro de registros, suplantación de identidad, paralización de actividades de usuarios o servidores SIP debido a ataques por inundación de mensajes INVITE, denegación de servicio por envío de mensaje BYE, debilidad por el uso del algoritmo MD5 en http digest, degradación de la calidad o reinicio de dispositivos por inundación RTP, recepción de mensajes no solicitados debido a SPIT (*Spam over Internet Telephony*).

4.1.7.1 Http digest

Una de las herramientas descritas en la recomendación se basa en el uso de http digest, el cual es utilizado para proveer autenticación y protección contra replicas de los mensajes de registro, de inicio y fin de sesión, la autenticación puede llevarse a cabo por un usuario que autentifica a otro o por un servidor Proxy o cualquier otro servidor de la arquitectura que autentifica a un usuario. Http digest es una forma liviana de autenticación que permite el uso de secretos compartidos, una forma más robusta hace uso de la encriptación.

Un punto importante dentro de la seguridad es la integridad de los datos, http digest únicamente puede entregar autenticación, para proveer integridad se hace necesario el uso de TLS, IPsec, S/MIME (*Secure/Multipurpose Internet Mail Extensions*), todos ellos al igual que http digest son recomendaciones del RFC 3261.

4.1.7.2 TLS

El uso de TSL en SIP para proveer privacidad es conocido como *SIPS URI scheme* o *Secure SIP*, trabaja de manera similar que SIP normal pero su medio de transporte no es TCP o UDP sino TLS. TLS puede trabajar de forma conjunta con http digest para aumentar la seguridad en las redes SIP. Las conexiones TLS se efectúan entre cliente y servidor y no entre extremos, para poder realizar conexiones entre extremos debe de existir una conexión entre el cliente y el SIP Server de su dominio y una conexión entre ambos SIP server.

Un protocolo similar a TLS es DTLS (*Datagram Transport Layer Security*), destinado a dar seguridad a conexiones UDP lo cual no hace TLS ya que solamente corre sobre TCP, la implementación de este protocolo hace mayor el rango de aplicaciones a las cuales se les puede brindar seguridad. DTLS se encuentra definido en la recomendación IETF RFC 4347.

4.1.7.3 S/MIME

Protocolo utilizado para proveer confidencialidad, no repudio de los mensajes, integridad y autenticación extremo a extremo o a través de servidores SIP. Puede ser utilizado por TCP o UDP, además permite seleccionar que parte del mensaje se quiere proteger al contrario de TLS que abarca todo el mensaje. El algoritmo de firma digitales SHA1 y el algoritmo de encriptación 3DES son utilizados por S/MIME para proveer la seguridad de los mensajes aunque pueden ser usados otros algoritmos, además se requiere de una infraestructura de claves públicas para su implementación, cuestión que lo coloca en desventaja con respecto a TLS que no requiere de esta infraestructura. Este protocolo esta definido dentro de la recomendación RFC 3851.

4.1.7.4 Firewall

Al igual que H.323 la implantación de SIP en una red con firewall hace necesario conocer los puertos utilizados por este para permitir el flujo de información entre los usuarios del sistema. La tabla IV muestra los puertos usados por SIP.

Tabla IV. Requerimientos de firewall para SIP

	PUERTO
SIP	5060/TCP
SIP/TLS	5061/TCP
RTP-RTCP	1024-65535/UDP

Fuente: Porter, Thomas y otros. **Practical VOIP Security**. Pág. 533.

4.1.8 Monitoreo de la red

El uso de firewall, NAT o cualquier otro sistema usado para prevenir ataques a las redes, ya sean de datos o VOIP son de gran importancia en la seguridad, pero no todos los ataques provienen de redes externas, también pueden venir desde adentro de la propia red, además los elementos usados para la seguridad también pueden ser objeto de ataques y accesos no autorizados. El uso de mecanismos para monitorear la red y prever ataques o intrusiones también es de gran importancia dentro de la infraestructura de seguridad.

Los NIDS (*Network Intrusion Detection Systems*) y los HIDS (*Host Intrusion Detection Systems*) son herramientas utilizadas para detectar tráfico malicioso en una red, accesos a áreas no autorizadas o determinar que usuarios realizan acciones que puedan resultar perjudiciales para la seguridad de la red.

NIDS trabaja a nivel de red mientras que HIDS trabaja en un determinado host, la información obtenida por estas herramientas son guardadas en archivos denominados logs, que pueden ser revisados posteriormente por el administrador de red. Estos detectores pueden ser pasivos o activos, lo cual depende de si toman alguna acción sobre el ataque o solamente informan sobre el, además el rastreo realizado es en tiempo real. Uno de sus principales problemas es que no pueden analizar el flujo de datos cifrados.

Estas herramientas no son susceptibles a ataques a ellos mismos, un intruso podría lograr inutilizar al detector o enmascararse y entregar información confiable al detector o simplemente podría tener acceso a los logs y modificarlos para no dejar huella de su paso por la red y no ser descubierto hasta que ocurra un problema de seguridad. En redes donde se utilizan firewall se suelen utilizar los NIDS antes o después del firewall, en la misma máquina o uno adelante y otro atrás del firewall.

Snort es un NIDS que puede funcionar de forma pasiva o activa, es gratuito (Licencia GPL) y puede ser utilizado en sistemas operativos windows y Unix. Al igual que Snort existen otras herramientas que funcionan como NIDS o HIDS, ya sea de forma gratuitas o propietaria, cada uno con su pro y contra. Si se usan estas herramientas es indispensable mantenerlas actualizadas para minimizar los posibles ataques. La seguridad en telefonía IP es tema bastante extenso, ya que al igual que en las redes de datos día a día se crean o encuentran nuevas vulnerabilidades en los sistemas, por lo que es necesario seguir ciertas normas básicas para minimizar en lo posible fallas en la seguridad.

Actualmente, las redes corporativas o domesticas se encuentran conectadas al Internet donde existen miles de usuarios que podrían capturar nuestros datos o conversaciones si no se toman las medidas necesarias, algunos ataques podrían tener repercusiones mientras que otros no, nunca se sabe quien quiere atacar nuestra red o robar el flujo de información por lo que se debe estar preparado para poder hacer frente a este problema y no caer ante cualquier ataque.

A continuación se listan algunos pasos básicos necesarios para proveer de seguridad a los dispositivos y redes en telefonía IP:

- Cambiar los password y nombre de usuario que traen por defecto los dispositivos y en todo lo posible cambiarlos periódicamente.
- Hacer uso de firewall y deshabilitar todos aquellos servicios innecesarios en los teléfonos y servidores VOIP como por ejemplo: FTP, HTML, TELNET y algunos otros.
- Realizar la segregación del tráfico de voz y datos por medio de VLAN.
- No hacer uso de Softphone, si se utilizan es recomendable utilizar las actualizaciones del sistema operativo sobre el cual se ejecuta este, no utilizar aquellos que contengan publicidad o almacenen información del usuario sin ningún tipo de cifrado.
- Utilizar las actualizaciones del software que se ejecuta en los teléfonos IP, servidores y todo elemento que intervenga en la comunicación y utilice software.
- Utilizar cifrado para proveer de privacidad a las comunicaciones.

4.2 QoS

La calidad de servicio o QoS (*Quality of Service*) es un punto fundamental en la implementación de la telefonía IP ya que el uso de redes IPv4 introducen una serie de problemas al flujo de datos multimedia, esto debido a que estas redes fueron diseñadas para el tráfico de datos que no tienen requerimientos de tiempo real contrario a VOIP que si los tiene. En el capítulo 3 se abordaron los problemas de retardo, jitter y pérdida de paquetes que afectan en menor grado al flujo de datos, pero en telefonía IP estos podrían convertirse en serios problemas y más si se utiliza la internet, ya que pueden provocar que la fluidez de una conversación telefónica se vea afectada, lo que provocaría una comunicación poco entendible y satisfactoria. En los últimos años el tema de calidad de servicio se ha hecho popular debido a que los usuarios se han vuelto más exigentes en cuanto a la calidad de servicio que desean recibir, además la competencia entre los distintos proveedores de servicios hace que la calidad ofrecida de un servicio en particular sea mejor. El uso de firewall y NAT puede llegar a degradar el QoS, debido a que el procesamiento que se lleva a cabo sobre los paquetes introduce retardo y jitter.

La calidad de servicio en telefonía IP está orientada a mejorar parámetros como: retardo, jitter, pérdida de paquetes, ancho de banda y eliminación de eco, y aunque no es posible asegurar un nivel determinado de QoS si se le puede optimizar, el hecho de que no se pueda asegurar un nivel de QoS es debido a que las redes IP se basan en un sistema de el mejor esfuerzo, es decir que no hay garantía en la entrega, retraso y sincronización de los datos, por lo que es necesario hacer uso de mecanismos que permitan manejar los parámetros de calidad requeridos, al hacer esto se logra obtener una mejor calidad de la voz percibida por los usuarios.

La recomendación ITU G.1010 provee los parámetros de calidad de servicio para distintas aplicaciones, con respecto a voz en tiempo real con velocidades entre 4 y 64 Kbps se tiene los siguientes datos:

- Tiempo de transmisión en un sentido: Se recomienda retardos menores a 150 ms pero se puede permitir retardos no mayores a los 400 ms. Además debe existir un mecanismo de control de eco.
- Jitter: Se recomiendan valores menores a 1 ms.
- Relación de pérdida de paquetes: Se recomiendan valores menores al 3%. La pérdida de paquetes suele ser más crítica al hacer uso de la Internet, en redes privadas se tiene un mayor control sobre el flujo de información.

La tabla V muestra los retardos introducidos por algunos de los codec tratados en el capítulo 3, estos datos son de acuerdo a la recomendación ITU G.114 para aplicaciones basadas en IP con una trama por paquete. Algunos codec para mejorar el nivel de compresión miran la trama siguiente, a esto se le conoce como indagación. Los retardos unidireccionales medios mínimo y máximo son calculados de acuerdo a dos ecuaciones las cuales son:

Retardo mínimo = 2 * tamaño de trama + indagación.

Retardo máximo = 3 * tamaño de trama + indagación.

Tabla V. Retardo introducido por codecs en aplicaciones basada en IP.

Codec	Bit Rate Kbps	Tamaño de trama(ms)	Indagación (ms)	Retardo mínimo (ms)	Retardo máximo (ms)
G.711	64	0.125	0	0.25	0.375
G.726	40, 32, 24 y 16	0.125	0	0.25	0.375
G.728	16	0.625	0	1.25	1.875
G.729	8	10	5	25	35
G.723.1	5.3 y 6.3	30	7.5	67.5	97.5

Fuente: ITU-T G-114. **Tiempo de Transmisión en un sentido.** Pág 9.

Los proveedores diseñan sus redes/capacidades considerando tanto los objetivos de calidad de servicio (QoS) que podrán satisfacer las necesidades de sus clientes como la repercusión en los costos de la red, ya que los clientes examinan tanto el precio como la calidad cuando toman sus decisiones de adquisición⁵⁷.

4.2.1 Ancho de banda

Un parámetro importante dentro de la calidad de servicio es el ancho de banda mínimo para la transmisión de una llamada o varias llamadas, con un ancho de banda insuficiente se agravarían los problemas de retardo y pérdida de paquetes debido al congestionamiento en la red. El ancho de banda necesario para una red VOIP depende del tipo de codec a utilizar el tamaño de la carga útil (Payload), la sobrecarga por cabeceras y los protocolos de enlace como por ejemplo: Ethernet, ATM y Frame Relay.

La sobrecarga de cabecera correspondiente para una llamada típica es de 12 bytes de RTP, 8 de UDP y 20 bytes de IP, lo que da un total de 40 byte de sobrecargo de cabecera, aunque esto se podría incrementar al hacer uso de los campos opcionales que contienen las cabecera de RTP e IP. Algunas técnicas usadas para mejorar la gestión del ancho de banda son: supresión de silencios, compresión de cabeceras.

La tabla VI muestra el ancho de banda necesario para algunos codec VOIP, los datos fueron obtenidos al hacer uso de la calculadora *VOIP Bandwidth Calculator* de la empresa Packetizer, Inc., los cálculos se realizaron en línea desde la dirección <http://www.bandcalc.com/es/>.

⁵⁷ Grupo de expertos sobre telefonía IP del UIT-D. **Informe Esencial sobre Telefonía IP**. (Suiza: Unión Internacional de Telecomunicaciones, 2003). p.31

Tabla VI Ancho de banda en VOIP

Codec	Retardo de empaquetado ms	Tramas por paquete	Ancho de banda en Kbps
G.711	5	40	128
	20	160	80
G.726 (32Kbps)	5	40	96
	20	160	48
G.729	10	1	40
	20	2	24
G.723.1 (5,3Kbps)	30	1	16
	60	2	10.7

En los datos mostrados en la tabla 6 no se ha tomado en cuenta ningún protocolo de la capa de enlace, tampoco se toma en cuenta la supresión de silencios o protocolos de gestión de ancho de banda, además el ancho de banda corresponde a un canal unidireccional.

Según los datos obtenidos se puede observar que el ancho de banda disminuye al aumentar el número de tramas por paquete, pero hay un aumento del retardo de empaquetado, lo que podría repercutir en la calidad recibida ya que al aumentar el retardo total también hay un aumento del eco en el canal, pero esto puede minimizarse al hacer uso de supresores o compensadores de eco. El acople entre redes de paquetes y de conmutación de circuitos también genera eco, por lo que los gateway deberían de incluir un sistema que anule este problema.

4.2.1.1 Supresores de Silencio

La supresión de silencios es una técnica usada para liberar ancho de banda en los momentos en que uno de los usuarios participante de una llamada está solamente escuchando mientras la otra habla, o durante las pausas entre la conversación. Esto se consigue al no enviar paquetes durante los silencios, por lo que se hace uso del VAD (*Voice Activity Detection*), el cual reconoce la diferencia entre voz y silencio, el VAD envía paquetes con ruido ambiente o de confort para que el usuario que habla no crea que la conexión ha finalizado, esto es debido a que los usuarios del sistema telefónico tradicional están acostumbrados a escuchar algún tipo de ruido en la línea durante las conversaciones, y al ya no escuchar nada se cree que la otra parte ha finalizado la conexión.

4.2.1.2 Compresión de cabecera

La compresión de cabecera es una técnica usada para reducir la cabecera RTP/UDP/IP de 40 bytes típicos a 2 ó 4 bytes, lo cual depende de si se utiliza el campo checksum en UDP. Al hacer uso de compresión el extremo receptor es el responsable de la descompresión. Entre los esquemas estandarizados de compresión tenemos: RFC 3545, utilizado en aplicaciones de extremo-extremo con alto retardo, pérdida y re-envío de paquetes, el RFC 2508 utilizado en enlaces seriales de baja velocidad y el RFC 3095 ROHC (*Robust Header Compression*) utilizado principalmente en enlaces inalámbricos, este esquema además comprime cabeceras UDP/IP y ESP/IP.

4.2.2 RSVP

El protocolo de reservación de recursos o RSVP (*Resource Reservation Protocol*) es utilizado por las aplicaciones en una red IP para reservar los recursos necesarios para obtener QoS. Funciona a nivel de enrutadores y host en la capa de transporte, y aunque funcione en esta capa, es más bien un protocolo de control. En una sesión RSVP el flujo es unidireccional para el flujo de datos, es transparente para los enrutadores que no lo soportan y puede operar en IPv4 o IPv6 ya sea unicast o multicast.

En aplicaciones como VOIP es importante mantener un buen nivel de ancho de banda y reducción de retardo durante una conversación, esto es posible conseguirlo con RSVP, ya que este crea un camino dedicado entre los usuarios que se comunican. Si una aplicación hace una solicitud de calidad de servicio, RSVP se encarga de solicitar a los enrutadores en el trayecto mantener un nivel de calidad de servicio establecido para la aplicación solicitante, por lo que los hosts solicitan y los enrutadores entregan QoS, para que RSVP pueda crear un camino óptimo para los datos hace uso de las tablas de enrutado, no las modifica únicamente busca el mejor camino que pueda entregar los recursos solicitados. Al iniciarse una sesión esta se define por tres parámetros: Dirección de destino (DestAddress), el ID del protocolo (ProtocolID) y el puerto destino (DstPort). El camino por el cual circularan los datos es marcado con un identificador, al enviarse los datos estos son recibidos por los encaminadores conjuntamente con mensajes RSVP que especifican los parámetros reservados a lo largo del camino hasta el destino, para el inicio de sesión se hace uso de los mensajes Path, enviado por el remitente o transmisor, este mensaje contiene las características de los datos que serán enviados. El mensaje Resv (*Reservation Request*), enviado por los destinatarios o receptores, y contiene los recursos requeridos que se deben reservar, se realiza encaminador por encaminador, desde el destino hasta el origen.

La figura 40 muestra el envío de estos mensajes a través de una nube de enrutadores, el mensaje Resv es una respuesta al mensaje Path por lo que viaja a través de los mismos enrutadores por los que ha pasado el mensaje Path, pero en sentido contrario. En un inicio de sesión quien solicita un nivel de calidad de servicio es el extremo receptor y no el transmisor, esto es de gran utilidad en aplicaciones IP multicasting.

Una vez finalizado la comunicación se debe iniciar la desconexión entre los usuarios, podría hacerse parando el envío de mensajes RSVP y esperar que los recursos reservados en los enrutadores expire, pero esto sería una manera informal, para realizarlo formalmente se debe enviar el mensaje respectivo para iniciar la desconexión. Este mensaje puede ser enviado por cualquiera de los usuarios que participa en la comunicación o por algún enrutador dentro del camino creado. Si el mensaje es enviado por el remitente, entonces se envía un PathTear (*Path Teardown*), pero si el mensaje es enviado por el destinatario, entonces se envía un ResvTear (*Reservation Teardown*).

Figura 40. Mensajes de reservación de recursos



RVSP es un protocolo estandarizado de la IETF que se encuentra detallado en la recomendación RFC2205. Existen otras extensiones del protocolo como el RFC2207, el cual especifica el uso de RSVP en un flujo de datos IPsec, soporta ambos modos: AH y ESP, aunque de manera limitada.

El RFC3209 el cual es una extensión RVSP-TE (*RSVP-Traffic Engineering*) para túneles LSP, estos túneles serán tratados en el tema de MPLS mas adelante. El RFC4230 especifica las políticas de seguridad para el protocolo, en esta recomendación se definen al igual que en el RFC2205 los denominados objetos, un objeto principal dentro de la seguridad RVSP es el INTEGRITY, el cual provee integridad y protección de repetición durante el intercambio de señalización RSVP entre dos enrutadores en la ruta o entre un enrutador y un host, además se incluye otros objeto denominado POLICY_DATA. Este objeto forma parte de las políticas de control las cuales se encargan de ver si se cuenta con los requerimientos solicitados y si quien solicita esta autorizado a hacerlo.

4.2.3 Int-Serv

El modelo de servicios integrados o Int-Serv (*Integrated Services*), es un sistema de reservación de recursos que da un tratamiento individual al flujo de datos dentro de una red. Es decir que cada una de las aplicaciones que se ejecuten puede reservar sus recursos sin tomar en cuenta a las demás. El sistema hace uso de RSVP para la reservación de recursos, puede funcionar en sistema unicast o multicast. Además el modelo tiene como objetivo que el tráfico en tiempo real pueda ser garantizado y previsible. La función realizada por los enrutadores para crear distintos niveles de calidad de servicio para las aplicaciones se le conoce como control de tráfico y se basa en tres componentes, los cuales son:

- Planificador de paquetes: Este es el encargado del envío del flujo de datos, hace uso de un conjunto de colas o utiliza el cronometraje.
- Clasificador: Este se encarga de clasificar los paquetes entrantes, para que el planificador de paquetes pueda tratarlos de la misma manera.

- Control de admisión: Este se encarga de determinar si un nuevo flujo de datos puede recibir los recursos solicitados, ya que si no ya no existen suficientes recursos se deben negar las peticiones para no dejar de dar un servicio garantizado a las demás aplicaciones que ya han reservado recursos.

El uso de Int-Serv se limita a redes de pequeña escala debido a su falta de escalabilidad, esto debido a que cada enrutador que participe en la comunicación debe reservar recursos por cada una de las aplicaciones que lo solicitan, lo que puede llegar a ser muy elevado y difícil de manejar en redes de mayor escala como la Internet. El modelo se encuentra definido en el RFC1633.

4.2.4 Diff-Serv

El modelo de servicios diferenciados o Diff-serv (*Differentiated Service*) tiene una manera distinta de compartir los recursos de una red, a diferencia de Int-serv este se basa en dar el mismo tratamiento a los diferentes flujos que tengan la misma clase de servicio. Para llevar a cabo esta tarea Diff-Serv hace uso del campo TOS de la cabecera IPv4 o el campo Traffic Class en IPv6, estos campos al ser usados por Diff-Serv se le denomina campo DS. Diff-Serv hace uso de 6 de los 8 bits del campo DS y se le denomina DSCP (*Differentiated Service CodePoint*), que es utilizado para seleccionar a un PHB (*Per Hop Behavior*), el cual se encarga de que se le de el tratamiento específico a cada paquete a través de la red. El PHB define distintos niveles de prioridad, tales como: Prioridad de servicio y de descarte. La prioridad de servicio tiene a su cargo determinar que paquetes deben de ser atendidos antes que cualquier otro, mientras que la prioridad de descarte especifica que paquetes deben de ser descartados antes que cualquier otro, el descarte de paquetes suele suceder en los periodos pico del tráfico en las redes. Además se manejan dos tipos de PHB los cuales son:

- EF (Expedited Forwarding): También se conoce servicio *Premium*, ya que entrega bajos niveles de retardo, jitter y pérdida de paquetes, ideal para aplicaciones de tiempo real.
- AF (Assured Forwarding): Aquí se definen cuatro niveles de servicio y cada nivel tiene tres niveles de prioridad de descarto: bajo, medio y alto.

En el modelo se manejan nodos de frontera y nodos internos, los nodos de frontera se encarga de seleccionar y marcar los flujos entrantes, mientras que los nodos internos se encargan de entregar las prioridades de acuerdo al valor establecido en el campo DSCP. Diff-serv provee mayor escalabilidad en comparación con Int-sev, esto debido a que no se almacena ninguna información de sesión, toda la información que se necesita se encuentra en el campo DSCP, pero no entrega recursos extremo-extremo sino salto por salto (*hop-by-hop*).

Para utilizar Diff-serv es necesario el establecimiento previo de un acuerdo SLA (*Service Layer Agreement*) sobre el nivel de servicio entre el proveedor del servicio, el cual puede ser un ISP (*Internet Service Provider*), y el cliente. El modelo se encuentra definido en los RCF 2475, 2474, 2597 y 3246.

4.2.5 MPLS

El protocolo MPLS (*Multiprotocol Label Switching*), es un sistema de conmutación de paquetes IP basado en la información incorporada dentro de una etiqueta, este sistema permite a las redes IP poder funcionar con cierta orientación a conexión.

Las etiquetas MPLS son usadas para representar a las denominadas FEC (*Forwarding Equivalente Class*), en una red todos los paquetes que contengan la misma FEC recibirán el mismo tratamiento, las etiquetas son asignadas a los paquetes al ingresar a la red, y al ser enviados hacia el próximo salto (enrutador) también se envía la etiqueta asignada, la asignación de una etiqueta a un paquete suele referirse como etiquetado de paquetes, y se realiza antes del envío de los datos. La información contenida dentro de las etiquetas indica el siguiente salto, y por cada salto se asigna una nueva etiqueta. Las etiquetas además pueden contener un nivel de prioridad o clase de servicio, en MPLS es permitido, pero no obligatorio, el uso de prioridad. Por lo que una etiqueta puede representar a una FEC y un nivel de prioridad o clase de servicio.

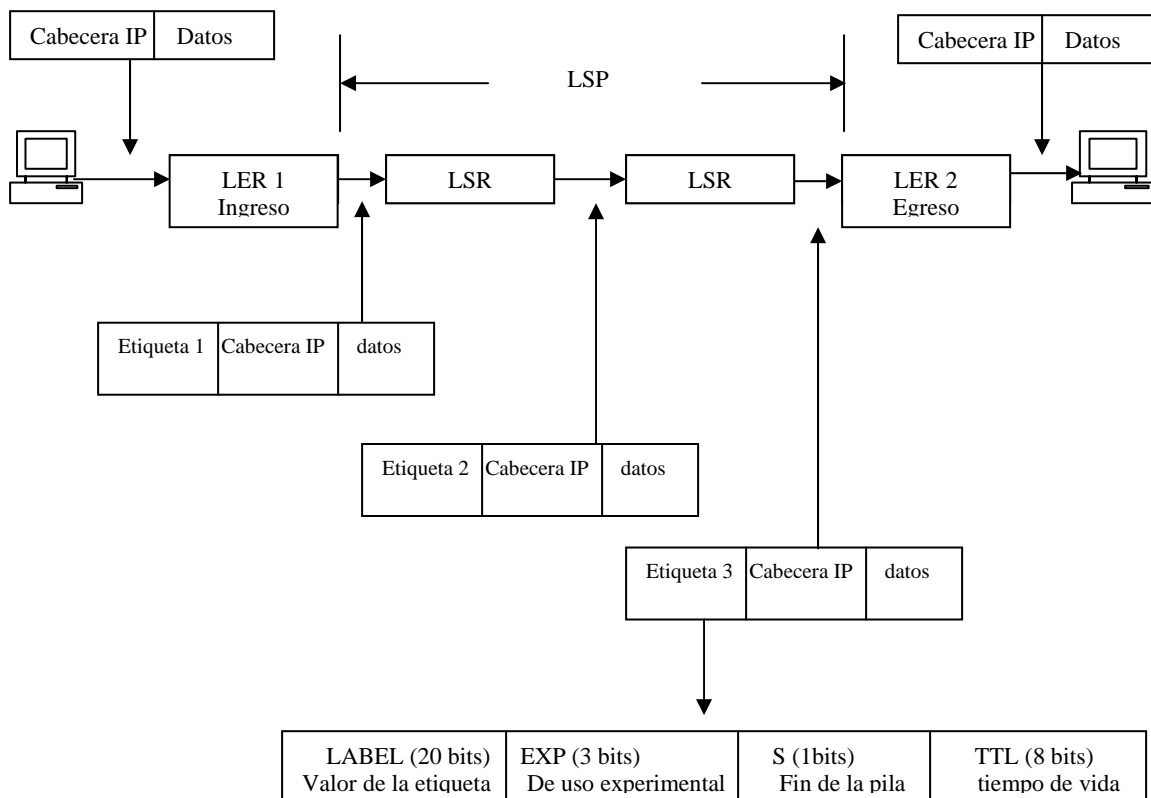
A los enrutadores que soportan MPLS se les conoce como LSR (*Label Switching Router*), estos tiene a su cargo el encaminamiento de los paquetes en función de sus etiquetas y las tablas contenidas dentro de ellos, además se tiene los LER (*Label Edge Router*), los cuales se encargan de asignar y suprimir etiquetas durante el ingreso y egreso del trafico en la red, sirven de interfaz con otras redes. Al camino seguido por una etiqueta a través de la red y establecido por las etiquetas asignadas se le denomina LSP (*Label Switching Path*). Al protocolo encargado de asignar etiquetas es denominado LDP (*Label Distribution Protocol*), además de este protocolo puede usar algunos otros como: CR-LDP (*Constrained Routing LDP*), RVSP o BGP (*Border-Gateway Protocol*).

Un Tunel puede ser formado al hacer uso de los LSP y la conmutación de etiquetas, en lugar del encapsulado en la capa de red, para hacer viajar los paquetes por los tuneles. Una secuencia de enrutadores, R1 hasta Rn, en donde R1 es el extremo transmisor y Rn es el extremo receptor del túnel, es llamado túnel LSP. Los tuneles LSP permiten implementar una variedad de políticas con objetivo de optimizar las características de la red.

Una de las principales funciones de MPLS es la implementación de la ingeniería de tráfico, que es la habilidad de definir distintos caminos para repartir el tráfico de la red, para equilibrar y aprovechar todos los recursos disponibles. Además está diseñado para proveer clase de servicio (*CoS*) y permite la creación de VPN. Esta arquitectura se encuentra definida en el RFC3031, 3032 y 2702 que trata el tema de la ingeniería de tráfico sobre MPLS.

MPLS⁵⁸ puede ser implementado sobre cualquier protocolo de la capa de red y la capa de enlace, las etiquetas se colocan frente a la cabecera IP, lo que equivale a colocar una nueva capa entre las de red y de enlace. La figura 41 muestra la arquitectura MPLS y el formato de las etiquetas.

Figura 41. Arquitectura MPLS



⁵⁸ MPLS en conjunto con redes IP forman parte esencial de las llamadas Redes de nueva generación (NGN)

Una de las principales dificultades de la telefonía IP es lograr una calidad de servicio similar a la que están acostumbrados los usuarios de las redes telefónicas. Esta dificultad surge, por un lado, de las consideraciones técnicas específicas de la transferencia de datos en el modo de las redes IP y, por otro lado, de las consideraciones relacionadas con la organización y el modo de prestación del servicio por las redes de datos en general y por la red IP en particular⁵⁹.

⁵⁹ Grupo de expertos sobre telefonía IP del UIT-D. **Informe Esencial sobre Telefonía IP**. (Suiza: Unión Internacional de Telecomunicaciones, 2003). p.34

5. HARDPHONE, SOFTPHONE Y PBX IP

5.1 Hardphone

El hardphone o teléfono IP es el dispositivo encargado al igual que el teléfono usado en la PSTN de transmitir y recibir la voz en una conversación telefónica. Aunque para el usuario pareciera ser un teléfono normal, ya que las funciones que realiza son transparentes para este, tal vez con algunas diferencias en su aspecto, el teléfono IP es un dispositivo más sofisticado que se conecta a una red de datos a través de un conector RJ-45 en lugar de la conexión telefónica tradicional que utiliza conectores RJ-11, al igual que una computadora el teléfono dispone de una NIC y una dirección MAC para su interconexiones a redes Ethernet, algunos teléfonos incluyen más de un conector RJ-45 para conectar más dispositivos a la red, incluso algunos disponen de un conector RJ-11 para conectarlo a la red tradicional. En el interior del teléfono IP residen los codec soportados por el dispositivo, estos codec puede ser para audio y video, ya que algunos teléfono incluyen una cámara de video para video-conferencias, una diferencia con respecto al teléfono tradicional que no soporta esta característica. Los codec suelen ser implementados en un DSP (*Digital Signal Processor*), los cuales son microprocesadores para aplicaciones de tiempo real.

Los teléfonos IP deben de soportar los protocolos H.323 y SIP, no necesariamente debe de soportar a ambos pero como mínimo debe de incluir uno. La asignación de dirección IP al teléfono se puede hacer de manera estática o dinámica, para esta última el teléfono debe de tener soporte para un servidor DHCP, también se puede incluir acceso a servidores DNS.

Además un teléfono puede incluir un VAD, canceladores de eco y generadores de ruido de confort, algunos terminales más avanzados puede contener soporte para NAT. Es recomendable mantener actualizado el firmware del teléfono para poder sumar nuevas funciones o para corregir errores de las versiones anteriores, esto es similar a las actualizaciones de los sistemas operativos en computadoras. Algunas otras características sumadas a los teléfonos son: Llamada en espera, transferencia de llamada, correo de voz (voicemail), música de espera, bloqueo de llamada, identificador de llamada.

La configuración de los teléfonos puede hacerse vía Telnet o por HTTP, ya sea de manera remota o local, aunque se recomienda realizarla de manera local. Una parte fundamental de la configuración es en cuanto a seguridad, ya que se debe renovar la clave y usuario que viene por defecto en el dispositivo, además se pueden cerrar puertos que no se utilicen para evitar que algún escaneo encuentre algunos abiertos y sin uso, por los cuales se puede iniciar un ataque al teléfono o a la red. En la configuración también se puede especificar que tipos de funciones se permitirán realizar al teléfono.

La figura 42 muestra el teléfonos IP SI-150 de ADtech que es compatible únicamente con SIP e incluye soporte de tarjetas inteligentes (SmartCard), provee varios codecs como: G.711 (ley u o A), G.929 y G.723.1 el cual incluye la función de un VAD, además cuenta con cancelar de eco, e incluye soporte para DHCP y DNS. El SI-160 incluye soporte para SIP y H.323, e incluye cifrado de voz por 3DES y autenticación de usuarios por RSA.

Figura 42. Telefono IP SI-150



Fuente: <http://www.adtech.be/text/si150.php>

La figura 43 muestra el teléfono IP Unified 7975G de la empresa Cisco, tiene soporte para los codec G.711 (ley A o U), G.729 e iLBC. La asignación de dirección IP se puede realizar de manera estática o a través de DHCP. Tiene soporte para los protocolos SIP y SCCP (*Skinny Client Control Protocol*), el cual es un protocolo propietario de Cisco, y sirve para comunicar sus teléfonos IP con sus CallManager.

Figura 43. Teléfono IP 7975G



Fuente: http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps8538/product_data_sheet0900aecd8069bdb7.html

Un elemento hardware que puede formar parte en una arquitectura de telefonía IP es el ATA (*Analog Telephone Adaptor*), el cual permite convertir un teléfono tradicional en un teléfono IP. Este dispositivo dispone de uno o más conectores RJ-11 para conectar los teléfonos tradicionales y uno o más conectores RJ-45 para conexión a la red de datos, por lo que este es el encargado de toda la conversión de señalización y voz a paquetes que puedan ser enviados a través de la red y viceversa.

5.2 Softphone

Los softphone son programas de computadora que permiten emular las funciones y características de un teléfono IP. Se ejecutan sobre la mayoría de los sistemas operativos actuales, en su mayoría Windows, pero también se les puede encontrar para Linux y MAC OS. Al utilizar un softphone se hace uso de la tarjeta de sonido de la máquina sobre el cual se corre el programa, por lo cual, se debe de poseer bocinas y micrófono para poder conversar, si el softphone incluye soporte para video se debe contar con una cámara web si se desea utilizar esta opción. El uso de un softphone o hardphone, permite realizar llamadas que involucren a ambas tecnologías, es decir que se pueden realizar llamadas de la siguiente forma: Softphone-Softphone, Softphone-Hardphone o viceversa y hardphone-hardphone.

A continuación se listan algunos de los softphone que se pueden encontrar ya sea de forma gratuita o de paga en Internet. En su mayoría la configuración no es complicada, gracias a sus interfaces graficas intuitivas. También se disponen de guías de instalación, configuración y funcionamiento de los softphone provistos por los mismos fabricantes o por los mismos usuarios del programa.

- X-Lite: Soporta el protocolo SIP, permite video-conferencias, provee calidad de servicio para audio y video. Se ejecuta sobre Windows 2000, XP y MAC OS X 10.4. Se puede utilizar en una máquina con procesador de 700 MHz, memoria RAM de 256 MB 30 MB de espacio de disco duro, y tarjeta de sonido de 16 bit full-duplex. Tiene soporte para redes Wireless y contiene un sofisticado mecanismo de detección de NAT.
- Kphone: Soporta el protocolo SIP, se ejecuta sobre Linux y tiene soporte para G.711 e iLBC, permite video-conferencias. Se distribuye bajo licencia GNU GPL (*General Public License*).
- Linphone: Soporta el protocolo SIP, se ejecuta sobre Linux y Unix y tiene soporte para: G.711 e iLBC, H.263 y Mpeg4 para video, ENUM e IPV6. Además incluye un sistema de anulación de eco y utiliza el protocolo STUN. Se distribuye bajo licencia GNU GPL.
- Skype: Es un softphone de protocolo propietario, existen versiones gratuitas y de paga, se puede ejecutar sobre Windows, Linux, MAC OS X.
- Adore Softphone: Soporta protocolo SIP, codec G.729, Firewall, NAT y DNS. Se ejecuta sobre Windows 2000, NT 2003 y XP. No tiene soporte para Linux ni MAC OS X. En su página oficial se dispone de un demo, la versión completa es de paga.
- Netmeeting: Cliente VOIP para video conferencias de Microsoft, soporta el protocolo H.323. Puede operar dentro de una red privada y detrás de firewall.

Como se puede observar la mayoría de softphone tiene soporte únicamente para SIP, esto puede deberse a que este protocolo es más sencillo en aplicación y arquitectura, y a que su sintaxis y semántica se basa en el protocolo HTTP usado en la web por lo que hereda muchas de sus características. Aunque esto se paga con vulnerabilidades en la seguridad ya que en su mayoría la señalización se transmite en texto plano, lo que conlleva el tener que desplegar una arquitectura de cifrado y otros métodos que ayuden a mejorar la seguridad en este protocolo. La figura 44 muestra la interfaz gráfica del softphone Adore.

Figura 44. **Softphone.**



Fuente: <http://www.adoresoftphone.com/softphone.html>

5.3 PBX IP

5.3.1 IAX2

El Inter-Asterisk Exchange (IAX) es el protocolo nativo de Asterisk, actualmente se habla de IAX2 la versión más reciente. El protocolo provee soporte para transmitir y controlar flujo multimedia a través de redes IP, pero su principal objetivo es el control de llamadas VOIP, además de minimizar el uso de ancho de banda para control y flujo multimedia, también proveer soporte para NAT y Firewall.

IAX es un protocolo punto a punto (*Peer to Peer*) binario, que optimiza el ancho de banda y da prioridad a llamadas individuales, su funcionamiento se basa en la multiplexación de la señalización y el flujo multimedia sobre un mismo puerto UDP, el cual corresponden al 4569, esto permite evitar los problemas asociados a NAT en protocolos como SIP y H.323, IAX además incluye dentro de él mismo a los protocolos de señalización y de transporte, por lo que el uso de RTP queda relegado. Aunque el uso de un único puerto provee algunas ventajas, también hace susceptible al sistema a ataques de denegación de servicio.

Los datos de señalización, de control o el flujo multimedia son transportados dentro de cuadros (Frames), los frames definidos en IAX son los siguientes:

- Full-Frame: Estos son usados para transportar señalización y control de inicio, establecimiento y finalización de llamadas, algunas veces se le utiliza para llevar datos multimedia, aunque no de manera óptima. Este frame al ser enviados requieren de una respuesta de aceptación, para lo cual se suele usar el mensaje ACK como respuesta al envío de un Full-Frame. La estructura del frame contiene una cabecera de 12 octetos y entre los campos que la componen tenemos:

- Bit F: Usado para indicar si un frame es o no full. Si está a uno es full de lo contrario no lo es.
- Source call Number: Valor de 15 bits usado para identificar el número de llamada de origen, no puede ser utilizado en otra llamada mientras este activa la sesión actual.
- Bit R: Usado para indicar si el frame es retransmitido o no. Si se encuentra a cero indica que el frame es transmitido por primera vez, a uno especifica que se retransmite.
- Destination Call Number: Valor de 15 bits que identifica el número de llamada destino.
- Time Stamp: Campo de 32 bits usado para representar una cantidad en milisegundos desde el inicio de la transmisión de una llamada.
- Oseqno: Campo de 8 bits que representa un número de secuencia del flujo saliente, inicialmente se encuentra en cero y se incrementa conforme se envían Full-Frame, si se desborda se inicializa.
- Iseqno: Campo de 8 bits que representa un número de secuencia del flujo entrante, inicialmente se encuentra en cero y se incrementa por cada Full-Frame recibido, si se desborda se inicializa.
- Frame Type: Identifica el tipo de mensaje transportado por el Frame. Estos tipos pueden ser: DTMF, voz, video, control, nulo, IAX control, texto, imágenes, Html o ruido de confort.
- Bit C: Determina como se interpretan los 7 bits pertenecientes al campo subclass. Si el bit es uno se interpreta como una potencia de dos sino como un entero sin signo.
- Subclass: Puede contener dígitos DTM o especificar el formato de compresión para voz, video e imágenes.

- Mini-Frame: Son usados para transportar flujo multimedia, su cabecera es de 4 octetos, y está compuesta por los campos siguientes: Bit F, Source Call Number y Timestamp, el cual contiene solamente la mitad de los bits utilizados en un Full-Frame.
- Meta-Frame: Son usados para transportar los llamados Meta video Frame o Meta Trunk Frame. Los primeros permiten la transmisión de flujo de video con una cabecera optimizada para tal propósito, funcionan de manera similar a la Mini-Frames. Además de los campos F, Destination Call Number y TimeStamp, se tienen otros dos campos, uno denominado V y el otro Meta Indicator. El campo V al estar a uno indica que se trata de un video Frame mientras que el campo Meta Indicator que es un Meta Frame, los quince bits que lo conforman se encuentran a cero. El segundo tipo permite la transmisión de múltiples flujos multimedia entre dos puntos, para lo cual hace uso de una sola cabecera, lo cual permite un ahorro en el ancho de banda. A este tipo de transmisión también se le conoce como Trunking. Aquí se incluyen los campos Meta Command, campo de 7 bits y Command Data, campo de 8 bits, usados para indicar si el Frame es Trunk o no y definir las opciones que se le aplican a una llamada tipo Trunk respectivamente.

Los mensajes en IAX se pueden transportar de dos distintas formas, las cuales son: Confiable y no garantizado. Los confiables son los que se transportan en Full-Frame. Los no garantizados son transportados por Mini-Frame y Meta-Frame, por lo que la voz y el video son enviados sin garantías para poder cumplir con los requisitos de tiempo real impuesta por estas aplicaciones. Durante una transmisión ocurren pérdidas de paquetes y la retransmisión no es permitida en aplicaciones de tiempo real como VOIP ya que rompería con la secuencia que debe mantenerse en una conversación.

Dentro de los Frame-Full se puede agregar lo que se conoce como IE (*Information Element*) que sirven para identificar datos de usuario o de una llamada en particular. Los IE se añaden a la cabecera dentro del campo de datos (*Data*), en una trama pueden ir uno, varios o ningún IE. A continuación se lista y describe diez de los cincuenta y un IE definidos que pueden ser agregados en un Frame-Full:

- Called Number: Número o extensión que se llama.
- Calling Number: Número que llama
- Calling Name: Nombre del que llama
- Capability: Indica la capacidad de codec en un peer (usuario).
- User Name: Nombre de usuario para autenticación.
- Password: Contraseña para autenticación.
- Encryption: Método de cifrado soportado por un Peer IAX.
- RR Jitter: Indica la cantidad de jitter recibido en una llamada.
- RR Loss: Indica el número de Frames perdidos en una llamada.
- RR Delay: Indica el máximo retardo en milisegundos que puede sufrir un Frame en una llamada.

Al igual que en SIP en IAX la identificación de usuarios se realiza a través de URI's, un IAX URI contiene la suficiente información para iniciar una llamada y puede representar un teléfono, una dirección de correo de voz, una dirección hacia la PSTN o un gateway. Un IAX URI se construye en base al siguiente formato:

`iax:[username@]host[:port][/number[?context]]`

En donde:

Iax: Representa el nombre del protocolo usado.

Username: Cadena de caracteres usado para propósitos de identificación.

Host: Identifica al dominio del recurso. Puede ser un nombre de dominio, preferiblemente full Qualified o una dirección IP ya sea versión 4 o 6. Si es versión 6 debe encerrarse entre llaves [].

Port: Identifica al número de puerto UDP.

Number: Nombre o número que identifica al recurso en un host.

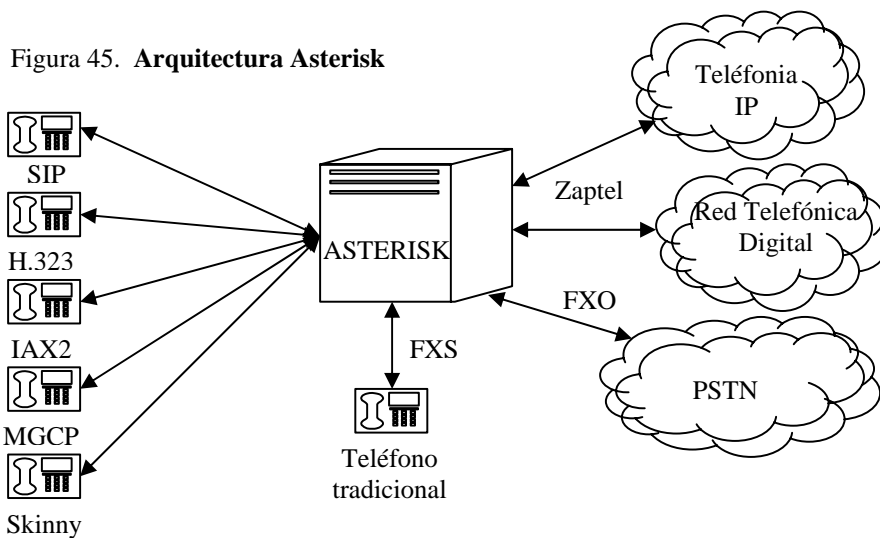
Context: Nombre de la partición de host en la cual se identifica o procesa el servicio.

Con respecto a la seguridad IAX permite el cifrado de llamadas a través de claves simétricas y AES. Si el terminal llamado soporta cifrado, entonces en la cabecera de un Frame-Full se agrega el IE Encryption, si no lo soporta no se agrega el IE y la llamada puede terminar, si se continúa no habrá cifrado de datos. La autenticación se realiza a través de RSA y Hash MD5.

5.3.2 Asterisk

Asterisk es una aplicación cliente-servidor, en la cual los clientes conectados al servidor pueden transmitir voz y vídeo en tiempo real, para lo cual hacen uso de cualquiera de los protocolos y códec's soportados por la PBX. Es un software de código abierto desarrollado por Digium, que permite instalar, configurar y ejecutar una PBX IP, compatible con los protocolos: H.323, SIP, MGCP, Skinny e IAX. Este último desarrollado conjuntamente con Asterisk y que ha tomando en cuenta el uso de firewall y NAT en las actuales redes, lo que permite corregir en su mayoría los problemas que aquejan a los otros protocolos, además soporta codec's como G.711 (A y U), G.729, ILBC y G.723.

Asterisk puede ser implementado en la mayoría de las distribuciones Linux, aunque puede ejecutarse sobre MAC OS y Windows, pero no con los mismos resultados obtenidos en Linux. Con el uso de tarjetas FXO (Foreign eXchange Office) se puede interconectar a la PSTN, y con FXS (Foreign eXchange Station) se pueden interconectar los teléfonos tradicionales a la PBX, además se puede conectar a líneas telefónicas digitales como ISDN. La figura 45 muestra las distintas conexiones desde y hacia un servidor Asterisk.



A continuación se listan algunas de las funciones de la PBX.

- Transferencia de llamada.
- Llamada en espera.
- Caller ID.
- Música de espera.
- Grabación de llamadas
- Salas de conferencias.
- Colas de llamada.

- Prioridad de cola.
- Buzón de correo de voz
- Registro de llamadas en base de datos.
- Lista negra.
- Pickup de llamada
- Llamadas de emergencia
- Autenticación de accesos
- ENUM
- Recepción y transmisión de Fax

Estas características en conjunto con las posibles conexiones que se pueden realizar, y el hecho de ser software de código abierto hacen de Asterisk una buena elección a la hora de implementar una PBX, ya sea para telefonía IP o tradicional. La interacción entre la telefonía tradicional e IP en Asterisk permite construir arquitecturas de telefonía avanzadas y soluciones CTI (*Computer Telephony Integration*), y facilita la transición de la tecnología tradicional telefónica a la nueva tecnología.

La instalación de Asterisk en cualquier distribución Linux, requiere de descargar ciertos paquetes que contienen todo lo necesario para su instalación, estos paquetes son: asterisk, Zaptel y Libpri, estos paquetes pueden ser descargados desde la página oficial de forma gratuita, ya que Asterisk se distribuye bajo licencia GPL. Aunque los últimos dos no son necesarios si solamente se requiere una red puramente VOIP, ya que Zaptel es utilizado si se requiere el uso de tarjetas Zaptel analógicas o digitales, y libpri si se utilizan interfaces ISDN PRI. Aunque estos son los paquetes básicos se requiere de otros para su correcta instalación en el sistema. Entre algunos paquetes importantes está GCC, necesario para la compilación de los códigos fuentes. Bison necesario para funcionalidades CLI (*Command Line Interface*) y OpenSSL, que es la librería criptográfica. Estos paquetes pueden estar incluidos en la distribución o se les puede descargar desde la Internet.

Existe otra opción que permite instalar Asterisk en una forma más amigables, esta es Trixbox, el cual contiene todo lo necesario para instalar la PBX, utiliza el sistema operativos CentOs, y no se requiere la manipulación de los archivos de configuración, aunque puede hacerse si se requiere. Toda la configuración se realiza a través de una página web proporcionada por el sistema.

El funcionamiento de Asterisk se basa en la configuración de archivos con extensión conf (*.conf), dentro de estos archivos tenemos: Archivo de configuración maestro, archivo de configuración de módulos, archivo de configuración Dialplan y archivos de configuración de canal, para poder incluir clientes, eliminar o cambiar las propiedades de estos dentro de la PBX se hace uso de los siguientes archivos de configuración de canal: Sip.conf, H.323.conf, Iax.conf y MGCP.conf. Cada uno de estos archivos es usado en dependencia al tipo de cliente que se vaya a crear. Para poder trabajar estos archivos, se pueden editar o puede hacerse desde el CLI del programa.

La estructura de los archivos de canal esta definida en: Sección General, clientes y servidores. En la sección general se definen las propiedades globales que afectaran a todos los usuarios creados. En la sección cliente y servidores, se agregan las propiedades de cada uno de los usuarios, existe una sección cliente o servidor por cada usuario creado. A continuación se muestra la sintaxis y estructura para el sip.conf:

[General]

port = 5060	; Define el Puerto UDP por el cual debe escuchar.
bindaddr = xx.xx.xx.xx	; Dirección IP de escucha. Todas las x = 0, escucha en ; todas las direcciones.
context = default	;Indica el contexto asociado en el dialplan para un usuario.
srvlookup = yes	; Habilita uso del registro DNS SRV

videosupport=yes ; Permite soporte para video
disallow=all ; Deshabilita todos los codecs
allow=ulaw ; Permite codec de ley u

[Usac]

type = friend ; Define el tipo de usuario
allow = g729 ; Permite el uso de codec G.729
username = usac ; Usado para autenticación
callerid = ingeniería <10> ; Identificación del llamante.
secret = electrónica ; Clave de acceso.
nat = yes ; Usuario esta detrás de NAT.
host = dynamic ; Indica el uso de direcciones dinámicas.

La propiedad type en la sección cliente tiene tres tipos de valores los cuales son:

user: envía llamadas a Asterisk.

peer: recibe llamadas de Asterisk.

friend: recibe y envía llamadas.

Las propiedades expuestas en la sección general y Usac son únicamente algunas de las que pueden asociarse a estas secciones. Durante la instalación de Asterisk, se crean estos archivos de configuración en donde se detalla de manera más extensa las posibles configuraciones.

En el ejemplo anterior se tiene únicamente un usuario llamado Usac y sus respectivas características. Todo lo que se encuentra delante de un punto y coma es tomado como un comentario por Asterisk. Así se podrían deshabilitar algunas propiedades si se desea, únicamente poniéndolo como comentario.

La creación de usuarios IAX, H.323 y MGCP es similar a la utilizada para los usuarios SIP, con algunas diferencias entre sus propiedades, dentro de éstas diferencias se tiene el número de puerto de escucha.

La configuración del archivo `extensions.conf` (*Dial Plan*), también es de importancia dentro del funcionamiento de la PBX, en este archivo están los pasos de cómo Asterisk debe manejar las llamadas entrantes y salientes, es decir, que es el encargado de la lógica del sistema. La estructura de este archivo se basa en contextos y extensiones, donde un contexto es un conjunto de extensiones, y una extensión es una serie de pasos que Asterisk debe seguir en una llamada, los nombres de contexto se escriben dentro de llaves [].

Dentro de la estructura del archivo se tiene dos contextos importantes los cuales son: contexto general y global. En el contexto general se definen parámetros generales que afectaran a los demás contextos, en global se definen las variables que serán utilizadas por los demás contextos, la variable es llamada al hacer uso de `${nombre_variable}` en cualquier parte del archivo. En el contexto general se encuentran tres parámetros los cuales son:

- `static`: Establece si es permitido guardar cambios en el dial plan desde el CLI.
- `writeprotection`: En conjunto con el parámetro anterior permiten cambios en el archivo. Si `static = yes` y `writeprotection = no`, se podrá guardar cualquier cambio desde el CLI.
- `autofallthrough`: Se utiliza para indicar a Asterisk que termine una llamada si la extensión se ha quedado sin acciones que realizar, para lo cual se coloca `yes`. Si se coloca `no`, Asterisk se quedara en espera de que otra extensión sea marcada. Se recomienda colocarla en `yes`.

A continuación se muestra el formato usado para generar una extensión:

exten => extensión, prioridad, acción

Donde:

Extensión: Define el nombre o número de la extensión.

Prioridad: Cada extensión puede tener múltiples pasos, al paso se le llama prioridad. El valor de paso inicial es uno y se ejecutan de manera secuencial.

Acción: Instrucción a ejecutar al ser llamada la extensión.

Existen algunos nombres reservados para las extensiones, estos se listan a continuación:

- s (Start extensión): Si no se define ninguna extensión esta se ejecuta.
- t (Timeout extension): Se ejecuta si un usuario requiere una entrada que no es atendida con prontitud.
- i (Invalid extension): Se ejecuta al ingresarse una extensión no válida.
- fax (Fax call): Si se detecta un fax, la llamada es encaminada hacia esta extensión.

A continuación se listan algunas de las acciones utilizadas en las extensiones:

- Answer: Usado para aceptar una llamada.
- Playback (filename): Este comando ejecuta el archivo (filename) que debe de estar en formato .wav o .gsm. Para su utilización se debe usar antes Answer.
- Background (filename): Usado comúnmente para crear menús de voz, para aplicaciones en las cuales dirige a un usuario hacia la extensión apropiada.
- WaitExten(): Usado para esperar a que un usuario ingrese dígitos DTMF, comúnmente se le coloca un argumento que define el tiempo de espera en segundos. Al ser usado en conjunto con Background se le coloca después de este.

- Goto (context, extension, priority): Utilizado para saltar hacia el contexto, extensión y prioridad seleccionada.
- Voicemail (extension): Transfiere la llamada actual al correo de voz.
- VoicemailMain: Permite a los usuarios escuchar sus mensajes, además de permite configurar el mensaje de bienvenida y algunas otras opciones.
- Hangup: Utilizado para finalizar una llamada
- Dial (): Usado para conectar a usuarios que utilizan diferentes métodos de comunicación. Comúnmente estos métodos pueden ser SIP, IAX y Zap (T1, E1 y líneas analógicas).

El comando Dial es una herramienta de gran importancia, ya que permite la interacción entre la PSTN, la ISDN y la telefonía IP, además permite la conexión hacia múltiples destinos (multi dial). Este comando trabaja en conjunto con cuatro parámetros, los cuales son:

- Technology: Comúnmente puede ser: IAX, SIP y ZAP (líneas analógicas, E1 y T1) y es el tipo de canal que se desea utilizar para la comunicación. Este suele ser acompañado por un identificador del nombre del canal con el cual se desea establecer la comunicación.
- Timeout: Tiempo de espera en segundos para establecer la comunicación.
- Option: Características que modifican la conducta del comando. Se tiene las siguientes opciones:
 - t: Permite que el usuario llamado pueda transferir una llamada al presionar la tecla #.
 - T: Igual que la anterior pero para el usuario que llama.
 - r: Indica el timbrado al usuario que realiza la llamada.
 - m: Permite música de espera al usuario que realiza la llamada.
 - h: Permite al usuario que realiza la llamada poderla terminar al presionar la tecla *.

- g: Permite seguir en el contexto si el destino termina la llamada.
- URL: Permite el envío de un URL, solamente si el destino lo soporta.

El formato general para este comando se muestra a continuación, únicamente la propiedad `technology/id` es obligatoria, las demás se colocan si se desea.

Dial (technology/id, timeout, option, URL)

A continuación se muestra un ejemplo básico de la configuración del `extensions.conf`, aunque su configuración puede ser sencilla, también puede llegar a ser muy compleja.

[general]

static = yes

writeprotection = no

autofallthrough = yes

[global]

[default]

exten => Usac, 1, Answer() ;Constestar llamada.

exten => Usac, 2, voicemail (Usac@default) ; Si no contesta pasar a correo de voz.

exten => Usac, 3, Hangup () ; Terminar llamada.

exten => 100, 1, Dial (sip/Usac) ;Se realiza una llamada usando un canal SIP hacia canal Usac.

exten => 100, 2, voicemail (Usac@default) ; Si no contesta pasar a correo de voz.

exten => 100, 3, Hangup () ; terminar llamada.

Para poder hacer uso de voicemail en el ejemplo anterior, antes se tuvo que haber declarado en la sección clientes de los archivos SIP, IAX o H.323.conf. Esto se realiza sumando la línea mailbox = ID@nombre de contexto o únicamente el ID. También debe de estar declarado dentro del archivo voicemail.conf. Para crear un mailbox dentro de este archivo se hace uso del siguiente formato:

mailbox => password, username, emailaddress, pageraddress, options

Donde:

- Mailbox: corresponde al nombre o número de la extensión asociado al extensions.conf y el archivo de canal utilizado (SIP, IAX o H.323).
- Password: Clave utilizada por el usuario para acceder al correo de voz
- Username: Nombre del dueño del correo
- Emailaddress: Dirección del correo en donde se envían los mensajes.
- Pageraddress: Dirección de correo de beeper o celular en donde se envían mensajes cortos de notificación.
- Options: Sirve para sobre escribir los parámetros definidos en el contexto [general] del archivo voicemail.conf o especificar una zona horaria para el usuario dentro del mismo. Se puede utilizar cualquiera de las nueve siguientes opciones: attach, serveremail, tz, saycid, review, operator, callback, dialout and exitcontext. Se puede utilizar más de una, para lo cual se hace uso del símbolo (|) para separarlas. A Continuación se describe cada una de las opciones anteriores:
 - attach: Indica a Asterisk si se debe o no de agregar el archivo de sonido que contiene el mensaje conjuntamente con las notificaciones de correo, por defecto se coloca no.
 - serveremail: Provee la dirección de correo de a quien se le deben de enviar las notificaciones.

- sycid: Se muestra primero la información del llamante y luego el mensaje si sycid = yes.
- review: Permite a los usuarios revisar y re escuchar sus mensajes antes de guardarlos, por defecto se coloca en no.
- operator: Permite a los llamantes marcar cero (0) antes, después de o mientras se graba un mensajes para alcanzar otra extensión.
- callback: Define el contexto para permitir que un cliente solicite se le llame de vuelta, si el destino no esta disponible.
- dialout: Hace referencia al destino o destinos que podrá alcanzar la extensión.
- Exitcontext: Contexto optativo en el que se le permite al usuario abandonar después de haber dejado un mensaje de voz, al marcar * o 0.

Estos parámetros pueden ser modificados como ya se menciona desde el formato de mailbox, en la sección general además de estas propiedades pueden aparece algunas otras como:

- format: Especifica el formato con el cual se almacenan los mensajes de voz estos pueden ser: wav49, gsm o wav.
- maxmsg: Establece el número máximo de mensajes que pueden ser almacenados.
- maxmessage: Establece la longitud máxima de un mensaje en segundos.
- minmessage: Establece la longitud mínima de un mensaje en segundos.
- maxlogin: Establece el número máximo de intentos de autenticación.

Anteriormente se describieron ocho de los nuevo parámetros que pueden ser reescritos en el contexto general, el parámetro tz no se incluye dentro de ellos ya que este modifica propiedades dentro del contexto [zonemessage].

En este contexto se definen las características de zona horarias necesaria para informar al usuario sobre la fecha y hora de la recepción de los mensajes de voz. Esta información suele tomarse del propio sistema operativo sobre el cual se ejecuta Asterisk. La configuración de una zona voicemail sigue el siguiente formato:

zonename = timezone | time_format

donde:

- zonename: Es un nombre arbitrario que identificara la zona.
- Timezone: Define el nombre del sistema de la zona de tiempo. Para sistemas Linux se pueden encontrar las zonas de tiempo en el directorio /usr/share/zoneinfo.
- Time_format: Define el formato de cómo se mostrara la fecha y hora. Se tiene las siguientes opciones:
 - filename: Nombre del archivo de audio a reproducir.
 - \${var}: Llamado de variable.
 - A o a: Nombre del día.
 - B, b o h: Nombre del mes.
 - d o e: Valor número del día del mes (primero, segundo, ...)
 - Y: Año
 - I o i: La hora, en formato de 12 horas.
 - H: La hora, en formato de 24 horas.
 - M: Minutos
 - P o p: A.M. o P.M.
 - Q: hoy, ayer o ABdY
 - R: Tiempo en 24 horas incluido minutos.

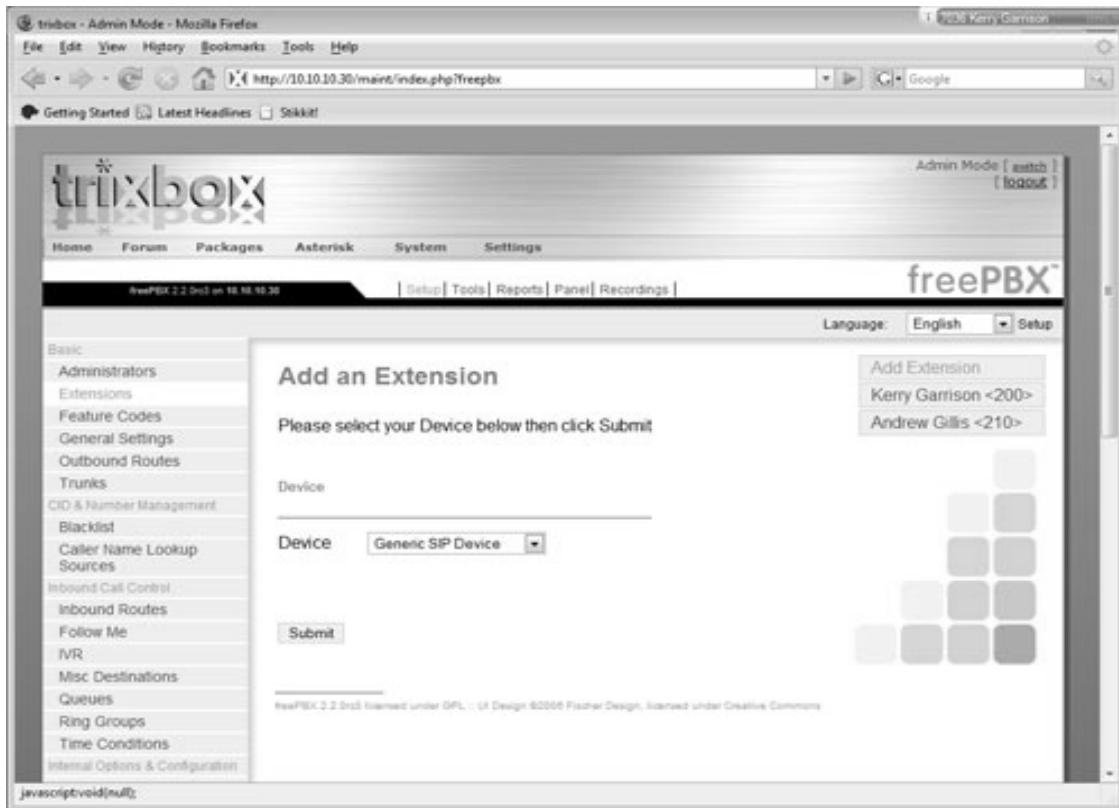
A continuación se muestra un ejemplo de una zona voicemail:

Mi_ubicación = America/Guatemala | ABY IMP

Párrafos atrás se indico que Asterisk puede interactuar con la PSTN o ISDN, para poder trabajar con estas tecnologías es necesario hacer uso de los archivos de configuración Zaptel.conf. y zapata.conf.

Los archivos de configuración aquí mencionados no son los únicos dentro de Asterisk, para la versión 1.4.19 se generan sesenta y dos archivos dentro del directorio /etc/asterisk, en sistemas Linux. Aunque a primera vista pareciera que la configuración es relativamente sencilla, conforme se adentra a las múltiples posibilidades que presenta la PBX, se ve que también hay un incremento en la complejidad de la configuración. A pesar de esto Asterisk es una herramienta poderosa dentro de la telefonía IP, actualmente existen interfaces gráficas que ayudan a minimizar la complejidad de la configuración, sistemas como Trixbox (Antes conocido como Asterisk@home) ayudan a realizar la configuración de Asterisk de una manera más amigable, a través de una interfaz web, en la que no se hace necesario trabajar directamente sobre los archivos de configuración. Pero si se desea entender a fondo el funcionamiento de Asterisk se hace necesario adentrarse en estos archivos. La figura 46 se muestra la interfaz web utilizada en Trixbox para crear una nueva extensión.

Figura 46. Trixbox



Fuente: <http://trixbox.org/wiki/screenshots>

CONCLUSIONES

1. La interacción entre la PSTN y la telefonía IP es algo que se mantendrá durante algunos años, ya que la primera es una red de comunicaciones con fuerte presencia en la actualidad, por lo que es de importancia tener conocimiento de ambas tecnologías para comprender las actuales implementaciones que incluyen usuarios de ambas partes.
2. Los niveles de calidad de servicio y seguridad en la telefonía IP son parámetros de importancia a la hora de considerarse a esta tecnología, los usuarios esperarían recibir los mismos niveles de calidad a los que están acostumbrados en su sistema actual. Para las empresas, gobiernos y personas particulares es imprescindible la seguridad en sus comunicaciones, nunca se sabe que podría hacer alguien no autorizado con nuestra información. Por lo que debe hacerse todo lo posible por mantener los sistemas a salvo de todo tipo de ataque, ya sea que provengan del exterior o interior de la propia red.
3. A la hora de seleccionar un teléfono IP, ya sea este *Hardware* o *Software* debe observarse las opciones que el fabricante proporciona al usuario para conocer los posibles servicios que se pueden utilizar de acuerdo a nuestras necesidades. En una empresa es imprescindible mantener bajos niveles de inversión; poder optar a herramientas gratuitas, confiables y potentes sería una gran ayuda, Asterisk es una buena elección a la hora de implementar una PBX. Gran parte del buen funcionamiento de esta herramienta se basa en una buena configuración, para lo cual se hace necesario estar familiarizado con esta herramienta.

RECOMENDACIONES

1. Las telecomunicaciones se rigen en base a estandarizaciones, principalmente publicadas por dos instituciones, la ITU y el IETF. Dentro de sus publicaciones podemos encontrar información detallada de las herramientas y tecnologías aplicables a la telefonía IP. Una lectura de estos documentos puede ayudar al lector a tener una mejor visión de esta tecnología, ya que estos documentos contienen datos proporcionados por cada desarrollador.
2. Actualmente, el protocolo IPv4 está arraigado en la mayoría de pequeñas y grandes redes, este no fue diseñado para señales de tiempo real como voz, audio y video y aunque existen métodos que hacen que este sea compatible mudarse a IPv6 sería lo ideal, este ayuda a obtener una mejor implementación de la telefonía IP al permitir el manejo de señales de tiempo real, además de resolver los problemas de agotamiento de direcciones y los presentados por NAT y Firewall en VOIP.
3. En las redes de datos, las tecnologías de seguridad evolucionan en gran medida a las fallas encontradas durante su utilización, estas evoluciones les permite proporcionar un servicio confiable a los usuarios. La telefonía IP no se queda atrás, al basarse en redes de datos hereda en su mayoría las fallas de esta. Es importante hacer uso de las actuales técnicas utilizadas para proveer protección a esta tecnología y así evitar pérdidas de información, denegación de servicio y algunos otros fallos muy comunes que pueden evitarse con unas pocas herramientas y la correcta configuración de los dispositivos usados en cada arquitectura.

Cambiar el nombre de usuario y clave que traen por defecto los dispositivos es una buena práctica en la configuración de los elementos de la red, la omisión de esto puede conllevar serias fallas en la seguridad, tanto en el dispositivo como en la red al que pertenece.

4. Un buen conocimiento de las herramientas utilizadas por aquellos que atacan las redes sería de gran ayuda a la hora de protegerlas. En su mayoría los programas desarrollados para depurarlas son las utilizadas por los atacantes. Una buena depuración de la red ayudara a encontrar las posibles vías por las cuales un atacante podría dañar el sistema. Es mejor encontrar estas fallas a tiempo antes que alguien más lo haga y pueda libremente realizar un ataque.

5. Antes de implementar un sistema de telefonía IP con Asterisk, se deben tener fundamentos sólidos sobre su funcionamiento, aunque con pocos conocimientos puede realizarse una configuración no se haría uso de todo el potencial que esta herramienta representa. Conocer los archivos de configuración es vital a la hora de implantar un sistema complejo en el que se manejan muchos usuarios, donde cada uno de ellos tendrá sus respectivas opciones de generar y recibir llamadas, además se debe tomar en cuenta que estos usuarios pueden ser una mezcla de la telefonía tradicional e IP. Con un buen conocimiento de Asterisk se aprovechara al máximo su rendimiento, además de proveer un servicio óptimo.

BIBLIOGRAFÍA

1. Anttalainen, Tarmo. **Introduction to telecommunications network Engineering**. 2^a ed. s.l. Artech House, Inc., 2003. 393pp.
2. Bigelow, Stephen J. y otros. **Understanding telephone electronics**. 4^a ed. EE.UU: Newnes, 2001. 410pp.
3. Brandl, Margit y otros. **IP telephony cookbook**. s.l. Terena, 2004. 228pp.
4. Brown, Kevin. **IP telephony Unveiled**. EE.UU: Cisco Press, 2004. 200pp.
5. Davidson, Jonathan y otros. **Voice over IP fundamental**. 2^a ed. EE.UU: Cisco Press, 2006. 432pp.
6. Dryburgh, Lee y Jeff Hewett. **Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services**. EE.UU: Cisco Press, 2004. 744pp.
7. Goralski, Walter J. y Kolon Matthew C. **IP telephony**. EE.UU: McGraw-Hill, 2000. 468pp.
8. Harte, Lawrence. **Introduction to IP telephony**. EE.UU: Athos Publishing, 2003. 79pp.
9. Johnston, Alan B. **SIP Understanding the Sesion Initial Protocol**. 2^a ed. s.l. Artech House, Inc, 2004. 303pp.
10. Khasnabish, Bhumip. **Implementing voice over IP**. EE.UU: John Wiley And Son, Inc, 2003. 221pp.

11. Meggelen, Jim Van y otros. **Asterisk: The future of telephony**. 2^a ed. EE.UU: O'Reilly Media, Inc, 2007. 596pp.
12. Prasad, K. V. **Principles of digital communication systems and computer networks**. EE.UU: Charles River Media, Inc., 2003. 742pp.
13. Porter, Thomas. **Practical VOIP Security**. Canada: Syngress Publishing, Inc, 2006. 585pp.
14. Stallng, Williams. **Data and computer communications**. 5^a ed. EE.UU: Princes Hall, 1997. 800pp.
15. Stevens, Richard W. **TCP/IP illustrated**. (The Protocols, volumen 1).EE.UU: Addison Wesley, 1993. 600pp.
16. Tanenbaum, Andrew S. **Redes de computadoras**. 3^a ed. México: Princes Hall Hispanoamericana, S.A., 1997. 813pp.
17. Zwicky, Elizabeth D. y otros. **Building Internet Firewall**. 2^a. ed. EE.UU: O'Reilly Media, Inc, 2000. 890pp.

ANEXOS

1. Empresas Guatemaltecas interesadas en migrar a Telefonía IP

- Un 65% de los entrevistados está en proceso de implementar o evaluar la Telefonía IP.
- Cisco Systems considerada por la mayoría de empresas como la primera opción del mercado para migrar a Telefonía IP.
- Ciudad de Guatemala, Guatemala, 13 de Julio de 2004. Un 65% de los empresarios guatemaltecos encuestados manifestó que está instalando sistemas de telefonía IP, está evaluando su uso o planea hacerlo, y de ellos unos 8 de cada 10 empresarios piensa hacerlo en los próximos 18 meses.

Así se desprende del estudio “**Perspectivas y actitudes de los empresarios guatemaltecos en torno a las comunicaciones IP**”, patrocinado por Cisco Systems y realizado por la firma de investigación de mercados independiente Unimer RI, entre el 26 de abril y el 17 de mayo del presente año, a 80 empresarios, el cual ofrece un 90% de confiabilidad.

“El estudio reveló que gran parte de las empresas guatemaltecas piensa migrar de centrales telefónicas tradicionales a centrales telefónicas IP, dado que estas últimas ofrecen importantes ventajas, tales como la reducción de costos operativos”, dijo Esteban Valverde, Gerente de Mercadeo y Comunicaciones de Cisco Systems para América Central.

La telefonía IP utiliza los fundamentos de comunicación de Internet, tales como sus protocolos y estándares, para transportar servicios de voz a través de la red de datos empresarial. La Telefonía IP requiere de dispositivos tales como: teléfonos IP, una red de datos y convertidores de voz IP que transporten las comunicaciones de voz de una empresa.

Como parte de los resultados del estudio, Cisco Systems es percibido como la primera opción en el mercado que las empresas considerarían para implementar soluciones de Telefonía IP con un 58% de las menciones.

“Entre las principales razones por las cuales los empresarios harán uso de la Telefonía IP están la facilidad de manejar el sistema (52%), reducción de costos operativos (27%), seguido por el incremento de funciones respecto de la telefonía tradicional (17%) y para incrementar productividad (2%).”, agregó Valverde.

Este es el primer estudio de su tipo realizado en Guatemala. El objetivo central de la encuesta fue medir el grado de conocimiento, uso y opinión sobre la Telefonía IP (PBX) en empresarios guatemaltecos.

Tonny Ramírez, Ingeniero de Sistemas de Cisco Systems, indicó que a través de la Telefonía IP una empresa puede obtener ahorro de dinero en equipos, instalación y mantenimiento al contar con una única red tanto para las computadoras como para los teléfonos, en lugar de tener redes especializadas y separadas para cada uno de ellos.

Otra ventaja importante es la reducción de llamadas telefónicas entre oficinas de una misma firma, debido a que se utiliza la misma red para transmitir la voz. La Telefonía IP es ideal para compañías de cualquier tamaño que deseen aprovechar al máximo sus infraestructuras de comunicaciones, tanto si la empresa se dispone a instalar un sistema telefónico nuevo o requiere ampliar las capacidades de su central telefónica existente.

“Una de las grandes ventajas de la Telefonía IP es el grado de madurez que ha alcanzado en el mercado mundial, circunstancia que se demuestra en el estudio con el grado de confiabilidad que las empresas guatemaltecas tienen en esta tecnología”, agregó Ramírez.

"Además, las aplicaciones de la Telefonía IP le permiten a las empresas contar con un retorno real en la inversión que ayuda a las compañías a ser más competitivas y eficientes", finalizó.

Fuente: **Redacción virtual Cisco Systems**

http://www.ciscoredaccionvirtual.com/redaccion/comunicados/ver_comunicados.asp?Id=874

2. Universidad Francisco Marroquín; Sistema de Telefonía IP, Ofrece mejoras en la comunicación y atención de los estudiantes y personal administrativo.

La Universidad Francisco Marroquín (UFM), ubicada en Ciudad de Guatemala, está disfrutando de todos los beneficios que brinda la telefonía IP. La solución de telefonía sobre redes de datos les permite acceso a comunicación telefónica que combina servicios de voz y datos, integrados en la infraestructura de una sola red de área local, y que permite conexión a Internet. La UFM cuenta con una red inalámbrica que abarca todas sus aulas, troncales de alta velocidad, entre otras tecnologías de punta, la que convierte a esta universidad como una de las pioneras en presentar tecnología al servicio de la educación.

Fundada en 1971, la Universidad Francisco Marroquín, es reconocida por su excelencia académica y una formación profesional rigurosa. La misión de la UFM es la enseñanza y difusión de los principios éticos, jurídicos y económicos propios de una sociedad de personas libres y responsables para lograr sus objetivos, la UFM trabaja con personas altamente capacitadas de la comunidad Guatemalteca y extranjera.

Actualmente la UFM cuenta con 2.500 estudiantes en 15 disciplinas académicas entre las que se encuentran Arquitectura, Ciencias Económicas, Derecho, Medicina, Ingeniería en sistemas, Odontología y Administración en Empresas. Una de las características principales de la UFM es una gestión empresarial que ayuda no sólo a la eficiente y ágil toma de decisiones e inversiones inteligentes, si no también a asumir un compromiso. A mantener a la vanguardia en la tecnología. Desde sus inicios la UFM ha visto la tecnología como un medio para alcanzar sus metas académicas y anticiparse a los cambios y avances tecnológicos. Como la tecnología de voz IP.

La Universidad Francisco Marroquín es una institución pionera en presentar los mejores adelantos tecnológicos al servicio de la educación y lo ha demostrado al suministrar servicios de acceso remoto a sus alumnos, así como habilitar prácticamente todas sus aulas con conexión a la red inalámbrica interna con que los usuarios, aun sin cableado, pueden conectarse desde cualquier parte del campus. Es una de las pocas universidades de la región centroamericana que ha invertido en tecnologías de troncales de alta velocidad de transmisión de datos en todos sus edificios, y su columna principal es una Intranet construida a base de fibra óptica.

Infraestructura de Red, única y unificada

Considerando la demanda telefónica de la universidad Francisco Marroquín y con el objetivo de brindar un mejor servicio a los estudiantes, docentes y clientes, se implementó el sistema de comunicaciones SuperStack 3 NBX, de 3COM. Esta solución permite la integración en un solo sistema y la administración basada en web. Esta solución por su infraestructura y alcance se convierte en la primera instalación de telefonía sobre LAN y la más grande de toda Centroamérica.

Según Juan Carlos López, Director del centro de operaciones de la UFM, mediante el SuperStack 3NBX, se han conseguido mejoras: “Hemos agilizado la comunicación entre los estudiantes y la universidad. Antes era difícilísimo, la operadora se nos cargaba demasiado y no teníamos un mecanismo por el cual los estudiantes pudieran comunicarse de forma directa a cada departamento. Ahora el estudiante tiene una mejor comunicación y atención. Se ha descargado en un 80% la operadora manual de la universidad”. Esta ventaja es muy importante para la UFM ya que su estilo de educación se caracteriza por la atención personalizada.

Además, el nuevo sistema de comunicaciones permite utilizar al máximo cada una de las líneas telefónicas existentes ya que es posible atender hasta 300 llamadas simultáneamente con la tercera parte de las líneas físicas con las que se contaba anteriormente.

Cada usuario tiene el beneficio de programar y direccionar su extensión telefónica hacia el teléfono que desee, ya sea internamente, al celular, o al teléfono de su casa. Incluso, al combinar la tecnología de voz y datos en un solo sistema, en caso de que una persona tenga que ausentarse de la oficina, puede configurar el teléfono para que los correos de voz se conviertan en documentos adjuntos en su correo electrónico y revisarlos no importa el lugar del mundo donde se encuentre.

También ofrece la posibilidad de efectuar la gestión de todo tipo de llamadas de direcciones de la computadora a un directorio telefónico y unificar los mensajes de voz de teléfono y correo electrónico.

Este sistema de telefonía dispone de los servicios de voz más modernos del mercado, de acuerdo con la dirección técnica de la UFM; “Ahora todos los teléfonos tienen identificación de llamada, tienen pantalla de status. Sabemos quienes son las personas que nos hacen las llamadas. Sabemos quien llama de dentro y de fuera, podemos atender hasta un máximo de 4 llamadas simultáneas en cada anexo, y a esas 4 personas no les va a sonar ocupado, y para una quinta está programado que se vaya a un buzón de mensajes; las personas que nos llaman de fuera de la universidad probablemente nunca van a escuchar un teléfono ocupado”.

Quizás uno de los mayores beneficios para la UFM es la reducción de costos en horas-hombre. Ante cualquier cambio en la configuración de los menús o traslados físicos. Ya no tienen que llamar al proveedor especializado de servicios técnicos; la dirección técnica de la universidad puede realizar las modificaciones de manera simple y rápida. Sin duda, el mayor beneficio lo ha recibido el estudiante de la UFM, que se puede comunicar de manera eficaz con su centro de enseñanza.

La universidad Francisco Marroquín, a 30 años de su fundación, confirma, con su compromiso con la tecnología en sus planes de estudio y la calidad de sus egresados, que es uno de los centros educativos más relevantes de Latinoamérica.

Fuente: **Raytel Telecomunicaciones**
www.raytel.cl/Pdf/publicaciones/1.pdf

3. VoIP al alcance de su mano

La telefonía a través de IP o de la infraestructura de la red ha sido un tema recurrente durante los últimos años. En Guatemala son conocidas las opciones web pero cada vez son más accesibles las versiones con teléfonos convencionales.

La conversación telefónica es, hasta el momento, la mejor manera de hablar en tiempo real con otra persona. Sin embargo, los altos costos de llamar al extranjero desde una línea fija o teléfono celular nos persuaden de hacerlo. Por medio de las principales compañías telefónicas de Guatemala el costo de una llamada a Estados Unidos y Centroamérica oscila entre US\$0.10 y US\$0.85 el minuto, casi cinco veces más que las llamadas locales.

Aun así, es más barato que llamar al resto de América, Europa o Asia, donde el costo aumenta a US\$1 por minuto en la mayoría de casos. El avance tecnológico y la popularización de un mayor ancho de banda para conectarse a Internet ofrecen otras opciones más accesibles.

Una de ellas es el Voice over Internet Protocol (VoIP) o Voz sobre Protocolo de Internet (Voz sobre IP), una tecnología que se utiliza para convertir la voz en datos y transmitirla por medio de redes IP, sostiene Julio Ochoa, jefe de servicios de Ecssa. No diferencia el lugar donde se genera la llamada, como ocurre con la telefonía tradicional, por lo que las llamadas son más económicas, menciona Ignacio Ramos, director ejecutivo de Codevoz.

Oferta nacional

Yego.com.gt ofrece un servicio de VoIP a clientes individuales mediante un adaptador conocido como SPA 2102 para llamar de teléfono a teléfono. Este funciona en cualquier lugar donde exista una conexión permanente a Internet (cableado). Existen cinco planes mensuales, entre ellos uno de Q100 donde el minuto a Estados Unidos y Canadá cuesta US\$0.05; también ofrecen un plan prepago o con recarga, donde el minuto a Estados Unidos y Canadá tiene un costo de US\$0.10. Ecssa.com.gt ofrece un servicio a grupos de usuarios a través de redes privadas físicas o virtuales.

Estos pueden estar ubicados en un mismo sitio o en diferentes localidades o países. Por esta razón está dirigido a empresas (pequeña, mediana y grande) y al mercado de call centers. La misma empresa ofrece teléfonos y adaptadores para conectar a una red IP.

Codevoz.com ofrece soluciones personalizadas a empresas de telefonía, software y hardware para plantas telefónicas y centros de llamadas. Además, cuenta con la representación de Asterisk de Digium, un PBX IP que funciona con una plataforma de software libre basada en Linux.

Oferta internacional

El servicio vía web que realmente popularizó el concepto de VoIP es Skype.com, un servicio de telefonía peer to peer fundada por los mismos creadores de Kazaa, adquirida en 2005 por eBay y que además compite con otros protocolos VoIP como SIP, IAX y H.323.

Este consta de un programa que se descarga a la computadora para luego, con la opción de SkypeOut llamar a cualquier teléfono tradicional o celular con tarifas muy bajas.

Para llamar (SkypeOut) se debe comprar un crédito mínimo de US\$13. Una llamada de Guatemala a Estados Unidos le costaría US\$0.153 el minuto a teléfono fijo y celular mientras que a El Salvador US\$0.126 por la misma cantidad de tiempo, siendo esta última no muy conveniente al comparar con el costo desde los operadores locales. Otra opción es contratar el servicio de recibir llamadas (SkypeIn) por 12 meses a US\$40 con buzón de voz incluido. La idea es comprar un número real correspondiente a la región geográfica a donde más llama. Quienes le llamen de ese país pagarán una llamada local y quienes llamen de otro país o estado (Estados Unidos) pagarán una llamada internacional.

Ambos funcionan con Windows, Mac, Linux y Pocket PC.

Yor.net es una empresa con sede en California que ofrece un servicio que se puede utilizar en Guatemala. El servicio YorVoice, al igual que Skype ofrece llamadas salientes. Se puede adquirir el adaptador de banda ancha Linksys PAP2 para llamar de teléfono a teléfono o descargar un programa de teléfono virtual (Softphone). Las opciones son contratar un plan prepago (US\$0.022 a Estados Unidos) o uno ilimitado (US\$0.020).

Vivophone.com requiere comprar un teléfono virtual (software), un teléfono con adaptador o uno que ya lo tiene integrado. A cambio la empresa asigna un número para realizar llamadas gratuitas a usuarios registrados. Un servicio opcional permite llamar a un teléfono fuera de la red con el costo de US\$0.015 si llama a Estados Unidos y desde US\$0.13 para llamar a Centroamérica.

Oferta web

Jajah.com conecta dos teléfonos estándar, sin importar que sean fijos o móviles o el lugar donde estén. No necesita la instalación de software porque funciona desde el navegador. Para llamar debe llenar las casillas que solicita la página (números de teléfono destinatario y de quien hace la llamada) y esperar a que el teléfono suene para hacer el enlace telefónico.

Debe suscribirse para acceder al servicio desde Guatemala. Si llama del país a Estados Unidos paga US\$0.13 por el minuto, un costo más alto que el de los operadores locales. Sin embargo, entre usuarios registrados y activos del servicio las llamadas son gratuitas.

Legalidad

Pese a que se trata de una comunicación computadora-computadora o computadora-teléfono que se vale de un enlace dentro de la red de Internet, la Superintendencia de Telecomunicaciones de Guatemala (SIT) no regula ningún aspecto relacionado con los servicios o proveedores de IP, señaló Aldo Bonilla, coordinador del área internacional de la SIT.

Según Bonilla las empresas internacionales son las que pagan el costo de las llamadas a los operadores locales. “No se ha hecho una legislación porque en este momento no pueden hacer modificaciones legales”, aseveró.

Los aparatos

Estos son algunos de los dispositivos listos para servicios de VoIP en Guatemala.

* TRENDnet TVP-SP1BK (Q771), un teléfono Bluetooth IP, configurado para utilizarse con Skype (Intelaf.com).

* Adaptadores y teléfonos como el VivoCordless, con conexión USB (US\$70) y la VivoVoiceKey (US\$50), un adaptador USB. El PenDrive VivoInside, una memoria USB con la versión portátil del programa descargable VivoSoft para hacer llamadas desde la computadora está disponible desde 256MB (US\$20) hasta 4GB (US\$90) e incluye 10 minutos de llamadas gratis.

* Belkin Wi-Fi iPhone (US\$180), que funciona con puntos de red inalámbrica (Skype.com).

* Teléfonos para call centers y centrales telefónicas de marca Avaya (Ecsa/2379-9000).

* Adaptador de teléfono Sipura/Linksys, modelo SPA 2102 (Q960) que se conecta al teléfono y la red (Yego.com).

* Adaptador de teléfono de banda ancha Linksys PAP2 de Yoc.net que se conecta a cualquier teléfono análogo o inalámbrico.

* Teléfono de escritorio V85 NetComm, tiene para servicios empresariales productos como la tarjeta de interconexión Sangoma, la tarjeta Digion TE-100P de un puerto, terminales de usuario Sipura, el adaptador Egdewater Ethemet para 30 usuarios, el adaptador/router V300 NetComm, y servidores (Codevoz.com).

Fuente: Rocio del Valle

El Periódico. Guatemala, jueves 15 de febrero de 2007

<http://www.elperiodico.com.gt/es/20070215/14/36773/>

4. Crece oferta de voz IP

Telefonía: Surgen nuevos servicios basados en Internet

Las pequeñas y medianas empresas (Pyme) pueden reducir hasta en 80 por ciento sus gastos en llamadas telefónicas, con el uso de telefonía IP (Internet Protocol).

En Guatemala ya se utiliza ese recurso tecnológico, mediante páginas en Internet que permiten efectuar llamadas desde la computadora a teléfonos fijos y móviles, mediante la compra de tiempo, y gratuitas, entre usuarios con computadoras, como el caso de Skype.

De acuerdo con expertos, en los próximos dos años las comunicaciones de este tipo crecerán en 500 por ciento cada año, lo que revolucionará el actual formato de servicio de pago por minuto y lo transformará en otro a pago de paquetes.

El concepto se ha ampliado, y compañías nacionales que han incursionado en esa área aseguran que la ventaja del servicio ofrecido en el país es menor costo en llamadas locales y más seguridad, ya que no se requiere utilizar tarjeta de crédito a través de Internet.

Jorge Guillén, gerente regional para Centroamérica y el Caribe de D-Link, comentó que, pese a que esta tecnología no es nueva en el mercado, con anterioridad sólo estaba al alcance de las grandes corporaciones o empresas.

Según el ejecutivo, con menos de US\$1 mil 500, una Pyme puede instalar una red mínima (con cuatro líneas) que le permitirá tener comunicación telefónica con sus sucursales en el país y reducir sus precios en llamadas internacionales. Todo, sin tener contrato con una compañía de telefonía.

Agregó que el sistema Easy IP, que la empresa lanzó recientemente al mercado guatemalteco, reúne en una misma solución las redes de voz con datos, y además permite conexión a Internet de banda ancha.

Nueva opción de Telgua

Telgua presentó ayer este sistema de telefonía, diseñado como complemento o segunda línea, y lo puso a disposición de clientes que poseen servicio Turbonett.

El interesado en adquirir el servicio deberá comprar un paquete de conexión a un precio de US\$28, que incluye los aparatos para conexión y un teléfono con número local asignado.

Se paga una cuota mensual de US\$9, que permite acceder a tarifas como US\$0.04 en llamadas locales y US\$0.05 hacia Estados Unidos, y Centroamérica (excepto Nicaragua).

También hay paquetes de US\$11 adicionales, que incluyen 500 minutos locales y uno similar para llamadas internacionales. Las llamadas entre usuarios IP son gratis, y se ofrecen servicios como identificador y desvío de llamadas, entre otros.

Para utilizar el servicio no se necesita estar conectado a una computadora o tenerla encendida; basta con poseer una línea fija de Telgua, contrato con el servicio Turbonett (con tarifas entre US\$19 y US\$55, según la velocidad) y adquirir el paquete de telefonía IP.

Fuente: **Byron Dardón, Leonel Díaz**

Prensa Libre. Guatemala, jueves 20 de septiembre de 2007

<http://www.prensalibre.com/pl/2007/septiembre/20/182937.html>